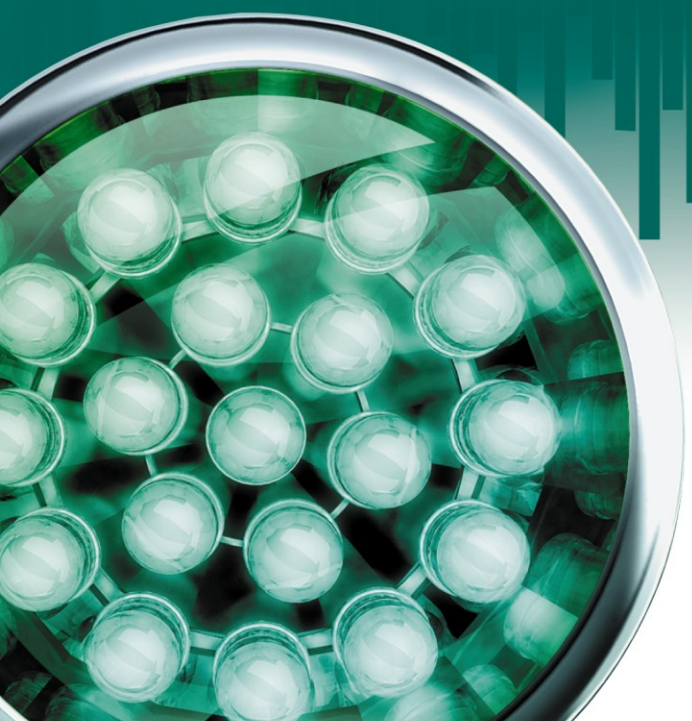
Kaspersky CRYSTAL

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

ВЕРСИЯ ПРОГРАММЫ: 9.1



KASPERSKY lab

Уважаемый пользователь!

Спасибо за то, что выбрали наш продукт. Мы надеемся, что этот документ поможет вам в работе и ответит на большинство возникающих вопросов.

Документ может быть изменен без предварительного уведомления. Последнюю версию документа вы можете найти на сайте «Лаборатории Касперского» по адресу http://www.kaspersky.ru/docs.

Дата редакции документа: 27.09.2010

http://www.kaspersky.ru
http://support.kaspersky.ru

СОДЕРЖАНИЕ

ОБ ЭТОМ РУКОВОДСТВЕ 11
В этом документе 11
Условные обозначения 12
ДОПОЛНИТЕЛЬНЫЕ ИСТОЧНИКИ ИНФОРМАЦИИ 14
Источники информации для самостоятельного поиска 14
Обсуждение программ «Лаборатории Касперского» на веб-форуме 15
Обращение в Департамент продаж 15
Обращение в Группу разработки документации 15
KASPERSKY CRYSTAL 16
Комплект поставки 16
Организация защиты домашней сети 17
Сервис для зарегистрированных пользователей 19
Аппаратные и программные требования 20
УСТАНОВКА И УДАЛЕНИЕ ПРОГРАММЫ 21
Установка программы на компьютер 22
Шаг 1. Поиск более новой версии программы 23
Шаг 2. Проверка соответствия системы необходимым условиям установки 24
Шаг 3. Выбор типа установки 24
Шаг 4. Просмотр лицензионного соглашения 24
Шаг 5. Положение об использовании Kaspersky Security Network 24
Шаг 6. Выбор папки назначения 25
Шаг 7. Выбор компонентов программы для установки 25
Шаг 8. Поиск других антивирусных программ 26
Шаг 9. Отключение сетевого экрана Microsoft Windows 26
Шаг 10. Подготовка к установке 26
Шаг 11. Установка 27
Шаг 12. Активация программы 27
Шаг 13. Проверка данных 27
Шаг 14. Регистрация пользователя 27
Шаг 15. Завершение активации 28
Шаг 16. Ограничение доступа к программе 28
Шаг 17. Выбор режима защиты 29
Шаг 18. Настройка обновления программы 29
Шаг 19. Выбор обнаруживаемых угроз 30
Шаг 20. Анализ системы 30
Шаг 21. Завершение работы мастера 30
Начало работы 31
Изменение, восстановление и удаление программы с помощью мастера установки 32
Шаг 1. Стартовое окно программы установки 32
Шаг 2. Выбор операции 32
Шаг 3. Завершение операции восстановления, изменения или удаления программы 33
УПРАВЛЕНИЕ ЛИЦЕНЗИЕЙ 34
О лицензионном соглашении 34
О лицензии 34

О коде активации 35
Просмотр информации о лицензии 35
ИНТЕРФЕЙС ПРОГРАММЫ 37
Значок в области уведомлений панели задач 37
Контекстное меню 38
Главное окно Kaspersky CRYSTAL 39
Защита компьютера 41
Резервное копирование 42
Родительский контроль 43
Окно Менеджера паролей 44
Значок в области уведомления 44
Контекстное меню Менеджера паролей 45
Окно базы паролей 45
Окно настройки параметров 46
Кнопка быстрого запуска 47
Расширения и плагины 47
Указатель 47
Окно настройки параметров программы 48
Окна уведомлений и всплывающие сообщения 49
ЗАПУСК И ОСТАНОВКА ПРОГРАММЫ 51
Включение и отключение автоматического запуска 51
Запуск и остановка программы вручную 51
СОСТОЯНИЕ ЗАЩИТЫ ДОМАШНЕЙ СЕТИ 52
Диагностика и устранение проблем в защите 52
Включение / отключение защиты компьютера 53
Приостановка защиты 54
Использование интерактивного режима защиты 54
РЕШЕНИЕ ТИПОВЫХ ЗАДАЧ 56
Как активировать программу 56
Как приобрести лицензию или продлить срок ее действия 57
Что делать при появлении уведомлений программы 58
Как обновить базы и модули программы 58
Как проверить важные области компьютера на вирусы 58
Как проверить на вирусы файл, папку, диск или другой объект 59
Как выполнить полную проверку компьютера на вирусы 61
Как проверить компьютер на уязвимости 61
Как удаленно проверить состояние защиты компьютеров домашней сети 62
Как защитить ваши личные данные от кражи 63
Защита от фишинга 63
Виртуальная клавиатура 64
Менеджер паролей 64
Шифрование данных 65
Что делать, если вы подозреваете, что объект заражен вирусом 66
Как восстановить удаленный или вылеченный программой объект 67
Что делать, если вы подозреваете, что ваш компьютер заражен 67
Как создать резервные копии ваших данных 69
Как ограничить доступ к параметрам Kaspersky CRYSTAL 70

Как ограничить использование компьютера и интернета для разных пользователей 71
Как создать и использовать диск аварийного восстановления 71
Создание диска аварийного восстановления 72
Загрузка компьютера с помощью диска аварийного восстановления 73
Что делать с большим количеством спам-сообщений 73
Как просмотреть отчет о защите компьютера 75
Как восстановить стандартные параметры работы программы 75
Как перенести параметры программы на другой компьютер 76
РАСШИРЕННАЯ НАСТРОЙКА ПРОГРАММЫ 78
Защита компьютера 79
Проверка компьютера 79
Проверка на вирусы 80
Поиск уязвимостей 87
Обновление 87
Выбор источника обновлений 88
Формирование расписания запуска обновления 90
Откат последнего обновления 91
Проверка карантина после обновления 91
Использование прокси-сервера 92
Запуск обновления с правами другого пользователя 92
Файловый Антивирус 93
Включение и отключение Файлового Антивируса 94
Автоматическая приостановка работы Файлового Антивируса 94
Формирование области защиты 95
Изменение и восстановление уровня безопасности 96
Изменение режима проверки 96
Использование эвристического анализа 97
Технология проверки 97
Изменение действия над обнаруженными объектами 98
Проверка составных файлов 98
Оптимизация проверки 99
Почтовый Антивирус 99
Включение и отключение Почтового Антивируса 101
Формирование области защиты 101
Изменение и восстановление уровня безопасности 102
Использование эвристического анализа 102
Изменение действия над обнаруженными объектами 103
Фильтрация вложений 103
Проверка составных файлов 104
Проверка почты в Microsoft Office Outlook 104
Проверка почты в The Bat! 104
Веб-Антивирус 105
Включение и отключение Веб-Антивируса 107
Изменение и восстановление уровня безопасности 107
Изменение действия над обнаруженными объектами 108
Блокирование опасных скриптов 108
Проверка ссылок по базам фишинговых и подозрительных адресов 108
Использование эвристического анализа 109

Оптимизация проверки 109
Модуль проверки ссылок 110
Формирование списка доверенных адресов 111
IM-Антивирус 111
Включение и отключение IM-Антивируса 112
Формирование области защиты 112
Выбор метода проверки 112
Анти-Спам 113
Включение и отключение Анти-Спама 115
Изменение и восстановление уровня безопасности 115
Обучение Анти-Спама 116
Проверка ссылок в сообщениях 119
Определение спама по фразам и адресам. Формирование списков 119
Регулировка пороговых значений фактора спама 124
Использование дополнительных признаков фильтрации спама 125
Выбор алгоритма распознавания спама 125
Добавление метки к теме сообщения 126
Фильтрация писем на сервере. Диспетчер писем 126
Исключение из проверки сообщений Microsoft Exchange Server 127
Настройка обработки спама почтовыми клиентами 128
Анти-Баннер 130
Включение и отключение Анти-Баннера 130
Выбор методов проверки 131
Формирование списков запрещенных и разрешенных адресов баннеров 131
Экспорт и импорт списков адресов 131
Контроль программ 133
Включение и отключение Контроля программ 133
Распределение программ по группам 134
Просмотр активности программ 135
Изменение группы доверия 135
Правила Контроля программ 136
Защита ресурсов операционной системы и персональных данных 139
Проактивная защита 140
Включение и отключение Проактивной защиты 141
Формирование группы доверенных программ 141
Использование списка опасной активности 142
Изменение правила контроля опасной активности 142
Откат действий вредоносной программы 143
Защита сети 143
Сетевой экран 144
Защита от сетевых атак 147
Проверка защищенных соединений 150
Мониторинг сети 152
Настройка параметров прокси-сервера 152
Формирование списка контролируемых портов 152
Доверенная зона 154
Формирование списка доверенных программ 155
Создание правил исключений 155
Безопасная среда исполнения программ 157

Запуск программы в безопасной среде 157
Формирование списка программ для запуска в безопасной среде 158
Создание ярлыка для запуска программ 159
Очистка данных безопасной среды 159
Использование общей папки 160
Карантин и резервное хранилище 160
Хранение объектов карантина и резервного хранилища 161
Работа с объектами на карантине 162
Резервное копирование 164
Создание хранилища 164
Подключение ранее созданного хранилища 165
Очистка хранилища 165
Удаление хранилища 166
Создание задачи резервного копирования 166
Запуск резервного копирования 167
Восстановление данных 167
Поиск резервных копий 168
Просмотр данных резервной копии 169
Просмотр отчета о событиях 170
Родительский контроль 171
Настройка Родительского контроля пользователя 172
Включение и отключение контроля 172
Сохранение и загрузка параметров Родительского контроля 173
Отображение учетной записи в Kaspersky CRYSTAL 173
Время работы на компьютере 174
Запуск программ 174
Время работы в интернете 174
Посещение веб-сайтов 175
Загрузка файлов из интернета 175
Режим безопасного поиска 176
Переписка через интернет-пейджеры 176
Переписка в социальных сетях 177
Пересылка конфиденциальной информации 178
Поиск ключевых слов 179
Просмотр отчетов о действиях пользователя 179
Шифрование данных 180
Создание и подключение ранее созданного контейнера 180
Блокирование и разблокирование доступа к данным в контейнере 181
Добавление файлов в контейнер 182
Настройка параметров контейнера 182
Создание ярлыка для быстрого доступа к контейнеру 183
Центр управления 184
Настройка удаленного управления 184
Проверка домашней сети на вирусы и уязвимости 185
Удаленное обновление баз на компьютерах в сети 185
Включение / отключение компонентов защиты на компьютерах в сети 186
Удаленное управление Родительским контролем 186
Запуск резервного копирования на компьютерах в сети 187
Удаленное управление лицензиями на компьютерах в сети 187

Менеджер паролей 189
Управление базой паролей 190
Доступ к базе паролей 190
Добавление персональных данных 191
Использование персональных данных 198
Поиск паролей 199
Удаление персональных данных 200
Импорт / экспорт данных 200
Резервное копирование / Восстановление базы паролей 201
Настройка параметров программы 203
Мастер настройки параметров 204
Использование имени пользователя по умолчанию 204
Часто используемые учетные записи 205
Игнорируемые веб-адреса 206
Доверенные веб-адреса 206
Горячие клавиши 207
Расположение файла базы паролей 207
Создание новой базы паролей 208
Расположение резервной копии 209
Выбор метода шифрования 209
Автоматическое блокирование базы паролей 210
Изменение способа авторизации Менеджера паролей 211
Использование USB-, Bluetooth-устройств для авторизации 211
Изменение мастер-пароля 212
Поддерживаемые веб-браузеры 212
Управление шаблонами личных заметок 213
Отображение кнопки быстрого запуска 214
Время хранения пароля в буфере обмена 214
Уведомления 215
Действие по двойному щелчку мыши 215
Создание надежных паролей 216
Использование переносной версии Менеджера паролей 217
Создание и подключение переносной версии 217
Синхронизация базы паролей 218
Производительность и совместимость с другими программами 219
Выбор категорий обнаруживаемых угроз 220
Технология лечения активного заражения 220
Распределение ресурсов компьютера при проверке на вирусы 221
Параметры программы при работе в полноэкранном режиме. Игровой профиль 221
Энергосбережение при работе от аккумулятора 222
Самозащита Kaspersky CRYSTAL 222
Включение и отключение самозащиты 222
Защита от внешнего управления 223
Внешний вид программы 223
Активные элементы интерфейса 223
Графическая оболочка Kaspersky CRYSTAL 224
Новостной агент 224
Дополнительные инструменты 225
Необратимое удаление данных 226

Устранение следов активности 227
Удаление неиспользуемой информации 228
Настройка браузера 230
Отчеты 231
Формирование отчета для выбранного компонента 232
Фильтрация данных 232
Поиск событий 233
Сохранение отчета в файл 234
Хранение отчетов 234
Очистка отчетов 235
Запись некритических событий 235
Настройка напоминания о готовности отчета 235
Уведомления 235
Включение и отключение уведомлений 236
Настройка способа уведомления 236
Участие в Kaspersky Security Network 237
ПРОВЕРКА КОРРЕКТНОСТИ НАСТРОЙКИ KASPERSKY CRYSTAL 239
Тестовый «вирус» EICAR и его модификации 239
Тестирование защиты HTTP-трафика 240
Тестирование защиты SMTP-трафика 241
Проверка корректности настройки Файлового Антивируса 241
Проверка корректности настройки задачи проверки на вирусы 242
Проверка корректности настройки защиты от нежелательной почты 242
ОБРАЩЕНИЕ В СЛУЖБУ ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ 243
Личный кабинет 243
Техническая поддержка по телефону 244
Создание отчета о состоянии системы 244
Создание файла трассировки 245
Отправка файлов данных 245
Выполнение скрипта AVZ 246
ПРИЛОЖЕНИЯ 248
Статусы подписки 248
Работа с программой из командной строки 249
Активация программы 250
Запуск программы 251
Остановка программы 251
Управление компонентами и задачами программы 251
Проверка на вирусы 253
Обновление программы 255
Откат последнего обновления 256
Экспорт параметров защиты 256
Импорт параметров защиты 257
Получение файла трассировки 257
Просмотр справки 257
Коды возврата командной строки 258
Список уведомлений Kaspersky CRYSTAL 259
Лечение объекта невозможно 259
Недоступный сервер обновлений 260

Обнаружен вредоносный объект 260
Обнаружен опасный объект на трафике 261
Обнаружен подозрительный объект 261
Обнаружена опасная активность в системе 262
Обнаружен скрытый процесс 262
Обнаружена попытка доступа к системному реестру 263
Обнаружена сетевая активность программы 264
Обнаружена новая сеть 264
Обнаружена попытка фишинг-атаки 265
Обнаружена подозрительная ссылка 265
Обнаружен некорректный сертификат 266
Ограничение времени использования программы 266
Ошибка восстановления данных 266
Требуется специальная процедура лечения 266
ГЛОССАРИЙ ТЕРМИНОВ 268
ЗАО «ЛАБОРАТОРИЯ КАСПЕРСКОГО» 278
ИНФОРМАЦИЯ О СТОРОННЕМ КОДЕ 279
Программный код 279
AGG (ANTI-GRAIN GEOMETRY) 2.4 280
BISON PARSER SKELETON 2.3 281
BOOST 1.30.0, 1.39.0, 1.43.0 281
BZIP2/LIBBZIP2 1.0.5 282
EXPAT 1.2, 2.0.1 282
FASTSCRIPT 1.9 282
GECKO SDK 1.8 282
INFO-ZIP 5.51 282
LIBJPEG 6B 283
LIBNKFM 2.0.5 284
LIBPNG 1.2.8, 1.2.29 284
LIBSPF2 1.2.9 284
LIBUNGIF 3.0 285
LIBXDR 285
NDIS INTERMEDIATE MINIPORTDRIVER SAMPLE 285
NDIS SAMPLE NDIS LIGHTWEIGHT FILTER DRIVER 286
NETWORK CONFIGURATION SAMPLE 286
OPENSSL 0.9.8D 286
PCRE 3.0, 7.4, 7.7 287
PROTOCOL BUFFER 288
QT 4.6.1 288
RFC1321-BASED (RSA-FREE) MD5 LIBRARY 294
TINICONV 1.0.0 294
WINDOWS TEMPLATE LIBRARY 7.5 299
WINDOWS TEMPLATE LIBRARY 8.0 302
ZLIB 1.2, 1.2.2 302
Другая информация 302
ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ 303

ОБ ЭТОМ РУКОВОДСТВЕ

Этот документ представляет собой Руководство по установке, настройке и использованию программы Kaspersky CRYSTAL 9.1 (далее Kaspersky CRYSTAL). Документ предназначен для широкой аудитории. Пользователи программы должны обладать начальными навыками работы с персональным компьютером: быть знакомыми с интерфейсом операционной системы Microsoft Windows, владеть основными приемами работы в ней, уметь пользоваться распространенными компьютерными программами для работы с электронной почтой и интернетом, например Microsoft Office Outlook и Microsoft Internet Explorer.

Цель документа:

- помочь пользователю самостоятельно установить программу на компьютер, активировать ее и оптимально настроить программу с учетом задач пользователя;
- обеспечить быстрый поиск информации для решения вопросов, связанных с программой;
- рассказать об альтернативных источниках информации о программе и способах получения технической поддержки.

В ЭТОМ РАЗДЕЛЕ

В этом документе 11

Условные обозначения 12

В ЭТОМ ДОКУМЕНТЕ

В Руководство пользователя Kaspersky CRYSTAL включены следующие основные разделы:

Дополнительные источники информации

Этот раздел содержит описание дополнительных источников получения информации о программе и об интернет-ресурсах, на которых можно обсудить программу, поделиться идеями, задать вопросы и получить ответы на них.

Kaspersky CRYSTAL

Этот раздел содержит описание возможностей программы, а также краткую информацию о ее отдельных компонентах и основных функциях. Из раздела вы узнаете о назначении комплекта поставки и о комплексе услуг, доступных зарегистрированным пользователям программы. В разделе приведены аппаратные и программные требования, которым должен отвечать компьютер, чтобы на него можно было установить Kaspersky CRYSTAL.

Установка и удаление программы

Этот раздел содержит инструкции, которые помогут вам установить программу на компьютер или обновить предыдущую версию программы. В этом же разделе описано, как удалить программу с компьютера.

Управление лицензией

Этот раздел содержит информацию об основных понятиях, используемых в контексте лицензирования программы. Из раздела вы узнаете также о возможности автоматического продления срока действия лицензии и о том, где просмотреть информацию о текущей лицензии.

Интерфейс программы

Этот раздел содержит описание основных элементов графического интерфейса программы: значка и контекстного меню программы, главного окна, окон настройки, окон уведомлений.

Запуск и остановка программы

Этот раздел содержит информацию о том, как запустить программу или завершить работу с ней.

Состояние защиты домашней сети

Этот раздел содержит информацию о том, как определить, защищен ли в данный момент компьютер или существуют угрозы его безопасности, а также о том, как устранить возникшие угрозы. В этом же разделе вы найдете информацию о включении, отключении и временной приостановке защиты во время работы Kaspersky CRYSTAL, а также о возможных режимах защиты.

Решение типовых задач

Этот раздел содержит инструкции к основным задачам программы, с которыми пользователи сталкиваются наиболее часто.

Расширенная настройка программы

Раздел содержит подробное описание каждого компонента программы и информацию о ее настройке для гибкой и максимально эффективной защиты.

Проверка корректности настройки программы

Этот раздел содержит рекомендации по проверке корректности настройки компонентов программы.

Обращение в Службу технической поддержки

Этот раздел содержит рекомендации по обращению за помощью в «Лабораторию Касперского» из Личного кабинета на веб-сайте Службы технической поддержки и по телефону.

Приложения

Этот раздел содержит справочную информацию, которая дополняет основной текст документа.

Глоссарий терминов

Этот раздел содержит список терминов, которые встречаются в документе, и их определения.

Условные обозначения

В документе используются условные обозначения, описанные в таблице ниже.

Таблица 1. Условные обозначения

Пример текста	Описание условного обозначения
Обратите внимание на то, что...	Предупреждения выделяются красным цветом и заключаются в рамку. В предупреждениях содержится важная информация, например, связанная с критическими для безопасности компьютера действиями.

Пример текста	Описание условного обозначения
Рекомендуется использовать...	Примечания заключаются в рамку. В примечаниях содержится вспомогательная и справочная информация.
Пример: ...	Примеры приводятся в блоке на желтом фоне под заголовком «Пример».
Обновление – это...	Новые термины выделяются курсивом.
ALT+F4	Названия клавиш клавиатуры выделяются полужирным шрифтом и прописными буквами. Названия клавиш, соединенные знаком «плюс», означают комбинацию клавиш.
Включить	Названия элементов интерфейса, например, полей ввода, команд меню, кнопок, выделяются полужирным шрифтом.
Чтобы настроить расписание задачи, выполните следующие действия:	Вводные фразы инструкций выделяются курсивом.
`help`	Тексты командной строки или тексты сообщений, выводимых программой на экран, выделяются специальным шрифтом.
<IP-адрес вашего компьютера>	Переменные заключаются в угловые скобки. Вместо переменной в каждом случае требуется подставить соответствующее ей значение, угловые скобки при этом опускаются.

ДОПОЛНИТЕЛЬНЫЕ ИСТОЧНИКИ ИНФОРМАЦИИ

Если у вас возникли вопросы, связанные с выбором, приобретением, установкой или использованием Kaspersky CRYSTAL, вы можете получить ответы на них, используя различные источники информации. Вы можете выбрать наиболее удобный для себя источник информации в зависимости от важности и срочности вопроса.

В ЭТОМ РАЗДЕЛЕ

Источники информации для самостоятельного поиска 14

Обсуждение программ «Лаборатории Касперского» на веб-форуме 15

Обращение в Департамент продаж 15

Обращение в Группу разработки документации 15

Источники информации для самостоятельного поиска

«Лаборатория Касперского» предоставляет следующие источники информации о программе:

- страница программы на веб-сайте «Лаборатории Касперского»;
- страница программы на веб-сайте Службы технической поддержки (в Базе знаний);
- страница сервиса Интерактивной поддержки;
- электронная справочная система.

Страница на веб-сайте «Лаборатории Касперского»

На этой странице http://www.kaspersky.ru/kaspersky-crystal вы получите общую информацию о программе, ее возможностях и особенностях.

Страница на веб-сайте Службы технической поддержки (База знаний)

На этой странице http://support.kaspersky.ru/crystal вы найдете статьи, опубликованные специалистами Службы технической поддержки.

Эти статьи содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании программы. Они сгруппированы по темам, например «Работа с лицензией продукта», «Настройка Обновления» или «Устранение сбоев в работе». Статьи могут отвечать на вопросы, которые относятся не только к этой программе, но и к другим продуктам «Лаборатории Касперского». Кроме того, статьи могут содержать новости Службы технической поддержки в целом.

Сервис Интерактивной поддержки

На странице данного сервиса вы можете найти регулярно обновляемую базу часто задаваемых вопросов и ответов, связанных с работой программы. Для использования сервиса необходимо подключение к интернету.

- Чтобы перейти на страницу сервиса, в главном окне программы перейдите по ссылке **Поддержка** и в открывшемся окне нажмите на кнопку **Интерактивная поддержка**.

Электронная справочная система

В комплект поставки программы входит файл полной и контекстной справки. Он содержит информацию о том, как управлять защитой компьютера: просматривать состояние защиты, проверять различные области компьютера на вирусы, выполнять другие задачи. Кроме того, в файле полной и контекстной справки вы можете найти информацию о каждом окне программы: перечень и описание представленных в нем параметров и список решаемых задач.

Чтобы открыть файл справки, нажмите на кнопку **Справка** в интересующем вас окне или на клавишу **F1**.

Обсуждение программ «Лаборатории Касперского» на веб-форуме

Если ваш вопрос не требует срочного ответа, его можно обсудить со специалистами «Лаборатории Касперского» и другими пользователями на нашем форуме по адресу http://forum.kaspersky.com.

На форуме вы можете просматривать опубликованные темы, оставлять свои комментарии, создавать новые темы, пользоваться поиском.

Обращение в Департамент продаж

Если у вас возникли вопросы по выбору, приобретению Kaspersky CRYSTAL или продлению срока его использования, вы можете поговорить с сотрудниками Департамента продаж в нашем центральном офисе в Москве по телефонам:

+7 (495) 797-87-00, **+7 (495) 645-79-39**, **+7 (495) 956-70-00**

Обслуживание осуществляется на русском и английском языках.

Вы можете задать вопрос сотрудникам Департамента продаж по электронной почте, по адресу sales@kaspersky.com.

Обращение в Группу разработки документации

Если у вас возникли вопросы, связанные с документацией, или вы обнаружили в ней ошибку, или хотите оставить отзыв о наших документах, вы можете обратиться к сотрудникам Группы разработки технической документации. Для обращения в Группу разработки документации отправьте письмо по адресу docfeedback@kaspersky.com. В качестве темы письма укажите «Kaspersky Help Feedback: Kaspersky CRYSTAL».

KASPERSKY CRYSTAL

Этот раздел содержит описание возможностей программы, а также краткую информацию о ее отдельных компонентах и основных функциях. Из раздела вы узнаете о назначении комплекта поставки и о комплексе услуг, доступных зарегистрированным пользователям программы. В разделе приведены аппаратные и программные требования, которым должен отвечать компьютер, чтобы на него можно было установить Kaspersky CRYSTAL.

В ЭТОМ РАЗДЕЛЕ

Комплект поставки 16

Организация защиты домашней сети 17

Сервис для зарегистрированных пользователей 19

Аппаратные и программные требования 20

Комплект поставки

Kaspersky CRYSTAL вы можете приобрести у наших партнеров (коробочный вариант), а также в одном из интернет-магазинов (например, http://www.kaspersky.ru, раздел **Интернет-магазин**).

Если вы приобретаете продукт в коробке, то в комплект поставки программного продукта входят:

- Запечатанный конверт с установочным компакт-диском, на котором записаны файлы программного продукта и документация в формате pdf.
- Документация в печатном виде, представленная документом Краткое руководство пользователя.
- Лицензионное соглашение (в зависимости от региона).
- Активационная карта, содержащая код активации и инструкцию по активации программы (в зависимости от региона).

Лицензионное соглашение – это юридическое соглашение между вами и ЗАО «Лаборатория Касперского», в котором указано, на каких условиях вы можете пользоваться приобретенным вами программным продуктом.

Внимательно прочитайте лицензионное соглашение!

Организация защиты домашней сети

Kaspersky CRYSTAL обеспечивает комплексную защиту вашей домашней сети. Понятие комплексная защита включает в себя защиту компьютера, защиту данных и защиту пользователей, а также удаленное управление функциями Kaspersky CRYSTAL на всех компьютерах сети.

Для решения задач комплексной защиты предназначены разные функциональные модули в составе Kaspersky CRYSTAL.

Защита компьютера

Компоненты защиты предназначены для защиты компьютера от известных и новых угроз, сетевых и мошеннических атак, спама и другой нежелательной информации. Каждый тип угроз обрабатывается отдельным компонентом защиты (см. описание компонентов далее в этом разделе). Компоненты можно включать и отключать независимо друг от друга, а также настраивать их работу подходящим для вас способом.

В дополнение к постоянной защите, реализуемой компонентами защиты, рекомендуется периодически выполнять *проверку* вашего компьютера на присутствие вирусов. Это необходимо делать, чтобы исключить возможность распространения вредоносных программ, которые не были обнаружены компонентами защиты, например из-за установленного низкого уровня защиты или по другим причинам.

Для поддержки Kaspersky CRYSTAL в актуальном состоянии необходимо *обновление* баз и программных модулей, используемых в работе программы.

Программы, в безопасности которых вы не уверены, можно запускать в специальной *безопасной среде*.

Некоторые специфические задачи, которые требуется выполнять эпизодически, а не постоянно, реализуются с помощью *дополнительных инструментов и мастеров*: например, настройка браузера Microsoft Internet Explorer или устранение следов активности пользователя в системе.

Защита вашего компьютера в реальном времени обеспечивается следующими компонентами защиты:

Файловый Антивирус

Файловый Антивирус позволяет избежать заражения файловой системы компьютера. Компонент запускается при старте операционной системы, постоянно находится в оперативной памяти компьютера и проверяет все открываемые, сохраняемые и запускаемые файлы на вашем компьютере и на всех присоединенных дисках. Kaspersky CRYSTAL перехватывает каждое обращение к файлу и проверяет этот файл на присутствие известных вирусов. Дальнейшая работа с файлом возможна только в том случае, если файл не заражен или был успешно вылечен программой. Если файл по каким-либо причинам невозможно вылечить, он будет удален. При этом копия файла будет сохранена в резервном хранилище или помещена на карантин.

Почтовый Антивирус

Почтовый Антивирус проверяет входящие и исходящие почтовые сообщения на вашем компьютере. Письмо будет доступно адресату только в том случае, если оно не содержит опасных объектов.

Веб-Антивирус

Веб-Антивирус перехватывает и блокирует выполнение скрипта, расположенного на веб-сайте, если он представляет угрозу. Контролю также подвергается весь веб-трафик. Кроме того, компонент блокирует доступ к опасным веб-сайтам.

IM-Антивирус

IM-Антивирус обеспечивает безопасность работы с интернет-пейджерами. Компонент защищает информацию, поступающую на ваш компьютер по протоколам интернет-пейджеров. IM-Антивирус обеспечивает безопасную работу со многими программами, предназначенными для быстрого обмена сообщениями.

Проактивная защита

Проактивная защита позволяет обнаружить новую вредоносную программу еще до того, как она успеет нанести вред. Работа компонента основана на контроле и анализе поведения всех программ, установленных на вашем компьютере. В зависимости от выполняемых ими действий Kaspersky CRYSTAL принимает решение о том, является ли программа потенциально опасной. Таким образом, ваш компьютер защищен не только от уже известных вирусов, но и от новых, еще не исследованных.

Контроль программ

Контроль программ регистрирует действия, совершаемые программами в системе, и регулирует деятельность программ, исходя из того, к какой группе компонент относит данную программу. Для каждой группы программ задан набор правил. Эти правила регламентируют доступ программ к различным ресурсам операционной системы.

Сетевой экран

Сетевой экран обеспечивает безопасность вашей работы в локальных сетях и интернете. Компонент производит фильтрацию всей сетевой активности согласно правилам двух типов: *правилам для программ* и *пакетным правилам*.

Мониторинг сети

Компонент, предназначенный для просмотра информации о сетевой активности в реальном времени.

Защита от сетевых атак

Защита от сетевых атак*запускается при старте операционной системы и отслеживает во входящем трафике активность, характерную для сетевых атак. Обнаружив попытку атаки на компьютер, Kaspersky CRYSTAL блокирует любую сетевую активность атакующего компьютера в отношении вашего компьютера.*

Анти-Спам

Анти-Спам встраивается в установленный на вашем компьютере почтовый клиент и контролирует все поступающие почтовые сообщения на предмет спама. Все письма, содержащие спам, помечаются специальным заголовком. Предусмотрена также возможность настройки Анти-Спама на обработку спама (автоматическое удаление, помещение в специальную папку и т.д.).

Анти-Фишинг

Компонент, встроенный в Веб-Антивирус, Анти-Спам и IM-Антивирус, который позволяет проверять веб-адреса на принадлежность к спискам фишинговых и подозрительных веб-адресов.

Анти-Баннер

Анти-Баннер блокирует рекламную информацию, размещенную на специальных баннерах, встроенных в интерфейс различных программ, установленных на вашем компьютере, и находящихся в интернете.

Защита информации

Для защиты данных от утери, несанкционированного доступа или кражи предназначены функции Резервного копирования, Шифрования данных, Менеджера паролей.

Резервное копирование

Данные на компьютере могут быть утеряны или повреждены по разным причинам: например, в результате действия вируса, изменения или удаления информации другим пользователем и т. п. Чтобы избежать потери важной информации, необходимо регулярно осуществлять резервное копирование данных.

Резервное копирование позволяет создавать резервные копии данных в специальном хранилище на выбранном носителе. Для этого настраиваются задачи резервного копирования. После запуска задачи вручную или автоматически по расписанию в хранилище создаются резервные копии выбранных файлов.

При необходимости из резервной копии можно восстановить нужную версию сохраненного файла. Таким образом, регулярное резервное копирование обеспечивает дополнительную сохранность данных.

Шифрование данных

Конфиденциальная информация, которая хранится в электронном виде, требует дополнительной защиты от несанкционированного доступа. Такую защиту обеспечивает хранение данных в зашифрованном контейнере.

Шифрование данных позволяет создавать специальные зашифрованные контейнеры на выбранном носителе. В системе такие контейнеры отображаются как виртуальные съемные диски. При этом для доступа к данным, хранящимся в зашифрованном контейнере, необходимо ввести пароль.

Менеджер паролей

В настоящее время для доступа к большинству услуг и ресурсов требуется регистрация пользователя и последующий ввод учетных данных для аутентификации. При этом в целях безопасности не рекомендуется использовать одинаковые учетные записи для разных ресурсов, а также записывать свои имя пользователя и пароль. В итоге современному человеку становится не под силу держать в голове огромное количество учетных данных. Это обстоятельство делает проблему надежного хранения паролей особенно актуальной.

Менеджер паролей обеспечивает хранение в зашифрованном виде различных персональных данных (например, имен пользователей, паролей, адресов, номеров телефонов и кредитных карт). Доступ к данным защищен единым мастер-паролем. После ввода мастер-пароля Менеджер паролей позволяет автоматически заполнять поля различных форм авторизации. Таким образом, для управления всеми учетными данными достаточно запомнить только один мастер-пароль.

Родительский контроль

Для защиты детей и подростков от угроз, связанных с работой на компьютере и в интернете, предназначены функции Родительского контроля.

Родительский контроль позволяет установить гибкие ограничения доступа к интернет-ресурсам и программам для разных пользователей компьютера в зависимости от их возраста. Кроме того, эта функция позволяет просматривать статистические отчеты о действиях контролируемых пользователей.

Центр управления

Часто домашняя сеть включает в себя несколько компьютеров, что затрудняет управление безопасностью. Уязвимость одного компьютера ставит под угрозу всю сеть.

Центр управления позволяет запускать задачи проверки на вирусы и обновления для всей сети или для выбранных компьютеров, управлять резервным копированием данных, а также настраивать параметры родительского контроля на всех компьютерах сети непосредственно со своего рабочего места. Таким образом, обеспечивается удаленное управление безопасностью всех компьютеров, входящих в домашнюю сеть.

СЕРВИС ДЛЯ ЗАРЕГИСТРИРОВАННЫХ ПОЛЬЗОВАТЕЛЕЙ

ЗАО «Лаборатория Касперского» предлагает своим легальным пользователям комплекс услуг, позволяющих увеличить эффективность использования программы.

Приобретая лицензию, вы становитесь зарегистрированным пользователем и в течение срока действия лицензии можете получать следующие услуги:

- ежечасное обновление баз программы и предоставление новых версий данного программного продукта;
- консультации по вопросам, связанным с установкой, настройкой и эксплуатацией программного продукта, оказываемые по телефону и через Личный кабинет;
- оповещение о выходе новых программных продуктов «Лаборатории Касперского» и о новых вирусах, появляющихся в мире. Данная услуга предоставляется пользователям, подписавшимся на рассылку

новостей ЗАО «Лаборатория Касперского» на веб-сайте Службы технической поддержки (http://support.kaspersky.ru/subscribe/).

Консультации по вопросам функционирования и использования операционных систем, стороннего программного обеспечения, а также работы различных технологий не проводятся.

Аппаратные и программные требования

Для нормального функционирования Kaspersky CRYSTAL, компьютер должен удовлетворять следующим минимальным требованиям:

Общие требования:

- 500 МБ свободного места на жестком диске.
- CD-ROM (для установки Kaspersky CRYSTAL с дистрибутивного CD-диска).
- Microsoft Internet Explorer 6.0 или выше (для обновления баз и программных модулей через интернет).
- Microsoft Windows Installer 2.0.
- Манипулятор мышь.
- Наличие соединения с интернетом для активации Kaspersky CRYSTAL.

- *Microsoft Windows XP Home Edition (Service Pack 3),* Microsoft Windows XP Professional (Service Pack 3), Microsoft Windows XP Professional x64 Edition (Service Pack 2)*:*
  - Процессор Intel Pentium 300 МГц или выше (или совместимый аналог).
  - 256 МБ оперативной памяти.
- *Microsoft Windows Vista Home Basic (32-bit/64-bit, Service Pack 2), Microsoft Windows Vista Home Premium (32-bit/64-bit, Service Pack 2), Microsoft Windows Vista Business (32-bit/64-bit, Service Pack 2), Microsoft Windows Vista Enterprise (32-bit/64-bit, Service Pack 2), Microsoft Windows Vista Ultimate (32-bit/64-bit, Service Pack 2):*
  - Процессор Intel Pentium 1 ГГц 32-bit (x86)/ 64-bit (x64) или выше (или совместимый аналог).
  - 1 ГБ оперативной памяти.
- *Microsoft Windows 7 Home Premium, Microsoft Windows 7 Professional, Microsoft Windows 7 Ultimate:*
  - Процессор Intel Pentium 1 ГГц 32-bit (x86)/ 64-bit (x64) или выше (или совместимый аналог).
  - 1 ГБ оперативной памяти (32-bit); 2 ГБ оперативной памяти (64-bit).

УСТАНОВКА И УДАЛЕНИЕ ПРОГРАММЫ

Этот раздел содержит инструкции, которые помогут вам установить программу на компьютер или обновить предыдущую версию программы. В этом же разделе описано, как удалить программу с компьютера.

В ЭТОМ РАЗДЕЛЕ

Установка программы на компьютер 22

Изменение, восстановление и удаление программы с помощью мастера установки 32

Установка программы на компьютер

Kaspersky CRYSTAL устанавливается на компьютер в интерактивном режиме с помощью мастера установки.

Мастер состоит из последовательности окон (шагов), переключение между которыми осуществляется нажатием на кнопки **Назад** и **Далее**. Работа мастера завершается нажатием на кнопку **Завершить**. Для прекращения работы мастера на любом этапе следует нажать на кнопку **Отмена**.

Перед началом установки рекомендуется закрыть все работающие программы.

- *Чтобы установить Kaspersky CRYSTAL на ваш компьютер,*

  на CD-диске с продуктом запустите файл дистрибутива (файл с расширением exe).

Процесс установки Kaspersky CRYSTAL с дистрибутива, полученного через интернет, полностью совпадает с ходом установки программы с дистрибутивного CD-диска.

В этом разделе

Шаг 1. Поиск более новой версии программы 23

Шаг 2. Проверка соответствия системы необходимым условиям установки 24

Шаг 3. Выбор типа установки 24

Шаг 4. Просмотр лицензионного соглашения 24

Шаг 5. Положение об использовании Kaspersky Security Network 24

Шаг 6. Выбор папки назначения 25

Шаг 7. Выбор компонентов программы для установки 25

Шаг 8. Поиск других антивирусных программ 26

Шаг 9. Отключение сетевого экрана Microsoft Windows 26

Шаг 10. Подготовка к установке 26

Шаг 11. Установка 27

Шаг 12. Активация программы 27

Шаг 13. Проверка данных 27

Шаг 14. Регистрация пользователя 27

Шаг 15. Завершение активации 28

Шаг 16. Ограничение доступа к программе 28

Шаг 17. Выбор режима защиты 29

Шаг 18. Настройка обновления программы 29

Шаг 19. Выбор обнаруживаемых угроз 30

Шаг 20. Анализ системы 30

Шаг 21. Завершение работы мастера 30

Начало работы 31

Шаг 1. Поиск более новой версии программы

Перед установкой проверяется наличие более актуальной версии Kaspersky CRYSTAL на серверах обновлений «Лаборатории Касперского».

Если более новой версии программы на серверах обновлений «Лаборатории Касперского» не обнаружено, будет запущен мастер установки текущей версии.

Если на серверах обновлений выложена более новая версия Kaspersky CRYSTAL, вам будет предложено загрузить и установить ее на ваш компьютер. Рекомендуется устанавливать новую версию программы, так как в новые версии вносятся улучшения, позволяющие более эффективно защищать ваш компьютер. В случае отказа от установки более новой версии будет запущен мастер установки текущей версии. Если же вы примете решение установить более новую версию, файлы дистрибутива будут скопированы на ваш компьютер, и мастер

установки новой версии будет запущен автоматически. Дальнейшее описание установки более новой версии читайте в документации к соответствующей версии программы.

Шаг 2. Проверка соответствия системы необходимым условиям установки

Перед установкой Kaspersky CRYSTAL на вашем компьютере проверяется соответствие операционной системы и пакетов обновлений (Service Pack) программным требованиям для установки (см. стр. 20). Помимо этого, проверяется наличие требуемого программного обеспечения, а также прав на установку программного обеспечения. Если какое-либо из перечисленных условий не выполнено, на экран будет выведено соответствующее уведомление.

Шаг 3. Выбор типа установки

На данном этапе установки вы можете выбрать тип установки Kaspersky CRYSTAL:

- *Быстрая установка*. При выборе этого варианта (флажок **Выборочная установка** снят) программа будет полностью установлена на ваш компьютер с параметрами защиты, которые рекомендуют специалисты «Лаборатории Касперского». Мастер установки предложит вам ознакомиться с лицензионным соглашением, а также с положением об использовании Kaspersky Security Network, после чего программа будет установлена на ваш компьютер.

- *Выборочная установка*. При выборе этого варианта (флажок **Выборочная установка** установлен) вы можете изменить параметры установки: выбрать компоненты программы, которые вы хотите установить, и указать папку, куда будет установлена программа. Для каждого выбранного компонента будут установлены параметры защиты, рекомендованные специалистами «Лаборатории Касперского».

  Выборочный метод установки рекомендуется использовать только опытным пользователям.

Независимо от выбранного варианта по окончании установки вы сможете активировать Kaspersky CRYSTAL и настроить параметры защиты программы от несанкционированного доступа.

Для продолжения установки нажмите на кнопку **Далее**.

Шаг 4. Просмотр лицензионного соглашения

На данном этапе следует ознакомиться с лицензионным соглашением, которое заключается между вами и «Лабораторией Касперского».

Внимательно прочтите соглашение и, если вы согласны со всеми его пунктами, нажмите на кнопку **Я согласен**. Установка программы на ваш компьютер будет продолжена.

Чтобы отказаться от установки программы, нажмите на кнопку **Отмена**.

Шаг 5. Положение об использовании Kaspersky Security Network

На этом этапе вам предлагается принять участие в программе Kaspersky Security Network. Участие в программе предусматривает отправку в ЗАО «Лаборатория Касперского» информации о новых угрозах, обнаруженных на вашем компьютере, о запускаемых программах и о загружаемых подписанных программах, отправку уникального идентификатора, присвоенного вашему экземпляру Kaspersky CRYSTAL, и информации о системе. При этом гарантируется, что персональные данные отправляться не будут.

Ознакомьтесь с положением об использовании Kaspersky Security Network. Чтобы ознакомиться с полным текстом положения, нажмите на кнопку **Полное KSN-соглашение**. Если вы согласны со всеми его пунктами, установите флажок **Я принимаю условия участия в Kaspersky Security Network**.

Для продолжения установки нажмите на кнопку **Установить** (при быстрой установке) или **Далее** (при выборочной установке).

Шаг 6. Выбор папки назначения

Этот шаг мастера установки доступен в том случае, если выполняется выборочная установка Kaspersky CRYSTAL (см. стр. 24). При стандартной установке шаг пропускается и программа устанавливается в папку, предусмотренную по умолчанию.

На этом этапе вы можете выбрать папку, в которую будет установлен Kaspersky CRYSTAL. По умолчанию задан следующий путь:

- **<диск> \ Program Files \ Kaspersky Lab \ Kaspersky CRYSTAL** – для 32-разрядных систем;
- **<диск> \ Program Files (x86) \ Kaspersky Lab \ Kaspersky CRYSTAL** – для 64-разрядных систем.

Чтобы установить Kaspersky CRYSTAL в другую папку, укажите путь к ней в поле ввода или нажмите на кнопку **Обзор** и выберите папку в открывшемся окне.

Обратите внимание на следующие ограничения:

- Нельзя устанавливать программу на сетевые и съемные диски, а также на виртуальные диски (диски, созданные с помощью команды `SUBST`).
- Не рекомендуется устанавливать программу в папку, содержащую файлы или другие папки, так как впоследствии к ней будет запрещен доступ на редактирование.
- Путь к папке установки должен быть не длиннее 200 символов и не должен содержать спецсимволы **/**, **?**, **:**, *****, **"**, **>**, **<** и **|**.

Для продолжения установки нажмите на кнопку **Далее**.

Шаг 7. Выбор компонентов программы для установки

Этот шаг мастера установки доступен в том случае, если выполняется выборочная установка Kaspersky CRYSTAL (см. стр. 24). При стандартной установке шаг пропускается и программа устанавливается на компьютер полностью.

На данном этапе вы можете выбрать компоненты программы, которые будут установлены на вашем компьютере. По умолчанию выбраны все компоненты защиты и ядро программы.

Чтобы принять решение об установке какого-либо компонента, в нижней части окна можно просмотреть краткую информацию о выбранном компоненте и выяснить, сколько места на жестком диске требуется для его установки.

Чтобы выбрать компонент для последующей установки, нажмите на значок рядом с именем компонента и выберите пункт **Компонент будет установлен на локальный жесткий диск**. Чтобы отказаться от установки компонента, выберите пункт меню **Компонент будет недоступен**. Помните, что отменяя установку компонентов Антивируса, вы лишаетесь защиты от целого ряда опасных программ.

Чтобы узнать подробную информацию о свободном месте на жестких дисках вашего компьютера, нажмите на кнопку **Диск**. Информация будет представлена в открывшемся окне.

После того как выбор устанавливаемых компонентов будет завершен, нажмите на кнопку **Далее**. Чтобы вернуться к списку устанавливаемых компонентов по умолчанию, нажмите на кнопку **Сброс**.

Шаг 8. Поиск других антивирусных программ

На этом этапе осуществляется поиск других установленных на вашем компьютере антивирусных продуктов, в том числе продуктов «Лаборатории Касперского», совместное использование с которыми Kaspersky CRYSTAL может привести к возникновению конфликтов.

При обнаружении таких программ на вашем компьютере их список будет выведен на экран. Вам будет предложено удалить их, прежде чем продолжить установку.

Для удаления обнаруженных антивирусных программ воспользуйтесь кнопкой **Удалить**.

Для продолжения установки нажмите на кнопку **Далее**.

Шаг 9. Отключение сетевого экрана Microsoft Windows

Этот шаг мастера установки доступен в том случае, если Kaspersky CRYSTAL устанавливается на компьютер с включенным сетевым экраном Microsoft Windows, и в числе устанавливаемых компонентов присутствует Сетевой экран.

На данном этапе установки Kaspersky CRYSTAL вам предлагается отключить сетевой экран операционной системы Microsoft Windows. В состав Kaspersky CRYSTAL входит компонент Сетевой экран, который обеспечивает полную защиту вашей работы в сети. Поэтому в дополнительной защите средствами операционной системы нет необходимости.

Если вы хотите использовать Сетевой экран в качестве основного средства защиты при работе в сети, нажмите на кнопку **Далее**. Сетевой экран Microsoft Windows будет автоматически отключен.

Если вы хотите защищать свой компьютер с помощью сетевого экрана Microsoft Windows, выберите вариант **Использовать сетевой экран Microsoft Windows**. В этом случае компонент Сетевой экран будет установлен, но отключен во избежание конфликтов в работе программ.

Шаг 10. Подготовка к установке

Этот шаг мастера установки доступен в том случае, если выполняется выборочная установка Kaspersky CRYSTAL (см. стр. 24). При стандартной установке шаг пропускается.

На данном этапе вам будет предложено произвести завершающую подготовку к установке Kaspersky CRYSTAL на ваш компьютер.

При первоначальной установке программы не рекомендуется снимать флажок **Защитить процесс установки**. Если в ходе установки программы возникнут ошибки, включенная защита позволит провести корректную процедуру отката установки. При повторной попытке установки рекомендуется снять данный флажок.

При удаленной установке программы на компьютер через *Windows Remote Desktop* рекомендуется снимать флажок **Защитить процесс установки**. Если такой флажок установлен, процедура установки может быть не проведена или проведена некорректно.

Для продолжения установки нажмите на кнопку **Установить**.

В процессе установки в составе Kaspersky CRYSTAL компонентов, перехватывающих сетевой трафик, происходит разрыв текущих сетевых соединений. Большинство прерванных соединений восстанавливаются через некоторое время.

Шаг 11. Установка

Установка программы занимает некоторое время. Дождитесь ее завершения.

После установки автоматически запустится мастер настройки Kaspersky CRYSTAL.

В случае возникновения ошибки установки, которая может быть вызвана наличием на компьютере вредоносного программного обеспечения, препятствующего установке антивирусных программ, мастер установки предложит скачать специальное средство для устранения заражения – *утилиту Kaspersky Virus Removal Tool*.

Если вы согласитесь установить утилиту, мастер установки загрузит ее с серверов «Лаборатории Касперского», после чего автоматически запустится установка утилиты. Если мастер не сможет загрузить утилиту, вам будет предложено загрузить ее самостоятельно, перейдя по предлагаемой ссылке.

После завершения работы с утилитой ее необходимо удалить и запустить установку Kaspersky CRYSTAL с начала.

Шаг 12. Активация программы

Активация – это процедура введения в действие лицензии, дающей право на использование полнофункциональной версии программы в течение срока действия лицензии.

Для активации программы необходимо подключение к интернету.

Вам предлагаются следующие варианты активации Kaspersky CRYSTAL:

- **Активировать коммерческую версию**. Выберите этот вариант и введите код активации (см. раздел «О коде активации» на стр. 35), если вы приобрели коммерческую версию программы.

- **Активировать пробную версию**. Выберите данный вариант активации, если вы хотите установить пробную версию программы перед принятием решения о покупке коммерческой версии. Вы сможете использовать полнофункциональную версию программы в течение срока действия, ограниченного лицензией для пробной версии программы. По истечении срока действия лицензии возможность повторной активации пробной версии будет недоступна.

- **Активировать позже**. При выборе этого варианта этап активации Kaspersky CRYSTAL пропускается. Программа будет установлена на ваш компьютер, но при этом не будут доступны некоторые функции программы, например обновление (обновить программу вы сможете только один раз после установки), создание зашифрованного контейнера, дополнительные инструменты и др. Вариант **Активировать позже** доступен только при первом запуске мастера активации, сразу после установки программы.

Шаг 13. Проверка данных

На этом шаге Kaspersky CRYSTAL отправляет данные на сервер активации для проверки.

Для проверки данных необходимо подключение к интернету.

Шаг 14. Регистрация пользователя

Этот шаг доступен только при активации коммерческой версии программы. При активации пробной версии шаг пропускается.

Чтобы в дальнейшем иметь возможность обращаться за помощью в Службу технической поддержки «Лаборатории Касперского», вам нужно зарегистрироваться.

Если вы согласны зарегистрироваться, для отправки своих регистрационных данных укажите их в соответствующих полях и затем нажмите на кнопку **Далее**.

Шаг 15. Завершение активации

Мастер настройки информирует вас об успешном завершении активации Kaspersky CRYSTAL. Кроме того, приводится информация о лицензии: тип (коммерческая или пробная), дата окончания срока действия лицензии, а также количество компьютеров, на которые эта лицензия распространяется.

В случае активации подписки вместо даты окончания срока действия лицензии приводится информация о статусе подписки (см. стр. 248).

Нажмите на кнопку **Далее**, чтобы продолжить работу мастера.

Шаг 16. Ограничение доступа к программе

Этот шаг мастера настройки доступен в том случае, если выполняется выборочная установка Kaspersky CRYSTAL (см. стр. 24). При стандартной установке шаг пропускается и программа устанавливается без ограничения доступа. В дальнейшем вы сможете включить это ограничение вручную (см. стр. 70) в окне настройки программы.

Ограничение доступа к Kaspersky CRYSTAL позволяет предотвратить попытки несанкционированного отключения защиты и настройки параметров компонентов, входящих в состав Kaspersky CRYSTAL.

Ограничение доступа с помощью пароля может быть полезно в следующих случаях:

- если персональный компьютер используют несколько человек, в том числе с разным уровнем компьютерной грамотности;
- если Kaspersky CRYSTAL обеспечивает безопасность нескольких компьютеров, объединенных в домашнюю сеть;
- если есть риск, что защита может быть отключена вредоносными программами.

Для включения защиты установите флажок **Включить защиту паролем** и заполните поля **Пароль** и **Подтверждение**.

Ниже укажите область, на которую будет распространяться ограничение доступа:

- **Настройка параметров программы** – запрос пароля при попытке пользователя сохранить изменения параметров Kaspersky CRYSTAL.
- **Управление Резервным копированием** – запрос пароля перед запуском задач резервного копирования.
- **Управление Родительским контролем** – запрос пароля перед запуском задач родительского контроля.
- **Удаленное управление безопасностью на компьютерах домашней сети** – запрос пароля перед изменением параметров Kaspersky CRYSTAL через сеть.
- **Завершение работы программы** – запрос пароля при попытке пользователя завершить работу программы.

Шаг 17. Выбор режима защиты

Этот шаг мастера настройки доступен в том случае, если выполняется выборочная установка Kaspersky CRYSTAL (см. стр. 24). При стандартной установке этот шаг пропускается и по умолчанию программа работает в автоматическом режиме защиты. В дальнейшем вы сможете выбрать режим защиты вручную (см. стр. 54).

Выберите режим защиты, предоставляемой Kaspersky CRYSTAL.

Для выбора доступны два режима:

- *Автоматический*. При возникновении важных событий Kaspersky CRYSTAL автоматически выполняет действие, рекомендуемое специалистами «Лаборатории Касперского». При обнаружении угрозы программа пытается вылечить объект, а если это невозможно, удаляет его. Подозрительные объекты пропускаются без обработки. О возникающих событиях информируют всплывающие сообщения.

- *Интерактивный*. В этом режиме программа реагирует на возникновение событий заданным вами образом. При возникновении событий, требующих вашего вмешательства, программа выводит на экран уведомления, предлагающие возможность выбора действия.

Уведомление об обнаружении активного заражения выводится на экран вне зависимости от выбранного режима защиты.

Шаг 18. Настройка обновления программы

Этот шаг мастера настройки доступен в том случае, если выполняется выборочная установка Kaspersky CRYSTAL (см. стр. 24). При стандартной установке шаг пропускается и по умолчанию выполняется автоматическое обновление. В дальнейшем вы сможете выбрать режим обновления вручную (см. стр. 90).

Качество защиты вашего компьютера напрямую зависит от своевременного получения обновлений баз и модулей программы. В данном окне мастера настройки вам предлагается выбрать режим обновления и сформировать параметры расписания:

- **Автоматическое обновление**. Программа проверяет наличие пакета обновлений в источнике обновления с заданной периодичностью. Частота проверки может увеличиваться во время вирусных эпидемий и сокращаться при их отсутствии. Обнаружив свежие обновления, программа скачивает их и устанавливает на компьютер. Такой режим используется по умолчанию.

- **Обновление по расписанию** (в зависимости от параметров расписания интервал может изменяться). Обновление будет запускаться автоматически по сформированному расписанию. Параметры расписания можно установить в окне, открывающемся нажатием на кнопку **Настройка**.

- **Обновление вручную**. В этом случае вы будете самостоятельно запускать обновление программы.

Обратите внимание, что базы и модули программы, входящие в дистрибутив, на момент установки Kaspersky CRYSTAL могут устареть. Поэтому мы рекомендуем получить самые последние обновления. Для этого нажмите на кнопку **Обновить сейчас**. В этом случае программа получит необходимый набор обновлений с серверов обновлений в интернете и установит их на ваш компьютер.

Если базы, входящие в состав дистрибутива, сильно устарели, то пакет обновлений может иметь значительный размер и создать дополнительный интернет-трафик (до нескольких десятков мегабайт).

Если вы хотите перейти к настройке параметров обновления (выбрать ресурс, с которого будет происходить обновление, настроить запуск обновления с правами определенной учетной записи и т.д.), нажмите на кнопку **Настройка**.

Шаг 19. Выбор обнаруживаемых угроз

Этот шаг мастера настройки доступен в том случае, если выполняется выборочная установка Kaspersky CRYSTAL (см. стр. 24). При стандартной установке шаг пропускается и устанавливаются параметры по умолчанию. В дальнейшем вы сможете выбрать обнаруживаемые угрозы вручную (см. стр. 220).

На данном этапе вы можете выбрать категории угроз, обнаруживаемые Kaspersky CRYSTAL. Программы, способные нанести вред вашему компьютеру, Kaspersky CRYSTAL ищет всегда. К таким типам программ относятся вирусы, черви и троянские программы.

Шаг 20. Анализ системы

На данном этапе производится сбор информации о программах, входящих в состав Microsoft Windows. Эти программы попадают в список доверенных программ, которые не имеют ограничений на действия, совершаемые в системе.

Анализ других программ происходит после первого их запуска после установки Kaspersky CRYSTAL.

Шаг 21. Завершение работы мастера

Последнее окно мастера настройки информирует вас о завершении установки программы. Чтобы начать работу Kaspersky CRYSTAL, убедитесь, что флажок **Запустить Kaspersky CRYSTAL** установлен, и нажмите на кнопку **Завершить**.

В некоторых случаях может потребоваться перезагрузка операционной системы. Если перед завершением работы мастера вы установили флажок **Запустить Kaspersky CRYSTAL**, после перезагрузки программа будет запущена автоматически. Если вы сняли этот флажок, программу нужно будет запустить вручную (см. стр. 51).

Начало работы

После установки и настройки программа готова к работе. Чтобы обеспечить должную защиту вашего компьютера, рекомендуем сразу после установки и настройки выполнить следующие действия:

- Обновить базы программы (см. раздел «Как обновить базы и модули программы» на стр. 58).
- Проверить компьютер на вирусы (см. раздел «Как выполнить полную проверку компьютера на вирусы» на стр. 61), а также на уязвимости.
- Проверить состояние защиты компьютера и при необходимости устранить проблемы в защите (см. раздел «Диагностика и устранение проблем в защите» на стр. 52).

Входящий в состав Kaspersky CRYSTAL компонент Анти-Спам использует самообучающийся алгоритм для распознавания нежелательных сообщений. Запустите мастер обучения Анти-Спама, чтобы настроить компонент для работы с вашей корреспонденцией.

Для быстрого восстановления данных в случае утраты настройте резервное копирование (см. раздел «Как создать резервные копии ваших данных» на стр. 69).

Для защиты конфиденциальной информации от несанкционированного доступа создайте зашифрованные контейнеры для хранения данных (см. раздел «Шифрование данных» на стр. 65).

Для защиты детей и подростков от угроз, связанных с использованием компьютера, задайте ограничения Родительского контроля (см. раздел «Как ограничить использование компьютера и интернета для разных пользователей» на стр. 71).

Изменение, восстановление и удаление программы с помощью мастера установки

Восстановление программы полезно проводить в том случае, если вы обнаружили в ее работе какие-либо ошибки, возникшие вследствие некорректной настройки или повреждения ее файлов.

Изменение компонентного состава позволяет вам доустановить недостающие компоненты Kaspersky CRYSTAL или удалить те из них, которые мешают вам в работе или не требуются.

- *Чтобы перейти к восстановлению исходного состояния программы, установке компонентов Kaspersky CRYSTAL, которые не были установлены изначально, или удалению программы, выполните следующие действия:*

  1. Вставьте CD-диск с дистрибутивом программы в CD/DVD-ROM-устройство, если установка программы производилась с него. В случае установки Kaspersky CRYSTAL из другого источника (папка общего доступа, папка на жестком диске и т. д.) убедитесь, что дистрибутив программы присутствует в данном источнике и у вас есть к нему доступ.

  2. Выберите **Пуск → Программы → Kaspersky CRYSTAL9.1 → Изменение, восстановление или удаление**.

В результате будет запущена программа установки, которая выполнена в виде мастера. Рассмотрим подробнее шаги, необходимые для восстановления, изменения компонентного состава программы и ее удаления.

В этом разделе

Шаг 1. Стартовое окно программы установки 32

Шаг 2. Выбор операции 32

Шаг 3. Завершение операции восстановления, изменения или удаления программы 33

Шаг 1. Стартовое окно программы установки

Если вы провели все описанные выше действия, необходимые для восстановления или изменения состава программы, на экране будет открыто приветственное окно программы установки Kaspersky CRYSTAL. Для продолжения нажмите на кнопку **Далее**.

Шаг 2. Выбор операции

На данном этапе вам нужно определить, какую именно операцию вы хотите выполнить над программой: вам предлагается изменить компонентный состав программы, восстановить исходное состояние установленных компонентов или удалить какие-либо компоненты либо программу полностью. Для выполнения нужной вам операции нажмите на соответствующую кнопку. Дальнейшее действие программы установки зависит от выбранной операции.

Изменение компонентного состава выполняется аналогично выборочной установке программы: можно указать, какие компоненты вы хотите установить, а также выбрать те, которые хотите удалить.

Восстановление программы производится исходя из установленного компонентного состава. Будут обновлены все файлы тех компонентов, которые были установлены, и для каждого из них будет установлен **Рекомендуемый** уровень обеспечиваемой защиты.

При удалении программы вы можете выбрать, какие данные, сформированные и используемые в работе программы, вы хотите сохранить на вашем компьютере. Чтобы удалить все данные Kaspersky CRYSTAL,

выберите вариант **Удалить программу полностью**. Для сохранения данных нужно выбрать вариант **Сохранить объекты программы** и указать, какие именно объекты не нужно удалять:

- *Информация об активации* – файл ключа, необходимый для работы программы.
- *Базы Анти-Спама* – база данных, на основе которой распознается нежелательная электронная корреспонденция. Эта база содержит подробную информацию о том, какая почта является для вас спамом, а какая – полезной почтой.
- *Объекты резервного хранилища и объекты карантина*. Объекты резервного хранилища – это резервные копии удаленных или вылеченных объектов. Такие объекты рекомендуется сохранить для возможности последующего восстановления. Объекты карантина – это объекты, возможно зараженные вирусами или их модификациями. Такие объекты содержат код, который похож на код известного вируса, но однозначно сделать вывод об их вредоносности нельзя. Рекомендуется их сохранить, поскольку они могут оказаться незараженными или их излечение станет возможным после обновления баз программы.
- *Параметры защиты* – значения параметров работы всех компонентов программы.
- *Данные iSwift и iChecker* – база, содержащая информацию о проверенных объектах файловой системы NTFS. Она позволяет ускорить проверку объектов. Используя данные этой базы, Kaspersky CRYSTAL проверяет только те объекты, которые изменились со времени последней проверки.
- *Данные общей папки безопасной среды* – данные, которые доступны при работе и в безопасной среде и в обычной среде.

Если между удалением одной версии Kaspersky CRYSTAL и установкой другой прошло достаточно продолжительное время, не рекомендуем вам использовать базу iSwift и iChecker, сохраненную с предыдущей установки программы. За это время на компьютер может проникнуть опасная программа, вредоносные действия которой не будут выявлены при использовании данной базы, и это может привести к заражению компьютера.

Для запуска выбранной операции нажмите на кнопку **Далее**. Запустится процесс копирования необходимых файлов на ваш компьютер или удаления выбранных компонентов и данных.

Шаг 3. Завершение операции восстановления, изменения или удаления программы

Процесс восстановления, изменения или удаления отображается на экране, после чего вы будете уведомлены о его завершении.

Удаление, как правило, требует последующей перезагрузки компьютера, поскольку это необходимо для учета изменений в системе. Запрос на перезагрузку компьютера будет выведен на экран. Нажмите на кнопку **Да**, чтобы выполнить перезагрузку немедленно. Чтобы перезагрузить компьютер позже вручную, нажмите на кнопку **Нет**.

УПРАВЛЕНИЕ ЛИЦЕНЗИЕЙ

Этот раздел содержит информацию об основных понятиях, используемых в контексте лицензирования программы. Из раздела вы узнаете также о возможности автоматического продления срока действия лицензии и о том, где просмотреть информацию о текущей лицензии.

В ЭТОМ РАЗДЕЛЕ

О лицензионном соглашении 34

О лицензии 34

О коде активации 35

Просмотр информации о лицензии 35

О ЛИЦЕНЗИОННОМ СОГЛАШЕНИИ

Лицензионное соглашение – это договор между физическим или юридическим лицом, правомерно владеющим экземпляром Kaspersky CRYSTAL, и ЗАО «Лаборатория Касперского». Соглашение входит в состав каждой программы «Лаборатории Касперского». В нем приводится детальная информация о правах и ограничениях на использование Kaspersky CRYSTAL.

В соответствии с лицензионным соглашением, приобретая и устанавливая программу «Лаборатории Касперского», вы получаете бессрочное право на владение ее копией.

О ЛИЦЕНЗИИ

Лицензия – это право на использование Kaspersky CRYSTAL и связанных с ним дополнительных услуг, предоставляемых вам «Лабораторией Касперского» или ее партнерами.

Каждая лицензия характеризуется сроком действия и типом.

Срок действия лицензии – период, в течение которого вам предоставляются дополнительные услуги:

- техническая поддержка;
- обновление баз и модулей программы.

Объем предоставляемых услуг зависит от типа лицензии.

Предусмотрены следующие типы лицензий:

- *Пробная* – бесплатная лицензия с ограниченным сроком действия, например, 30 дней, предназначенная для ознакомления с Kaspersky CRYSTAL.

  Пробная лицензия может использоваться только один раз.

  Пробная лицензия поставляется вместе с пробной версией программы. При наличии пробной лицензии вы можете обращаться в Службу технической поддержки только по вопросам активации программы или приобретения коммерческой лицензии. По завершении срока действия пробной лицензии Kaspersky

CRYSTAL прекращает выполнять все свои функции. Для продолжения работы программы ее нужно активировать.

- *Коммерческая* – платная лицензия с ограниченным сроком действия (например, один год), предоставляемая при покупке Kaspersky CRYSTAL. Для каждой лицензии задано определенное количество компьютеров, на которые можно установить Kaspersky CRYSTAL с этой лицензией.

  Во время действия коммерческой лицензии доступны все функции программы и дополнительные услуги.

  По окончании срока действия коммерческой лицензии Kaspersky CRYSTAL продолжает выполнять все свои функции, однако обновление антивирусных баз не производится. Вы по-прежнему можете осуществлять антивирусную проверку компьютера и использовать компоненты защиты, но только на основе антивирусных баз, актуальных на дату окончания срока действия лицензии. За две недели до истечения срока действия лицензии программа уведомит вас об этом, и вы сможете заблаговременно продлить срок действия лицензии.

- *Коммерческая с подпиской на обновление* и *коммерческая с подпиской на обновление и защиту* – платная лицензия с возможностью гибкого управления: вы можете приостанавливать и возобновлять подписку, продлять срок ее действия в автоматическом режиме, отказываться от подписки. Лицензия с подпиской распространяется поставщиками услуг. Управление подпиской осуществляется через персональный кабинет пользователя на веб-ресурсе поставщика услуги.

  Подписка может быть с ограниченным сроком (например, на один год) или с неограниченным. Подписку с ограниченным сроком необходимо самостоятельно продлевать по истечении срока ее действия. Подписка с неограниченным сроком продлевается автоматически при условии своевременного внесения предоплаты поставщику подписки.

  Если срок подписки ограничен, по окончании этого срока вам будет предоставлен льготный период для продления подписки, в течение которого функциональность программы будет сохранена.

  Если подписка не продлена, по истечении льготного периода Kaspersky CRYSTAL прекращает обновление баз программы (для лицензии с подпиской на обновление), а также прекращает осуществлять защиту компьютера и запускать задачи проверки (для лицензии с подпиской на обновление и защиту).

  При использовании подписки вы не сможете воспользоваться другим кодом активации для продления срока действия лицензии. Это будет возможно только после окончания срока подписки.

  Если на момент активации подписки у вас уже была активирована лицензия с ограниченным сроком действия, она будет заменена лицензией с подпиской. Чтобы отказаться от подписки, необходимо связаться с поставщиком услуг, у которого вы приобрели Kaspersky CRYSTAL.

  В зависимости от поставщика подписки, набор возможных действий с подпиской может различаться. Кроме того, может не предоставляться льготный период, в течение которого доступно продление подписки.

О коде активации

Код активации – это код, который предоставляется вам при покупке коммерческой лицензии Kaspersky CRYSTAL. Этот код необходим для активации программы.

Код активации представляет собой последовательность латинских букв и цифр, разделенных дефисами на четыре блока по пять символов, например AA111-AA111-AA111-AA111.

Просмотр информации о лицензии

➧ *Чтобы просмотреть информацию о текущей лицензии, выполните следующие действия:*

1. Откройте главное окно программы.

2. По ссылке **Лицензия** в нижней части окна откройте окно **Управление лицензиями**.

   В этом окне вы можете запустить процесс активации программы, покупки новой лицензии или продления срока действия текущей.

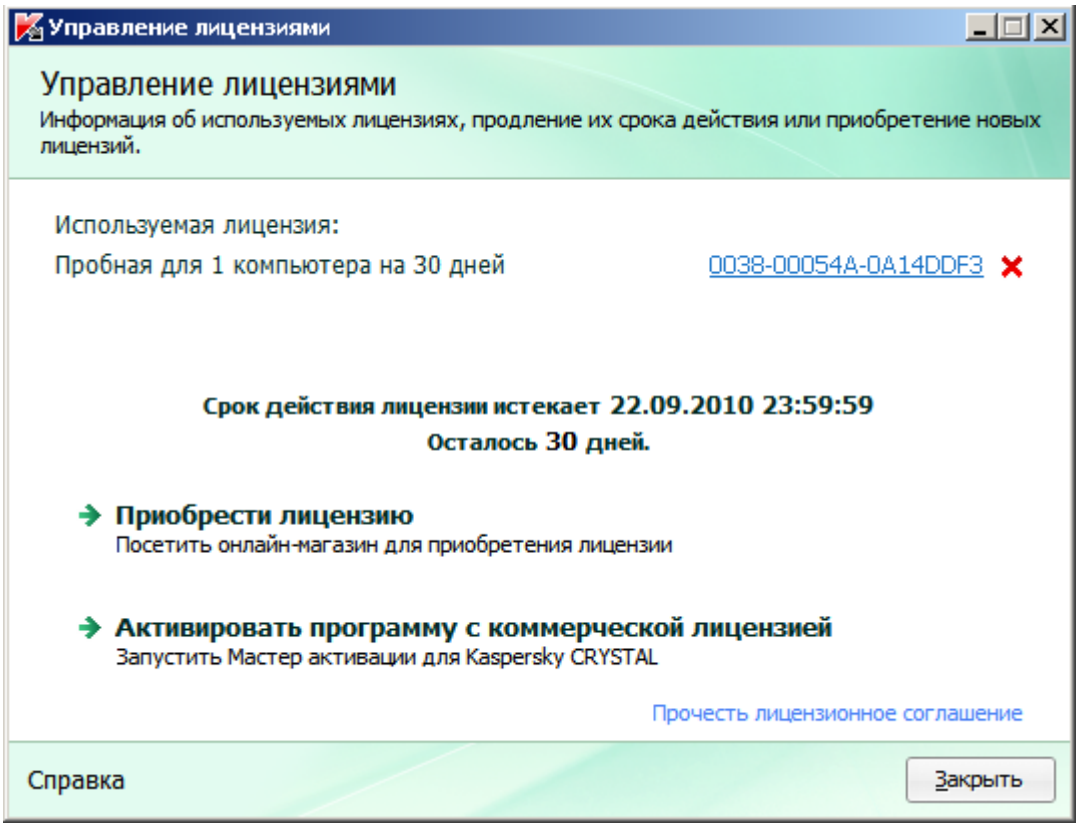


Рисунок 1. Окно Управление лицензиями

ИНТЕРФЕЙС ПРОГРАММЫ

В данной главе рассматриваются основные элементы интерфейса Kaspersky CRYSTAL.

В ЭТОМ РАЗДЕЛЕ

Значок в области уведомлений панели задач 37

Контекстное меню 38

Главное окно Kaspersky CRYSTAL..... 39

Окно настройки параметров программы 48

Окна уведомлений и всплывающие сообщения 49

Значок в области уведомлений панели задач

Сразу после установки Kaspersky CRYSTAL его значок появляется в области уведомлений панели задач Microsoft Windows.

Значок выполняет следующие основные функции:

- служит индикатором работы программы;
- обеспечивает доступ к контекстному меню, главному окну программы и окну просмотра новостей.

Индикация работы программы

Значок служит индикатором работы программы. Он отражает состояние защиты, а также показывает ряд основных действий, выполняемых программой на текущий момент:

 – проверяется почтовое сообщение;

 – проверяется веб-трафик;

 – обновляются базы и модули программы;

 – требуется перезагрузка компьютера для применения обновлений;

 – произошел сбой в работе какого-либо компонента программы.

По умолчанию включена анимация значка: например, при проверке почтового сообщения на фоне значка программы пульсирует миниатюрный значок письма, а при обновлении баз программы – вращается значок глобуса. Вы можете выключить анимацию (см. стр. 223).

При выключенной анимации значок может принимать следующий вид:

 (цветной значок) – все или некоторые компоненты защиты работают;

 (черно-белый значок) – все компоненты защиты выключены.

Доступ к контекстному меню и окнам программы

С помощью значка вы можете открыть контекстное меню (см. стр. 38) и главное окно программы (см. стр. 39).

- *Чтобы открыть контекстное меню,*

  наведите курсор на значок и нажмите на правую клавишу мыши.

- *Чтобы открыть главное окно программы,*

  наведите курсор на значок и нажмите на левую клавишу мыши.

При появлении новостей от «Лаборатории Касперского» в области уведомлений панели задач Microsoft Windows появляется значок . Двойным щелчком мыши на этом значке можно открыть окно новостей (см. стр. 224).

Контекстное меню

Контекстное меню позволяет перейти к выполнению основных задач защиты.

Меню Kaspersky CRYSTAL содержит следующие пункты:

- **Обновление** – запускает процесс обновления баз и модулей программы.
- **Полная проверка компьютера** – запускает полную проверку компьютера на присутствие вредоносных объектов (см. стр. 61).
- **Проверка на вирусы** – запускает проверку выбранных объектов на присутствие вредоносных объектов (см. стр. 59).
- **Виртуальная клавиатура** – открывает виртуальную клавиатуру (см. стр. 64).
- **Kaspersky CRYSTAL** – открывает главное окно программы (см. стр. 39).
- **Настройка** – открывает окно настройки параметров работы программы (см. стр. 48).
- **Активация** – запускает мастер активации Kaspersky CRYSTAL. Этот пункт меню присутствует только в том случае, если программа не активирована.
- **О программе** – открывает информационное окно со сведениями о программе.
- **Приостановить / Возобновить защиту** – временно отключает / включает работу компонентов постоянной защиты. Этот пункт меню не влияет на обновление программы и на выполнение задач поиска вирусов.
- **Приостановить / Включить Родительский контроль** – временно отключает / включает контроль всех пользователей. Этот пункт меню присутствует только в том случае, если установлен компонент Родительский контроль.
- **Блокировать сетевой трафик / Разблокировать сетевой трафик** – временно блокирует / возобновляет все сетевые соединения компьютера.

- **Выход** – завершает работу Kaspersky CRYSTAL (при выборе этого пункта меню программа будет выгружена из оперативной памяти компьютера).

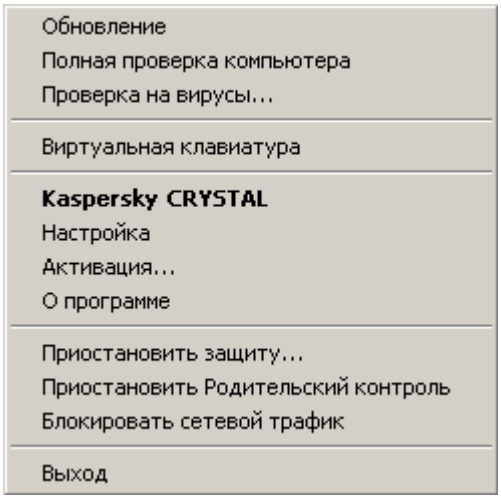


Рисунок 2. Контекстное меню

Если в момент открытия контекстного меню запущена какая-либо задача проверки на вирусы или задача обновления программы, ее название будет отражено в контекстном меню с указанием результата выполнения в процентах. Выбрав пункт меню с названием задачи, вы можете перейти к главному окну с отчетом о текущих результатах ее выполнения.

Чтобы открыть контекстное меню,

наведите курсор мыши на значок программы в области уведомлений панели задач и нажмите на правую клавишу мыши.

Главное окно Kaspersky CRYSTAL

В главном окне сосредоточены элементы интерфейса, предоставляющие доступ ко всем основным функциям программы.

Главное окно можно условно разделить на три части.

- Верхняя часть окна сигнализирует о текущем состоянии защиты вашего компьютера.

Существует три возможных состояния защиты, каждое из которых обозначено цветом. Зеленый цвет означает, что защита вашего компьютера осуществляется на должном уровне; желтый и красный предупреждают о наличии разного рода угроз безопасности. К угрозам относятся не только вредоносные программы, но и устаревшие базы программы, некоторые выключенные компоненты защиты, минимальные параметры работы программы и т. д.

По мере возникновения угроз безопасности их необходимо устранять (см. раздел «Диагностика и устранение проблем в защите» на стр. 52).

- Средняя часть окна позволяет перейти к основным функциям программы, а также возобновить / приостановить защиту, выполнить проверку на вирусы, запустить процесс резервного копирования данных и т. д. В верхней части окна расположены основные модули Kaspersky CRYSTAL:

- **Резервное копирование** – создание и хранение резервных копий файлов, обеспечивающих восстановление данных в случае утраты.
- **Защита компьютера** – компоненты защиты компьютера от различных угроз.
- **Родительский контроль** – ограничение доступа пользователей к компьютеру и интернет-ресурсам.

- Нижняя часть окна позволяет перейти к дополнительным функциям, которые обеспечивают расширенную защиту и оптимизируют работу системы. В нижней части окна расположены следующие компоненты и сервисы:
  - **Дополнительные инструменты** – оптимизация работы системы и решение специфических задач по обеспечению безопасности компьютера.
  - **Виртуальная клавиатура** – предотвращение перехвата данных, введенных с помощью клавиатуры.
  - **Центр управления (см. стр. 184) –** удаленное администрирование Kaspersky CRYSTAL.
  - **Шифрование данных** – предотвращение несанкционированного доступа к конфиденциальной информации.
  - **Менеджер паролей** – защита персональных данных, таких как: пароли, имена пользователей, номера интернет-пейджеров, контактные данные и т. д.

Рисунок 3. Главное окно программы

Также вы можете воспользоваться следующими кнопками и ссылками:

- **Настройка** – переход к настройке общих параметров программы (см. стр. 48).

- **Справка** – переход к справочной системе Kaspersky CRYSTAL.
- **Личный кабинет** – переход в личный кабинет пользователя (https://my.kaspersky.ru) на сайте Службы технической поддержки.
- **Поддержка** – открытие окна с информацией о системе и ссылками на информационные ресурсы «Лаборатории Касперского» (сайт Службы технической поддержки, форум).
- **Лицензия** – переход к активации Kaspersky CRYSTAL, продление срока действия лицензии.

Вы можете менять внешний вид (см. раздел «Внешний вид программы» на стр. 223) Kaspersky CRYSTAL, создавая и используя собственные графические элементы и выбранную цветовую палитру.

Защита компьютера

Окно **Защита компьютера** можно условно разделить на две части:

- Левая часть окна позволяет быстро перейти к работе с любой функцией программы, к выполнению задач проверки на вирусы или обновления и т. д.

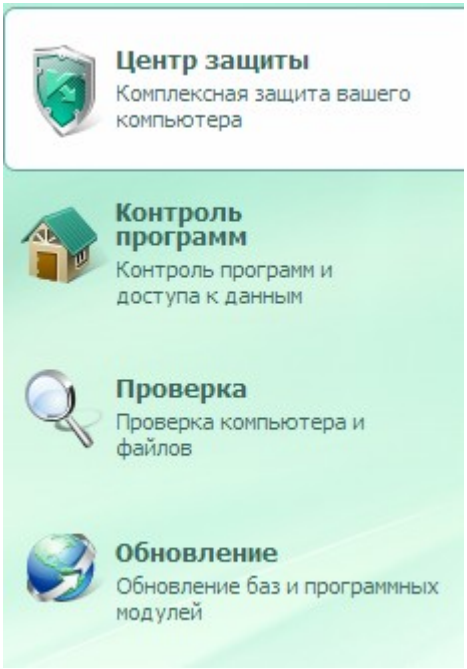


Рисунок 4. Левая часть окна Защита компьютера

- Правая часть окна содержит информацию о выбранной в левой части функции программы, позволяет настроить ее параметры, предоставляет инструменты для выполнения задач проверки на вирусы, получения обновлений и т. д.

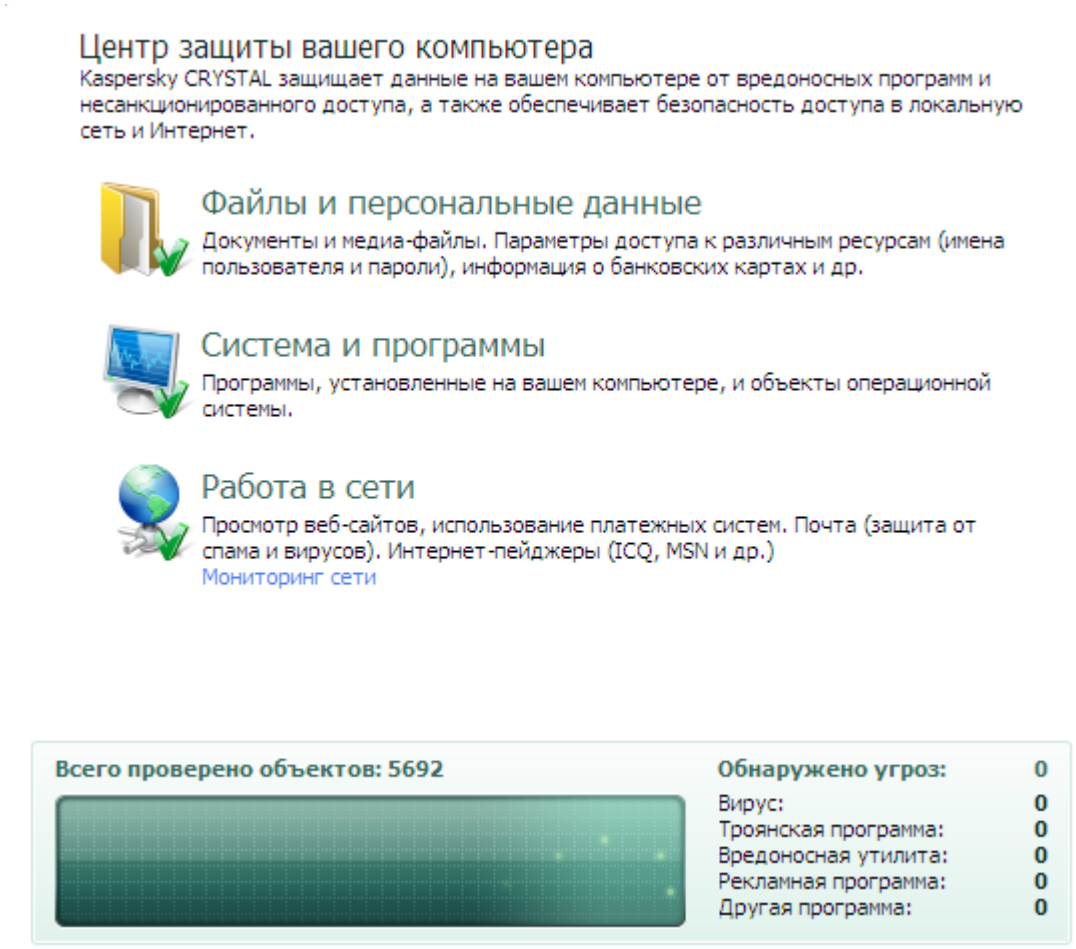


Рисунок 5. Правая часть окна Защита компьютера

Также вы можете воспользоваться следующими ссылками:

- **Настройка** – переход к окну настройки параметров защиты компьютера.
- **Карантин** – переход к работе с объектами, помещенными на карантин.
- **Отчет** – переход к списку событий, произошедших в работе программы.
- **Справка** – переход к справочной системе Kaspersky CRYSTAL.

Резервное копирование

Окно **Резервное копирование** состоит из двух частей:

- левая часть окна позволяет перейти к работе с основными функциями Резервного копирования: управлению задачами резервного копирования и хранилищами резервных копий, а также восстановлению данных;

- правая часть окна содержит перечень параметров выбранной в левой части функции.

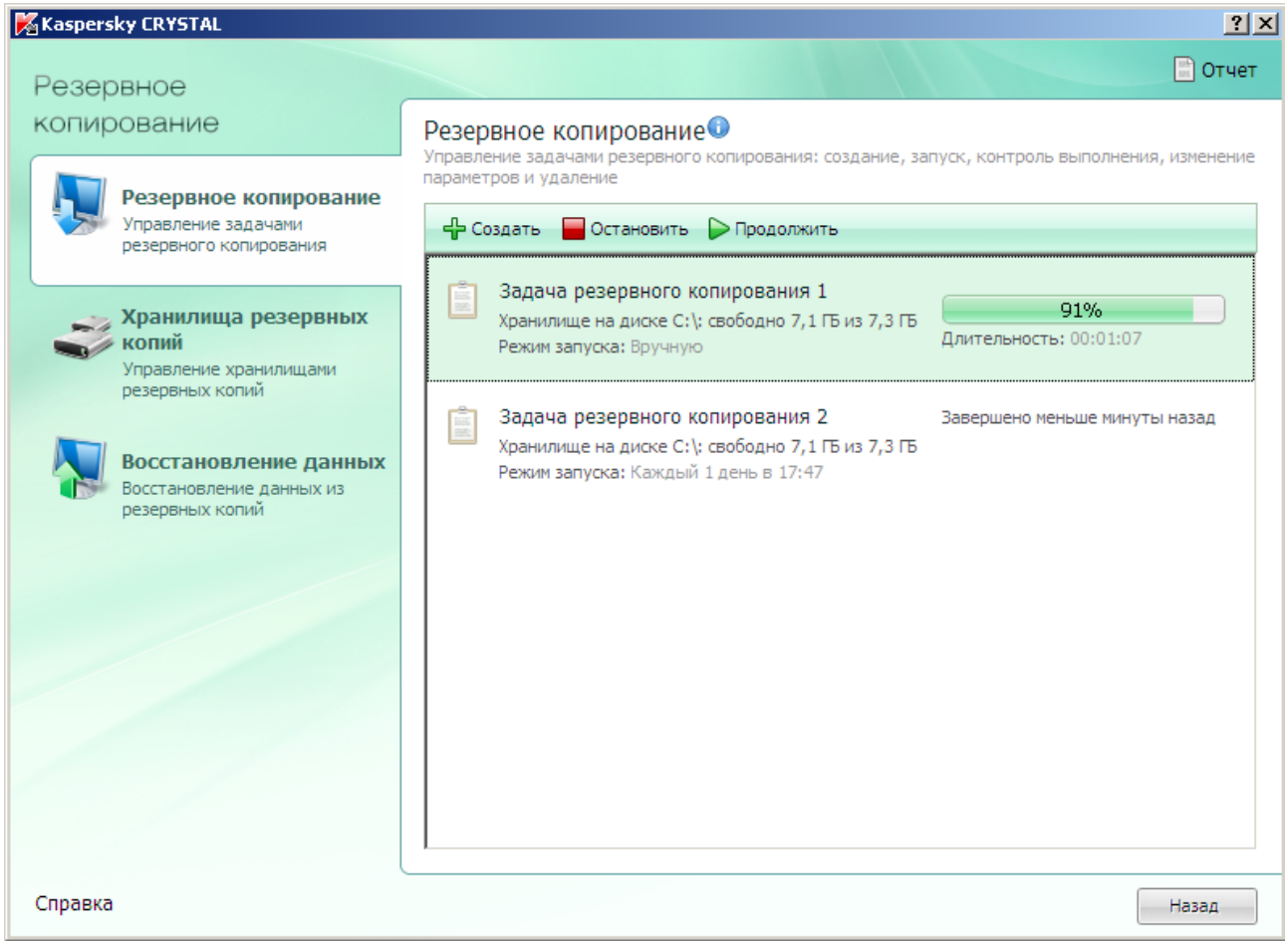


Рисунок 6. Главное окно модуля Резервное копирование

Родительский контроль

Окно **Родительский контроль** состоит из двух частей:

- левая часть окна позволяет перейти к работе с основными функциями Родительского контроля: настройке контроля для пользователей компьютера и просмотру отчетов;

- правая часть окна содержит перечень параметров выбранной в левой части функции.

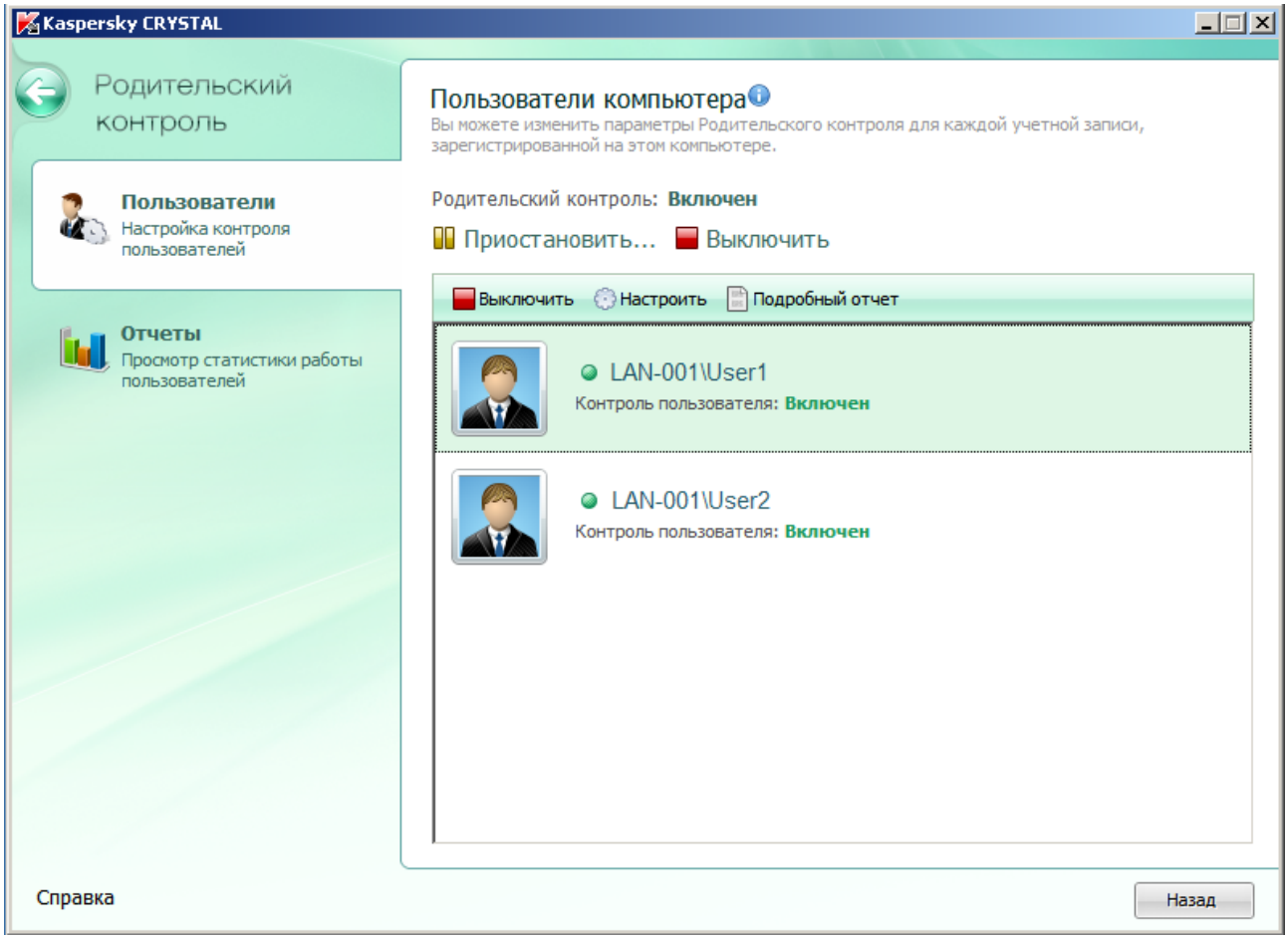


Рисунок 7. Главное окно модуля Родительский контроль

Окно Менеджера паролей

Окно **Менеджер паролей** состоит из трех частей:

- кнопка блокирования / разблокирования базы паролей (см. стр. 190);
- кнопки быстрого доступа к основным функциям Менеджера паролей: созданию пароля, созданию визитки, управлению базой паролей, настройке параметров работы и созданию и синхронизации переносной версии Менеджера паролей (недоступны, если база паролей заблокирована);
- кнопка генератора паролей (см. стр. 216).

Вы также можете воспользоваться следующими кнопками и ссылками:

- **Справка** - переход к справочной системе Менеджера паролей;
- **Назад** - переход к главному окну Kaspersky CRYSTAL (см. стр. 39).

Значок в области уведомления

Сразу после запуска Менеджера паролей его значок появляется в области уведомлений панели задач Microsoft Windows.

В зависимости от ситуации, значок Менеджера паролей принимает следующий вид:

-  активный (зеленый) – Менеджер паролей разблокирован, доступ к персональным данным разрешен;
-  неактивный (красный) – Менеджер паролей заблокирован, персональные данные недоступны.

По нажатию на значок доступны следующие элементы интерфейса:

- контекстное меню (см. стр. 45);
- указатель Менеджера паролей.

Контекстное меню Менеджера паролей

Контекстное меню Менеджера паролей позволяет перейти к выполнению основных задач и содержит следующие пункты:

- **Заблокировать / Разблокировать** – запрет / разрешение доступа к вашим персональным данным.
- **Учетные записи** – быстрый доступ к наиболее часто используемым учетным записям. В скобках указано количество учетных записей в базе паролей. Список часто используемых учетных записей формируется автоматически. Список присутствует, если настроено его отображение в контекстном меню (см. стр. 205). При первом запуске программы список будет отсутствовать, поскольку ни одна запись еще не будет использована.
- **Личные заметки** – быстрый доступ к личным заметкам. В скобках указано количество личных заметок в базе паролей.
- **Добавить учетную запись** – переход к добавлению новой учетной записи в Менеджер паролей.
- **Менеджер паролей** – переход к главному окну программы (см. стр. 44).
- **Настройка** – переход к настройке параметров программы.
- **Переносная версия** - запуск мастера создания переносной версии программы (см. стр. 217).
- **Генератор паролей** – создание надежных паролей (см. стр. 216).
- **Справка** – переход к справочной системе программы.
- **Выход** – завершение работы с программой (при выборе данного пункта меню программа будет выгружена из оперативной памяти компьютера).

Если программа не разблокирована, доступ к вашим персональным данным будет запрещен. В этом случае в контекстном меню будут присутствовать только следующие пункты: **Разблокировать**, **Генератор паролей**, **Справка** и **Выход**.

Чтобы открыть контекстное меню,

наведите курсор мыши на значок Менеджер паролей в области уведомлений панели задач и нажмите на правую клавишу мыши.

Окно базы паролей

Окно базы паролей состоит из трех частей:

- верхняя часть окна позволяет быстро выбирать функции Менеджера паролей, выполнять основные задачи;
- средняя часть окна содержит список всех учетных записей и других персональных данных, а кроме того, позволяет управлять персональной информацией;
- нижняя часть окна содержит ссылки для управления базой паролей в целом.

Вы также можете воспользоваться строкой поиска в верхней части окна. Строка поиска позволяет найти нужную информацию в базе паролей по ключевому слову.

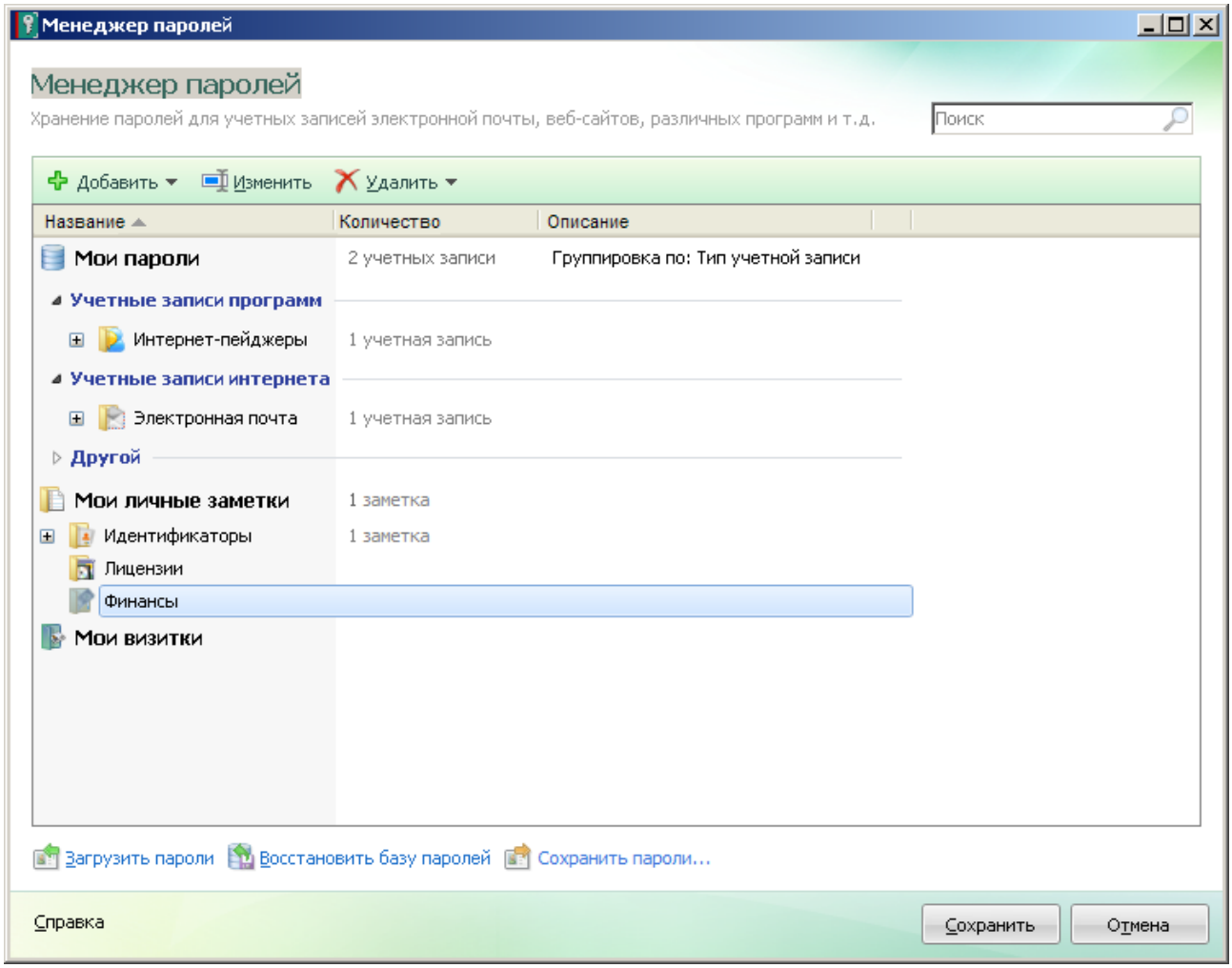


Рисунок 8. Окно базы паролей

Окно настройки параметров

Окно настройки параметров Менеджера паролей можно открыть одним из следующих способов:

- из контекстного меню Менеджера паролей (см. стр. 45) – для этого выберите пункт **Настройка** в контекстном меню Менеджера паролей;
- из окна Kaspersky CRYSTAL **–** для этого нажмите на кнопку **Настройка**.

Окно настройки состоит из двух частей:

- в левой части окна содержится список функций программы;

- в правой части окна доступен перечень параметров для выбранной функции, задачи и т. п.

Кнопка быстрого запуска

Кнопка быстрого запуска позволяет работать с вашими персональными данными из окна программы / веб-страницы. Кнопка расположена в правом верхнем углу программы.

По кнопке быстрого запуска открывается меню со списком имен пользователей, которые привязаны к программе / веб-странице. При выборе имени пользователя Менеджер паролей автоматически заполнит поля авторизации на основе данных из базы паролей.

Кнопка быстрого запуска активна  , если Менеджер паролей не заблокирован (см. стр. 190). Нажав на нее, можно перейти к следующим действиям:

- **Добавить учетную запись** – переход к добавлению новой учетной записи.
- **Изменить учетную запись** – переход к добавлению имени пользователя / редактированию активированной учетной записи. Пункт меню присутствует, если учетная запись активирована.
- **Учетные записи интернета** – просмотр списка всех учетных записей для интернета и запуск одной из них. В скобках указано количество учетных записей в базе паролей.
- Список часто используемых учетных записей – запуск учетной записи из списка. Список формируется автоматически на основе частоты использования учетных записей. Список присутствует в меню, если дополнительно настроено его отображение (см. стр. 205).
- **Визитки** – просмотр списка созданных визиток и выбор визитки для регистрационной формы.
- **Справка** – переход к справке программы.

Кнопка быстрого запуска неактивна  , если Менеджер паролей заблокирован. В этом случае перейти к действиям по нажатию этой кнопки будет невозможно. Неактивная кнопка отображается в окне программы, если дополнительно настроены параметры кнопки быстрого запуска (см. стр. 214).

Расширения и плагины

Менеджер паролей имеет компоненты расширения (плагины), которые встраиваются в программы, требующие авторизации. Вы можете самостоятельно устанавливать плагины для нужных вам веб-браузеров. Установленные плагины обеспечивают доступ к функциям Менеджера паролей из интерфейса программ / веб-браузеров.

Указатель

Указатель Менеджера паролей позволяет быстро выбирать программу / веб-страницу для автоматического ввода персональных данных.

Чтобы использовать указатель Менеджера паролей, выполните следующие действия:

1. Наведите курсор мыши на значок Менеджера паролей в области уведомления панели задач и подождите несколько секунд.
2. Появившийся указатель Менеджера паролей перетащите на нужное окно программы / веб-страницы. Менеджер паролей автоматически определит действие для выбранной программы / веб-страницы.

Окно настройки параметров программы

Окно настройки параметров Kaspersky CRYSTAL предназначено для настройки параметров работы программы в целом, отдельных компонентов защиты, задач проверки и обновления, а также для выполнения других задач расширенной настройки (см. стр. 78).

Окно настройки состоит из трех частей:

- верхняя часть содержит категории задач и функций Kaspersky CRYSTAL;
- левая часть окна обеспечивает доступ к задачам и функциям Kaspersky CRYSTAL в выбранной категории;
- правая часть окна содержит перечень параметров выбранной в левой части функции программы или задачи.

Окно настройки можно открыть из главного окна (см. стр. 39) или контекстного меню (см. стр. 38). Чтобы открыть окно настройки, перейдите по ссылке **Настройка** в верхней части главного окна либо выберите одноименный пункт в контекстном меню программы.

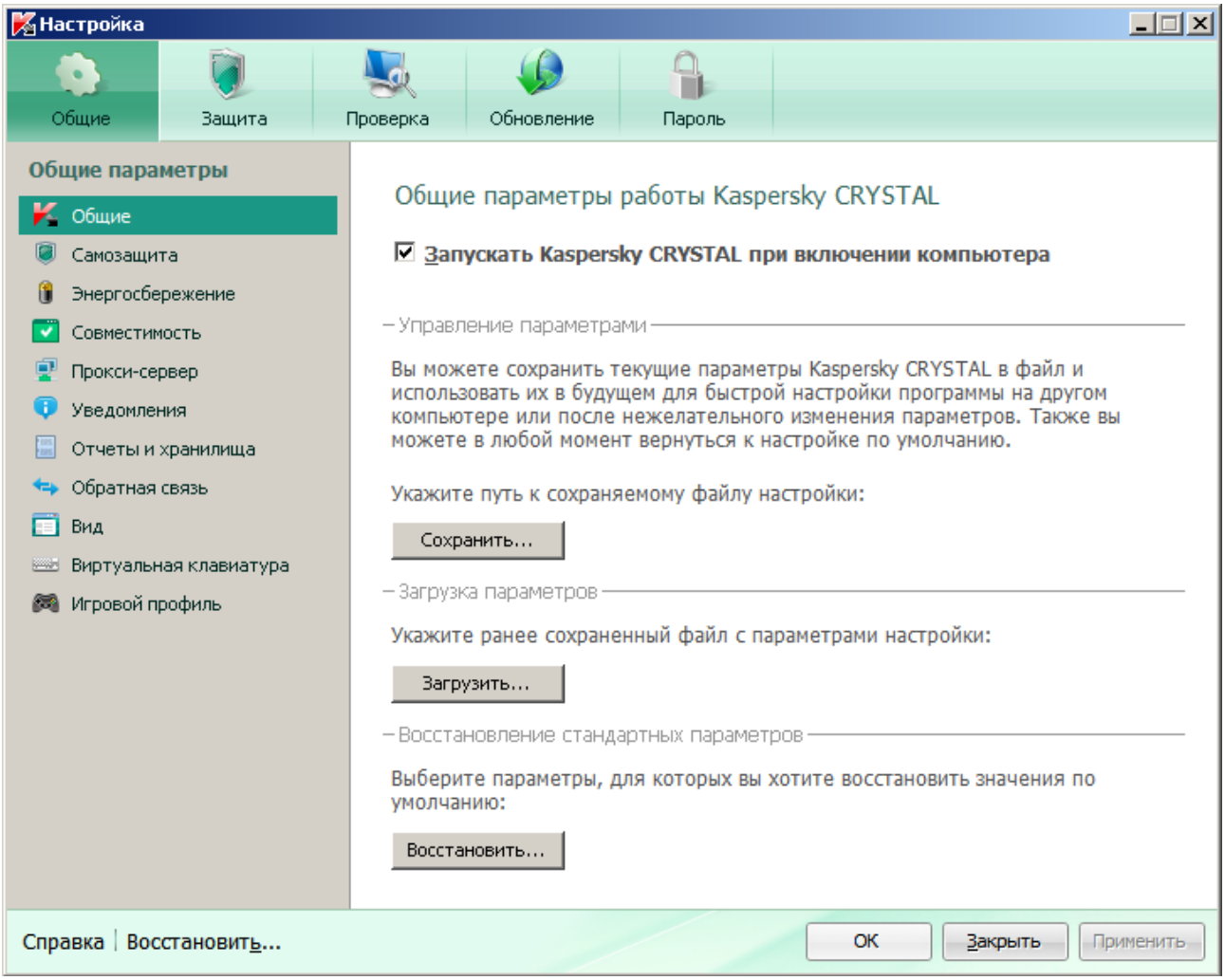


Рисунок 9. Настройка параметров Kaspersky CRYSTAL

Окна уведомлений и всплывающие сообщения

Kaspersky CRYSTAL уведомляет вас о значимых событиях, происходящих в процессе его работы, с помощью *окон уведомлений* и *всплывающих сообщений*, которые появляются над значком программы в области уведомлений панели задач.

Окна уведомлений Kaspersky CRYSTAL выводит на экран в тех случаях, когда возможны различные варианты действий в связи с событием: например, при обнаружении вредоносного объекта вы можете заблокировать доступ к нему, удалить его или попытаться вылечить. Программа предложит вам выбрать действие из числа возможных. Окно уведомления исчезает с экрана только после того, как вы выберете одно из предложенных действий.

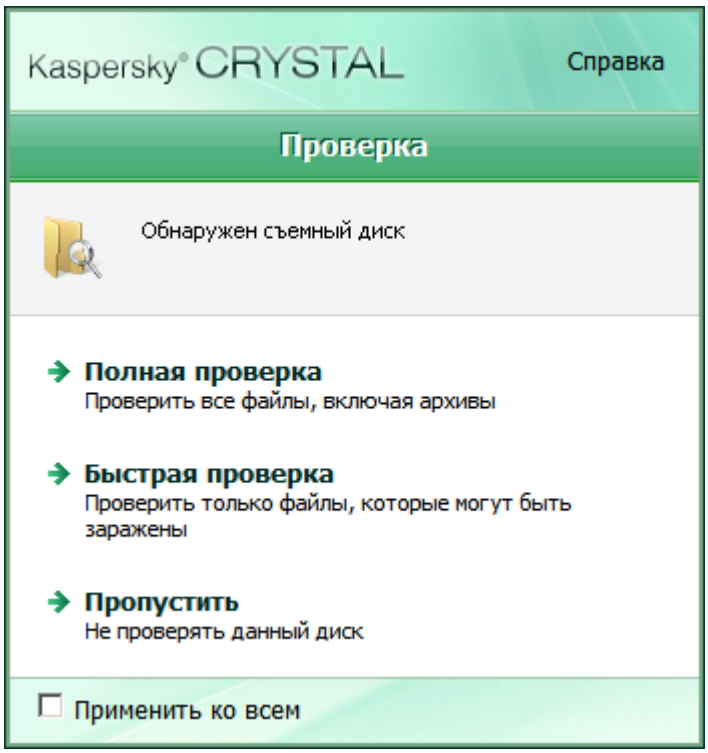


Рисунок 10. Окно уведомления

Всплывающие сообщения Kaspersky CRYSTAL выводит на экран, чтобы проинформировать о событиях, не требующих от вас обязательного выбора действия. В некоторых всплывающих сообщениях доступны ссылки, с помощью которых вы можете выполнить предлагаемое действие (например, запустить обновление баз или перейти к активации программы). Всплывающие сообщения автоматически исчезают с экрана вскоре после появления.

Рисунок 11. Всплывающее сообщение

В зависимости от степени важности события с точки зрения безопасности компьютера, уведомления могут быть отнесены к следующим типам:

- Критические – информируют о событиях, имеющих первостепенную важность с точки зрения безопасности компьютера: например, об обнаружении вредоносного объекта или опасной активности в системе. Окна уведомлений и всплывающие сообщения такого типа имеют красный цвет.

- Важные – информируют о событиях, потенциально важных с точки зрения безопасности компьютера: например, об обнаружении возможно зараженного объекта или подозрительной активности в системе. Окна уведомлений и всплывающие сообщения такого типа имеют желтый цвет.

- Информационные – информируют о событиях, не имеющих первостепенной важности с точки зрения безопасности. Окна уведомлений и всплывающие сообщения такого типа имеют зеленый цвет.

ЗАПУСК И ОСТАНОВКА ПРОГРАММЫ

После установки Kaspersky CRYSTAL запускается автоматически. В дальнейшем по умолчанию предусмотрен автоматический запуск программы после старта операционной системы.

В ЭТОМ РАЗДЕЛЕ

Включение и отключение автоматического запуска 51

Запуск и остановка программы вручную 51

ВКЛЮЧЕНИЕ И ОТКЛЮЧЕНИЕ АВТОМАТИЧЕСКОГО ЗАПУСКА

Под автоматическим запуском программы подразумевается запуск Kaspersky CRYSTAL, который выполняется без вашего участия сразу после старта операционной системы. Такой вариант запуска предусмотрен по умолчанию.

- *Чтобы отключить автоматический запуск программы, выполните следующие действия:*

  1. Откройте главное окно программы.
  2. В верхней части окна перейдите по ссылке **Настройка**.
  3. В левой части окна выберите в разделе **Общие параметры** подраздел **Общие**.
  4. В правой части окна снимите флажок **Запускать Kaspersky CRYSTAL при включении компьютера**.

ЗАПУСК И ОСТАНОВКА ПРОГРАММЫ ВРУЧНУЮ

«Лаборатория Касперского» не рекомендует останавливать Kaspersky CRYSTAL, поскольку в этом случае защита компьютера и ваших личных данных окажется под угрозой. Если это действительно очень нужно, рекомендуется приостановить защиту компьютера (см. стр. 54) на необходимый срок, не завершая работу программы.

Запускать Kaspersky CRYSTAL вручную нужно в том случае, если вы отключили автоматический запуск программы (см. стр. 51).

- *Чтобы запустить программу вручную,*

  в меню **Пуск** выберите пункт **Программы** → **Kaspersky CRYSTAL** → **Kaspersky CRYSTAL**.

- *Чтобы завершить работу программы,*

  по правой клавише мыши вызовите контекстное меню значка программы, расположенного в области уведомлений панели задач, и выберите в меню пункт **Выход**.

СОСТОЯНИЕ ЗАЩИТЫ ДОМАШНЕЙ СЕТИ

Этот раздел содержит информацию о том, как определить, защищена ли в данный момент домашняя сеть или существуют угрозы ее безопасности, а также о том, как устранить возникшие угрозы.

В этом же разделе вы найдете информацию о включении, отключении и временной приостановке защиты во время работы Kaspersky CRYSTAL.

Диагностика и устранение проблем в защите

О появлении проблем в защите компьютера сигнализирует индикатор, расположенный в верхней части главного окна Kaspersky CRYSTAL. Индикатор меняет цвет в зависимости от состояния защиты компьютера: зеленый цвет означает, что компьютер защищен, желтый цвет свидетельствует о наличии проблем в защите, красный – о серьезной угрозе безопасности компьютера. Проблемы и угрозы безопасности рекомендуется немедленно устранять.

Нажав на кнопку **Исправить**, можно открыть окно **Общее состояние защиты** (см. рис. ниже), в котором приведена подробная информация о состоянии защиты компьютера и предложены варианты действий для устранения проблем и угроз.

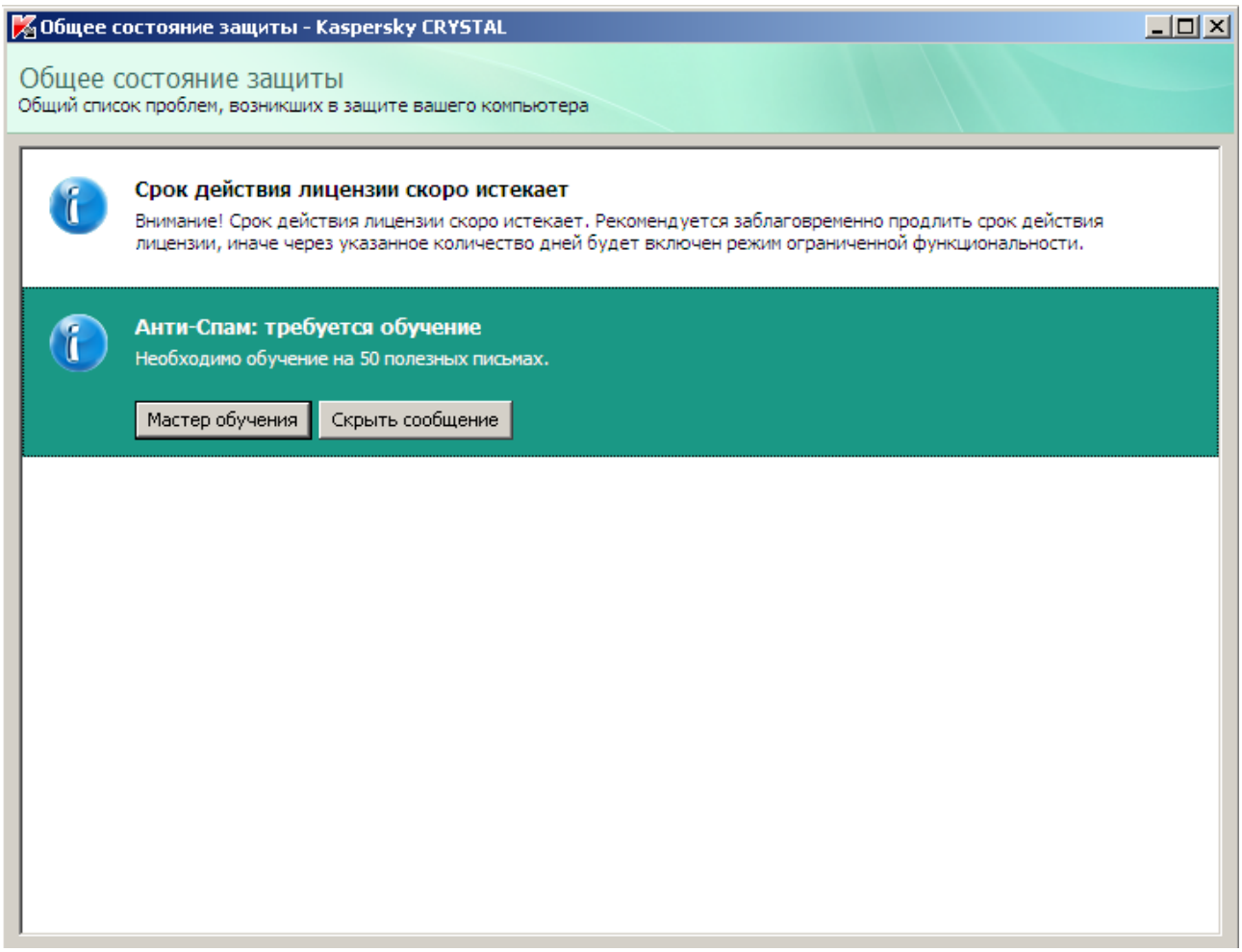


Рисунок 12. Окно Общее состояние защиты

В окне приведен список проблем в защите, в том числе обусловленных отклонениями от оптимальной работы

программы (например, устареванием баз). Для устранения проблем и угроз предлагаются следующие варианты действий:

- Немедленно устранить. Нажатие на кнопку с предложенным вариантом действия позволит перейти к непосредственному устранению проблемы. Это действие является рекомендуемым.

- Отложить устранение. Если по какой-либо причине немедленное устранение проблемы невозможно, вы можете отложить данное действие и вернуться к нему позже. Для этого нажмите на кнопку **Скрыть сообщение**.

  Обратите внимание, что для серьезных проблем возможность отложить устранение не предусмотрена. К числу таких проблем относятся, например, наличие невылеченных вредоносных объектов, сбой в работе одного или нескольких компонентов, повреждение файлов программы.

Чтобы ранее скрытые сообщения были вновь отображены в общем списке, нажмите на кнопку **Восстановить скрытые сообщения**, в элементе списка **Некоторые сообщения скрыты**.

Проанализировать уровень защиты домашней сети с рабочего места администратора вы можете с помощью Центра управления (см. раздел «Как удаленно проверить состояние защиты компьютеров домашней сети» на стр. 62).

Включение / отключение защиты компьютера

По умолчанию Kaspersky CRYSTAL запускается при старте операционной системы и защищает ваш компьютер в течение всего сеанса работы. Все компоненты защиты работают.

Вы можете полностью или частично отключить защиту, обеспечиваемую Kaspersky CRYSTAL.

Специалисты «Лаборатории Касперского» настоятельно рекомендуют **не отключать защиту**, поскольку это может привести к заражению вашего компьютера и потере данных.

При отключении защиты работа всех ее компонентов останавливается. Об этом свидетельствуют следующие признаки:

- неактивный (серый) значок Kaspersky CRYSTAL (см. раздел «Значок в области уведомлений панели задач» на стр. 37) в области уведомлений панели задач;

- красный цвет индикатора безопасности.

Обратите внимание, что в данном случае защита рассматривается именно в контексте компонентов защиты. Отключение или приостановка работы компонентов защиты не оказывает влияния на выполнение задач проверки на вирусы и обновления Kaspersky CRYSTAL.

Чтобы отключить защиту полностью, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Защита компьютера**.

2. В открывшемся окне перейдите по ссылке **Настройка** в верхней части окна.

3. В открывшемся окне выберите раздел **Центр защиты**.

4. Снимите флажок **Включить защиту**.

Чтобы включить / отключить отдельный компонент защиты, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Защита компьютера**.

   Откроется окно **Защита компьютера**.

2. В левой части окна выберите раздел **Центр защиты** и в правой части окна нажмите на кнопку с названием нужной защищаемой категории.

3. В открывшемся окне **Компоненты защиты** включите / отключите нужный компонент защиты щелчком мыши по значку статуса справа от названия компонента.

Приостановка защиты

Приостановка защиты означает отключение на некоторое время всех ее компонентов.

В результате временного отключения работа всех компонентов защиты приостанавливается. Об этом свидетельствуют:

- неактивный (серый) значок программы (см. раздел «Значок в области уведомлений панели задач» на стр. 37) в области уведомлений панели задач;

- красный цвет значка статуса и панели окна защиты компьютера.

Если в момент приостановки защиты были установлены сетевые соединения, на экран будет выведено уведомление о разрыве этих соединений.

Чтобы приостановить защиту компьютера, выполните следующие действия:

1. В контекстном меню (см. раздел «Контекстное меню» на стр. 38) программы выберите пункт **Приостановка защиты**.

2. В открывшемся окне **Приостановка защиты** выберите период, по истечении которого защита будет включена:

   - **Приостановить на <временной интервал> –** защита будет включена через указанное время. Для выбора значения временного интервала воспользуйтесь раскрывающимся списком.

   - **Приостановить до перезагрузки –** защита будет включена после перезапуска программы или перезагрузки системы (при условии, что включен режим запуска Kaspersky CRYSTAL при включении компьютера).

   - **Приостановить –** защита будет включена только тогда, когда вы сами ее запустите. Для включения защиты выберите пункт **Возобновление защиты** в контекстном меню программы.

Использование интерактивного режима защиты

Kaspersky CRYSTAL взаимодействует с пользователем в двух режимах:

- *Интерактивный режим защиты*. Kaspersky CRYSTAL уведомляет пользователя обо всех опасных и подозрительных событиях в системе. В этом режиме пользователю предстоит самостоятельно принимать решение о разрешении или запрещении каких-либо действий.

- *Автоматический режим защиты*. Kaspersky CRYSTAL будет автоматически применять рекомендуемое экспертами «Лаборатории Касперского» действие при возникновении опасных событий.

Чтобы выбрать режим защиты, выполните следующие действия:

1. Откройте главное окно программы.

2. В верхней части окна перейдите по ссылке **Настройка**.

3. В левой части окна выберите в разделе **Центр защиты** подраздел **Основные параметры**.

4. В правой части окна в блоке **Интерактивная защита** снимите или установите флажки в зависимости от выбранного вами режима защиты:

   - чтобы установить интерактивный режим защиты, снимите флажок **Выбирать действие автоматически**;

   - чтобы установить автоматический режим защиты, установите флажок **Выбирать действие автоматически**.

   Чтобы Kaspersky CRYSTAL не удалял подозрительные объекты при работе в автоматическом режиме, установите флажок **Не удалять подозрительные объекты**.

РЕШЕНИЕ ТИПОВЫХ ЗАДАЧ

Этот раздел содержит инструкции к основным задачам программы, с которыми пользователи сталкиваются наиболее часто.

В ЭТОМ РАЗДЕЛЕ

Как активировать программу 56

Как приобрести лицензию или продлить срок ее действия 57

Что делать при появлении уведомлений программы 58

Как обновить базы и модули программы 58

Как проверить важные области компьютера на вирусы 58

Как проверить на вирусы файл, папку, диск или другой объект 59

Как выполнить полную проверку компьютера на вирусы 61

Как проверить компьютер на уязвимости 61

Как удаленно проверить состояние защиты компьютеров домашней сети 62

Как защитить ваши личные данные от кражи 63

Что делать, если вы подозреваете, что объект заражен вирусом 66

Как восстановить удаленный или вылеченный программой объект 67

Что делать, если вы подозреваете, что ваш компьютер заражен 67

Как создать резервные копии ваших данных 69

Как ограничить доступ к параметрам Kaspersky CRYSTAL 70

Как ограничить использование компьютера и интернета для разных пользователей 71

Как создать и использовать диск аварийного восстановления 71

Что делать с большим количеством спам-сообщений 73

Как просмотреть отчет о защите компьютера 75

Как восстановить стандартные параметры работы программы 75

Как перенести параметры программы на другой компьютер 76

Как активировать программу

Активация – это процедура введения в действие лицензии, дающей право на использование полнофункциональной версии программы в течение срока действия лицензии.

Если вы не активировали программу в процессе установки (см. стр. 27), можно сделать это позже. О необходимости активировать программу вам будут напоминать уведомления Kaspersky CRYSTAL, появляющиеся в области уведомлений панели задач.

Чтобы запустить мастер активации Kaspersky CRYSTAL, выполните одно из следующих действий:

- Перейдите по ссылке **Пожалуйста, активируйте программу** в окне уведомления Kaspersky CRYSTAL, появляющегося в области уведомлений панели задач.

- Перейдите по ссылке **Лицензия**, расположенной в нижней части главного окна программы. В открывшемся окне **Управление лицензиями** нажмите на кнопку **Активировать программу с новой лицензией**.

Рассмотрим шаги мастера подробнее.

Шаг 1. Выбор типа лицензии и ввод кода активации

Убедитесь, что в окне Мастера активации выбран вариант **Активировать коммерческую версию**, введите код активации (см. раздел «О коде активации» на стр. 35) в соответствующее поле и нажмите на кнопку **Далее**.

Шаг 2. Запрос на активацию

На первом шаге мастер посылает на сервер активации запрос на активацию коммерческой версии программы. При успешном выполнении запроса мастер автоматически переходит к следующему шагу.

Шаг 3. Завершение работы мастера

В этом окне мастера отображается информация о результатах активации: тип используемой лицензии и дата окончания срока ее действия.

Нажмите на кнопку **Завершить**, чтобы завершить работу мастера.

КАК ПРИОБРЕСТИ ЛИЦЕНЗИЮ ИЛИ ПРОДЛИТЬ СРОК ЕЕ ДЕЙСТВИЯ

Если вы установили Kaspersky CRYSTAL, не имея лицензии, можно приобрести лицензию уже после установки программы. Когда срок действия лицензии подходит к концу, вы можете его продлить. Вы получите код активации, с помощью которого нужно активировать программу.

Чтобы приобрести лицензию, выполните следующие действия:

1. Откройте главное окно программы.

2. Нажмите на кнопку **Приобрести лицензию**, расположенную в нижней части окна.

   Откроется веб-страница интернет-магазина, где вы можете приобрести лицензию.

Чтобы продлить срок действия лицензии, выполните следующие действия:

1. Откройте главное окно программы и перейдите по ссылке **Лицензия**, расположенной в нижней части главного окна.

   Откроется окно **Управление лицензиями**.

2. Нажмите на кнопку **Продлить срок действия лицензии**.

Откроется веб-страница центра обновления лицензий, где вы можете продлить срок действия вашей лицензии.

Что делать при появлении уведомлений программы

Уведомления программы, появляющиеся в области уведомлений панели задач, информируют о событиях, происходящих в процессе работы программы и требующих вашего внимания. В зависимости от степени важности события уведомления могут быть следующих типов:

- Критические – информируют о событиях, имеющих первостепенную важность с точки зрения безопасности компьютера: например, об обнаружении вредоносного объекта или опасной активности в системе. Окна уведомлений и всплывающие сообщения такого типа имеют красный цвет.

- Важные – информируют о событиях, потенциально важных с точки зрения безопасности компьютера: например, об обнаружении возможно зараженного объекта или подозрительной активности в системе. Окна уведомлений и всплывающие сообщения такого типа имеют желтый цвет.

- Информационные – информируют о событиях, не имеющих первостепенной важности с точки зрения безопасности. Окна уведомлений и всплывающие сообщения такого типа имеют зеленый цвет.

При появлении на экране уведомления следует выбрать один из предложенных вариантов действия. Оптимальный вариант – тот, который рекомендован экспертами «Лаборатории Касперского» по умолчанию.

Как обновить базы и модули программы

По умолчанию Kaspersky CRYSTAL автоматически проверяет наличие обновлений на серверах обновлений «Лаборатории Касперского». Если на сервере содержится набор последних обновлений, Kaspersky CRYSTAL в фоновом режиме скачивает и устанавливает их. Вы можете запустить обновление Kaspersky CRYSTAL в любой момент.

Для загрузки обновлений с серверов «Лаборатории Касперского» требуется наличие соединения с интернетом.

Для поддержания защиты вашего компьютера в актуальном состоянии рекомендуется обновить Kaspersky CRYSTAL сразу после установки.

- *Чтобы запустить обновление из контекстного меню,*

  выберите пункт **Обновление** в контекстном меню значка программы.

- *Чтобы запустить обновление из главного окна, выполните следующие действия:*

  Откройте главное окно программы, в блоке **Защита компьютера** нажмите на кнопку **Быстрый запуск задач** и выберите пункт **Выполнить обновление баз**.

Как проверить важные области компьютера на вирусы

Под быстрой проверкой подразумевается проверка объектов, которые загружаются при запуске операционной системы, проверка системной памяти, загрузочных секторов диска, а также объектов, добавленных пользователем. Быстрая проверка автоматически выполняется на момент установки Kaspersky CRYSTAL.

Вы можете запустить задачу быстрой проверки следующими способами:

- с помощью ранее созданного ярлыка (см. стр. 87);
- из главного окна программы (см. раздел «Главное окно Kaspersky CRYSTAL» на стр. 39)
- .

Чтобы запустить задачу быстрой проверки с помощью ярлыка, выполните следующие действия:

1. Откройте окно Проводника Microsoft Windows и перейдите в папку, в которой вы создали ярлык.
2. Двойным щелчком мыши на ярлыке запустите проверку.

Чтобы запустить задачу быстрой проверки из главного окна программы, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Защита компьютера**.
2. В левой части открывшегося окна выберите раздел **Проверка**.
3. В правой части окна нажмите на кнопку **Выполнить быструю проверку**.

   Информация о выполняемой проверке отображается:

   - в блоке **Защита компьютера** главного окна программы, в поле **Проверка**;
   - в разделе **Проверка** окна **Защита компьютера**, в блоке **Остановить быструю проверку**;
   - в окне **Быстрая проверка**, которое открывается при переходе по ссылке **Окончание** в блоке **Остановить быструю проверку**;
   - в контекстном меню значка программы (см. стр. 38).

Чтобы остановить быструю проверку, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Защита компьютера**.
2. В левой части открывшегося окна выберите раздел **Проверка**.
3. В правой части окна нажмите на кнопку **Остановить быструю проверку**.

КАК ПРОВЕРИТЬ НА ВИРУСЫ ФАЙЛ, ПАПКУ, ДИСК ИЛИ ДРУГОЙ ОБЪЕКТ

Проверить на вирусы отдельный объект вы можете следующими способами:

- с помощью контекстного меню объекта;
- из главного окна программы (см. раздел «Главное окно Kaspersky CRYSTAL» на стр. 39).

Чтобы запустить задачу проверки на вирусы из контекстного меню объекта, выполните следующие действия:

1. Откройте окно Проводника Microsoft Windows и перейдите в папку с объектом, который нужно проверить.
2. По правой клавише мыши откройте контекстное меню объекта (см. рисунок ниже) и выберите пункт **Проверить на вирусы**.

Процесс и результат выполнения задачи будут отображаться в открывшемся окне **Проверка на вирусы**.

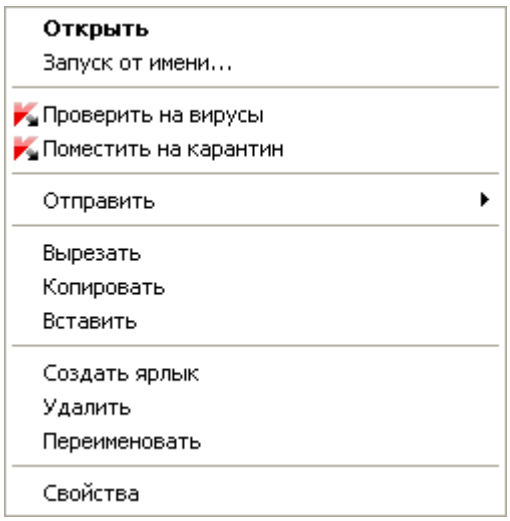


Рисунок 13. Контекстное меню объекта в Microsoft Windows

Чтобы запустить проверку объекта на вирусы из главного окна программы, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Защита компьютера**.
2. В левой части открывшегося окна выберите раздел **Проверка**.
3. В правой части окна в блоке **Выполнить проверку объектов** перейдите по ссылке **Добавить**.
4. В открывшемся окне **Выбор объекта для проверки** укажите расположение объекта, который вы хотите проверить на вирусы.
5. В блоке **Выполнить проверку объектов** установите флажки для тех объектов, которые вы хотите проверить.
6. Нажмите на кнопку **Выполнить проверку объектов**.

   Информация о выполняемой проверке отображается:

   - в блоке **Защита компьютера** главного окна программы, в поле **Проверка**;
   - в разделе **Проверка** окна **Защита компьютера**, в блоке **Остановить проверку объектов**;
   - в окне **Проверка объектов**, которое открывается при переходе по ссылке **Окончание** в блоке **Остановить проверку объектов**;
   - в контекстном меню значка программы (см. стр. 38).

Чтобы остановить проверку объектов, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Защита компьютера**.
2. В левой части открывшегося окна выберите раздел **Проверка**.
3. В правой части окна нажмите на кнопку **Остановить проверку объектов**.

Как выполнить полную проверку компьютера на вирусы

Вы можете запустить задачу полной проверки на вирусы следующими способами:

- с помощью ранее созданного ярлыка (см. стр. 87);
- из главного окна программы (см. раздел «Главное окно Kaspersky CRYSTAL» на стр. 39).

Чтобы запустить задачу полной проверки с помощью ярлыка, выполните следующие действия:

1. Откройте окно Проводника Microsoft Windows и перейдите в папку, в которой вы создали ярлык.
2. Двойным щелчком мыши на ярлыке запустите проверку.

Чтобы запустить задачу полной проверки из главного окна программы, выполните следующие действия:

Откройте главное окно программы, в блоке **Защита компьютера** нажмите на кнопку **Быстрый запуск задач** и выберите пункт **Выполнить полную проверку**.

Как проверить компьютер на уязвимости

Уязвимости – это незащищенные места программного кода, которые злоумышленники могут использовать в своих целях: например, копировать данные, используемые программами с незащищенным кодом. Проверка вашего компьютера на наличие потенциальных уязвимостей позволяет найти такие «слабые места» в защите компьютера. Найденные уязвимости рекомендуется устранить.

Запустить поиск уязвимостей вы можете следующими способами:

- из главного окна программы (см. раздел «Главное окно Kaspersky CRYSTAL» на стр. 39);
- с помощью ранее созданного ярлыка.

Чтобы запустить задачу с помощью ярлыка, выполните следующие действия:

1. Откройте окно Проводника Microsoft Windows и перейдите в папку, в которой вы создали ярлык.
2. Двойным щелчком мыши на ярлыке запустите задачу поиска уязвимостей.

   Процесс выполнения задачи будет отображен в открывшемся окне **Поиск уязвимостей**.

Чтобы запустить задачу из главного окна программы, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Защита компьютера**.
2. В левой части открывшегося окна выберите раздел **Проверка**.
3. Нажмите на кнопку **Открыть окно поиска уязвимостей**.
4. В открывшемся окне нажмите на кнопку **Выполнить поиск уязвимостей**.

   Процесс выполнения задачи будет отображен в открывшемся окне **Поиск уязвимостей**. Найденные уязвимости будут отображены на закладках **Уязвимости системы** и **Уязвимые программы**.

Как удаленно проверить состояние защиты компьютеров домашней сети

Для удаленного управления программой Kaspersky CRYSTAL, установленной на компьютерах домашней сети, с рабочего места администратора предназначены функции Центра управления (см. стр. 184).

Вы можете проанализировать уровень защиты домашней сети в целом или просмотреть перечень проблем на отдельном компьютере сети и удаленно устранить некоторые из них.

- *Чтобы получить подробную информацию о проблемах в защите сети и устранить их, выполните следующие действия:*

1. Откройте главное окно программы и в нижней части окна нажмите на кнопку **Центр управления**.
2. При первом запуске автоматически запускается мастер настройки удаленного управления. Рассмотрим подробнее шаги мастера:
   a. Введите или измените пароль администратора в окне **Защита паролем**.
   b. Выберите сеть для удаленного управления в окне **Опрос сети**.
   c. Выберите способ обновления антивирусных баз в окне **Источник обновлений**.
   d. Подтвердите выбранные параметры в окне **Сводка**.

   При последующих запусках потребуется ввести пароль администратора.
3. В открывшемся окне **Центр управления** нажмите на значок статуса или панель, на которой он расположен.

   В открывшемся окне **Состояние защиты сети** отображаются текущие проблемы.

- *Чтобы получить список проблем на компьютере в локальной сети, выполните следующие действия:*

1. Откройте главное окно программы и в нижней части окна нажмите на кнопку **Центр управления**.
2. При первом запуске автоматически запускается мастер настройки удаленного управления. Рассмотрим подробнее шаги мастера:
   a. Введите или измените пароль администратора в окне **Защита паролем**.
   b. Выберите сеть для удаленного управления в окне **Опрос сети**.
   c. Выберите способ обновления антивирусных баз в окне **Источник обновлений**.
   d. Подтвердите выбранные параметры в окне **Сводка**.

   При последующих запусках потребуется ввести пароль администратора.
3. В верхней части открывшегося окна **Центр управления** выберите компьютер, для которого требуется отобразить список проблем, и перейдите в раздел **Информация**.
4. В правой части окна выберите пункт **Перечень проблем**.
5. В открывшемся окне **Состояние защиты** отображаются текущие проблемы на выбранном компьютере.

Как защитить ваши личные данные от кражи

С помощью Kaspersky CRYSTAL вы можете защитить от кражи свои личные данные, например следующие:

- пароли, имена пользователя и другие регистрационные данные;
- номера счетов и кредитных карт;
- конфиденциальные файлы.

В состав Kaspersky CRYSTAL входят компоненты и инструменты, позволяющие защитить ваши личные данные от кражи злоумышленниками, использующими такие методы, как фишинг и перехват данных, вводимых с клавиатуры.

Для защиты от фишинга предназначен Анти-Фишинг, включенный в состав компонентов Веб-Антивирус, Анти-Спам и IM-Антивирус.

Для защиты от перехвата данных с клавиатуры предназначены виртуальная клавиатура и Менеджер паролей.

Для защиты файлов от несанкционированного доступа предназначено Шифрование данных.

В этом разделе

Защита от фишинга 63

Виртуальная клавиатура 64

Менеджер паролей 64

Шифрование данных 65

Защита от фишинга

Фишинг (phishing) – вид интернет-мошенничества, который заключается в «выуживании» у пользователей номеров их кредитных карт, ПИН-кодов и других личных данных с целью кражи денежных средств.

Фишинг часто связан с интернет-банкингом. Злоумышленники создают точную копию веб-сайта выбранного банка, затем рассылают от имени этого банка письма его клиентам. Они сообщают о том, что из-за выхода из строя или смены программного обеспечения в системе интернет-банкинга утеряны учетные данные пользователя, и он должен подтвердить или изменить их на веб-сайте банка. Пользователь переходит по ссылке, ведущей на созданный злоумышленниками веб-сайт, и вводит там свои данные, которые таким образом попадают к злоумышленникам.

Для защиты от фишинга предназначен Анти-Фишинг, включенный в состав компонентов Веб-Антивирус, Анти-Спам и IM-Антивирус. Включите работу этих компонентов, чтобы обеспечить максимально эффективную защиту от фишинга.

Чтобы включить работу компонентов, обеспечивающих защиту от фишинга, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Веб-Антивирус**.
4. В правой части окна установите флажок **Включить Веб-Антивирус**.

5. Повторите шаги 3 и 4 для компонентов **Анти-Спам** и **IM-Антивирус**.

   Будут включены компоненты, в состав которых входит Анти-Фишинг.

Виртуальная клавиатура

При работе за компьютером часто возникают ситуации, когда необходимо указать персональные данные, а также имя пользователя и пароль. Это происходит при регистрации на интернет-сайтах, при совершении покупок в интернет-магазинах и т. д.

В таких случаях существует опасность перехвата персональной информации с помощью аппаратных перехватчиков, либо клавиатурных шпионов – программ, регистрирующих нажатие клавиш.

Виртуальная клавиатура позволяет избежать перехвата данных, вводимых с клавиатуры.

Виртуальная клавиатура не может защитить ваши персональные данные в случае взлома сайта, требующего ввод таких данных, так как в данном случае информация попадет непосредственно в руки злоумышленников.

Многие программы-шпионы обладают функциями снятия снимков экрана, которые автоматически передаются злоумышленнику для последующего анализа и извлечения персональных данных пользователя. Виртуальная клавиатура защищает вводимые персональные данные от перехвата посредством снятия снимков (screenshot).

Виртуальная клавиатура защищает от перехвата персональной информации только при работе с интернет-браузерами Microsoft Internet Explorer и Mozilla Firefox.

- *Чтобы использовать виртуальную клавиатуру, выполните следующие действия:*

  1. Откройте главное окно программы и в нижней части окна нажмите на кнопку **Виртуальная клавиатура**.

  2. Введите нужные данные, нажимая на кнопки виртуальной клавиатуры. Убедитесь, что данные введены в нужное поле. При нажатии функциональных клавиш (**Shift**, **Alt**, **Ctrl**) виртуальной клавиатуры специальный режим ввода фиксируется (например, при нажатии **Shift** все символы будут вводиться в верхнем регистре). Для отмены специального режима нажмите функциональную клавишу повторно.

Переключение языка для виртуальной клавиатуры осуществляется с помощью сочетания клавиш **Ctrl** + нажатие правой клавишей мыши на клавишу **Shift**, или **Ctrl** + нажатие правой клавишей мыши на клавишу **Left Alt** в зависимости от установленных параметров.

Менеджер паролей

Менеджер паролей обеспечивает защиту ваших персональных данных (например, имен пользователей, паролей, адресов, номеров телефонов и кредитных карт).

Вся информация в зашифрованном виде хранится в базе паролей, доступ к которой защищен мастер-паролем. Менеджер паролей связывает пароли и учетные записи с программами Microsoft Windows или веб-страницами, для которых они используются. После запуска веб-страницы или программы Менеджер паролей автоматически вводит пароль, имя пользователя и другие персональные данные. Таким образом, вам достаточно запомнить один пароль и необязательно запоминать остальные.

- *Чтобы использовать Менеджер паролей для автоматического заполнения формы авторизации, выполните следующие действия:*

  1. Откройте главное окно программы и в нижней части окна нажмите на кнопку **Менеджер паролей**.

  2. При первом запуске автоматически запускается мастер настройки Менеджера паролей. Рассмотрим подробнее шаги мастера:

a. Создайте мастер-пароль для защиты вашей базы паролей в окне **Мастер-пароль**.

b. Выберите способ авторизации для доступа к вашей базе паролей в окне **Управление доступом**.

c. Задайте время, по истечении которого Менеджер паролей будет автоматически заблокирован, в окне **Таймаут перед блокированием**.

При последующих запусках потребуется ввести мастер-пароль.

3. В открывшемся окне нажмите на кнопку **Добавить пароль**.

4. В открывшемся мастере создания учетной записи выберите тип учетной записи (учетная запись интернета, учетная запись программы или пользовательский режим) и нажмите на кнопку **Далее**.

   - Если вы выбрали учетную запись интернета или программы, укажите веб-сайт или программу, для которой будет использоваться учетная запись, и нажмите на кнопку **Далее**.

   - Если вы выбрали расширенный режим, в открывшемся окне на закладке **Связь** укажите путь к программе / веб-странице и задайте параметры использования учетной записи.

5. В верхней части окна в поле **Имя** введите или отредактируйте название новой учетной записи.

6. На закладке **Регистрационные данные** введите имя пользователя и пароль.

7. На закладке **Редактирование формы вручную** при необходимости настройте параметры заполнения других полей для веб-страницы.

8. На закладке **Комментарий** при необходимости дополнительно введите поясняющий текст для учетной записи. Чтобы комментарий отображался в уведомлении после активизации учетной записи, установите флажок **Показывать комментарии в уведомлении**.

9. Закройте окно, нажав на кнопку **ОК**.

10. Запустите программу / веб-страницу, для которой была создана учетная запись.

    Форма авторизации будет заполнена автоматически на основе данных учетной записи.

ШИФРОВАНИЕ ДАННЫХ

Чтобы защитить от несанкционированного доступа конфиденциальную информацию, рекомендуется хранить ее в зашифрованном виде в специальном контейнере.

Создайте контейнер, сохраните в нем данные, а затем зашифруйте данные. После этого для доступа к данным в контейнере потребуется ввести пароль.

Чтобы создать зашифрованный контейнер, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Шифрование данных**.

2. В открывшемся окне нажмите на кнопку **Создать контейнер**.

3. Будет запущен мастер создания зашифрованного контейнера. Рассмотрим подробнее шаги мастера:

   a. Введите название контейнера, размер и пароль доступа в окне **Основные параметры**.

   b. Укажите расположение файла контейнера в окне **Расположение**.

   c. Выберите букву виртуального диска для подключения контейнера, задайте дополнительные параметры, если это необходимо, и подтвердите создание контейнера с указанными параметрами в окне **Сводка**.

Чтобы сохранить данные в контейнере, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Шифрование данных**.
2. В открывшемся окне выберите контейнер в списке и нажмите на кнопку **Открыть**.

   Контейнер открывается в окне Проводника Microsoft Windows.
3. Сохраните в контейнере данные, которые требуется зашифровать.
4. В окне **Шифрование данных** нажмите на кнопку **Зашифровать данные**.

Чтобы получить доступ к данным в контейнере, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Шифрование данных**.
2. В открывшемся окне выберите контейнер в списке и нажмите на кнопку **Расшифровать данные**.
3. В открывшемся окне введите пароль доступа к контейнеру.
4. В окне **Шифрование данных** нажмите на кнопку **Открыть**.

Что делать, если вы подозреваете, что объект заражен вирусом

Если вы подозреваете, что объект может быть заражен, прежде всего проверьте его с помощью Kaspersky CRYSTAL (см. раздел «Как проверить на вирусы файл, папку, диск или другой объект» на стр. 59).

Если в результате проверки программа сообщит, что объект не заражен, но вы подозреваете обратное, можно поступить следующим образом:

- Поместить объект на *карантин*. Объекты, помещенные на карантин, не представляют угрозы для вашего компьютера. Возможно, после обновления баз Kaspersky CRYSTAL сможет однозначно определить угрозу и обезвредить ее.
- Отправить объект в *Вирусную лабораторию*. Специалисты Вирусной лаборатории проверят объект и, если он действительно заражен вирусом, незамедлительно внесут описание нового вируса в базы, которые будут загружены программой в процессе обновления (см. раздел «Как обновить базы и модули программы» на стр. 58).

Поместить объект на карантин можно двумя способами:

- с помощью ссылки **Поместить на карантин** в окне **Состояние защиты**;
- с помощью контекстного меню объекта.

Чтобы поместить объект на карантин из окна Состояние защиты, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Защита компьютера**.
2. По ссылке **Карантин**, расположенной в верхней части открывшегося окна, откройте окно **Состояние защиты**.
3. На закладке **Обнаруженные угрозы** перейдите по ссылке **Поместить на карантин**.
4. В открывшемся окне выберите объект, который нужно поместить на карантин.

- *Чтобы поместить объект на карантин с помощью контекстного меню, выполните следующие действия:*

1. Откройте окно Проводника Microsoft Windows и перейдите в папку с объектом, который нужно поместить на карантин.

По правой клавише мыши откройте контекстное меню объекта и выберите пункт **Поместить на карантин**.

- *Чтобы отправить объект в Вирусную лабораторию, выполните следующие действия:*

1. Перейдите на страницу отправки запроса в Вирусную лабораторию (http://support.kaspersky.ru/virlab/helpdesk.html).

2. Следуйте инструкциям, приведенным на странице, чтобы отправить запрос.

КАК ВОССТАНОВИТЬ УДАЛЕННЫЙ ИЛИ ВЫЛЕЧЕННЫЙ ПРОГРАММОЙ ОБЪЕКТ

«Лаборатория Касперского» не рекомендует восстанавливать удаленные и вылеченные объекты, поскольку они могут представлять угрозу для вашего компьютера.

Если необходимо восстановить удаленный или вылеченный объект, используется его резервная копия, созданная программой в ходе проверки объекта.

- *Чтобы восстановить удаленный или вылеченный программой объект, выполните следующие действия:*

1. Откройте главное окно программы и нажмите на кнопку **Защита компьютера**.

2. По ссылке **Карантин**, расположенной в верхней части открывшегося окна, откройте окно **Состояние защиты**.

3. На закладке **Обнаруженные угрозы** в раскрывающемся списке, расположенном над списком угроз, выберите элемент **Нейтрализованные**.

   На закладке **Обнаруженные угрозы** отобразится список вылеченных и удаленных объектов. Объекты сгруппированы в соответствии с их статусом. Чтобы отобразить список объектов, входящих в группу, нажмите на значок **+** слева от заголовка группы.

4. По правой клавише мыши откройте контекстное меню объекта, который нужно восстановить, и выберите в меню пункт **Восстановить**.

ЧТО ДЕЛАТЬ, ЕСЛИ ВЫ ПОДОЗРЕВАЕТЕ, ЧТО ВАШ КОМПЬЮТЕР ЗАРАЖЕН

Если вы подозреваете, что ваш компьютер заражен, используйте *Мастер восстановления системы*, устраняющий следы пребывания в системе вредоносных объектов. Специалисты «Лаборатории Касперского» рекомендуют также запускать мастер после лечения компьютера, чтобы убедиться, что все возникшие угрозы и повреждения устранены.

В ходе работы мастер проверяет наличие в системе каких-либо изменений, к числу которых могут относиться следующие: блокировка доступа к сетевому окружению, изменение расширений файлов известных форматов, блокировка панели управления и т. п. Причины появления таких повреждений различны. Это могут быть активность вредоносных программ, некорректная настройка системы, системные сбои или применение некорректно работающих программ – оптимизаторов системы.

После проведенного исследования мастер анализирует собранную информацию с целью выявления в системе повреждений, которые требуют немедленного вмешательства. По результатам исследования составляется список действий, которые следует выполнить, чтобы устранить повреждения. Мастер группирует действия по категориям с учетом серьезности обнаруженных проблем.

Мастер состоит из последовательности окон (шагов), переключение между которыми осуществляется нажатием на кнопки **Назад** и **Далее**. Работа мастера завершается нажатием на кнопку **Завершить**. Для прекращения работы мастера на любом этапе следует нажать на кнопку **Отмена**.

Чтобы запустить Мастер восстановления системы, выполните следующие действия:

1. Откройте главное окно программы и в нижней части окна нажмите на кнопку **Дополнительные инструменты**.

2. В открывшемся окне **Дополнительные инструменты** нажмите на кнопку **Восстановление после заражения**.

Рассмотрим подробнее шаги мастера.

Шаг 1. Запуск восстановления системы

Убедитесь, что в окне мастера выбран вариант **Провести поиск проблем, связанных с активностью вредоносного ПО**, и нажмите на кнопку **Далее**.

Шаг 2. Поиск проблем

Мастер выполняет поиск проблем и возможных повреждений, которые следует исправить. По окончании поиска мастер автоматически переходит к следующему шагу.

Шаг 3. Выбор действий для устранения проблем

Все найденные на предыдущем шаге повреждения группируются с точки зрения опасности, которую они представляют. Для каждой группы повреждений специалистами «Лаборатории Касперского» предлагается набор действий, выполнение которых поможет устранить повреждения. Всего выделено три группы действий:

- *Настоятельно рекомендуемые действия* помогут избавиться от повреждений, представляющих серьезную проблему. Рекомендуем вам выполнить все действия данной группы.

- *Рекомендуемые действия* направлены на устранение повреждений, которые могут представлять потенциальную опасность. Действия данной группы также рекомендуется выполнять.

- *Дополнительные действия* предназначены для устранения неопасных в данный момент повреждений системы, которые в дальнейшем могут поставить безопасность компьютера под угрозу.

Для просмотра действий, включенных в группу, нажмите на значок **+**, расположенный слева от названия группы.

Чтобы мастер выполнил какое-либо действие, установите флажок слева от названия действия. По умолчанию выполняются все рекомендуемые и настоятельно рекомендуемые действия. Если вы не хотите выполнять какое-либо действие, снимите флажок рядом с ним.

Настоятельно не рекомендуется снимать флажки, установленные по умолчанию, поскольку в результате этого действия безопасность вашего компьютера останется под угрозой.

Сформировав набор действий для выполнения мастером, нажмите на кнопку **Далее**.

Шаг 4. Устранение проблем

Мастер выполняет выбранные на предыдущем шаге действия. Устранение проблем может занять некоторое время. По завершении устранения проблем мастер автоматически перейдет к следующему шагу.

Шаг 5. Завершение работы мастера

Нажмите на кнопку **Завершить**, чтобы завершить работу мастера.

КАК СОЗДАТЬ РЕЗЕРВНЫЕ КОПИИ ВАШИХ ДАННЫХ

Основной способ защиты важных данных от потери – своевременное резервное копирование. Kaspersky CRYSTAL позволяет автоматически выполнять регулярное резервное копирования выбранных данных в указанное хранилище по заданному расписанию. Вы также можете выполнить резервное копирование однократно.

Для начала работы нужно создать хранилище резервных копий на выбранном диске. В этом хранилище будут создаваться резервные копии нужных файлов. После этого можно настроить задачи резервного копирования (выбрать файлы, для которых необходимо создавать резервные копии, задать расписание регулярного автоматического запуска и другие условия резервного копирования).

- *Чтобы создать хранилище резервных копий, выполните следующие действия:*

1. Откройте главное окно программы и нажмите на кнопку **Резервное копирование**.
2. В открывшемся окне выберите раздел **Хранилища резервных копий** и нажмите на кнопку **Создать**.
3. Будет запущен мастер создания хранилища резервных копий. Рассмотрим подробнее шаги мастера:
   a. Выберите тип информационного носителя, который будет использоваться в качестве хранилища, в левой части окна **Диск**.

      Для безопасности данных рекомендуется создавать хранилища резервных копий на съемных дисках.

   b. Установите пароль для защиты данных в хранилище от несанкционированного доступа в окне **Защита** (если это необходимо).
   c. Задайте ограничение количества версий файлов, которые будут одновременно находиться в хранилище, а также время хранения резервных копий в окне **Версии файлов** (если это необходимо).
   d. Введите название нового хранилища и подтвердите создание хранилища с указанными параметрами в окне **Сводка**.

- *Чтобы выполнить резервное копирование, выполните следующие действия:*

1. Откройте главное окно программы и нажмите на кнопку **Резервное копирование**.
2. В открывшемся окне выберите раздел **Резервное копирование** и нажмите на кнопку **Создать**.
3. Будет запущен мастер создания задачи резервного копирования. Рассмотрим подробнее шаги мастера:
   a. Выберите объекты, для которых будут создаваться резервные копии, в окне **Содержимое**.
   b. Выберите хранилище, в котором будут создаваться резервные копии файлов, в окне **Хранилище**.
   c. Задайте условия запуска задачи в окне **Расписание**.

> Если вы хотите выполнить однократное резервное копирование, не устанавливайте флажок **Запускать по расписанию**.

d. Введите название новой задачи и нажмите на кнопку **Завершить** в окне **Сводка**.

Чтобы восстановить данные из резервной копии, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Резервное копирование**.
2. В открывшемся окне выберите раздел **Восстановление данных**.
3. Выберите хранилище, в котором находятся нужные резервные копии, и нажмите на кнопку **Восстановить данные**.
4. В верхней части окна **Восстановление данных из хранилища** выберите в раскрывающемся списке архив (набор данных, сохраненных в рамках выполнения одной задачи).
5. Выберите файлы, которые нужно восстановить. Для этого установите флажки рядом с нужными файлами в списке. Для выбора всех файлов нажмите на кнопку **Выбрать все** внизу списка. Нажмите на кнопку **Восстановить** в верхней части окна.
6. В открывшемся окне **Восстановление** выберите место сохранения восстановленных файлов и условие сохранения при совпадении имен. Нажмите на кнопку **Восстановить**.

   Будут восстановлены последние версии выбранных файлов.

Как ограничить доступ к параметрам Kaspersky CRYSTAL

Персональный компьютер могут использовать несколько пользователей, имеющих разные уровни компьютерной грамотности. Неограниченный доступ пользователей к Kaspersky CRYSTAL и его параметрам может привести к снижению уровня защищенности компьютера в целом.

Чтобы ограничить доступ к программе, вы можете задать пароль и указать, при выполнении каких действий он должен запрашиваться:

- изменение параметров работы программы;
- управление резервным копированием;
- управление родительским контролем;
- удаленное управление безопасностью сети;
- завершение работы программы.

Чтобы защитить доступ к Kaspersky CRYSTAL с помощью пароля, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Пароль администратора** подраздел **Основные параметры**.
4. В правой части окна в блоке **Защита паролем** установите флажок **Включить защиту паролем** и заполните поля **Новый пароль** и **Подтверждение пароля**.

5. В блоке **Область действия пароля** укажите область, на которую будет распространяться ограничение доступа. Теперь при попытке любого пользователя выполнить на вашем компьютере выбранные вами действия Kaspersky CRYSTAL всегда будет запрашивать пароль.

Чтобы изменить пароль для доступа к Kaspersky CRYSTAL, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Пароль администратора** подраздел **Основные параметры**.
4. В правой части окна в блоке **Защита паролем** заполните поля **Старый пароль**, **Новый пароль** и **Подтверждение пароля**.

КАК ОГРАНИЧИТЬ ИСПОЛЬЗОВАНИЕ КОМПЬЮТЕРА И ИНТЕРНЕТА ДЛЯ РАЗНЫХ ПОЛЬЗОВАТЕЛЕЙ

Непосредственно после установки Kaspersky CRYSTAL для пользователей компьютера не установлено никаких ограничений. Чтобы защитить детей и подростков от угроз, связанных с использованием компьютера и интернета, необходимо своевременно настроить параметры Родительского контроля для всех пользователей компьютера.

Если вы не включили защиту паролем при установке программы (см. раздел «Шаг 16. Ограничение доступа к программе» на стр. 28), то при первом запуске Родительского контроля рекомендуется установить пароль для защиты от несанкционированного изменения параметров контроля. После этого можно включить Родительский контроль и настроить ограничения использования компьютера и интернета для всех учетных записей на компьютере.

Чтобы настроить Родительский контроль для учетной записи, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Родительский контроль**.
2. В открывшемся окне выберите раздел **Пользователи**.
3. В правой части окна нажмите на кнопку **Включить**.
4. В списке учетных записей выберите учетную запись, для которой требуется настроить параметры контроля, и нажмите на кнопку **Настроить**.
5. В левой части открывшегося окна выберите тип ограничения и задайте параметры контроля в правой части окна.

КАК СОЗДАТЬ И ИСПОЛЬЗОВАТЬ ДИСК АВАРИЙНОГО ВОССТАНОВЛЕНИЯ

Диск аварийного восстановления рекомендуется создать после того, как вы установили и настроили Kaspersky CRYSTAL, с его помощью проверили компьютер и убедились, что он не заражен. В дальнейшем вы сможете использовать диск аварийного восстановления для проверки и лечения зараженного компьютера, который нельзя вылечить другим способом (например, с помощью антивирусных программ).

В этом разделе

Создание диска аварийного восстановления 72

Загрузка компьютера с помощью диска аварийного восстановления..... 73

Создание диска аварийного восстановления

Создание диска аварийного восстановления заключается в формировании образа диска (файла iso) с актуальными антивирусными базами и конфигурационными файлами.

Исходный образ диска, на основе которого формируется новый файл, может быть загружен с сервера «Лаборатории Касперского» или скопирован с локального источника.

Диск аварийного восстановления создается с помощью *Мастера создания диска аварийного восстановления*. Сформированный мастером файл образа rescuecd.iso сохраняется на жестком диске вашего компьютера:

- в операционной системе Microsoft Windows XP – в папке Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP9\Data\Rdisk\;
- в операционных системах Microsoft Windows Vista и Microsoft Windows 7 – в папке ProgramData\Kaspersky Lab\AVP9\Data\Rdisk\.

Мастер состоит из последовательности окон (шагов), переключение между которыми осуществляется нажатием на кнопки **Назад** и **Далее**. Работа мастера завершается нажатием на кнопку **Завершить**. Для прекращения работы мастера на любом этапе следует нажать на кнопку **Отмена**.

Чтобы запустить Мастер создания диска аварийного восстановления, выполните следующие действия:

1. Откройте главное окно программы и в нижней части окна нажмите на кнопку **Дополнительные инструменты**.
2. В открывшемся окне **Дополнительные инструменты** нажмите на кнопку **Диск аварийного восстановления**.

Рассмотрим подробнее шаги мастера.

Шаг 1. Выбор источника образа диска

На данном этапе вам следует выбрать источник файла образа из предложенных вариантов:

- Выберите вариант **Копировать образ с локального или сетевого диска**, если у вас уже есть записанный диск аварийного восстановления или подготовленный для него образ, сохраненный на вашем компьютере или на ресурсе локальной сети.
- Выберите вариант **Загрузить образ с сервера «Лаборатории Касперского»**, если у вас нет сформированного файла образа, и вы хотите загрузить его с сервера «Лаборатории Касперского» (размер файла составляет примерно 175 МБ).

Шаг 2. Копирование (загрузка) образа диска

Если на предыдущем шаге вы выбрали вариант копирования образа из локального источника (**Копировать образ с локального или сетевого диска**), то на данном шаге вам следует указать путь к файлу образа диска. Для этого нажмите на кнопку **Обзор**. Указав путь к файлу, нажмите на кнопку **Далее**. В окне мастера будет отображен процесс копирования образа диска.

Если же вы выбрали вариант **Загрузить образ с сервера «Лаборатории Касперского»**, то процесс загрузки образа диска отображается сразу.

По завершении копирования или загрузки образа диска мастер автоматически переходит к следующему шагу.

Шаг 3. Обновление файла образа

Процедура обновления файла образа включает:

- обновление антивирусных баз;
- обновление конфигурационных файлов.

Конфигурационные файлы определяют возможность загрузки компьютера с CD / DVD-диска, записанного с помощью образа диска аварийного восстановления, полученного в результате работы мастера.

При обновлении антивирусных баз используются базы, полученные при последнем обновлении Kaspersky CRYSTAL. Если базы устарели, рекомендуется выполнить задачу обновления и запустить мастер создания диска аварийного восстановления заново.

Для начала обновления файла образа нажмите на кнопку **Далее**. В окне мастера будет отображен ход выполнения обновления.

Шаг 4. Завершение работы мастера

Для завершения работы мастера нажмите на кнопку **Завершить**. Созданный файл .iso вы можете записать на CD / DVD-диск и использовать для последующей загрузки компьютера.

Загрузка компьютера с помощью диска аварийного восстановления

Если в результате вирусной атаки невозможно загрузить операционную систему, воспользуйтесь диском аварийного восстановления.

Для загрузки операционной системы необходим CD- / DVD-диск с записанным на него файлом образа (iso) загрузочного диска.

Чтобы произвести загрузку компьютера с диска аварийного восстановления, выполните следующие действия:

1. В параметрах BIOS включите загрузку с CD- / DVD-диска (подробную информацию можно получить из документации к материнской плате вашего компьютера).
2. Поместите в дисковод зараженного компьютера CD- / DVD-диск с предварительно записанным образом диска аварийного восстановления.
3. Перезагрузите компьютер.

Более подробную информацию об использовании диска аварийного восстановления можно найти в руководстве пользователя Kaspersky Rescue Disk.

Что делать с большим количеством спам-сообщений

Если вы получаете большое количество нежелательной почты (спама), включите компонент Анти-Спам и установите для него рекомендуемый уровень безопасности, а затем обучите компонент с помощью *Мастера*

обучения. Для корректного распознавания спама необходимо произвести обучение как минимум на 50 образцах полезной почты и 50 образцах нежелательной корреспонденции.

- *Чтобы включить Анти-Спам и установить рекомендуемый уровень безопасности, выполните следующие действия:*

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Анти-Спам**.
4. В правой части окна установите флажок **Включить Анти-Спам**.
5. В блоке **Уровень безопасности** по умолчанию должен быть установлен **Рекомендуемый** уровень безопасности.

   Если установлен уровень безопасности **Низкий** или **Другой**, нажмите на кнопку **По умолчанию**. Уровень безопасности будет автоматически установлен в значение **Рекомендуемый**.

- *Чтобы обучить Анти-Спам с помощью Мастера обучения, выполните следующие действия:*

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Анти-Спам**.
4. В правой части окна в блоке **Обучение Анти-Спама** нажмите на кнопку **Обучить**.

   Откроется окно мастера обучения.

Рассмотрим подробнее шаги мастера.

Шаг 1. Начало работы мастера

Нажмите на кнопку **Далее**, чтобы начать обучение.

Шаг 2. Выбор папок, содержащих полезную почту

На этом этапе вы можете выбрать папки, содержащие полезную корреспонденцию. Выбирать следует только те папки, в содержимом которых вы полностью уверены.

Для выбора доступны только папки учетных записей Microsoft Office Outlook и Microsoft Outlook Express (Windows Mail).

Шаг 3. Выбор папок, содержащих нежелательную почту

На этом этапе можно выбрать папки, содержащие нежелательную корреспонденцию (спам). Если в вашем почтовом клиенте нет таких папок, пропустите этот шаг мастера.

Для выбора доступны только папки учетных записей Microsoft Office Outlook и Microsoft Outlook Express (Windows Mail).

Шаг 4. Обучение Анти-Спама

На этом этапе выполняется автоматическое обучение Анти-Спама на папках, выбранных в ходе предыдущих шагов. Почтовые сообщения из этих папок пополняют базу Анти-Спама. Отправители полезной почты автоматически заносятся в список разрешенных отправителей.

Шаг 5. Сохранение результатов обучения

На этом этапе работы Мастера обучения необходимо сохранить результаты обучения одним из следующих способов:

- дополнить существующую базу Анти-Спама результатами обучения (выберите вариант **Добавить результаты обучения к существующей базе Анти-Спама**);
- заменить текущую базу новой, полученной в результате обучения (выберите вариант **Создать новую базу Анти-Спама**).

Нажмите на кнопку **Завершить**, чтобы завершить работу мастера.

КАК ПРОСМОТРЕТЬ ОТЧЕТ О ЗАЩИТЕ КОМПЬЮТЕРА

Kaspersky CRYSTAL ведет отчеты о работе каждого компонента защиты. С помощью отчета вы можете, например, узнать, сколько обнаружено и обезврежено вредоносных объектов (например, вирусов, троянских программ) в процессе работы программы за определенный период, сколько раз за это время обновлялась программа, сколько обнаружено спам-сообщений и многое другое.

Чтобы просмотреть отчет о работе программы, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Защита компьютера**.

   Откроется окно **Защита компьютера**.

2. По ссылке **Отчет** перейдите к окну отчетов Kaspersky CRYSTAL.

   В открывшемся окне на закладке **Отчет** отображаются отчеты о работе программы в виде диаграмм.

3. Если нужно просмотреть подробный отчет о работе программы (например, о работе каждого из ее компонентов), нажмите на кнопку **Подробный отчет**, расположенную в нижней части закладки **Отчет**.

   Откроется окно **Подробный отчет**, в котором данные представлены в табличном виде. Для удобства просмотра отчетов вы можете выбирать различные варианты группировки записей.

КАК ВОССТАНОВИТЬ СТАНДАРТНЫЕ ПАРАМЕТРЫ РАБОТЫ ПРОГРАММЫ

Вы всегда можете вернуться к рекомендуемым параметрам работы Kaspersky CRYSTAL. Они считаются оптимальными и рекомендованы специалистами «Лаборатории Касперского». Восстановление параметров осуществляется Мастером первоначальной настройки программы.

В открывшемся окне вам предлагается определить, какие параметры и для каких компонентов следует или не следует сохранять параллельно с восстановлением рекомендуемого уровня безопасности.

В списке представлены компоненты Kaspersky CRYSTAL, параметры которых были изменены пользователем или накоплены Kaspersky CRYSTAL в результате обучения компонентов Сетевой экран и Анти-Спам. Если для какого-либо компонента в процессе работы были сформированы уникальные параметры, они также будут представлены в списке.

Такими уникальными параметрами являются «белые» и «черные» списки фраз и адресов, используемых Анти-Спамом, списки доверенных интернет-адресов и телефонных номеров интернет-провайдеров, сформированные

правила исключений защиты для компонентов программы, правила фильтрации пакетов и программ Сетевого экрана.

Данные списки формируются в процессе работы с Kaspersky CRYSTAL с учетом индивидуальных задач и требований безопасности. Их формирование зачастую занимает много времени, поэтому мы рекомендуем сохранять их при восстановлении первоначальных параметров программы.

По завершении работы мастера для всех компонентов защиты будет установлен **Рекомендуемый** уровень безопасности с учетом тех параметров, которые вы решили сохранить при восстановлении. Кроме того, будут применены параметры, которые вы задали в ходе работы мастера.

- *Чтобы восстановить параметры защиты, выполните следующие действия:*

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Общие параметры** подраздел **Общие**.
4. В правой части окна нажмите на кнопку **Восстановить**.
5. В открывшемся окне нажмите на кнопку **Далее**. Это приведет к запуску Мастера настройки. Следуйте его указаниям.

Как перенести параметры программы на другой компьютер

Настроив программу, вы можете применить параметры ее работы к Kaspersky CRYSTAL, установленному на другом компьютере. В результате программа на обоих компьютерах будет настроена одинаково. Это полезно, например, в том случае, когда Kaspersky CRYSTAL установлен и на домашнем, и на офисном компьютере.

Параметры работы программы хранятся в специальном конфигурационном файле, который вы можете перенести с одного компьютера на другой. Последовательность действий при этом такова:

1. Выполните *экспорт* – сохраните параметры работы программы в конфигурационный файл.
2. Перенесите сохраненный файл на другой компьютер (например, перешлите по почте или переместите на съемном носителе).
3. Выполните *импорт* – примените параметры из конфигурационного файла к программе, установленной на другом компьютере.

- *Чтобы экспортировать текущие параметры работы Kaspersky CRYSTAL, выполните следующие действия:*

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Общие параметры** подраздел **Общие**.
4. В правой части окна нажмите на кнопку **Сохранить**.
5. В открывшемся окне введите название конфигурационного файла и укажите место его сохранения.

- *Чтобы импортировать параметры работы из конфигурационного файла, выполните следующие действия:*

1. Откройте главное окно программы.

2. В верхней части окна перейдите по ссылке **Настройка**.

3. В левой части окна выберите в разделе **Общие параметры** подраздел **Общие**.

4. В правой части окна нажмите на кнопку **Загрузить**.

5. В открывшемся окне выберите файл, из которого вы хотите импортировать параметры Kaspersky CRYSTAL.

РАСШИРЕННАЯ НАСТРОЙКА ПРОГРАММЫ

Этот раздел содержит подробную информацию о каждом компоненте программы с описанием алгоритма работы и настройки параметров компонента.

В ЭТОМ РАЗДЕЛЕ

Защита компьютера 79

Резервное копирование 164

Родительский контроль 171

Шифрование данных 180

Центр управления 184

Менеджер паролей 189

Производительность и совместимость с другими программами 219

Самозащита Kaspersky CRYSTAL 222

Внешний вид программы 223

Дополнительные инструменты 225

Отчеты 231

Уведомления 235

Участие в Kaspersky Security Network 237

Защита компьютера

Компоненты защиты компьютера обеспечивают защиту вашего компьютера от различных угроз, проверку объектов системы на вирусы и уязвимости, а также своевременное обновление баз и программных модулей Kaspersky CRYSTAL.

В этом разделе

Проверка компьютера 79

Обновление 87

Файловый Антивирус 93

Почтовый Антивирус 99

Веб-Антивирус 105

IM-Антивирус 111

Анти-Спам 113

Анти-Баннер 130

Контроль программ 133

Проактивная защита 140

Защита сети 143

Доверенная зона 154

Безопасная среда исполнения программ 157

Карантин и резервное хранилище 160

Проверка компьютера

Проверка компьютера на вирусы и уязвимости – одна из важнейших задач обеспечения безопасности компьютера. Необходимо регулярно проверять ваш компьютер на присутствие вирусов, чтобы исключить возможность распространения вредоносных программ, которые не были обнаружены компонентами защиты, например из-за установленного низкого уровня защиты или по другим причинам.

Задача поиска уязвимостей заключается в диагностике безопасности операционной системы и обнаружении в программном обеспечении особенностей, которые могут быть использованы злоумышленниками для распространения вредоносных объектов и для доступа к персональным данным.

Следующие разделы содержат подробную информацию об особенностях и настройке задач проверки, а также об уровнях безопасности, методах и технологиях проверки.

В этом разделе

Проверка на вирусы 80

Поиск уязвимостей 87

Проверка на вирусы

Для поиска вирусов в состав Kaspersky CRYSTAL включены следующие задачи:

- **Проверка объектов**. Проверяются объекты, выбранные пользователем. Можно проверить любой объект файловой системы компьютера. В рамках данной задачи вы можете настроить параметры проверки съемных дисков.
- **Полная проверка**. Тщательная проверка всей системы. По умолчанию проверяются следующие объекты: системная память, объекты, загрузка которых осуществляется при старте системы, резервное хранилище системы, почтовые базы, жесткие, съемные и сетевые диски.
- **Быстрая проверка**. Проверяются объекты, загрузка которых осуществляется при старте операционной системы.

Для задач полной и быстрой проверки не рекомендуется вносить изменения в списки объектов для проверки.

Каждая задача проверки выполняется в заданной области и может запускаться по заранее сформированному расписанию. Кроме того, каждая задача проверки характеризуется уровнем безопасности (набором параметров, влияющих на соотношение производительности и безопасности). По умолчанию всегда включен режим поиска угроз с помощью записей в базах программы. В дополнение можно задействовать различные методы и технологии (см. стр. 84) проверки.

После запуска задачи проверки на вирусы процесс ее выполнения отображается в разделе **Проверка** окна **Защита компьютера** в поле под названием запущенной задачи.

При обнаружении угрозы Kaspersky CRYSTAL присваивает найденному объекту один из следующих статусов:

- Статус одной из вредоносных программ (например, *вирус*, *троянская программа*).
- Статус *возможно зараженный* (подозрительный), если в результате проверки невозможно однозначно определить, заражен объект или нет. Возможно, в файле присутствует последовательность кода, свойственная вирусам, или модифицированный код известного вируса.

После этого программа отображает уведомление (см. стр. 235) об обнаруженной угрозе и выполняет заданное действие. Вы можете изменить действие при обнаружении угрозы.

Если вы работаете в автоматическом режиме (см. раздел «Использование интерактивного режима защиты» на стр. 54), Kaspersky CRYSTAL при обнаружении опасных объектов будет автоматически применять действие, рекомендуемое специалистами «Лаборатории Касперского». Для вредоносных объектов это действие **Лечить. Удалять, если лечение невозможно**, для подозрительных – **Поместить на карантин**. Если вы работаете в интерактивном режиме (см. раздел «Использование интерактивного режима защиты» на стр. 54), программа при обнаружении опасных объектов будет выводить на экран уведомление, в котором вы сможете выбрать нужное действие из числа предлагаемых.

Перед лечением или удалением зараженного объекта Kaspersky CRYSTAL формирует его резервную копию на тот случай, если впоследствии понадобится восстановить объект или появится возможность его вылечить. Подозрительные (возможно зараженные) объекты помещаются на карантин. Вы можете включить автоматическую проверку файлов на карантине после каждого обновления.

Информация о результатах проверки и обо всех событиях, произошедших при выполнении задач, записывается в отчет Kaspersky CRYSTAL.

В ЭТОМ РАЗДЕЛЕ

Изменение и восстановление уровня безопасности 81

Формирование расписания запуска проверки 82

Формирование списка объектов для проверки 82

Выбор метода проверки 83

Выбор технологии проверки 84

Изменение действия при обнаружении угрозы 84

Запуск проверки с правами другого пользователя 84

Изменение типа проверяемых объектов 84

Проверка составных файлов 85

Оптимизация проверки 86

Проверка съемных дисков при подключении 86

Создание ярлыка для запуска задачи 87

ИЗМЕНЕНИЕ И ВОССТАНОВЛЕНИЕ УРОВНЯ БЕЗОПАСНОСТИ

В зависимости от ваших текущих потребностей можно выбрать один из предустановленных уровней безопасности или настроить параметры проверки на вирусы самостоятельно.

Настраивая параметры выполнения задачи проверки, вы всегда можете вернуться к рекомендуемым. Они считаются оптимальными, рекомендованы специалистами «Лаборатории Касперского» и объединены в **Рекомендуемый** уровень безопасности.

Чтобы изменить установленный уровень безопасности, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Проверка компьютера** нужную задачу (**Полная проверка**, **Быстрая проверка** или **Проверка объектов**).
4. Для выбранной задачи в блоке **Уровень безопасности** установите нужный уровень безопасности или нажмите на кнопку **Настройка**, чтобы настроить параметры проверки вручную.

При настройке вручную название уровня безопасности изменится на **Другой**.

Чтобы восстановить рекомендуемые параметры проверки, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Проверка компьютера** нужную задачу (**Полная проверка**, **Быстрая проверка** или **Проверка объектов**).
4. Для выбранной задачи в блоке **Уровень безопасности** нажмите на кнопку **По умолчанию**.

Формирование расписания запуска проверки

Для автоматического запуска задач проверки можно сформировать расписание: задать периодичность запуска задачи, время запуска (если это необходимо), а также дополнительные параметры.

Если по каким-либо причинам запуск невозможен (например, в это время компьютер был выключен), вы можете настроить автоматический запуск пропущенной задачи, как только это станет возможным. Кроме того, можно включить автоматическую приостановку проверки в том случае, если выключен скринсейвер или компьютер разблокирован. Данная возможность позволяет отложить запуск задачи до того момента, пока пользователь не закончит свою работу на компьютере. Таким образом, задача проверки не будет занимать ресурсы компьютера во время его работы.

- *Чтобы настроить расписание запуска задачи проверки, выполните следующие действия:*

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Проверка компьютера** нужную задачу (**Полная проверка**, **Быстрая проверка**, **Проверка объектов** или **Поиск уязвимостей**).
4. Для выбранной задачи в блоке **Режим запуска** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Режим запуска** в блоке **Расписание** выберите вариант **По расписанию** и настройте режим запуска проверки.

- *Чтобы настроить автоматический запуск пропущенной задачи, выполните следующие действия:*

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Проверка компьютера** нужную задачу (**Полная проверка**, **Быстрая проверка**, **Проверка объектов** или **Поиск уязвимостей**).
4. Для выбранной задачи в блоке **Режим запуска** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Режим запуска** в блоке **Расписание** выберите вариант **По расписанию** и установите флажок **Запускать пропущенные задачи**.

- *Чтобы запускать проверку только после того, как пользователь закончит свою работу, выполните следующие действия:*

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Проверка компьютера** нужную задачу (**Полная проверка**, **Быстрая проверка**, **Проверка объектов** или **Поиск уязвимостей**).
4. Для выбранной задачи в блоке **Режим запуска** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Режим запуска** в блоке **Расписание** выберите вариант **По расписанию** и установите флажок **Приостанавливать проверку по расписанию, если выключен скринсейвер и разблокирован компьютер**.

Формирование списка объектов для проверки

По умолчанию каждой задаче проверки на вирусы соответствует свой список объектов. К таким объектам могут относиться как объекты файловой системы компьютера (например, логические диски, **Почтовые базы**), так и объекты других типов (например, сетевые диски). Вы можете внести в этот список изменения.

Если область проверки пуста или ни один из объектов, входящих в нее, не отмечен, то запустить задачу проверки невозможно.

- *Чтобы сформировать список объектов для задачи проверки объектов, выполните следующие действия:*

1. Откройте главное окно программы и нажмите на кнопку **Защита компьютера**.

   Откроется окно **Защита компьютера**.

2. В левой части окна выберите раздел **Проверка**.

3. В правой части окна по ссылке **Добавить** откройте список объектов для проверки.

4. В открывшемся окне **Выбор объекта для проверки** выберите объект и нажмите на кнопку **Добавить**. После добавления всех нужных объектов нажмите на кнопку **ОК**. Чтобы исключить какие-либо объекты из списка проверки, снимите флажок рядом с ними.

- *Чтобы сформировать список объектов для задач быстрой проверки, полной проверки или поиска уязвимостей, выполните следующие действия:*

1. Откройте главное окно программы.

2. В верхней части окна перейдите по ссылке **Настройка**.

3. В левой части окна выберите в разделе **Проверка компьютера** нужную задачу (**Полная проверка**, **Быстрая проверка** или **Поиск уязвимостей**).

4. Для выбранной задачи в блоке **Объекты для проверки** нажмите на кнопку **Настройка**.

5. В открывшемся окне **Объекты для проверки**с помощью ссылок **Добавить**, **Изменить**, **Удалить** сформируйте список. Чтобы исключить какие-либо объекты из списка проверки, снимите флажок рядом с ними.

   Объекты, добавленные в список по умолчанию, невозможно отредактировать или удалить.

ВЫБОР МЕТОДА ПРОВЕРКИ

При проверке компьютера на вирусы всегда используется метод *сигнатурного анализа*, в ходе которого Kaspersky CRYSTAL сравнивает найденный объект с записями в базах.

Для повышения эффективности поиска предназначены дополнительные методы проверки: *эвристический анализ* (анализ активности, которую объект производит в системе) и *поиск руткитов* (утилит, обеспечивающих сокрытие вредоносных программ в операционной системе).

- *Чтобы использовать нужные методы проверки, выполните следующие действия:*

1. Откройте главное окно программы.

2. В верхней части окна перейдите по ссылке **Настройка**.

3. В левой части окна выберите в разделе **Проверка компьютера** нужную задачу (**Полная проверка**, **Быстрая проверка** или **Проверка объектов**).

4. Для выбранной задачи в блоке **Режим запуска** нажмите на кнопку **Настройка**.

5. В открывшемся окне на закладке **Дополнительно** в блоке **Методы проверки** выберите нужные значения параметров.

Выбор технологии проверки

В дополнение к методам проверки вы можете задействовать специальные технологии, которые позволяют оптимизировать скорость проверки на вирусы за счет исключения файлов, не измененных с момента последней проверки.

Чтобы включить технологии проверки объектов, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Проверка компьютера** нужную задачу (**Полная проверка**, **Быстрая проверка** или **Проверка объектов**).
4. Для выбранной задачи в блоке **Режим запуска** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Дополнительно** в блоке **Технологии проверки** выберите нужное значение параметров.

Изменение действия при обнаружении угрозы

При обнаружении зараженных или возможно зараженных объектов программа выполняет заданное действие.

Чтобы изменить действие над обнаруженными объектами, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Проверка компьютера** нужную задачу (**Полная проверка**, **Быстрая проверка** или **Проверка объектов**).
4. Для выбранной задачи в блоке **Действие** укажите нужное действие.

Запуск проверки с правами другого пользователя

По умолчанию задачи проверки запускаются от имени учетной записи, с правами которой вы зарегистрировались в системе. Однако может возникнуть необходимость запустить задачу с правами другого пользователя. Вы можете указать учетную запись, с правами которой будет запускаться каждая задача проверки.

Чтобы запускать проверку с правами другого пользователя, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Проверка компьютера** нужную задачу (**Полная проверка**, **Быстрая проверка**, **Проверка объектов** или **Поиск уязвимостей**).
4. Для выбранной задачи в блоке **Режим запуска** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Режим запуска** в блоке **Пользователь** установите флажок **Запускать задачу с правами другого пользователя**. В полях ниже задайте имя пользователя и пароль.

Изменение типа проверяемых объектов

Указывая тип проверяемых объектов, вы определяете, файлы какого формата и размера будут проверяться при выполнении выбранной задачи проверки.

При выборе типа файлов помните следующее:

- Вероятность внедрения вредоносного кода в файлы некоторых форматов (например, txt) и его последующей активации достаточно низка. В то же время существуют файловые форматы, которые

содержат или могут содержать исполняемый код (например, exe, dll, doc). Риск внедрения в такие файлы вредоносного кода и его активации весьма высок.

- Злоумышленник может отправить вирус на ваш компьютер в исполняемом файле, переименованном в txt-файл. Если вы выбрали проверку файлов по расширению, то в процессе проверки такой файл будет пропущен. Если же выбрана проверка файлов по формату, то вне зависимости от расширения Файловый Антивирус проанализирует заголовок файла, в результате чего может выясниться, что файл имеет exe-формат. Такой файл будет подвергнут тщательной проверке на вирусы.

Чтобы изменить тип проверяемых файлов, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Проверка компьютера** нужную задачу (**Полная проверка**, **Быстрая проверка** или **Проверка объектов**).
4. Для выбранной задачи в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Область действия** в блоке **Типы файлов** выберите нужный вариант.

ПРОВЕРКА СОСТАВНЫХ ФАЙЛОВ

Распространенная практика сокрытия вирусов – внедрение их в составные файлы: архивы, базы данных и т. д. Чтобы обнаружить вирусы, скрытые таким образом, составной файл необходимо распаковать, что может привести к значительному снижению скорости проверки.

Для каждого типа составного файла вы можете выбрать, следует ли проверять все файлы или только новые. Для выбора перейдите по ссылке, расположенной рядом с названием объекта. Она меняет свое значение при нажатии на нее левой клавишей мыши. Если установлен режим проверки только новых и измененных файлов (см. стр. 86), ссылки для выбора проверки всех или только новых файлов будут недоступны.

Вы можете ограничить максимальный размер проверяемого составного файла. Составные файлы, размер которых превышает заданное значение, проверяться не будут.

Чтобы изменить список проверяемых составных файлов, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Проверка компьютера** нужную задачу (**Полная проверка**, **Быстрая проверка** или **Проверка объектов**).
4. Для выбранной задачи в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Область действия** в блоке **Проверка составных файлов** выберите нужные типы проверяемых составных файлов.

Чтобы задать максимальный размер составных файлов, которые будут проверяться, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Проверка компьютера** нужную задачу (**Полная проверка**, **Быстрая проверка** или **Проверка объектов**).
4. Для выбранной задачи в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Область действия** в блоке **Проверка составных файлов** нажмите на кнопку **Дополнительно**.

6. В открывшемся окне **Составные файлы** установите флажок **Не распаковывать составные файлы большого размера** и укажите максимальный размер проверяемых файлов.

При извлечении из архивов файлы больших размеров будут проверяться на вирусы даже в том случае, если установлен флажок **Не распаковывать составные файлы большого размера**.

Оптимизация проверки

Вы можете сократить время проверки и увеличить скорость работы Kaspersky CRYSTAL. Этого можно достичь, если проверять только новые файлы и те, что изменились с момента их предыдущего анализа. Такой режим проверки распространяется как на простые, так и на составные файлы.

Кроме того, можно задать ограничение длительности проверки одного объекта. По истечении заданного времени объект будет исключен из текущей проверки (кроме архивов и файлов, в состав которых входит несколько объектов).

- *Чтобы проверять только новые и измененные файлы, выполните следующие действия:*

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Проверка компьютера** нужную задачу (**Полная проверка**, **Быстрая проверка** или **Проверка объектов**).
4. Для выбранной задачи в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Область действия** в блоке **Оптимизация проверки** установите флажок **Проверять только новые и измененные файлы**.

- *Чтобы задать ограничение длительности проверки, выполните следующие действия:*

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Проверка компьютера** нужную задачу (**Полная проверка**, **Быстрая проверка** или **Проверка объектов**).
4. Для выбранной задачи в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Область действия** в блоке **Оптимизация проверки** установите флажок **Пропускать файлы, если их проверка длится более** и задайте длительность проверки одного файла.

Проверка съемных дисков при подключении

В последнее время широкое распространение получили вредоносные объекты, которые используют уязвимости операционной системы для распространения через локальные сети и съемные носители информации. Kaspersky CRYSTAL позволяет проверять на вирусы съемные диски при их подключении к компьютеру.

- *Чтобы настроить проверку съемных дисков при их подключении к компьютеру, выполните следующие действия:*

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Проверка компьютера** подраздел **Основные параметры**.
4. В правой части окна в блоке **Проверка съемных дисков при подключении** выберите действие и, если необходимо, укажите максимальный размер проверяемого диска в поле ниже.

СОЗДАНИЕ ЯРЛЫКА ДЛЯ ЗАПУСКА ЗАДАЧИ

Для быстрого запуска задач полной и быстрой проверки на вирусы, а также поиска уязвимостей в программе предусмотрена возможность создания ярлыков. Это позволяет запускать нужную задачу проверки, не открывая главного окна программы или контекстного меню.

Чтобы создать ярлык для запуска задачи проверки, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Проверка компьютера** подраздел **Основные параметры**.
4. В правой части окна в блоке **Быстрый запуск задач** нажмите на кнопку **Создать ярлык** рядом с названием нужной задачи (**Быстрая проверка**, **Полная проверка** или **Поиск уязвимостей**).
5. В открывшемся окне укажите путь для сохранения ярлыка и его имя. По умолчанию ярлык создается с именем задачи в папке *Мой компьютер* текущего пользователя компьютера.

Поиск уязвимостей

Уязвимости в операционной системе могут быть результатом ошибок программирования или проектирования, ненадежных паролей, действий вредоносных программ и т. п. В рамках поиска уязвимостей проводится изучение системы, поиск аномалий и повреждений в настройках операционной системы и браузера, поиск уязвимых служб и другие меры безопасности.

Диагностика может занять некоторое время. После ее проведения обнаруженные проблемы анализируются с точки зрения их опасности для системы.

После запуска задачи поиска уязвимостей (см. стр. 61) процесс ее выполнения отображается в окне **Поиск уязвимостей** в поле **Окончание**. Найденные в ходе проверки уязвимости в системе и программах отображаются в этом же окне на закладках **Уязвимости системы** и **Уязвимые программы**.

В ходе поиска угроз информация о его результатах записывается в отчет Kaspersky CRYSTAL.

Как и для задач проверки на вирусы, для задачи поиска уязвимостей можно задать расписание запуска, сформировать список объектов для проверки (см. стр. 82), выбрать учетную запись (см. раздел «Запуск проверки с правами другого пользователя» на стр. 84) и создать ярлык для быстрого запуска задачи. По умолчанию в качестве объекта проверки выбраны установленные на компьютере программы.

Обновление

Обновление баз и программных модулей Kaspersky CRYSTAL обеспечивает актуальность защиты вашего компьютера. Каждый день в мире появляются новые вирусы, троянские и другие вредоносные программы. Информация об угрозах и способах их нейтрализации содержится в базах Kaspersky CRYSTAL, поэтому регулярное обновление программы необходимо для обеспечения безопасности вашего компьютера и своевременного обнаружения новых угроз.

Для регулярного обновления требуется действительная лицензия на использование программы. При отсутствии лицензии выполнить обновление вы сможете только один раз.

Обновление программы загружает и устанавливает на ваш компьютер следующие объекты:

- Базы Kaspersky CRYSTAL.

  Защита информации обеспечивается на основании баз данных, содержащих описания сигнатур угроз и сетевых атак, а также методы борьбы с ними. Компоненты защиты используют их при поиске и обезвреживании опасных объектов на вашем компьютере. Базы регулярно пополняются записями о

новых угрозах и способах борьбы с ними. Поэтому базы настоятельно рекомендуется регулярно обновлять.

Наряду с базами Kaspersky CRYSTAL обновляются сетевые драйверы, обеспечивающие функциональность для перехвата сетевого трафика компонентами защиты.

- Программные модули.

  Помимо баз Kaspersky CRYSTAL, можно обновлять и программные модули. Пакеты обновлений устраняют уязвимости Kaspersky CRYSTAL, добавляют новые функции или улучшают существующие.

Основным источником обновлений Kaspersky CRYSTAL служат специальные серверы обновлений «Лаборатории Касперского». Одновременно с обновлением Kaspersky CRYSTAL вы можете копировать обновления баз и программных модулей, полученные с серверов «Лаборатории Касперского», в локальную папку, а затем предоставлять доступ к ним другим компьютерам сети. Это позволит экономить интернет-трафик.

Вы можете также настроить параметры автоматического запуска обновления.

Для успешной загрузки обновлений с серверов ваш компьютер должен быть подключен к интернету. По умолчанию параметры подключения к интернету определяются автоматически. Если вы используете прокси-сервер, может потребоваться настройка параметров подключения к нему.

В процессе обновления программные модули и базы на вашем компьютере сравниваются с актуальной версией, расположенной в источнике обновлений. Если текущие базы и модули отличаются от актуальной версии, на ваш компьютер будет установлена недостающая часть обновлений.

Если базы сильно устарели, то пакет обновлений может иметь значительный размер и создать дополнительный интернет-трафик (до нескольких десятков мегабайт).

Перед обновлением баз Kaspersky CRYSTAL создает их резервную копию на тот случай, если вы захотите вернуться к использованию баз предыдущей версии (см. раздел «Откат последнего обновления» на стр. 91).

Информация о текущем состоянии баз Kaspersky CRYSTAL отображается в разделе **Обновление** окна **Защита компьютера**.

Информация о результатах обновления и обо всех событиях, произошедших при выполнении задачи обновления, записывается в отчет Kaspersky CRYSTAL.

В этом разделе

Выбор источника обновлений 88

Формирование расписания запуска обновления 90

Откат последнего обновления 91

Проверка карантина после обновления 91

Использование прокси-сервера 92

Запуск обновления с правами другого пользователя 92

Выбор источника обновлений

Источник обновлений – это ресурс, содержащий обновления баз и модулей Kaspersky CRYSTAL. В качестве источника обновлений можно указать HTTP- или FTP-серверы, локальные или сетевые папки.

Основным источником обновлений служат серверы обновлений «Лаборатории Касперского», на которые выкладываются обновления баз и программных модулей для всех продуктов «Лаборатории Касперского».

Если серверы обновлений «Лаборатории Касперского» вам недоступны (например, ограничен доступ к интернету), вы можете обратиться в наш центральный офис (http://www.kaspersky.ru/contacts) и узнать адреса партнеров «Лаборатории Касперского», которые смогут предоставить вам обновления на съемном диске.

При заказе обновлений на съемных дисках обязательно уточняйте, хотите ли вы получить обновления программных модулей.

По умолчанию список источников обновлений содержит только серверы обновлений «Лаборатории Касперского». Если в качестве источников обновлений выбрано несколько ресурсов, в процессе обновления Kaspersky CRYSTAL обращается к ним строго по списку и обновляется с первого доступного источника.

Если в качестве источника обновлений выбран ресурс, расположенный вне локальной сети, для обновления необходимо соединение с интернетом.

Чтобы выбрать источник обновлений, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Обновление** подраздел **Параметры обновления**.
4. В правой части окна в блоке **Источник обновлений** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Источник** по ссылке **Добавить** откройте окно **Выбор источника обновлений**.
6. Выберите папку, которая содержит обновления, или введите адрес сервера, с которого требуется загружать обновления, в поле **Источник**.

В ЭТОМ РАЗДЕЛЕ

Выбор региона сервера обновлений 89

Обновление из папки общего доступа 90

ВЫБОР РЕГИОНА СЕРВЕРА ОБНОВЛЕНИЙ

Если в качестве источника обновлений вы используете серверы «Лаборатории Касперского», можно выбрать предпочтительное для вас местоположение сервера для загрузки обновлений. Серверы «Лаборатории Касперского» расположены в нескольких странах мира.

Использование географически ближайшего к вам сервера обновления «Лаборатории Касперского» поможет сократить время получения обновлений и увеличить его скорость. По умолчанию используется информация о текущем регионе из реестра операционной системы. Вы можете выбрать регион вручную.

Чтобы выбрать регион сервера, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Обновление** подраздел **Параметры обновления**.
4. В правой части окна в блоке **Источник обновлений** нажмите на кнопку **Настройка**.

5. В открывшемся окне на закладке **Источник** в блоке **Региональные настройки** выберите вариант **Выбрать из списка** и в раскрывающемся списке выберите ближайшую к вашему текущему местонахождению страну.

Обновление из папки общего доступа

Для экономии интернет-трафика можно настроить обновление Kaspersky CRYSTAL на компьютерах сети из папки общего доступа. При этом один из компьютеров сети получает пакет обновлений с серверов «Лаборатории Касперского» в интернете или с другого веб-ресурса, содержащего актуальный набор обновлений. Полученные обновления копируются в папку общего доступа, после чего другие компьютеры сети обращаются к этой папке для получения обновлений Kaspersky CRYSTAL.

Чтобы включить режим копирования обновлений, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Обновление** подраздел **Параметры обновления**.
4. В правой части окна в блоке **Дополнительно** установите флажок **Копировать обновления в папку** и в поле ниже укажите путь к папке общего доступа, в которую будут помещаться полученные обновления. Вы также можете выбрать папку, нажав на кнопку **Обзор**.

Чтобы обновление для данного компьютера выполнялось из указанной папки общего доступа, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Обновление** подраздел **Параметры обновления**.
4. В правой части окна в блоке **Источник обновлений** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Источник** по ссылке **Добавить** откройте окно **Выбор источника обновлений**.
6. Выберите папку или введите полный путь к ней в поле **Источник**.
7. На закладке **Источник** снимите флажок **Серверы обновлений «Лаборатории Касперского»**.

Формирование расписания запуска обновления

Для автоматического запуска задачи обновления можно сформировать расписание: задать периодичность запуска задачи, время запуска (если это необходимо), а также дополнительные параметры.

Если по каким-либо причинам запуск задачи невозможен (например, в это время компьютер был выключен), вы можете настроить автоматический запуск пропущенной задачи, как только это станет возможным.

Вы также можете отложить автоматический запуск задачи после старта программы. При этом все задачи по расписанию будут запускаться только по истечении указанного времени после старта Kaspersky CRYSTAL.

Чтобы настроить расписание запуска задачи обновления, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Обновление** подраздел **Параметры обновления**.
4. В правой части окна в блоке **Режим запуска** нажмите на кнопку **Настройка**.

5. В открывшемся окне на закладке **Режим запуска** в блоке **Расписание** выберите вариант **По расписанию** и настройте режим запуска обновления.

Чтобы включить автоматический запуск пропущенной задачи, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Обновление** подраздел **Параметры обновления**.
4. В правой части окна в блоке **Режим запуска** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Режим запуска** в блоке **Расписание** выберите вариант **По расписанию** и установите флажок **Запускать пропущенные задачи**.

Чтобы отложить запуск задач после старта программы, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Обновление** подраздел **Параметры обновления**.
4. В правой части окна в блоке **Режим запуска** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Режим запуска** в блоке **Расписание** выберите вариант **По расписанию**, затем в поле **Отложить запуск после старта программы на** укажите время, на которое нужно откладывать запуск задач.

Откат последнего обновления

После первого обновления баз и программных модулей Kaspersky CRYSTAL вам становится доступна функция отката к предыдущим базам.

Каждый раз, когда вы запускаете обновление, Kaspersky CRYSTAL создает резервную копию используемых баз и модулей и только потом приступает к их обновлению. Это позволяет вам вернуться к использованию предыдущих баз при необходимости. Возможность отката обновления полезна, например, в том случае, если новая версия баз содержит некорректную сигнатуру, из-за которой Kaspersky CRYSTAL блокирует безопасную программу.

При повреждении баз Kaspersky CRYSTAL рекомендуется запустить задачу обновления, чтобы загрузить действительный набор баз для актуальной защиты.

Чтобы вернуться к использованию предыдущей версии баз, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Защита компьютера**.

   Откроется окно **Защита компьютера**.

2. В левой части окна выберите раздел **Обновление**.
3. В правой части окна нажмите на кнопку **Откат к предыдущим базам**.

Проверка карантина после обновления

Если при проверке объекта не удалось точно определить, какими вредоносными программами он заражен, такой объект помещается на карантин. Возможно, после очередного обновления баз удастся однозначно определить

угрозу и обезвредить ее. Вы можете включить автоматическую проверку объектов на карантине после каждого обновления.

Рекомендуем вам периодически просматривать объекты на карантине. В результате проверки их статус может измениться. Ряд объектов можно будет восстановить в прежнее местоположение и продолжить работу с ними.

- *Чтобы включить проверку файлов на карантине после обновления, выполните следующие действия:*

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Обновление** подраздел **Параметры обновления**.
4. В правой части окна в блоке **Дополнительно** установите флажок **Проверять файлы на карантине после обновления**.

Использование прокси-сервера

Если для выхода в интернет используется прокси-сервер, необходимо настроить его параметры для корректного обновления Kaspersky CRYSTAL.

- *Чтобы настроить параметры прокси-сервера, выполните следующие действия:*

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Обновление** подраздел **Параметры обновления**.
4. В правой части окна в блоке **Источник обновлений** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Источник** нажмите на кнопку **Прокси-сервер**.
6. В открывшемся окне **Параметры прокси-сервера** настройте параметры прокси-сервера.

Запуск обновления с правами другого пользователя

По умолчанию обновление запускается от имени учетной записи, с правами которой вы зарегистрировались в системе. Однако обновление Kaspersky CRYSTAL может производиться из источника, к которому у вас нет доступа (например, из сетевой папки, содержащей обновления) или нет прав авторизованного пользователя прокси-сервера. Вы можете запускать обновление Kaspersky CRYSTAL от имени пользователя, обладающего такими привилегиями.

- *Чтобы запустить обновление с правами другого пользователя, выполните следующие действия:*

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Обновление** подраздел **Параметры обновления**.
4. В правой части окна в блоке **Режим запуска** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Режим запуска** в блоке **Пользователь** установите флажок **Запускать задачу с правами другого пользователя**. В полях ниже задайте имя пользователя и пароль.

Файловый Антивирус

Файловый Антивирус позволяет избежать заражения файловой системы компьютера. Компонент запускается при старте операционной системы, постоянно находится в оперативной памяти компьютера и проверяет все открываемые, сохраняемые и запускаемые файлы на вашем компьютере и на всех присоединенных дисках.

При обращении пользователя или программы к защищаемому файлу Файловый Антивирус проверяет наличие информации об этом файле в базах iChecker и iSwift и на основании полученных сведений принимает решение о необходимости проверки файла.

Специалисты «Лаборатории Касперского» не рекомендуют вам самостоятельно настраивать параметры работы Файлового Антивируса. В большинстве случаев достаточно изменить уровень безопасности.

Для тех случаев, когда проверку файловой системы нужно временно отключить, вы можете настроить автоматическую приостановку работы Файлового Антивируса, а при необходимости и отключить компонент.

Вы можете сформировать защищаемую область и выбрать режим проверки объектов.

По умолчанию всегда включен режим поиска угроз с помощью записей в базах программы. В дополнение можно задействовать эвристический анализ (см. стр. 97) и различные технологии проверки (см. стр. 97).

При обнаружении угрозы Kaspersky CRYSTAL присваивает найденному объекту один из следующих статусов:

- Статус одной из вредоносных программ (например, *вирус*, *троянская программа*).
- Статус *возможно зараженный* (подозрительный), если в результате проверки невозможно однозначно определить, заражен объект или нет. Возможно, в файле присутствует последовательность кода, свойственная вирусам, или модифицированный код известного вируса.

После этого программа выводит на экран уведомление (см. стр. 235) об обнаруженной угрозе и выполняет заданное действие. Вы можете изменить действие при обнаружении угрозы.

Если вы работаете в автоматическом режиме (см. раздел «Использование интерактивного режима защиты» на стр. 54), Kaspersky CRYSTAL при обнаружении опасных объектов будет автоматически применять действие, рекомендуемое специалистами «Лаборатории Касперского». Для вредоносных объектов это действие **Лечить. Удалять, если лечение невозможно**, для подозрительных – **Поместить на карантин**. Если вы работаете в интерактивном режиме (см. раздел «Использование интерактивного режима защиты» на стр. 54), программа при обнаружении опасных объектов будет выводить на экран уведомление, в котором вы сможете выбрать нужное действие из числа предлагаемых.

Перед лечением или удалением зараженного объекта Kaspersky CRYSTAL формирует его резервную копию на тот случай, если впоследствии понадобится восстановить объект или появится возможность его вылечить. Подозрительные (возможно зараженные) объекты помещаются на карантин. Вы можете включить автоматическую проверку файлов на карантине после каждого обновления.

В этом разделе

Включение и отключение Файлового Антивируса 94

Автоматическая приостановка работы Файлового Антивируса 94

Формирование области защиты 95

Изменение и восстановление уровня безопасности 96

Изменение режима проверки 96

Использование эвристического анализа 97

Технология проверки 97

Изменение действия над обнаруженными объектами 98

Проверка составных файлов 98

Оптимизация проверки 99

Включение и отключение Файлового Антивируса

По умолчанию Файловый Антивирус включен и работает в оптимальном режиме. Вы можете отключить Файловый Антивирус при необходимости.

Чтобы включить или отключить Файловый Антивирус, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Файловый Антивирус**.
4. В правой части окна снимите флажок **Включить Файловый Антивирус**, если нужно отключить компонент. Установите этот флажок, если компонент нужно включить.

Автоматическая приостановка работы Файлового Антивируса

При выполнении работ, требующих значительных ресурсов операционной системы, работу Файлового Антивируса можно приостанавливать. Чтобы снизить нагрузку и обеспечить быстрый доступ к объектам, вы можете настроить автоматическую приостановку работы компонента в указанное время или при работе с определенными программами.

Приостановка работы Файлового Антивируса при конфликте с определенными программами – это экстренная мера! Если при работе компонента возникают какие-либо конфликты, обратитесь в Службу технической поддержки «Лаборатории Касперского» (http://support.kaspersky.ru). Специалисты помогут вам наладить совместную работу Kaspersky CRYSTAL с другими программами на вашем компьютере.

Чтобы приостанавливать работу компонента в указанное время, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Файловый Антивирус**.

4. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

5. В открывшемся окне на закладке **Дополнительно** в блоке **Приостановка задачи** установите флажок **По расписанию** и нажмите на кнопку **Расписание**.

6. В окне **Приостановка задачи** укажите время (в формате чч:мм), в течение которого защита будет приостановлена (поля **Приостановить в** и **Возобновить в**).

Чтобы приостанавливать работу компонента при запуске указанных программ, выполните следующие действия:

1. Откройте главное окно программы.

2. В верхней части окна перейдите по ссылке **Настройка**.

3. В левой части окна выберите в разделе **Центр защиты** компонент **Файловый Антивирус**.

4. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

5. В открывшемся окне на закладке **Дополнительно** в блоке **Приостановка задачи** установите флажок **При запуске программ** и нажмите на кнопку **Выбрать**.

6. В окне **Программы** сформируйте список программ, при работе которых работа компонента будет приостановлена.

ФОРМИРОВАНИЕ ОБЛАСТИ ЗАЩИТЫ

Под областью защиты подразумеваются местоположение проверяемых объектов и тип файлов, которые следует проверять. По умолчанию Kaspersky CRYSTAL проверяет только потенциально заражаемые файлы, запускаемые со всех жестких, съемных и сетевых дисков.

Вы можете расширить или сузить область защиты, добавив / удалив объекты проверки или изменив тип проверяемых файлов. Например, можно выбрать для проверки только exe-файлы, запускаемые с сетевых дисков.

При выборе типа файлов помните следующее:

- Вероятность внедрения вредоносного кода в файлы некоторых форматов (например, txt) и его последующей активации достаточно низка. В то же время существуют файловые форматы, которые содержат или могут содержать исполняемый код (например, exe, dll, doc). Риск внедрения в такие файлы вредоносного кода и его активации весьма высок.

- Злоумышленник может отправить вирус на ваш компьютер в исполняемом файле, переименованном в txt-файл. Если вы выбрали проверку файлов по расширению, то в процессе проверки такой файл будет пропущен. Если же выбрана проверка файлов по формату, то вне зависимости от расширения Файловый Антивирус проанализирует заголовок файла, в результате чего может выясниться, что файл имеет exe-формат. Такой файл будет подвергнут тщательной проверке на вирусы.

Чтобы изменить список проверяемых объектов, выполните следующие действия:

1. Откройте главное окно программы.

2. В верхней части окна перейдите по ссылке **Настройка**.

3. В левой части окна выберите в разделе **Центр защиты** компонент **Файловый Антивирус**.

4. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

5. В открывшемся окне на закладке **Общие** в блоке **Область защиты** откройте окно выбора объектов по ссылке **Добавить**.

6. В окне **Выбор объекта для проверки** выберите объект и нажмите на кнопку **Добавить**.

7. После добавления всех нужных объектов нажмите на кнопку **ОК** в окне **Выбор объекта для проверки**.

8. Чтобы исключить объект из списка проверки, снимите флажок рядом с ним.

Чтобы изменить тип проверяемых файлов, выполните следующие действия:

1. Откройте главное окно программы.

2. В верхней части окна перейдите по ссылке **Настройка**.

3. В левой части окна выберите в разделе **Центр защиты** компонент **Файловый Антивирус**.

4. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

5. В открывшемся окне на закладке **Общие** в блоке **Типы файлов** выберите нужный параметр.

Изменение и восстановление уровня безопасности

В зависимости от текущих потребностей вы можете выбрать один из предустановленных уровней безопасности файлов и памяти или настроить параметры работы Файлового Антивируса самостоятельно.

Настраивая параметры работы компонента, всегда можно вернуться к рекомендуемым значениям. Эти значения считаются оптимальными, рекомендованы специалистами «Лаборатории Касперского» и объединены в **Рекомендуемый** уровень безопасности.

Перед включением низкого уровня безопасности рекомендуется провести полную проверку компьютера (см. раздел «Как выполнить полную проверку компьютера на вирусы» на стр. 61) с высоким уровнем безопасности.

Чтобы изменить установленный уровень безопасности файлов и памяти, выполните следующие действия:

1. Откройте главное окно программы.

2. В верхней части окна перейдите по ссылке **Настройка**.

3. В левой части окна выберите в разделе **Центр защиты** компонент **Файловый Антивирус**.

4. В правой части окна в блоке **Уровень безопасности** установите нужный уровень безопасности или нажмите на кнопку **Настройка**, чтобы настроить параметры работы вручную.

   При настройке вручную название уровня безопасности изменится на **Другой**.

Чтобы восстановить параметры защиты по умолчанию, выполните следующие действия:

1. Откройте главное окно программы.

2. В верхней части окна перейдите по ссылке **Настройка**.

3. В левой части окна выберите в разделе **Центр защиты** компонент **Файловый Антивирус**.

4. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **По умолчанию**.

Изменение режима проверки

Под режимом проверки подразумевается условие срабатывания Файлового Антивируса. По умолчанию Kaspersky CRYSTAL использует интеллектуальный режим, когда решение о проверке объекта принимается на основе операций, выполняемых с ним. Например, при работе с документом Microsoft Office Kaspersky CRYSTAL

проверяет файл при первом открытии и при последнем закрытии. Все промежуточные операции перезаписи файла из проверки исключаются.

Вы можете изменить режим проверки объектов. Выбор режима зависит от того, с какими файлами вы работаете большую часть времени.

- *Чтобы изменить режим проверки объектов, выполните следующие действия:*

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Файловый Антивирус**.
4. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Дополнительно** в блоке **Режим проверки** выберите нужный режим.

Использование эвристического анализа

При работе Файлового Антивируса всегда используется метод *сигнатурного анализа*, в ходе которого Kaspersky CRYSTAL сравнивает найденный объект с записями в базах.

Для повышения эффективности защиты вы можете использовать *эвристический анализ* (анализ активности, которую объект производит в системе). Этот анализ позволяет обнаруживать новые вредоносные объекты, записи о которых еще не попали в базы.

- *Чтобы включить или отключить использование эвристического анализа, выполните следующие действия:*

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Файловый Антивирус**.
4. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Производительность** в блоке **Методы проверки** установите флажок **Эвристический анализ** и задайте уровень детализации проверки. Снимите флажок **Эвристический анализ**, если этот метод проверки использовать не нужно.

Технология проверки

В дополнение к эвристическому анализу вы можете задействовать специальные технологии, которые позволяют оптимизировать скорость проверки объектов за счет исключения файлов, не измененных с момента последней проверки.

- *Чтобы включить технологии проверки объектов, выполните следующие действия:*

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Файловый Антивирус**.
4. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Дополнительно** в блоке **Технологии проверки** выберите нужные значения.

Изменение действия над обнаруженными объектами

При обнаружении зараженных или возможно зараженных объектов программа выполняет действие в зависимости от того, какой выбран режим работы: автоматический или интерактивный (см. раздел «Файловый Антивирус» на стр. 93). Вы можете изменить установленное действие.

Чтобы изменить установленное действие над обнаруженными объектами, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Файловый Антивирус**.
4. В правой части окна в блоке **Действие** выберите нужный вариант.

Проверка составных файлов

Распространенная практика сокрытия вирусов – внедрение их в составные файлы: архивы, базы данных и т. д. Чтобы обнаружить вирусы, скрытые таким образом, составной файл необходимо распаковать, что может привести к значительному снижению скорости проверки.

Для каждого типа составного файла вы можете выбрать, следует ли проверять все файлы или только новые.

По умолчанию Kaspersky CRYSTAL проверяет только вложенные OLE-объекты. Установочные пакеты и файлы, содержащие OLE-объекты, исполняются при открытии, что делает их более опасными, чем архивы.

При проверке составных файлов большого размера их предварительная распаковка может занять много времени. Это время можно сократить, включив распаковку составных файлов, превышающих заданный размер, в фоновом режиме. Если в ходе работы с таким файлом будет обнаружен вредоносный объект, Kaspersky CRYSTAL уведомит вас об этом.

Вы можете ограничить максимальный размер проверяемого составного файла. Составные файлы, размер которых превышает заданное значение, проверяться не будут.

Чтобы изменить список проверяемых составных файлов, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Файловый Антивирус**.
4. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Производительность** в блоке **Проверка составных файлов** выберите нужные типы проверяемых составных файлов.

Чтобы задать максимальный размер составных файлов, которые будут проверяться, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Файловый Антивирус**.
4. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

5. В открывшемся окне на закладке **Производительность** в блоке **Проверка составных файлов** нажмите на кнопку **Дополнительно**.

6. В окне **Составные файлы** установите флажок **Не распаковывать составные файлы большого размера** и укажите максимальный размер проверяемых файлов.

При извлечении из архивов файлы больших размеров будут проверяться на вирусы даже в том случае, если установлен флажок **Не распаковывать составные файлы большого размера**.

Чтобы распаковывать составные файлы большого размера в фоновом режиме, выполните следующие действия:

1. Откройте главное окно программы.

2. В верхней части окна перейдите по ссылке **Настройка**.

3. В левой части окна выберите в разделе **Центр защиты** компонент **Файловый Антивирус**.

4. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

5. В открывшемся окне на закладке **Производительность** в блоке **Проверка составных файлов** нажмите на кнопку **Дополнительно**.

6. В окне **Составные файлы** установите флажок **Распаковывать составные файлы в фоновом режиме** и укажите минимальный размер файла.

Оптимизация проверки

Вы можете сократить время проверки и увеличить скорость работы Kaspersky CRYSTAL. Этого можно достичь, если проверять только новые файлы и те, что изменились с момента их предыдущего анализа. Такой режим проверки распространяется как на простые, так и на составные файлы.

Чтобы проверять только новые и измененные файлы, выполните следующие действия:

1. Откройте главное окно программы.

2. В верхней части окна перейдите по ссылке **Настройка**.

3. В левой части окна выберите в разделе **Центр защиты** компонент **Файловый Антивирус**.

4. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

5. В открывшемся окне на закладке **Производительность** в блоке **Оптимизация проверки** установите флажок **Проверять только новые и измененные файлы**.

Почтовый Антивирус

Почтовый Антивирус проверяет входящие и исходящие сообщения на наличие в них опасных объектов. Он запускается при старте операционной системы, постоянно находится в оперативной памяти компьютера и проверяет все почтовые сообщения, получаемые или отправляемые по протоколам POP3, SMTP, IMAP, MAPI и NNTP, а также через защищенные соединения (SSL) по протоколам POP3 и IMAP (см. раздел «Проверка защищенных соединений» на стр. 150).

Индикатором работы компонента служит значок в области уведомлений панели задач, который принимает вид  каждый раз при проверке письма.

Каждое письмо, принимаемое или отправляемое пользователем, перехватывается и разбирается на составляющие его части: заголовок письма, тело, вложения. Тело и вложения почтового сообщения (в том числе вложенные OLE-объекты) проверяются на наличие угроз.

Специалисты «Лаборатории Касперского» не рекомендуют вам самостоятельно настраивать параметры работы Почтового Антивируса. В большинстве случаев достаточно выбрать уровень безопасности (см. раздел «Изменение и восстановление уровня безопасности» на стр. 102).

Вы можете указать типы сообщений, которые нужно проверять, и указать, какие из способов проверки необходимо использовать. По умолчанию всегда включен режим поиска угроз с помощью записей в базах программы. В дополнение к нему можно задействовать эвристический анализ. Кроме того, вы можете включить фильтрацию вложений (см. стр. 103), которая позволяет автоматически переименовывать или удалять файлы указанных типов.

При обнаружении угрозы Kaspersky CRYSTAL присваивает найденному объекту один из следующих статусов:

- Статус одной из вредоносных программ (например, *вирус*, *троянская программа*).
- Статус *возможно зараженный* (подозрительный), если в результате проверки невозможно однозначно определить, заражен объект или нет. Возможно, в файле присутствует последовательность кода, свойственная вирусам, или модифицированный код известного вируса.

После этого программа блокирует письмо, выводит на экран уведомление (см. стр. 235) об обнаруженной угрозе и выполняет заданное действие. Вы можете изменить действие при обнаружении угрозы (см. раздел «Изменение действия над обнаруженными объектами» на стр. 103).

Если вы работаете в автоматическом режиме (см. раздел «Использование интерактивного режима защиты» на стр. 54), Kaspersky CRYSTAL при обнаружении опасных объектов будет автоматически применять действие, рекомендуемое специалистами «Лаборатории Касперского». Для вредоносных объектов это действие **Лечить. Удалять, если лечение невозможно**, для подозрительных – **Поместить на карантин**. Если вы работаете в интерактивном режиме (см. раздел «Использование интерактивного режима защиты» на стр. 54), программа при обнаружении опасных объектов будет выводить на экран уведомление, в котором вы сможете выбрать нужное действие из числа предлагаемых.

Перед лечением или удалением зараженного объекта Kaspersky CRYSTAL формирует его резервную копию на тот случай, если впоследствии понадобится восстановить объект или появится возможность его вылечить. Подозрительные (возможно зараженные) объекты помещаются на карантин. Вы можете включить автоматическую проверку файлов на карантине после каждого обновления.

В результате успешного лечения письмо становится доступным для пользователя. Если же лечение произвести не удалось, зараженный объект из письма удаляется. В результате антивирусной обработки в тему письма помещается специальный текст, уведомляющий о том, что письмо обработано Kaspersky CRYSTAL.

При необходимости вы можете отключить Почтовый Антивирус (см. раздел «Включение и отключение Почтового Антивируса» на стр. 101).

Для почтовой программы Microsoft Office Outlook предусмотрен встраиваемый модуль расширения (см. раздел «Проверка почты в Microsoft Office Outlook» на стр. 104), позволяющий производить более тонкую настройку проверки почты.

Если вы используете почтовую программу The Bat!, Kaspersky CRYSTAL может использоваться наряду с другими антивирусными программами. При этом правила обработки почтового трафика (см. раздел «Проверка почты в The Bat!» на стр. 104) настраиваются непосредственно в программе The Bat! и превалируют над параметрами защиты почты программы.

При работе с остальными почтовыми программами (в том числе с Microsoft Outlook Express (Windows Mail), Mozilla Thunderbird, Eudora, Incredimail) Почтовый Антивирус проверяет почту на трафике по протоколам SMTP, POP3, IMAP и NNTP.

Обратите внимание, что при работе в почтовом клиенте Thunderbird не проверяются на вирусы почтовые сообщения, передаваемые по протоколу IMAP в случае, если используются фильтры, перемещающие сообщения из папки **Входящие**.

В ЭТОМ РАЗДЕЛЕ

Включение и отключение Почтового Антивируса 101

Формирование области защиты 101

Изменение и восстановление уровня безопасности 102

Использование эвристического анализа 102

Изменение действия над обнаруженными объектами 103

Фильтрация вложений 103

Проверка составных файлов 104

Проверка почты в Microsoft Office Outlook 104

Проверка почты в The Bat! 104

Включение и отключение Почтового Антивируса

По умолчанию Почтовый Антивирус включен и работает в оптимальном режиме. Вы можете отключить Почтовый Антивирус при необходимости.

Чтобы включить или отключить Почтовый Антивирус, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Почтовый Антивирус**.
4. В правой части окна снимите флажок **Включить Почтовый Антивирус**, если нужно отключить компонент. Установите этот флажок, если компонент нужно включить.

Формирование области защиты

Под областью защиты подразумевается тип сообщений, которые следует проверять. По умолчанию Kaspersky CRYSTAL проверяет как входящие, так и исходящие сообщения.

Если вы выбрали проверку только входящих сообщений, в самом начале работы с Kaspersky CRYSTAL рекомендуется проверить исходящую почту, поскольку существует вероятность того, что на вашем компьютере есть почтовые черви, которые используют электронную почту в качестве канала собственного распространения. Это позволит избежать неприятностей, связанных с неконтролируемой рассылкой зараженных электронных сообщений с вашего компьютера.

К области защиты относятся также параметры интеграции Почтового Антивируса в систему и проверяемые протоколы. По умолчанию Почтовый Антивирус интегрируется в почтовые клиенты Microsoft Office Outlook и The Bat!.

Чтобы отключить проверку исходящей почты, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Почтовый Антивирус**.

4. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

5. В открывшемся окне на закладке **Общие** в блоке **Область защиты** выберите вариант **Только входящие сообщения**.

Чтобы задать проверяемые протоколы и параметры интеграции Почтового Антивируса в систему, выполните следующие действия:

1. Откройте главное окно программы.

2. В верхней части окна перейдите по ссылке **Настройка**.

3. В левой части окна выберите в разделе **Центр защиты** компонент **Почтовый Антивирус**.

4. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

5. В открывшемся окне на закладке **Дополнительно** в блоке **Встраивание в систему** выберите нужные параметры.

Изменение и восстановление уровня безопасности

В зависимости от текущих потребностей вы можете выбрать один из предустановленных уровней безопасности почты или настроить параметры работы Почтового Антивируса самостоятельно.

Настраивая параметры работы компонента, всегда можно вернуться к рекомендуемым значениям. Эти значения считаются оптимальными, рекомендованы специалистами «Лаборатории Касперского» и объединены в **Рекомендуемый** уровень безопасности.

Чтобы изменить установленный уровень безопасности почты, выполните следующие действия:

1. Откройте главное окно программы.

2. В верхней части окна перейдите по ссылке **Настройка**.

3. В левой части окна выберите в разделе **Центр защиты** компонент **Почтовый Антивирус**.

4. В правой части окна в блоке **Уровень безопасности** установите нужный уровень безопасности или нажмите на кнопку **Настройка**, чтобы настроить параметры работы вручную.

> При настройке вручную название уровня безопасности изменится на **Другой**.

Чтобы восстановить параметры защиты почты по умолчанию, выполните следующие действия:

1. Откройте главное окно программы.

2. В верхней части окна перейдите по ссылке **Настройка**.

3. В левой части окна выберите в разделе **Центр защиты** компонент **Почтовый Антивирус**.

4. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **По умолчанию**.

Использование эвристического анализа

При работе Почтового Антивируса всегда используется метод *сигнатурного анализа*, в ходе которого Kaspersky CRYSTAL сравнивает найденный объект с записями в базах.

Для повышения эффективности защиты вы можете использовать *эвристический анализ* (анализ активности, которую объект производит в системе). Этот анализ позволяет обнаруживать новые вредоносные объекты, записи о которых еще не попали в базы.

Чтобы включить или отключить использование эвристического анализа, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Почтовый Антивирус**.
4. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Общие** в блоке **Методы проверки** установите флажок **Эвристический анализ** и задайте уровень детализации проверки. Снимите флажок **Эвристический анализ**, если этот метод проверки использовать не нужно.

Изменение действия над обнаруженными объектами

При обнаружении зараженных или возможно зараженных объектов программа выполняет действие в зависимости от того, какой выбран режим работы: автоматический или интерактивный (см. раздел «Почтовый Антивирус» на стр. 99). Вы можете изменить установленное действие.

Чтобы изменить установленное действие над обнаруженными объектами, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Почтовый Антивирус**.
4. В правой части окна в блоке **Действие** выберите нужный вариант.

Фильтрация вложений

Чаще всего вредоносные программы распространяются через почту в виде присоединенных к сообщению объектов. Для защиты компьютера, например, от автоматического запуска вложенного файла вы можете включить фильтрацию вложений, которая позволяет автоматически переименовывать или удалять файлы указанных типов.

Чтобы включить фильтрацию вложений, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Почтовый Антивирус**.
4. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Фильтр вложений** выберите режим фильтрации вложений. При выборе последних двух режимов становится активным список типов файлов (расширений), в котором вы можете выбрать нужные типы или добавить маску нового типа.

   Чтобы добавить в список маску нового типа, по ссылке **Добавить** откройте окно **Маска имени файла**, а затем введите в нем необходимые данные.

Проверка составных файлов

Распространенная практика сокрытия вирусов – внедрение их в составные файлы: архивы, базы данных и т. д. Чтобы обнаружить вирусы, скрытые таким образом, составной файл необходимо распаковать, что может привести к значительному снижению скорости проверки.

Вы можете включить или отключить проверку вложенных архивов, а также ограничить максимальный размер проверяемых архивов.

Если ваш компьютер не защищен какими-либо средствами локальной сети (выход в интернет осуществляется без участия прокси-сервера или сетевого экрана), отключать проверку вложенных архивов не рекомендуется.

Чтобы настроить параметры проверки составных файлов, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Почтовый Антивирус**.
4. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Общие** задайте нужные параметры.

Проверка почты в Microsoft Office Outlook

Если в качестве почтового клиента используется Microsoft Office Outlook, вы можете настроить дополнительные параметры проверки вашей почты на вирусы.

При установке Kaspersky CRYSTAL в Microsoft Office Outlook встраивается специальный модуль расширения. Он позволяет быстро перейти к настройке параметров Почтового Антивируса, а также определить, в какой момент почтовое сообщение будет проверено на присутствие опасных объектов.

Модуль расширения реализован в виде закладки **Защита почты**, расположенной в меню **Сервис** → **Параметры**.

Чтобы выбрать, в какой момент проверять почту, выполните следующие действия:

1. Откройте главное окно Microsoft Office Outlook.
2. В меню программы выберите пункт **Сервис** → **Параметры**.
3. На закладке **Защита почты** выберите нужные параметры.

Проверка почты в The Bat!

Действия над зараженными объектами почтовых сообщений в почтовой программе The Bat! определяются средствами самой программы.

Параметры Почтового Антивируса, определяющие необходимость проверки входящей и исходящей почты, а также действия над опасными объектами писем и исключения, игнорируются. Единственное, что принимается во внимание программой The Bat!, – это проверка вложенных архивов.

Параметры защиты почты распространяются на все установленные на компьютере антивирусные компоненты, поддерживающие работу с The Bat!.

Следует помнить, что при получении почтовых сообщений они сначала проверяются Почтовым Антивирусом и только потом – плагином почтового клиента The Bat!. При обнаружении вредоносного объекта Kaspersky

CRYSTAL обязательно уведомит вас об этом. Если при этом в окне уведомления Почтового Антивируса выбрать действие **Лечить** (**Удалить**), то действия по устранению угрозы будут выполнены именно Почтовым Антивирусом. Если в окне уведомления выбрать действие **Пропустить**, то обезвреживать объект будет плагин The Bat!. При отправлении почтовых сообщений сначала осуществляется проверка плагином, а затем Почтовым Антивирусом.

Вам нужно определить следующие критерии:

- какой поток почтовых сообщений (входящий, исходящий) следует подвергать проверке;
- в какой момент нужно производить проверку объектов письма (при открытии письма, перед сохранением на диске);
- какие действия будет предпринимать почтовый клиент при обнаружении опасных объектов в почтовых сообщениях. Например, вы можете выбрать:
  - **Попробовать излечить зараженные части** – при выборе этого варианта будет произведена попытка лечения зараженного объекта; если его вылечить невозможно, объект остается в письме.
  - **Удалить зараженные части** – при выборе этого варианта опасный объект письма будет удален независимо от того, является он зараженным или подозревается на заражение.

По умолчанию все зараженные объекты почтовых сообщений помещаются программой The Bat! на карантин без лечения.

Почтовые сообщения, содержащие опасные объекты, не отмечаются специальным заголовком в программе The Bat!.

Чтобы перейти к настройке параметров защиты почты в The Bat!, выполните следующие действия:

1. Откройте главное окно The Bat!.
2. В меню **Свойства** почтового клиента выберите пункт **Настройка**.
3. В дереве настройки выберите объект **Защита от вирусов**.

Веб-Антивирус

Каждый раз при работе в интернете вы подвергаете информацию, хранящуюся на вашем компьютере, риску заражения опасными программами. Они могут проникнуть на ваш компьютер, пока вы скачиваете бесплатные программы или просматриваете информацию на заведомо безопасных веб-сайтах, которые до вашего посещения подверглись атаке хакеров. Более того, сетевые черви могут проникать на ваш компьютер до открытия веб-страницы или скачивания файла – непосредственно при установлении соединения с интернетом.

Для обеспечения безопасности вашей работы в интернете предназначен компонент *Веб-Антивирус*. Он защищает информацию, поступающую на ваш компьютер по протоколам HTTP, HTTPS и FTP, а также предотвращает запуск на компьютере опасных скриптов.

Веб-защита предусматривает контроль потока данных, проходящего только через порты, указанные в списке контролируемых портов. Список портов, которые чаще всего используются для передачи данных, включен в комплект поставки Kaspersky CRYSTAL. Если вы используете порты, отсутствующие в данном списке, добавьте их в список контролируемых портов (см. раздел «Формирование списка контролируемых портов» на стр. 152), чтобы обеспечить защиту проходящего через них потока данных.

Проверка потока данных происходит с определенным набором параметров, который называется уровнем безопасности (см. раздел «Изменение и восстановление уровня безопасности» на стр. 107). При обнаружении угроз Веб-Антивирус выполняет заданное действие.

Специалисты «Лаборатории Касперского» не рекомендуют вам самостоятельно настраивать параметры работы Веб-Антивируса. В большинстве случаев достаточно выбрать подходящий уровень безопасности.

Алгоритм работы компонента

Веб-Антивирус защищает информацию, поступающую на компьютер и отправляемую с него по протоколам HTTP, HTTPS и FTP, а также предотвращает запуск на компьютере опасных скриптов. По умолчанию проверка защищенных соединений (по протоколу HTTPS) отключена, ее можно включить и настроить (см. раздел «Проверка защищенных соединений» на стр. 150).

Защита данных обеспечивается по следующему алгоритму:

1. Каждая веб-страница или файл, к которому обращаются пользователь или некоторая программа по протоколам HTTP, HTTPS или FTP, перехватывается и анализируется Веб-Антивирусом на присутствие вредоносного кода. Распознавание вредоносных объектов происходит на основании баз, используемых в работе Kaspersky CRYSTAL, а также с помощью эвристического алгоритма. Базы содержат описание всех известных в настоящий момент вредоносных программ и способов их обезвреживания. Эвристический алгоритм позволяет обнаруживать новые вирусы, еще не описанные в базах.

2. В результате анализа возможны следующие варианты поведения:

   - Если веб-страница или объект, к которому обращается пользователь, содержат вредоносный код, доступ к ним блокируется. При этом на экран выводится уведомление о том, что запрашиваемый объект или страница заражены.

   - Если файл или веб-страница не содержат вредоносного кода, они сразу же становятся доступными для пользователя.

Проверка скриптов выполняется по следующему алгоритму:

1. Каждый запускаемый скрипт перехватывается Веб-Антивирусом и анализируется на присутствие вредоносного кода.

2. Если скрипт содержит вредоносный код, Веб-Антивирус блокирует скрипт и уведомляет об этом пользователя, выводя на экран специальное сообщение.

3. Если в скрипте не обнаружено вредоносного кода, скрипт выполняется.

Веб-Антивирус перехватывает только скрипты, основанные на технологии Microsoft Windows Script Host.

В ЭТОМ РАЗДЕЛЕ

Включение и отключение Веб-Антивируса 107

Изменение и восстановление уровня безопасности 107

Изменение действия над обнаруженными объектами 108

Блокирование опасных скриптов 108

Проверка ссылок по базам фишинговых и подозрительных адресов 108

Использование эвристического анализа 109

Оптимизация проверки 109

Модуль проверки ссылок 110

Формирование списка доверенных адресов 111

Включение и отключение Веб-Антивируса

По умолчанию Веб-Антивирус включен и работает в оптимальном режиме. Вы можете отключить Веб-Антивирус при необходимости.

Чтобы включить или отключить Веб-Антивирус, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Веб-Антивирус**.
4. В правой части окна снимите флажок **Включить Веб-Антивирус**, если нужно отключить компонент. Установите этот флажок, если компонент нужно включить.

Изменение и восстановление уровня безопасности

В зависимости от текущих потребностей вы можете выбрать один из предустановленных уровней безопасности или настроить параметры работы Веб-Антивируса самостоятельно.

Настраивая параметры работы компонента, всегда можно вернуться к рекомендуемым значениям. Эти значения считаются оптимальными, рекомендованы специалистами «Лаборатории Касперского» и объединены в **Рекомендуемый** уровень безопасности.

Чтобы изменить установленный уровень безопасности веб-трафика, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Веб-Антивирус**.
4. В правой части окна в блоке **Уровень безопасности** установите нужный уровень безопасности или нажмите на кнопку **Настройка**, чтобы настроить параметры работы вручную.

При настройке вручную название уровня безопасности изменится на **Другой**.

Чтобы восстановить параметры защиты веб-трафика по умолчанию, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Веб-Антивирус**.
4. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **По умолчанию**.

Изменение действия над обнаруженными объектами

При обнаружении зараженных или возможно зараженных объектов программа выполняет действие в зависимости от того, какой выбран режим работы: автоматический или интерактивный.

Если вы работаете в автоматическом режиме (см. раздел «Использование интерактивного режима защиты» на стр. 54), Kaspersky CRYSTAL при обнаружении опасных объектов будет автоматически применять действие, рекомендуемое специалистами «Лаборатории Касперского». Для вредоносных объектов это действие **Лечить. Удалять, если лечение невозможно**, для подозрительных – **Поместить на карантин**. Если вы работаете в интерактивном режиме (см. раздел «Использование интерактивного режима защиты» на стр. 54), программа при обнаружении опасных объектов будет выводить на экран уведомление, в котором вы сможете выбрать нужное действие из числа предлагаемых.

Чтобы изменить установленное действие над обнаруженными объектами, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Веб-Антивирус**.
4. В правой части окна в блоке **Действие** выберите нужный вариант.

Блокирование опасных скриптов

Веб-Антивирус может проверять все скрипты, обрабатываемые в Microsoft Internet Explorer, а также любые WSH-скрипты (JavaScript, Visual Basic Script и др.), запускаемые при работе пользователя на компьютере. Если скрипт представляет опасность для компьютера, его выполнение будет заблокировано.

Чтобы Веб-Антивирус проверял и блокировал скрипты, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Веб-Антивирус**.
4. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
5. В открывшемся окне **Веб-Антивирус** в блоке **Дополнительно** должен быть установлен флажок **Блокировать опасные скрипты в Microsoft Internet Explorer**. Если флажок снят, установите его.

Проверка ссылок по базам фишинговых и подозрительных адресов

Веб-Антивирус проверяет веб-трафик на вирусы, а также устанавливает принадлежность ссылок к списку подозрительных веб-адресов и к списку фишинговых веб-адресов.

Проверка ссылок на принадлежность к списку фишинговых адресов позволяет избежать фишинг-атак, которые, как правило, представляют собой почтовые сообщения от якобы финансовых структур и содержат ссылки на веб-сайты таких организаций. Текст сообщения убеждает воспользоваться ссылкой и ввести на открывшемся веб-сайте конфиденциальную информацию, например номер кредитной карты или свои имя и пароль персональной страницы интернет-банка, где можно производить финансовые операции. Частным примером фишинг-атаки может служить письмо якобы от банка, клиентом которого вы являетесь, со ссылкой на официальный веб-сайт в интернете. Воспользовавшись ссылкой, вы попадаете на точную копию веб-сайта банка и даже можете видеть его адрес в браузере, однако реально находитесь на фиктивном веб-сайте. Все ваши дальнейшие действия на веб-сайте отслеживаются и могут быть использованы для кражи ваших денежных средств.

Списки фишинговых веб-адресов включены в комплект поставки Kaspersky CRYSTAL. Поскольку ссылка на фишинговый веб-сайт может содержаться не только в письме, но и, например, в тексте ICQ-сообщения, Веб-Антивирус отслеживает попытки перейти на фишинговый веб-сайт на уровне проверки веб-трафика и блокирует доступ к таким веб-сайтам.

- *Чтобы Веб-Антивирус проверял ссылки по базам подозрительных и фишинговых веб-адресов, выполните следующие действия:*

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Веб-Антивирус**.
4. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
5. В открывшемся окне **Веб-Антивирус** в блоке **Методы проверки** должны быть установлены флажки **Проверять ссылки по базе подозрительных веб-адресов** и **Проверять ссылки по базе фишинговых веб-адресов**. Если флажки сняты, установите их.

Использование эвристического анализа

При работе Почтового Антивируса всегда используется метод *сигнатурного анализа*, в ходе которого Kaspersky CRYSTAL сравнивает найденный объект с записями в базах..

Для повышения эффективности защиты вы можете использовать *эвристический анализ* (анализ активности, которую объект производит в системе). Этот анализ позволяет обнаруживать новые вредоносные объекты, записи о которых еще не попали в базы.

- *Чтобы включить или отключить использование эвристического анализа, выполните следующие действия:*

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Веб-Антивирус**.
4. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
5. В открывшемся окне **Веб-Антивирус** в блоке **Методы проверки** установите флажок **Эвристический анализ** и задайте уровень детализации проверки. Снимите флажок **Эвристический анализ**, если этот метод проверки использовать не нужно.

Оптимизация проверки

Для повышения эффективности обнаружения вредоносного кода Веб-Антивирусом применяется кеширование фрагментов объектов, загружаемых из интернета. Однако использование кеширования увеличивает время обработки объекта и может вызывать проблемы при копировании и обработке больших объектов. Чтобы оптимизировать работу с объектами, загружаемыми из интернета, вы можете ограничить время кеширования фрагментов объектов.

Чтобы ограничить время кеширования, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Веб-Антивирус**.
4. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
5. В открывшемся окне **Веб-Антивирус** в блоке **Оптимизация проверки** установите флажок **Ограничить время кеширования трафика** и задайте время (в секундах) в поле справа.

Модуль проверки ссылок

В состав Kaspersky CRYSTAL включен модуль проверки ссылок, который находится под управлением Веб-Антивируса. Модуль встраивается в веб-браузеры Microsoft Internet Explorer и Mozilla Firefox в виде плагина.

Модуль проверяет все ссылки, расположенные на веб-странице, на принадлежность к подозрительным и фишинговым веб-адресам. Вы можете сформировать список адресов веб-сайтов, содержимое которых не следует проверять на наличие подозрительных и фишинговых ссылок, или список адресов веб-сайтов, содержимое которых проверять необходимо. Вы также можете вовсе отказаться от проверки ссылок.

Чтобы включить модуль проверки ссылок, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Веб-Антивирус**.
4. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
5. В открывшемся окне **Веб-Антивирус** в блоке **Дополнительно** установите флажок **Отмечать фишинговые и подозрительные ссылки в Microsoft Internet Explorer и Mozilla Firefox**.

Чтобы сформировать список веб-адресов, содержимое которых не нужно проверять на наличие подозрительных и фишинговых ссылок, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Веб-Антивирус**.
4. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
5. В открывшемся окне **Веб-Антивирус** в блоке **Дополнительно** нажмите на кнопку **Настройка**.
6. В открывшемся окне **Модуль проверки ссылок** выберите вариант **Для всех веб-адресов** и нажмите на кнопку **Исключения**.
7. В открывшемся окне **Список доверенных веб-адресов** сформируйте список веб-адресов, содержимое которых не следует проверять на наличие подозрительных и фишинговых ссылок.

Чтобы сформировать список веб-адресов, содержимое которых необходимо проверять на наличие подозрительных и фишинговых ссылок, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.

3. В левой части окна выберите в разделе **Центр защиты** компонент **Веб-Антивирус**.

4. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

5. В открывшемся окне **Веб-Антивирус** в блоке **Дополнительно** нажмите на кнопку **Настройка**.

6. В открывшемся окне **Модуль проверки ссылок** выберите вариант **Для указанных веб-адресов** и нажмите на кнопку **Выбрать**.

7. В открывшемся окне **Список проверяемых веб-адресов** сформируйте список веб-адресов, содержимое которых необходимо проверять на наличие подозрительных и фишинговых ссылок.

ФОРМИРОВАНИЕ СПИСКА ДОВЕРЕННЫХ АДРЕСОВ

Вы можете сформировать список веб-адресов, содержанию которых вы безоговорочно доверяете. Веб-Антивирус не будет анализировать информацию с данных адресов на присутствие опасных объектов. Такая возможность может быть использована, например, в том случае, если Веб-Антивирус препятствует загрузке некоторого файла с известного вам веб-сайта.

Чтобы сформировать список доверенных веб-адресов, выполните следующие действия:

1. Откройте главное окно программы.

2. В верхней части окна перейдите по ссылке **Настройка**.

3. В левой части окна выберите в разделе **Центр защиты** компонент **Веб-Антивирус**.

4. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

5. В открывшемся окне **Веб-Антивирус** в блоке **Оптимизация проверки** установите флажок **Не проверять HTTP-трафик с доверенных веб-адресов** и нажмите на кнопку **Выбрать**.

6. В открывшемся окне **Список доверенных веб-адресов** сформируйте список адресов, содержимому которых вы доверяете.

Если в дальнейшем понадобится временно исключить адрес из списка доверенных, не нужно удалять этот адрес из списка – достаточно снять флажок слева от него.

IM-АНТИВИРУС

IM-Антивирус предназначен для проверки трафика, передаваемого с помощью программ для быстрого обмена сообщениями (так называемых *интернет-пейджеров*).

Сообщения, переданные через интернет-пейджеры, могут содержать ссылки на подозрительные веб-сайты, а также на веб-сайты, которые используются злоумышленниками для фишинг-атак. Вредоносные программы используют интернет-пейджеры для рассылки спам-сообщений, а также ссылок на программы (или самих программ), которые крадут номера и пароли пользователей.

Kaspersky CRYSTAL обеспечивает безопасную работу со многими программами для быстрого обмена сообщениями, в том числе ICQ, MSN, AIM, Yahoo! Messenger, Jabber, Google Talk, Mail.Ru Агент и IRC.

Некоторые интернет-пейджеры, например Yahoo! Messenger и Google Talk, используют защищенное соединение. Чтобы проверять трафик этих программ, требуется включить проверку защищенных соединений (см. стр. 150).

Сообщения перехватываются IM-Антивирусом и проверяются на наличие опасных объектов или ссылок. Вы можете выбрать типы сообщений (см. стр. 112), которые нужно проверять, и задействовать различные методы проверки.

Обнаружив угрозы в сообщении, IM-Антивирус заменяет это сообщение предупреждением для пользователя.

Передаваемые через интернет-пейджеры файлы проверяются компонентом Файловый Антивирус (на стр. 93) во время попытки их сохранения.

В этом разделе

Включение и отключение IM-Антивируса 112

Формирование области защиты 112

Выбор метода проверки 112

Включение и отключение IM-Антивируса

По умолчанию IM-Антивирус включен и работает в оптимальном режиме. Вы можете отключить IM-Антивирус при необходимости.

Чтобы включить или отключить IM-Антивирус, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **IM-Антивирус**.
4. В правой части окна снимите флажок **Включить IM-Антивирус**, если нужно отключить компонент. Установите этот флажок, если компонент нужно включить.

Формирование области защиты

Под областью защиты подразумевается тип сообщений, которые следует проверять. По умолчанию Kaspersky CRYSTAL проверяет как входящие, так и исходящие сообщения. Если вы уверены в том, что отправляемые вами сообщения не могут содержать опасных объектов, вы можете отказаться от проверки исходящего трафика.

Чтобы отключить проверку исходящих сообщений, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **IM-Антивирус**.
4. В правой части окна в блоке **Область защиты** выберите вариант **Только входящие сообщения**.

Выбор метода проверки

Под методами проверки подразумевается проверка ссылок, содержащихся в сообщениях интернет-пейджеров, на принадлежность к списку подозрительных веб-адресов и (или) к списку фишинговых веб-адресов.

Для повышения эффективности защиты вы можете использовать *эвристический анализ* (анализ активности, которую объект производит в системе). Этот анализ позволяет обнаруживать новые вредоносные объекты, записи о которых еще не попали в базы. При эвристическом анализе любой скрипт, содержащийся в сообщении интернет-пейджера, выполняется в защищенной среде. Если активность скрипта типична для вредоносных объектов, объект с достаточной долей вероятности будет признан вредоносным или подозрительным. По умолчанию эвристический анализ включен.

- *Чтобы проверять ссылки из сообщений по базе подозрительных веб-адресов, выполните следующие действия:*

  1. Откройте главное окно программы.
  2. В верхней части окна перейдите по ссылке **Настройка**.
  3. В левой части окна выберите в разделе **Центр защиты** компонент **IM-Антивирус**.
  4. В правой части окна в блоке **Методы проверки** установите флажок **Проверять ссылки по базе подозрительных веб-адресов**.

- *Чтобы проверять ссылки из сообщений по базе фишинговых веб-адресов, выполните следующие действия:*

  1. Откройте главное окно программы.
  2. В верхней части окна перейдите по ссылке **Настройка**.
  3. В левой части окна выберите в разделе **Центр защиты** компонент **IM-Антивирус**.
  4. В правой части окна в блоке **Методы проверки** установите флажок **Проверять ссылки по базе фишинговых веб-адресов**.

- *Чтобы включить использование эвристического анализа, выполните следующие действия:*

  1. Откройте главное окно программы.
  2. В верхней части окна перейдите по ссылке **Настройка**.
  3. В левой части окна выберите в разделе **Центр защиты** компонент **IM-Антивирус**.
  4. В правой части окна в блоке **Методы проверки** установите флажок **Эвристический анализ** и задайте уровень детализации проверки.

Анти-Спам

В состав Kaspersky CRYSTAL включен компонент *Анти-Спам*, позволяющий обнаруживать нежелательную корреспонденцию (спам) и обрабатывать ее в соответствии с правилами вашего почтового клиента. Наличие этого компонента экономит время при работе с электронной почтой.

Анти-Спам в виде модуля расширения встраивается в следующие почтовые клиенты:

- Microsoft Office Outlook (на стр. 128);
- Microsoft Outlook Express (Windows Mail) (на стр. 128);
- The Bat! (на стр. 129);
- Thunderbird (на стр. 130).

Путем формирования списков запрещенных и разрешенных отправителей вы можете указать Анти-Спаму, письма с каких адресов следует считать полезными, а с каких – спамом. Считаться спамом могут также письма, адресованные не вам (см. стр. 122). Кроме того, Анти-Спам может анализировать сообщение на наличие разрешенных и запрещенных фраз, а также фраз из списка нецензурных выражений.

Чтобы Анти-Спам эффективно распознавал спам и полезную почту, его следует обучить (см. раздел «Обучение Анти-Спама» на стр. 116).

Алгоритм работы компонента

Анти-Спам использует самообучающийся алгоритм, позволяющий компоненту с течением времени более точно различать спам и полезную почту. Источником данных для алгоритма является содержимое письма.

Работа компонента Анти-Спам разделена на два этапа:

1. Применение к сообщению жестких критериев фильтрации. Эти критерии позволяют быстро определить, является ли сообщение спамом. Анти-Спам присваивает сообщению статус *спам* или *не спам*, проверка останавливается и сообщение передается для обработки почтовому клиенту (см. ниже шаги алгоритма 1–5).

2. Изучение почтовых сообщений, прошедших жесткие критерии отбора предыдущих шагов. Такие сообщения уже нельзя однозначно расценивать как спам. Поэтому Анти-Спаму приходится вычислять *вероятность* их принадлежности к спаму.

Алгоритм работы Анти-Спама состоит из следующих шагов:

1. Адрес отправителя почтового сообщения проверяется на присутствие в списках разрешенных и запрещенных отправителей.

   - Если адрес отправителя находится в списке разрешенных, сообщению присваивается статус *не спам*.

   - Если адрес отправителя находится в списке запрещенных, почтовому сообщению присваивается статус *спам*.

2. Если сообщение было отправлено с помощью Microsoft Exchange Server и проверка таких сообщений выключена, то сообщению присваивается статус *не спам*.

3. Сообщение анализируется на наличие строк из списка разрешенных фраз. Если найдена хотя бы одна строка из этого списка, сообщению присваивается статус *не спам*. По умолчанию данный шаг пропускается.

4. Сообщение анализируется на наличие строк из списка запрещенных фраз и списка нецензурных фраз. При обнаружении в сообщении слов из этих списков их весовые коэффициенты суммируются. Если сумма коэффициентов превысит 100, сообщению будет присвоен статус *спам*. По умолчанию данный шаг пропускается.

5. Если текст сообщения содержит адрес, входящий в базу фишинговых или подозрительных веб-адресов, письму присваивается статус *спам*.

6. Сообщение анализируется с помощью эвристических правил. Если в результате этого анализа в сообщении найдены признаки, характерные для спама, вероятность того, что сообщение является спамом, увеличивается.

7. Сообщение анализируется с помощью технологии GSG. При этом Анти-Спам анализирует изображения в составе почтового сообщения. Если в них найдены признаки, характерные для спама, вероятность того, что сообщение является спамом, увеличивается.

8. Анализируются вложенные в сообщение документы в формате rtf. Анти-Спам ищет во вложенных документах признаки, характерные для спама. По окончании анализа Анти-Спам вычисляет, насколько увеличилась вероятность того, что сообщение является спамом. По умолчанию технология выключена.

9. Выполняются проверки на наличие дополнительных признаков, характерных для спама. Обнаружение каждого признака увеличивает вероятность того, что проверяемое сообщение является спамом.

10. Если Анти-Спам был обучен, сообщение проверяется с помощью технологии iBayes. Самообучающийся алгоритм iBayes вычисляет вероятность того, что сообщение является спамом, на основе частоты употребления в его тексте фраз, характерных для спама.

В результате анализа сообщения определяется вероятность того, что почтовое сообщение является спамом, выражаемая значением *фактора спама*. Сообщению присваивается статус *спам* или *потенциальный спам* в зависимости от пороговых значений фактора спама (см. раздел «Регулировка пороговых значений фактора

спама» на стр. 124). Кроме того, по умолчанию для спама и потенциального спама в поле **Тема** добавляется метка **[!! SPAM]** или **[?? Probable Spam]** (см. раздел «**Добавление метки к теме сообщения**» на стр. 126). Затем сообщение обрабатывается по заданным вами правилам для почтовых клиентов (см. раздел «Настройка обработки спама почтовыми клиентами» на стр. 128).

В ЭТОМ РАЗДЕЛЕ

Включение и отключение Анти-Спама 115

Изменение и восстановление уровня безопасности 115

Обучение Анти-Спама 116

Проверка ссылок в сообщениях 119

Определение спама по фразам и адресам. Формирование списков 119

Регулировка пороговых значений фактора спама 124

Использование дополнительных признаков фильтрации спама 125

Выбор алгоритма распознавания спама 125

Добавление метки к теме сообщения 126

Фильтрация писем на сервере. Диспетчер писем 126

Исключение из проверки сообщений Microsoft Exchange Server 127

Настройка обработки спама почтовыми клиентами 128

Включение и отключение Анти-Спама

По умолчанию Анти-Спам включен и работает в оптимальном режиме. Вы можете отключить Анти-Спам при необходимости.

Чтобы включить или отключить Анти-Спам, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Анти-Спам**.
4. В правой части окна снимите флажок **Включить Анти-Спам**, если нужно отключить компонент. Установите этот флажок, если компонент нужно включить.

Изменение и восстановление уровня безопасности

В зависимости от текущих потребностей вы можете выбрать один из предустановленных уровней безопасности или настроить параметры работы Анти-Спама самостоятельно.

Настраивая параметры работы компонента, всегда можно вернуться к рекомендуемым значениям. Эти значения считаются оптимальными, рекомендованы специалистами «Лаборатории Касперского» и объединены в **Рекомендуемый** уровень безопасности.

Чтобы изменить установленный уровень безопасности Анти-Спама, выполните следующие действия:

1. Откройте главное окно программы.

2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Анти-Спам**.
4. В правой части окна в блоке **Уровень безопасности** установите нужный уровень безопасности или нажмите на кнопку **Настройка**, чтобы настроить параметры работы вручную.

При настройке вручную название уровня безопасности изменится на **Другой**.

Чтобы восстановить параметры работы Анти-Спама по умолчанию, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Анти-Спам**.
4. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **По умолчанию**.

Обучение Анти-Спама

Один из инструментов распознавания спама – самообучающийся алгоритм iBayes. В результате выполнения этого алгоритма выносится решение о присвоении сообщению того или иного статуса на основе входящих в него фраз. До начала работы алгоритма iBayes необходимо предоставить Анти-Спаму образцы строк, входящих в полезные и спам-сообщения, – то есть *обучить* его.

Существует несколько подходов к обучению Анти-Спама:

- Использование Мастера обучения (пакетное обучение). Обучение с помощью Мастера обучения предпочтительно в самом начале работы с Анти-Спамом.
- Обучение Анти-Спама на исходящих сообщениях.
- Обучение непосредственно в процессе работы с электронной почтой с помощью почтового клиента, в окне которого предусмотрены специальные кнопки и пункты меню для обучения.
- Обучение при работе с отчетами Анти-Спама.

В этом разделе

Использование Мастера обучения 116

Обучение на исходящих сообщениях 117

Использование элементов интерфейса почтового клиента 117

Добавление адреса в список разрешенных отправителей 118

Обучение с помощью отчетов 118

Использование Мастера обучения

Мастер обучения позволяет провести обучение Анти-Спама в пакетном режиме. Для этого требуется указать, какие папки учетных записей почтовых клиентов Microsoft Office Outlook и Microsoft Outlook Express (Windows Mail) содержат спам, а какие – полезную почту.

Для корректного распознавания спама необходимо произвести обучение как минимум на 50 образцах полезной почты и 50 образцах нежелательной корреспонденции. Без выполнения этих действий алгоритм iBayes работать не будет.

В целях экономии времени Мастер производит обучение только на 50 письмах в каждой выбранной папке.

Мастер состоит из последовательности окон (шагов), переключение между которыми осуществляется нажатием на кнопки **Назад** и **Далее**. Работа мастера завершается нажатием на кнопку **Завершить**. Для прекращения работы мастера на любом этапе следует нажать на кнопку **Отмена**.

Чтобы запустить мастер, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Анти-Спам**.
4. В правой части окна в блоке **Обучение Анти-Спама** нажмите на кнопку **Обучить**.

При обучении на полезных письмах адреса их отправителей автоматически добавляются в список разрешенных отправителей. Вы можете отключить эту функцию (см. раздел «Добавление адреса в список разрешенных отправителей» на стр. 118).

См. также

Что делать с большим количеством спам-сообщений 73

Обучение на исходящих сообщениях

Вы можете обучить Анти-Спам на примере 50 исходящих сообщений. После включения обучения Анти-Спам будет анализировать каждое из отправляемых вами писем, используя его в качестве образца полезного сообщения. После отправки пятидесятого сообщения обучение будет завершено.

Чтобы включить обучение Анти-Спам на исходящих сообщениях, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Анти-Спам**.
4. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Дополнительно** в блоке **Исходящие сообщения** установите флажок **Обучаться на исходящих сообщениях**.

При обучении на исходящих сообщениях адреса получателей этих сообщений автоматически добавляются в список разрешенных отправителей. Вы можете отключить эту функцию (см. раздел «Добавление адреса в список разрешенных отправителей» на стр. 118).

Использование элементов интерфейса почтового клиента

Обучение Анти-Спама в процессе непосредственной работы с электронной корреспонденцией предполагает использование специальных элементов интерфейса вашего почтового клиента.

Кнопки для обучения Анти-Спама появляются в интерфейсе почтовых клиентов Microsoft Office Outlook и Microsoft Outlook Express (Windows Mail) только после установки Kaspersky CRYSTAL.

Чтобы обучить Анти-Спам с помощью почтового клиента, выполните следующие действия:

1. Запустите почтовый клиент.
2. Выберите письмо, с помощью которого вы хотите обучить Анти-Спам.
3. В зависимости от того, каким почтовым клиентов вы пользуетесь, выполните следующие действия:
   - нажмите на кнопку **Спам** или **Не Спам** в панели инструментов Microsoft Office Outlook;
   - нажмите на кнопку **Спам** или **Не Спам** в панели инструментов Microsoft Outlook Express (Windows Mail);
   - воспользуйтесь специальными пунктами **Пометить как спам** и **Пометить как НЕ спам** в меню **Специальное** почтового клиента The Bat!;
   - воспользуйтесь кнопкой **Спам/Не спам** в панели инструментов почтового клиента Mozilla Thunderbird.

После выбора одного из перечисленных выше действий Анти-Спам проводит обучение на выбранном письме. Если вы выделите несколько писем, обучение будет происходить на всех выделенных письмах.

Если письмо отмечено как полезное, происходит добавление адреса отправителя письма в список разрешенных отправителей.

Добавление адреса в список разрешенных отправителей

При обучении Анти-Спама на полезных письмах с помощью Мастера обучения, а также при обучении непосредственно в окне почтового клиента адреса отправителей полезных писем автоматически добавляются в список разрешенных отправителей (см. раздел «Запрещенные и разрешенные отправители» на стр. 122). В этот же список добавляются адреса получателей исходящих сообщений при обучении на исходящих сообщениях.

Вы можете отключить эту функцию, чтобы список разрешенных отправителей не пополнялся автоматически в результате обучения.

Чтобы отключить добавление адреса в список разрешенных отправителей, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Анти-Спам**.
4. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Точные методы** в блоке **Считать полезными следующие сообщения** установите флажок **От разрешенных отправителей** и нажмите на кнопку **Выбрать**.

   Откроется окно **Разрешенные отправители**.
6. Снимите флажок **Добавлять адреса разрешенных отправителей при обучении Анти-Спама в почтовом клиенте**.

Обучение с помощью отчетов

Предусмотрена возможность обучать Анти-Спам на основе его отчетов, в которых отображается информация о письмах, отнесенных к категории «потенциальный спам». Обучение заключается в присвоении письмам меток **спам** или **не спам**, а также в добавлении их в списки разрешенных или запрещенных отправителей.

Чтобы провести обучение Анти-Спама на основе отчета, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Защита компьютера**.

Откроется окно **Защита компьютера**.

2. По ссылке **Отчет** перейдите к окну отчетов Kaspersky CRYSTAL.
3. В открывшемся окне на закладке **Отчет** нажмите на кнопку **Подробный отчет**.

   Откроется окно **Подробный отчет**.
4. В раскрывающемся списке в левой верхней части окна выберите компонент **Анти-Спам**.
5. В правой части окна по записи в графе **Объект** определите письма, на основе которых вы хотите обучить Анти-Спам. Для каждого из таких писем откройте контекстное меню (по правой клавише мыши) и выберите один из пунктов меню в соответствии с тем, какое действие нужно выполнить с письмом:

   - Отметить как спам;
   - Отметить как не спам;
   - Добавить в список разрешенных отправителей;
   - Добавить в список запрещенных отправителей.

Проверка ссылок в сообщениях

Анти-Спам может проверять содержащиеся в почтовых сообщениях ссылки на принадлежность к списку подозрительных веб-адресов и к списку фишинговых веб-адресов. Эти списки включены в комплект поставки Kaspersky CRYSTAL. Если в письме обнаруживается фишинговая или подозрительная ссылка, а также если элементы фишинга обнаруживаются в тексте письма, то это письмо идентифицируется как спам.

Чтобы включить проверку ссылок по базам подозрительных и фишинговых адресов, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Анти-Спам**.
4. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Точные методы** в блоке **Считать спамом следующие сообщения** установите флажки **Со ссылками из базы подозрительных веб-адресов** и **С элементами фишинга**.

Определение спама по фразам и адресам. Формирование списков

Вы можете составить списки разрешенных, запрещенных и нецензурных ключевых фраз, а также списки разрешенных и запрещенных адресов отправителей и список ваших адресов. Если эти списки используются, Анти-Спам проверяет содержимое письма на наличие в нем словосочетаний, внесенных в списки фраз, а адреса отправителя и получателей – на соответствие записям в списках адресов. Обнаружив искомые фразу или адрес, Анти-Спам идентифицирует письмо как полезное или как спам в зависимости от того, в каком из списков присутствует найденная фраза или адрес.

Спамом считаются следующие письма:

- содержащие запрещенные или нецензурные фразы с суммарным весовым коэффициентом, превышающим 100;
- отправленные с запрещенного адреса или адресованные не вам.

Полезными считаются следующие письма:

- содержащие разрешенные фразы;
- отправленные с разрешенного адреса.

Маски ключевых фраз и адресов отправителей

В списках разрешенных, запрещенных и нецензурных фраз вы можете использовать *маски фраз*. В списках разрешенных и запрещенных адресов отправителей, а также в списке доверенных адресов вы можете использовать *маски адресов*.

Маска представляет собой строку-шаблон, с которой сверяется фраза или адрес. Некоторые символы в маске используются для замены других символов: ***** заменяет любую последовательность символов, а **?** – любой один символ. Если в маске используются такие символы, то ей могут соответствовать несколько фраз или несколько адресов (см. примеры ниже).

Если символ ***** или **?** входит в состав фразы (например, *Который час?*), перед ним нужно использовать символ \, чтобы Анти-Спам корректно его распознал. Таким образом, вместо символа ***** в маске нужно использовать сочетание *****, вместо символа **?** – сочетание **\?** (например, *Который час\?*).

Примеры масок фраз:

- *Посетите наш ** – этой маске соответствует письмо, начинающееся словами *Посетите наш* и имеющее любое продолжение.

Примеры масок адресов:

- *admin@test.com* – этой маске соответствует только адрес *admin@test.com*.
- *admin@** – этой маске соответствует адрес отправителя с именем *admin*, например: *admin@test.com*, *admin@example.org.*
- **@test** – этой маске соответствует адрес любого отправителя письма с почтового домена, начинающегося с *test*, например: *admin@test.com*, *info@test.org*.
- *info.*@test.???* – этой маске соответствует адрес любого отправителя письма, имя которого начинается с *info.* и имя почтового домена которого начинается с *test.* и оканчивается последними тремя любыми символами, например: *info.product@test.com*, *info.company@test.org*, но не *info.product@test.ru*.

В этом разделе

Запрещенные и разрешенные фразы 120

Нецензурные фразы 121

Запрещенные и разрешенные отправители 122

Ваши адреса 122

Экспорт и импорт списков фраз и адресов 123

Запрещенные и разрешенные фразы

В список *запрещенных фраз* вы можете внести фразы, которые, согласно вашим наблюдениям, характерны для спама, и задать для каждой фразы весовой коэффициент. *Весовой коэффициент* позволяет указать, насколько характерна фраза для спам-писем: чем выше коэффициент, тем более вероятно, что письмо с этой фразой является спамом. Весовой коэффициент фразы может принимать значения от 0 до 100. Если сумма весовых коэффициентов всех фраз, обнаруженных в письме, превысит 100, письмо будет идентифицировано как спам.

Ключевые фразы, характерные для полезных писем, можно внести в список *разрешенных фраз*. Обнаружив такую фразу в письме, Анти-Спам идентифицирует его как полезное (не спам).

В списки запрещенных и разрешенных фраз вы можете вносить как фразы целиком, так и их маски (см. раздел «Определение спама по фразам и адресам. Формирование списков» на стр. 119).

Чтобы сформировать список запрещенных или разрешенных фраз, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Анти-Спам**.
4. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Точные методы** выполните следующие действия:
   - Если нужно сформировать список запрещенных фраз, в блоке **Считать спамом следующие сообщения** установите флажок **С запрещенными фразами** и нажмите на кнопку **Выбрать**, расположенную правее.

     Откроется окно **Список запрещенных фраз**.
   - Если нужно сформировать список разрешенных фраз, в блоке **Считать полезными следующие сообщения** установите флажок **С разрешенными фразами** и нажмите на кнопку **Выбрать**, расположенную правее.

     Откроется окно **Список разрешенных фраз**.
6. По ссылке **Добавить** откройте окно **Запрещенная фраза** (или окно **Разрешенная фраза**).
7. Введите фразу целиком или маску фразы, для запрещенной фразы укажите весовой коэффициент, а затем нажмите на кнопку **ОК**.

Чтобы в дальнейшем отказаться от использования какой-либо маски, необязательно ее удалять – достаточно в окне со списком снять флажок рядом с ней.

НЕЦЕНЗУРНЫЕ ФРАЗЫ

Специалистами «Лаборатории Касперского» сформирован список нецензурных фраз, который входит в поставку Kaspersky CRYSTAL. В списке хранятся нецензурные фразы, наличие которых в сообщении с большой долей вероятности указывает на то, что сообщение является спамом. Вы можете дополнить данный список и внести в него как фразы целиком, так и их маски (см. раздел «Определение спама по фразам и адресам. Формирование списков» на стр. 119).

Чтобы откорректировать список нецензурных фраз, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Анти-Спам**.
4. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Точные методы** в блоке **Считать спамом следующие сообщения** установите флажок **С запрещенными фразами** и нажмите на кнопку **Выбрать**.

   Откроется окно **Список запрещенных фраз**.
6. Установите флажок **Считать запрещенными нецензурные фразы** и по ссылке **нецензурные фразы** откройте окно **Соглашение**.

7. Ознакомьтесь с текстом соглашения и, если вы согласны с условиями, изложенными в окне, установите флажок в нижней части окна и нажмите на кнопку **ОК**.

   Откроется окно **Список нецензурной лексики**.

8. По ссылке **Добавить** откройте окно **Запрещенная фраза**.

9. Введите фразу целиком или маску фразы, укажите весовой коэффициент фразы и нажмите на кнопку **ОК**.

Чтобы в дальнейшем отказаться от использования какой-либо маски, необязательно ее удалять – достаточно в окне **Список нецензурной лексики** снять флажок рядом с ней.

Запрещенные и разрешенные отправители

В список *запрещенных отправителей* вы можете внести адреса отправителей, письма от которых Анти-Спам будет идентифицировать как спам. Адреса отправителей писем, от которых не ожидается спама, хранятся в списке *разрешенных отправителей*. Этот список создается автоматически во время обучения компонента Анти-Спам (см. раздел «Добавление адреса в список разрешенных отправителей» на стр. 118). Кроме того, вы можете пополнить список самостоятельно.

В списки разрешенных и запрещенных отправителей вы можете внести как адреса полностью, так и маски адресов (см. раздел «Определение спама по фразам и адресам. Формирование списков» на стр. 119).

Чтобы сформировать список запрещенных или разрешенных отправителей, выполните следующие действия:

1. Откройте главное окно программы.

2. В верхней части окна перейдите по ссылке **Настройка**.

3. В левой части окна выберите в разделе **Центр защиты** компонент **Анти-Спам**.

4. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

5. В открывшемся окне на закладке **Точные методы** выполните следующие действия:

   - Если нужно сформировать список запрещенных отправителей, в блоке **Считать спамом следующие сообщения** установите флажок **От запрещенных отправителей** и нажмите на кнопку **Выбрать**, расположенную правее.

     Откроется окно **Список запрещенных отправителей**.

   - Если нужно сформировать список разрешенных отправителей, в блоке **Считать полезными следующие сообщения** установите флажок **От разрешенных отправителей** и нажмите на кнопку **Выбрать**, расположенную правее.

     Откроется окно **Список разрешенных отправителей**.

6. По ссылке **Добавить** откройте окно **Маска адреса электронной почты**.

7. Введите маску адреса и нажмите на кнопку **ОК**.

Чтобы в дальнейшем отказаться от использования какой-либо маски, необязательно ее удалять – достаточно в окне со списком снять флажок рядом с ней.

Ваши адреса

Вы можете сформировать список ваших адресов электронной почты, чтобы Анти-Спам отмечал как спам письма, адресованные не вам.

Чтобы сформировать список ваших адресов, выполните следующие действия:

1. Откройте главное окно программы.

2. В верхней части окна перейдите по ссылке **Настройка**.

3. В левой части окна выберите в разделе **Центр защиты** компонент **Анти-Спам**.

4. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

5. В открывшемся окне на закладке **Точные методы** установите флажок **Адресованные не мне** и нажмите на кнопку **Мои адреса**.

   Откроется окно **Мои адреса**.

6. По ссылке **Добавить** откройте окно **Маска адреса электронной почты**.

7. Введите маску адреса и нажмите на кнопку **ОК**.

Чтобы в дальнейшем отказаться от использования какой-либо маски, необязательно ее удалять – достаточно в окне **Мои адреса** снять флажок рядом с ней.

ЭКСПОРТ И ИМПОРТ СПИСКОВ ФРАЗ И АДРЕСОВ

Создав списки фраз и адресов, вы можете затем многократно использовать их: например, переносить адреса в аналогичный список на другом компьютере с установленным Kaspersky CRYSTAL.

Последовательность действий при этом такова:

1. Выполните *экспорт* – скопируйте записи из списка в файл.

2. Перенесите сохраненный файл на другой компьютер (например, перешлите по почте или переместите на съемном носителе).

3. Выполните *импорт* – внесите записи из файла в аналогичный список на другом компьютере.

При экспорте списка вам будет предложено копировать только выбранный элемент списка или весь список целиком. При импорте можно добавить новые элементы в список или заменить существующий список импортируемым.

Чтобы экспортировать записи из списка, выполните следующие действия:

1. Откройте главное окно программы.

2. В верхней части окна перейдите по ссылке **Настройка**.

3. В левой части окна выберите в разделе **Центр защиты** компонент **Анти-Спам**.

4. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.

5. В открывшемся окне на закладке **Точные методы** установите флажок в строке, содержащей название списка, из которого нужно экспортировать записи, и нажмите соответствующую ему кнопку справа.

6. В открывшемся окне со списком установите флажки напротив тех записей, которые нужно включить в файл.

7. Нажмите на ссылку **Экспорт**.

   Откроется окно с предложением экспортировать только выделенные элементы. В этом окне выполните одно из следующих действий:

   - нажмите на кнопку **Да**, если в файл нужно включить только выбранные записи;

   - нажмите на кнопку **Нет**, если нужно включить список полностью..

8. В открывшемся окне укажите тип и имя сохраняемого файла и подтвердите сохранение.

Чтобы импортировать записи из файла в список, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Анти-Спам**.
4. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Точные методы** установите флажок в строке, содержащей название списка, в который нужно импортировать записи, и нажмите на кнопку справа.
6. В окне со списком перейдите по ссылке **Импорт**. Если вы импортируете список разрешенных отправителей, то откроется меню, в котором нужно выбрать пункт **Импортировать из файла**. Для остальных списков выбор пункта меню не требуется.

   Если список не пуст, откроется окно с предложением добавить импортируемые элементы. В этом окне выполните одно из следующих действий:

   - нажмите на кнопку **Да**, если нужно добавить к списку записи из файла;
   - нажмите на кнопку **Нет**, если нужно заменить существующие записи списком из файла.
7. В открывшемся окне выберите файл со списком записей, которые нужно импортировать.

Импорт списка разрешенных отправителей из адресной книги

Для адресов из списка разрешенных отправителей предусмотрена возможность импорта адресов из адресной книги Microsoft Office Outlook / Microsoft Outlook Express (Windows Mail).

Чтобы импортировать список разрешенных отправителей из адресной книги, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Анти-Спам**.
4. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Точные методы** в блоке **Считать полезными следующие сообщения** установите флажок **От разрешенных отправителей** и нажмите на кнопку **Выбрать**.

   Откроется окно **Список разрешенных отправителей**.
6. Перейдите по ссылке **Импорт**, откройте меню выбора источника и выберите в нем пункт **Импортировать из адресной книги**.
7. В открывшемся окне выберите нужную адресную книгу.

Регулировка пороговых значений фактора спама

Распознавание спама основано на использовании современных технологий фильтрации, позволяющих научить (см. раздел «Обучение Анти-Спама» на стр. 116) Анти-Спам отличать спам и потенциальный спам от полезной почты. При этом каждому отдельному элементу полезной почты или спама присваивается коэффициент.

Когда в ваш почтовый ящик поступает почтовое сообщение, то в соответствии с технологией iBayes Анти-Спам проверяет письмо на наличие элементов спама и полезной почты. Коэффициенты каждого элемента спама (полезной почты) суммируются, в результате чего вычисляется *фактор спама*. Чем больше значение фактора

спама, тем выше вероятность того, что сообщение является спамом. По умолчанию сообщение считается полезным, если фактор спама не превышает 60. Если фактор спама выше 60, то сообщение считается потенциальным спамом. Если же значение превышает 90, сообщение считается спамом. Вы можете изменить пороговые значения фактора спама.

Чтобы изменить пороговые значения фактора спама, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Анти-Спам**.
4. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Экспертные методы** в блоке **Фактор спама** отрегулируйте значения фактора спама с помощью ползунков или полей ввода с прокруткой.

Использование дополнительных признаков фильтрации спама

На результат вычисления фактора спама могут влиять дополнительные признаки сообщений: например, отсутствие адреса получателя в поле «Кому» или слишком длинная тема сообщения (более 250 символов). При наличии этих признаков в сообщении вероятность того, что оно является спамом, увеличивается. Соответственно, увеличивается значение фактора спама. Вы можете выбрать, какие из дополнительных признаков должны учитываться при анализе сообщения.

Чтобы использовать дополнительные признаки, увеличивающие фактор спама, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Анти-Спам**.
4. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Экспертные методы** нажмите на кнопку **Дополнительно**.
6. В открывшемся окне **Дополнительно** установите флажок рядом с теми признаками, которые должны дополнительно учитываться при анализе сообщения, увеличивая фактор спама.

Выбор алгоритма распознавания спама

Анализ почтовых сообщений на предмет спама осуществляется на основе использования алгоритмов распознавания:

- **Эвристический анализ**. Анти-Спам анализирует сообщения с помощью эвристических правил. Эвристический анализ используется всегда.
- **Распознавание изображений (GSG)**. Анти-Спам применяет технологию GSG для распознавания спама, приходящего в виде изображений.
- **Анализ вложенных документов в формате rtf**. Анти-Спам анализирует документы, вложенные в сообщения, на предмет наличия в них признаков спама.
- **Самообучающийся алгоритм анализа текста (iBayes)**. В основе работы алгоритма iBayes лежит анализ частоты использования в тексте сообщения слов, характерных для спама. В результате анализа сообщение определяется как полезное или спам. До начала работы алгоритма iBayes вам необходимо обучить Анти-Спам (см. раздел «Обучение Анти-Спама» на стр. 116).

Чтобы использовать / не использовать какой-либо алгоритм распознавания спама при анализе почтовых сообщений, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Анти-Спам**.
4. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Экспертные методы** в блоке **Алгоритмы распознавания** установите / снимите соответствующие флажки.

Добавление метки к теме сообщения

Анти-Спам может добавлять в поле **Тема** сообщений, которые при проверке были признаны спамом или потенциальным спамом, соответствующие метки:

- **[!! SPAM]** – для сообщений, идентифицированных как спам.
- **[?? Probable Spam]** – для сообщений, идентифицированных как потенциальный спам.

Наличие таких меток в теме сообщения может вам помочь визуально отличать спам и потенциальный спам при просмотре списков сообщений.

Чтобы Анти-Спам добавлял / не добавлял метки к теме сообщений, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Анти-Спам**.
4. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Дополнительно** в блоке **Действия** установите флажки напротив названий тех меток, которые нужно добавлять к теме сообщения. Установив флажок, вы можете изменить текст метки. Чтобы метка не добавлялась, снимите соответствующий флажок.

Фильтрация писем на сервере. Диспетчер писем

Вы можете просматривать список сообщений электронной почты на сервере, не загружая их на свой компьютер. Это позволяет отказаться от приема некоторых сообщений, что не только обеспечивает экономию времени и трафика при работе с электронной корреспонденцией, но и снижает вероятность загрузки спама и вирусов на ваш компьютер.

Для работы с письмами на сервере предназначен *Диспетчер писем*.

Окно Диспетчера писем открывается каждый раз перед получением сообщений при условии, что он активирован.

Обратите внимание, окно Диспетчера писем открывается только при получении почты по протоколу POP3. Диспетчер писем не открывается, если POP3-сервер не поддерживает просмотр заголовков электронных сообщений, или если все письма на сервере были отправлены пользователями из списка разрешенных отправителей (см. стр. 122).

Список писем на сервере отображается в центральной части окна Диспетчера писем. Выберите сообщение в списке для детального изучения его заголовка.

Просмотр заголовков может пригодиться, например, в следующей ситуации: спамеры устанавливают на компьютер вашего коллеги вредоносную программу, которая рассылает спам от его имени, пользуясь контакт-листом его почтового клиента. Вероятность того, что ваш адрес находится в контакт-листе коллеги, весьма высока, следовательно, вредоносная программа может отправить на ваш адрес множество спам-сообщений.

В данной ситуации по адресу отправителя невозможно определить, отправлено ли письмо непосредственно вашим коллегой или спамером с помощью вредоносной программы. С помощью заголовка письма можно получить более подробную информацию: когда и кем было отправлено письмо, его объем, маршрут сообщения от отправителя до вашего почтового сервера. Перечисленные данные помогут вам определить, действительно ли необходимо загружать данное письмо с сервера или его лучше удалить.

- *Чтобы использовать Диспетчер писем, выполните следующие действия:*

  1. Откройте главное окно программы.
  2. В верхней части окна перейдите по ссылке **Настройка**.
  3. В левой части окна выберите в разделе **Центр защиты** компонент **Анти-Спам**.
  4. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
  5. В открывшемся окне на закладке **Дополнительно** в блоке **Входящие сообщения** установите флажок **Открывать Диспетчер писем при получении почты по протоколу POP3**.

- *Чтобы удалить сообщения с сервера при помощи Диспетчера писем, выполните следующие действия:*

  1. В окне Диспетчера писем, которое откроется перед получением сообщения, установите флажок напротив сообщения в столбце **Удалить**.
  2. В верхней части окна нажмите на кнопку **Удалить выбранные**.

Сообщения будут удалены с сервера. При этом вы получите уведомление, которое будет помечено как **[!! SPAM]** и обработано в соответствии с правилами вашего почтового клиента (см. раздел «Настройка обработки спама почтовыми клиентами» на стр. 128).

Исключение из проверки сообщений Microsoft Exchange Server

Вы можете исключить из проверки на спам почтовые сообщения, пересылаемые в рамках внутренней сети (например, корпоративная почта). Обратите внимание, что сообщения будут считаться внутренней почтой в том случае, если в качестве почтового клиента на всех компьютерах сети используется Microsoft Office Outlook, а почтовые ящики пользователей расположены на одном Exchange-сервере либо на серверах, соединенных X400-коннекторами.

По умолчанию Анти-Спам не проверяет сообщения Microsoft Exchange Server.

- *Чтобы Анти-Спам анализировал сообщения Microsoft Exchange Server, выполните следующие действия:*

  1. Откройте главное окно программы.
  2. В верхней части окна перейдите по ссылке **Настройка**.
  3. В левой части окна выберите в разделе **Центр защиты** компонент **Анти-Спам**.
  4. В правой части окна в блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
  5. В открывшемся окне на закладке **Дополнительно** в блоке **Исключения** снимите флажок **Не проверять сообщения Microsoft Exchange Server**.

Настройка обработки спама почтовыми клиентами

Если в результате проверки выясняется, что письмо является спамом или потенциальным спамом, дальнейшие действия Анти-Спама зависят от статуса письма и от выбранного действия. По умолчанию электронные сообщения, являющиеся спамом или потенциальным спамом, модифицируются: в поле **Тема** письма добавляется метка **[!! SPAM]** или **[?? Probable Spam]** соответственно (см. раздел «Добавление метки к теме сообщения» на стр. 126).

Вы можете выбрать дополнительные действия над спамом и потенциальным спамом. В почтовых клиентах Microsoft Office Outlook и Microsoft Outlook Express (Windows Mail) для этого предусмотрены специальные модули расширения. Для почтовых клиентов The Bat! и Thunderbird вы можете настроить правила фильтрации.

В этом разделе

Microsoft Office Outlook 128

Microsoft Outlook Express (Windows Mail) 128

Создание правила обработки сообщений на спам 128

The Bat! 129

Thunderbird 130

Microsoft Office Outlook

По умолчанию почтовая корреспонденция, которая классифицируется Анти-Спамом как спам или потенциальный спам, отмечается специальными метками **[!! SPAM]** или **[?? Probable Spam]** в поле **Тема**. Если требуется дополнительная обработка сообщений после их проверки Анти-Спамом, вы можете настроить Microsoft Office Outlook. Окно настройки обработки спама открывается автоматически при первой загрузке почтового клиента после установки Kaspersky CRYSTAL. Кроме того, параметры обработки спама и потенциального спама в Microsoft Office Outlook приведены на специальной закладке **Анти-Спам** в меню **Сервис** → **Параметры**.

Microsoft Outlook Express (Windows Mail)

По умолчанию почтовая корреспонденция, которая классифицируется Анти-Спамом как спам или потенциальный спам, отмечается специальными метками **[!! SPAM]** или **[?? Probable Spam]** в поле **Тема**. Если требуется дополнительная обработка сообщений после их проверки Анти-Спамом, вы можете настроить Microsoft Outlook Express (Windows Mail).

Окно настройки обработки спама открывается при первом запуске почтового клиента после установки программы. Его также можно открыть, нажав на кнопку **Настройка**, расположенную в панели инструментов почтового клиента рядом с кнопками **Спам** и **Не Спам**.

Создание правила обработки сообщений на спам

Ниже приведена инструкция по созданию правила обработки сообщений на спам с применением Анти-Спама в почтовом клиенте Microsoft Office Outlook. Вы можете воспользоваться этой инструкцией и на ее основе создать собственное правило.

Чтобы создать правило обработки сообщений на спам, выполните следующие действия:

1. Запустите программу Microsoft Office Outlook и воспользуйтесь командой **Сервис** → **Правила и оповещения** главного меню программы. Способ вызова мастера зависит от используемой вами версии Microsoft Office Outlook. В данной справке приведено описание создания правила с помощью Microsoft Office Outlook 2003.

2. В окне **Правила и оповещения** перейдите на закладку **Правила для электронной почты** и нажмите на кнопку **Новое**. В результате будет запущен мастер создания нового правила. Его работа состоит из последовательности окон / шагов:

a. Вам предлагается выбрать создание правила «с нуля» либо по шаблону. Выберите вариант **Создать новое правило** и в качестве условия проверки выберите **Проверка сообщений после получения**. Нажмите на кнопку **Далее**.

b. В окне выбора условий отбора сообщений, не устанавливая флажков, нажмите на кнопку **Далее**. Подтвердите применение данного правила ко всем получаемым сообщениям в окне запроса подтверждения.

c. В окне выбора действий над сообщениями установите в списке действий флажок **выполнить дополнительное действие**. В нижней части окна нажмите на ссылку **дополнительное действие**. В открывшемся окне выберите из раскрывающегося списка элемент **Kaspersky Anti-Spam**, нажмите на кнопку **ОК**.

d. В окне выбора исключений из правила, не устанавливая флажков, нажмите на кнопку **Далее**.

e. В окне завершения создания правила вы можете изменить его имя (по умолчанию установлено Kaspersky Anti-Spam). Проверьте, что флажок **Включить правило** установлен и нажмите на кнопку **Готово**.

3. Новое правило по умолчанию будет добавлено первым в список правил окна **Правила и оповещения**. Переместите это правило в конец списка, если хотите, чтобы оно применялось к сообщению последним.

Все сообщения, поступающие в почтовый ящик, обрабатываются на основе правил. Очередность применения правил зависит от приоритета, который задан для каждого правила. Правила начинают применяться с начала списка: приоритет каждого последующего правила ниже, чем предыдущее. Вы можете понижать или повышать приоритет применения правила к сообщению, перемещая правило вниз или вверх в списке. Если вы не хотите, чтобы после выполнения какого-либо правила сообщение дополнительно обрабатывалось правилом Анти-Спама, в параметрах этого правила требуется установить флажок **остановить дальнейшую обработку правил** (см. Шаг 3 окна создания правил).

THE BAT!

Действия над спамом и потенциальным спамом в почтовом клиенте The Bat! определяются средствами самого клиента.

➧ *Чтобы перейти к настройке правил обработки спама в The Bat!, выполните следующие действия:*

1. В меню **Свойства** почтового клиента выберите пункт **Настройка**.

2. В дереве настройки выберите объект **Защита от спама**.

Представленные параметры защиты от спама распространяются на все установленные на компьютере модули Анти-Спама, поддерживающие работу с The Bat!.

Вам нужно определить уровень рейтинга и указать, как поступать с сообщениями, которым присвоен тот или иной рейтинг (в случае Анти-Спама – вероятность того, что письмо является спамом):

- удалять сообщения с рейтингом, превышающим указанную величину;
- перемещать сообщения с определенным рейтингом в специальную папку для спам-сообщений;
- перемещать спам-сообщения, отмеченные специальным заголовком, в папку спама;
- оставлять спам-сообщения в папке **Входящие**.

В результате обработки почтового сообщения Kaspersky CRYSTAL присваивает письму статус спама и потенциального спама на основании фактора, значение которого вы можете регулировать. В почтовом клиенте The Bat! реализован собственный алгоритм рейтинга сообщений на предмет спама, также основанный на факторе спама. Чтобы исключить расхождения между фактором спама в Kaspersky CRYSTAL и в The Bat!, всем проверенным Анти-Спамом письмам присваивается рейтинг, соответствующий статусу письма: полезная почта – 0%, потенциальный спам – 50%, спам – 100%. Таким образом, рейтинг письма в почтовом клиенте The Bat! соответствует не фактору спама, заданному в Анти-Спаме, а фактору соответствующего статуса.

Подробнее о рейтинге спама и правилах обработки см. в документации к почтовому клиенту The Bat!.

Thunderbird

По умолчанию почтовая корреспонденция, которая классифицируется Анти-Спамом как спам или потенциальный спам, отмечается специальными метками **[!! SPAM]** или **[?? Probable Spam]** в поле **Тема**. Если требуется дополнительная обработка сообщений после их проверки Анти-Спамом, вы можете настроить Thunderbird, вызвав окно настройки с помощью команды меню **Инструменты** → **Фильтры сообщений** (подробнее о работе с почтовым клиентом см. справку Mozilla Thunderbird).

Модуль расширения Анти-Спама для Thunderbird позволяет проводить обучение на письмах, полученных и отправленных с помощью этого почтового клиента, а также проверять почтовую корреспонденцию на содержание спама. Модуль встраивается в Thunderbird и перенаправляет письма компоненту Анти-Спам для их проверки при выполнении команды меню **Инструменты** → **Запустить в папке антиспам-фильтры**. Таким образом, вместо Thunderbird проверку сообщений производит Kaspersky CRYSTAL. При этом функциональность Thunderbird не изменяется.

Статус модуля расширения Анти-Спама отображается в виде значка в строке состояния Thunderbird. Серый цвет значка информирует вас о том, что в работе плагина возникла проблема, или компонент Анти-Спам отключен. Двойным щелчком мыши на значке вы можете открыть окно настройки параметров Kaspersky CRYSTAL. Чтобы перейти к настройке параметров Анти-Спама, нажмите на кнопку **Настройка** в блоке **Анти-Спам**.

Анти-Баннер

Анти-Баннер предназначен для блокирования показа баннеров на просматриваемых вами веб-страницах и в интерфейсе некоторых компьютерных программ. Рекламная информация на баннерах может отвлекать вас от дел, а загрузка баннеров увеличивает объем скачиваемого трафика.

Прежде чем отобразиться на веб-странице или в окне компьютерной программы, баннер должен быть загружен из интернета. Анти-Баннер проверяет адрес, с которого загружается баннер. Если адрес соответствует какой-либо маске из списка, включенного в поставку Kaspersky CRYSTAL, либо из составленного вами списка запрещенных адресов баннеров, Анти-Баннер блокирует баннер. Для блокирования баннеров, маски адресов которых отсутствуют в упомянутых списках, используется эвристический анализатор.

Кроме того, вы можете создать список разрешенных адресов, на основании которого показ баннеров будет разрешен.

В этом разделе

Включение и отключение Анти-Баннера 130

Выбор методов проверки 131

Формирование списков запрещенных и разрешенных адресов баннеров 131

Экспорт и импорт списков адресов 131

Включение и отключение Анти-Баннера

По умолчанию Анти-Баннер включен и работает в оптимальном режиме. Вы можете отключить Анти-Баннер при необходимости.

Чтобы включить или отключить Анти-Баннер, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Анти-Баннер**.

4. В правой части окна снимите флажок **Включить Анти-Баннер**, если нужно отключить компонент. Установите этот флажок, если компонент нужно включить.

ВЫБОР МЕТОДОВ ПРОВЕРКИ

Вы можете указать, какие из методов должен использовать Анти-Баннер для проверки адресов, с которых могут быть загружены баннеры. В дополнение к этим методам Анти-Баннер проверяет адреса баннеров на соответствие маскам из списков разрешенных и запрещенных адресов, если они используются.

Чтобы выбрать методы проверки адресов Анти-Баннером, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Анти-Баннер**.
4. В правой части окна в группе **Методы проверки** установите флажки напротив названий методов, которые нужно использовать.

ФОРМИРОВАНИЕ СПИСКОВ ЗАПРЕЩЕННЫХ И РАЗРЕШЕННЫХ АДРЕСОВ БАННЕРОВ

С помощью списков запрещенных и разрешенных адресов баннеров вы можете указать, с каких адресов следует запретить загрузку и показ баннеров, а с каких – разрешить. Составьте список из масок запрещенных адресов, и Анти-Баннер заблокирует загрузку и показ баннеров с адресов, соответствующих этим маскам. Составьте список из масок разрешенных адресов, и Анти-Баннер будет загружать и показывать баннеры с адресов, соответствующих этим маскам.

Чтобы добавить маску в список запрещенных или разрешенных адресов, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Анти-Баннер**.
4. В правой части окна в блоке **Дополнительно** установите флажок **Использовать «Черный» список адресов** (или **Использовать «Белый» список адресов**) и нажмите на кнопку **Настройка**, расположенную справа от флажка.

   Откроется окно **«Черный» список** (или **«Белый» список**).
5. По ссылке **Добавить** откройте окно **Маска адреса (URL)**.
6. Введите маску запрещенного (или разрешенного) адреса баннера и нажмите на кнопку **ОК**.

Чтобы в дальнейшем отказаться от использования какой-либо маски, необязательно ее удалять – достаточно в окне со списком снять флажок рядом с маской.

ЭКСПОРТ И ИМПОРТ СПИСКОВ АДРЕСОВ

Создав списки разрешенных и запрещенных адресов баннеров, вы можете затем многократно их использовать: например, переносить адреса баннеров в аналогичный список на другом компьютере с установленным Kaspersky CRYSTAL.

Последовательность действий при этом такова:

1. Выполните *экспорт* – скопируйте записи из списка в файл.

2. Перенесите сохраненный файл на другой компьютер (например, перешлите по почте или переместите на съемном носителе).

3. Выполните *импорт* – внесите записи из файла в аналогичный список на другом компьютере.

При экспорте списка вам будет предложено копировать только выбранный элемент списка или весь список целиком. При импорте можно добавить новые элементы в список или заменить существующий список импортируемым.

Чтобы экспортировать адреса баннеров из списка разрешенных или запрещенных адресов баннеров, выполните следующие действия:

1. Откройте главное окно программы.

2. В верхней части окна перейдите по ссылке **Настройка**.

3. В левой части окна выберите в разделе **Центр защиты** компонент **Анти-Баннер**.

4. В правой части окна в блоке **Дополнительно** нажмите на кнопку **Настройка**, расположенную в строке с названием списка, адреса из которого следует копировать в файл.

5. В открывшемся окне **«Черный» список** (или **«Белый» список**) установите флажки напротив тех адресов, которые нужно включить в файл.

6. Нажмите на кнопку **Экспорт**.

   Откроется окно с предложением экспортировать только выделенные элементы. В этом окне выполните одно из следующих действий:

   - нажмите на кнопку **Да**, если в файл нужно включить только выбранные адреса;

   - нажмите на кнопку **Нет**, если в файл нужно включить список полностью.

7. В открывшемся окне введите имя для сохраняемого файла и подтвердите сохранение.

Чтобы импортировать адреса баннеров из файла в список разрешенных или запрещенных адресов, выполните следующие действия:

1. Откройте главное окно программы.

2. В верхней части окна перейдите по ссылке **Настройка**.

3. В левой части окна выберите в разделе **Центр защиты** компонент **Анти-Баннер**.

4. В правой части окна в блоке **Дополнительно** нажмите на кнопку **Настройка**, расположенную в строке с названием списка, в который нужно добавить адреса из файла.

5. В открывшемся окне **«Черный» список** (или **«Белый» список**) нажмите на кнопку **Импорт**.

   Если список не пуст, откроется окно с предложением добавить импортируемые элементы. В этом окне выполните одно из следующих действий:

   - нажмите на кнопку **Да**, если нужно добавить к списку записи из файла;

   - нажмите на кнопку **Нет**, если нужно заменить существующие записи списком из файла.

6. В открывшемся окне выберите файл со списком записей, которые нужно импортировать.

КОНТРОЛЬ ПРОГРАММ

Контроль программ предотвращает выполнение программами опасных для системы действий, а также обеспечивает контроль доступа к ресурсам операционной системы и вашим персональным данным.

Компонент отслеживает действия, которые совершают в системе программы, установленные на компьютере, и регулирует их на основании правил Контроля программ. Эти правила регламентируют потенциально опасную активность, в том числе доступ программ к защищаемым ресурсам (файлам и папкам, ключам реестра, сетевым адресам и т. д.).

Сетевая активность программ контролируется компонентом Сетевой экран.

При первом запуске программы на компьютере компонент Контроль программ проверяет ее безопасность и помещает в одну из групп доверия. Группа доверия определяет правила, которые Kaspersky CRYSTAL будет применять для контроля активности этой программы. Правила Контроля программ представляют собой набор прав доступа к ресурсам компьютера и ограничений для различных действий программ на компьютере.

Вы можете настроить условия распределения программ по группам (см. стр. 134), переместить программу в другую группу (см. стр. 135), а также изменить правила Kaspersky CRYSTAL (см. стр. 136).

Для более эффективной работы Контроля программ рекомендуем вам принять участие в Kaspersky Security Network (см. раздел «Участие в Kaspersky Security Network» на стр. 237). Данные, полученные с помощью Kaspersky Security Network, позволяют точнее относить программы к той или иной группе доверия, а также применять оптимальные правила контроля программ.

При повторном запуске программы Контроль программ проверяет ее целостность. Если программа не была изменена, компонент применяет к ней текущие правила. Если программа была изменена, Контроль программ заново исследует ее, как при первом запуске.

Для контроля доступа программ к различным ресурсам компьютера вы можете использовать предустановленный список защищаемых ресурсов или дополнить список пользовательскими ресурсами (см. стр. 139).

В ЭТОМ РАЗДЕЛЕ

Включение и отключение Контроля программ 133

Распределение программ по группам 134

Просмотр активности программ 135

Изменение группы доверия 135

Правила Контроля программ 136

Защита ресурсов операционной системы и персональных данных 139

ВКЛЮЧЕНИЕ И ОТКЛЮЧЕНИЕ КОНТРОЛЯ ПРОГРАММ

По умолчанию Контроль программ включен и работает в режиме, разработанном специалистами «Лаборатории Касперского», но вы можете отключить его при необходимости.

Чтобы включить или отключить Контроль программ, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.

3. В левой части окна выберите в разделе **Центр защиты** компонент **Контроль программ**.

4. В правой части окна снимите флажок **Включить Контроль программ**, если нужно отключить компонент. Установите этот флажок, если компонент нужно включить.

Распределение программ по группам

При первом запуске программы на компьютере компонент Контроль программ проверяет ее безопасность и помещает в одну из групп доверия.

На первом этапе проверки программы Kaspersky CRYSTAL ищет запись о программе во внутренней базе известных программ, а затем отправляет запрос в базу Kaspersky Security Network (при наличии подключения к интернету). Если запись о программе найдена в базе, то программа помещается в группу, зарегистрированную в базе.

Программы, не представляющие опасности для системы, помещаются в группу **Доверенные**. По умолчанию в эту группу помещаются программы, имеющие цифровую подпись, а также программы, у родительского объекта которых присутствует цифровая подпись.

Вы можете отключить автоматическое помещение в группу **Доверенные** программ, содержащихся в базе Kaspersky Security Network или имеющих цифровую подпись.

Поведение программ, которые Контроль программ помещает в группу **Доверенные**, будет тем не менее контролироваться компонентом Проактивная защита.

Для распределения по группам неизвестных программ (отсутствующих в базе Kaspersky Security Network и не имеющих цифровой подписи) по умолчанию Kaspersky CRYSTAL использует эвристический анализ. В процессе этого анализа определяется рейтинг опасности программы, на основании которого программа помещается в ту или иную группу. Вместо эвристического анализа вы можете указать группу, в которую Kaspersky CRYSTAL будет автоматически помещать все неизвестные программы.

По умолчанию Контроль программ проверяет программу в течение 30 секунд. Если по истечении этого времени определение рейтинга опасности не завершено, программа помещается в группу **Слабые ограничения**, а определение рейтинга опасности продолжается в фоновом режиме. Затем программа помещается в окончательную группу. Вы можете изменить время, которое отводится для проверки запускаемых программ. Если вы уверены, что все запускаемые на вашем компьютере программы не представляют угрозы для его безопасности, то время, отведенное для проверки, можно уменьшить. Если же вы устанавливаете на компьютер программное обеспечение, в безопасности которого не уверены, время проверки рекомендуется увеличить.

Если рейтинг опасности программы высок, то Kaspersky CRYSTAL уведомит вас об этом и предложит выбрать группу, в которую следует поместить эту программу. Уведомление содержит статистику использования этой программы участниками Kaspersky Security Network. На основании этой статистики, а также зная историю появления программы на вашем компьютере, вы можете принять более объективное решение о том, в какую группу следует поместить эту программу.

- *Чтобы отключить автоматическое помещение в группу **Доверенные** тех программ, которые содержатся в базе Kaspersky Security Network или имеют цифровую подпись, выполните следующие действия:*

  1. Откройте главное окно программы.

  2. В верхней части окна перейдите по ссылке **Настройка**.

  3. В левой части окна выберите в разделе **Центр защиты** компонент **Контроль программ**.

  4. В правой части окна в блоке **Доверенные программы** снимите флажки **Имеющие цифровую подпись** и **Содержащиеся в базе Kaspersky Security Network**.

- *Чтобы использовать эвристический анализ для распределения по группам неизвестных программ, выполните следующие действия:*

  1. Откройте главное окно программы.

2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Контроль программ**.
4. В правой части окна в блоке **Доверенные программы** выберите вариант **Использовать эвристический анализ для определения группы**.

Чтобы изменить время определения группы программы, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Контроль программ**.
4. В правой части окна в блоке **Дополнительно** отредактируйте значение параметра **Максимальное время определения группы программы**.

Чтобы помещать все неизвестные программы в указанную группу, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Контроль программ**.
4. В правой части окна в блоке **Доверенные программы** выберите вариант **Автоматически помещать в группу** и выберите нужную группу из раскрывающегося списка.

Просмотр активности программ

Вы можете просмотреть информацию обо всех программах, используемых на вашем компьютере, и обо всех процессах, выполняемых в данный момент.

Чтобы просмотреть активность программ, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Защита компьютера**.

   Откроется окно **Защита компьютера**.
2. В левой части окна выберите раздел **Контроль программ**.
3. Перейдите по ссылке **Активность программ**, расположенной в правой части окна.
4. В открывшемся окне **Активность программ** в списке **Категория** выберите нужную категорию программ.

Изменение группы доверия

При первом запуске программы Kaspersky CRYSTAL автоматически помещает ее в ту или иную группу (см. раздел «Распределение программ по группам» на стр. 134). При необходимости вы можете вручную переместить программу в другую группу.

Специалисты «Лаборатории Касперского» не рекомендуют перемещать программы из группы, назначенной автоматически, в другую. Вместо этого при необходимости измените правила для отдельной программы (см. раздел «Изменение правил программы» на стр. 137).

Чтобы переместить программу в другую группу, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Защита компьютера**.

Откроется окно **Защита компьютера**.

2. В левой части окна выберите раздел **Контроль программ**.
3. Перейдите по ссылке **Активность программ**, расположенной в правой части окна.
4. В открывшемся окне **Активность программ** в списке **Категория** выберите нужную категорию программ.
5. По правой клавише мыши откройте контекстное меню нужной программы и выберите в нем пункт **Переместить в группу → <название группы>**.

Чтобы вернуть программу в группу по умолчанию, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Защита компьютера**.

   Откроется окно **Защита компьютера**.
2. В левой части окна выберите раздел **Контроль программ**.
3. Перейдите по ссылке **Активность программ**, расположенной в правой части окна.
4. В открывшемся окне **Активность программ** в списке **Категория** выберите нужную категорию программ.
5. По правой клавише мыши откройте контекстное меню для нужной программы и выберите пункт **Переместить в группу → Восстановить группу по умолчанию**.

Правила Контроля программ

Правила Контроля программ представляют собой набор прав доступа к ресурсам компьютера и ограничений для различных действий программ на компьютере.

По умолчанию для контроля программы применяются правила группы доверия, в которую Kaspersky CRYSTAL поместил программу при первом ее запуске. Правила групп разработаны специалистами «Лаборатории Касперского» для оптимального контроля активности программ. При необходимости вы можете изменить эти правила, а также настроить их на уровне отдельной программы. Правила программы имеют более высокий приоритет, чем правила группы.

В этом разделе

Изменение правил группы 136

Изменение правил программы 137

Создание сетевого правила программы 137

Настройка исключений 138

Наследование ограничений родительского процесса 138

Удаление правил для программ 139

Изменение правил группы

По умолчанию для разных групп доверия заданы оптимальные наборы прав доступа к ресурсам компьютера. Вы можете изменить предустановленные правила группы.

Чтобы изменить правила группы, выполните следующие действия:

1. Откройте главное окно программы.

2. В верхней части окна перейдите по ссылке **Настройка**.

3. В левой части окна выберите в разделе **Центр защиты** компонент **Контроль программ**.

4. В правой части окна нажмите на кнопку **Настройка правил**.

5. В открывшемся окне **Правила групп программ** выберите нужную группу.

6. В открывшемся окне на закладке **Правила** измените права доступа для нужной категории ресурсов.

ИЗМЕНЕНИЕ ПРАВИЛ ПРОГРАММЫ

Во время первого запуска программы Контроль программ определяет ее статус и помещает в соответствующую группу. Далее компонент регистрирует действия, совершаемые этой программой в системе, и регулирует ее деятельность, исходя из того, к какой группе она относятся. При обращении программы к ресурсу компонент проверяет наличие у программы нужных прав доступа и выполняет действие, заданное правилом. Вы можете изменить правило, которое было сформировано для программы при определении ее статуса и помещении программы в соответствующую группу.

Чтобы изменить правило для программы, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Защита компьютера**.

   Откроется окно **Защита компьютера**.

2. В левой части окна выберите раздел **Контроль программ**.

3. Перейдите по ссылке **Активность программ**, расположенной в правой части окна.

4. В открывшемся окне **Активность программ** в списке **Категория** выберите нужную категорию программ.

5. Для нужной программы в графе **Группа** нажмите левой клавишей мыши на ссылку с названием группы программы.

6. В раскрывшемся меню выберите пункт **Параметры пользователя**.

7. В открывшемся окне на закладке **Правила** измените права доступа для нужной категории ресурсов.

СОЗДАНИЕ СЕТЕВОГО ПРАВИЛА ПРОГРАММЫ

При необходимости особым образом обрабатывать доступ программы к определенным сетевым сервисам, вы можете создать сетевое правило.

Чтобы создать правило, регулирующее сетевую активность программы, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Защита компьютера**.

   Откроется окно **Защита компьютера**.

2. В левой части окна выберите раздел **Контроль программ**.

3. Перейдите по ссылке **Активность программ**, расположенной в правой части окна.

4. В открывшемся окне **Активность программ** в списке **Категория** выберите нужную категорию программ

5. Для нужной программы в графе **Группа** нажмите левой клавишей мыши на ссылку с названием группы программы.

6. В раскрывшемся меню выберите пункт **Параметры пользователя**.

7. В открывшемся окне на закладке **Правила** в раскрывающемся списке выберите категорию **Сетевые правила** и перейдите по ссылке **Добавить**.

8. В открывшемся окне **Сетевое правило** задайте параметры сетевого правила.

9. Назначьте приоритет нового правила, переместив его вверх или вниз по списку, нажимая на кнопки **Вверх** и **Вниз**.

   После создания правила вы можете внести изменения в его параметры или удалить его с помощью кнопок в верхней части закладки. Чтобы отключить правило, снимите флажок рядом с его названием.

Настройка исключений

При создании правила для программы по умолчанию Kaspersky CRYSTAL контролирует любые действия программы: доступ к файлам и папкам, доступ к среде исполнения и доступ к сети. Вы можете исключить из проверки определенные действия программ.

Чтобы исключить действия программы из проверки, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Защита компьютера**.

   Откроется окно **Защита компьютера**.

2. В левой части окна выберите раздел **Контроль программ**.

3. Перейдите по ссылке **Активность программ**, расположенной в правой части окна.

4. В открывшемся окне **Активность программ** в списке **Категория** выберите нужную категорию программ

5. Для нужной программы в графе **Группа** нажмите левой клавишей мыши на ссылку с названием группы программы.

6. В раскрывшемся меню выберите пункт **Параметры пользователя**.

7. В открывшемся окне на закладке **Исключения** установите флажки, соответствующие исключаемым действиям. При исключении проверки сетевого трафика программы настройте дополнительные параметры исключения.

   Все исключения, созданные в правилах для программ, доступны в окне настройки параметров программы в разделе **Угрозы и исключения**.

Наследование ограничений родительского процесса

Инициатором запуска программы может быть как пользователь, так и другая запущенная программа. Если инициатором запуска служит другая программа, образуется последовательность запуска, состоящая из родительских и дочерних программ.

Когда программа пытается получить доступ к защищаемому ресурсу, Контроль программ анализирует права всех родительских процессов этой программы на доступ к ресурсу. При этом выполняется правило минимального приоритета: при сравнении прав доступа программы и родительского процесса к активности программы будут применены права доступа с минимальным приоритетом.

Приоритет прав доступа:

1. Разрешить. Данные права доступа имеют высший приоритет.

2. Запросить пользователя.

3. Блокировать. Данные права доступа имеют низший приоритет.

Этот механизм предотвращает использование доверенных программ недоверенными или ограниченными в правах программами с целью выполнения привилегированных действий.

Если активность программы блокируется по причине недостатка прав у одного из родительских процессов, вы можете изменить эти права (см. раздел «Изменение правил программы» на стр. 137) или отключить наследование ограничений родительского процесса.

Вносить изменения в права родительского процесса и отключать наследование ограничений следует только в том случае, если вы абсолютно уверены, что активность процесса не угрожает безопасности системы!

- *Чтобы отключить наследование ограничений родительского процесса, выполните следующие действия:*

1. Откройте главное окно программы и нажмите на кнопку **Защита компьютера**.

   Откроется окно **Защита компьютера**.

2. В левой части окна выберите раздел **Контроль программ**.

3. Перейдите по ссылке **Активность программ**, расположенной в правой части окна.

4. В открывшемся окне **Активность программ** в списке **Категория** выберите нужную категорию программ

5. Для нужной программы в графе **Группа** нажмите левой клавишей мыши на ссылку с названием группы программы.

6. В раскрывшемся меню выберите пункт **Параметры пользователя**.

7. В открывшемся окне на закладке **Правила** снимите флажок **Наследовать ограничения родительского процесса (программы)**.

УДАЛЕНИЕ ПРАВИЛ ДЛЯ ПРОГРАММ

По умолчанию правила программ, которые не запускались в течение 60 дней, автоматически удаляются. Вы можете изменить время хранения правил для неиспользуемых программ или отключить автоматическое удаление.

- *Чтобы задать время хранения правил программ, выполните следующие действия:*

1. Откройте главное окно программы и перейдите по ссылке **Настройка** в верхней части окна.

2. В открывшемся окне в разделе **Центр защиты** выберите компонент **Контроль программ**.

3. Для выбранного компонента в блоке **Дополнительно** установите флажок **Удалять правила для программ, не запускавшихся более** и укажите нужное количество дней.

- *Чтобы отключить автоматическое удаление правил для неиспользуемых программ, выполните следующие действия:*

1. Откройте главное окно программы и перейдите по ссылке **Настройка** в верхней части окна.

2. В открывшемся окне в разделе **Центр защиты** выберите компонент **Контроль программ**.

3. Для выбранного компонента в блоке **Дополнительно** снимите флажок **Удалять правила для программ, не запускавшихся более**.

ЗАЩИТА РЕСУРСОВ ОПЕРАЦИОННОЙ СИСТЕМЫ И ПЕРСОНАЛЬНЫХ ДАННЫХ

Контроль программ управляет правами программ на совершение действий над различными категориями ресурсов операционной системы и персональных данных.

Специалисты «Лаборатории Касперского» выделили предустановленные категории защищаемых ресурсов. Изменять этот список нельзя. Однако вы можете дополнить этот список пользовательскими категориями и (или) отдельными ресурсами, а также отказаться от контроля выбранных ресурсов.

- *Чтобы добавить защищаемые персональные данные, выполните следующие действия:*

1. Откройте главное окно программы и перейдите по ссылке **Настройка** в верхней части окна.
2. В открывшемся окне в разделе **Центр защиты** выберите компонент **Контроль программ**.
3. Для выбранного компонента нажмите на кнопку **Настройка**.
4. В открывшемся окне на закладке **Персональные данные** в раскрывающемся списке **Категория** выберите нужную категорию персональных данных и откройте окно для добавления ресурсов, перейдя по ссылке **Добавить**.
5. В открывшемся окне **Пользовательский ресурс** нажмите на кнопку **Обзор** и укажите необходимые данные в зависимости от добавляемого ресурса.

После добавления ресурса его можно изменить или удалить с помощью одноименных кнопок в верхней части закладки. Чтобы отказаться от контроля ресурса или категории, снимите флажок рядом с ним.

- *Чтобы создать категорию защищаемых персональных данных, выполните следующие действия:*

1. Откройте главное окно программы и перейдите по ссылке **Настройка** в верхней части окна.
2. В открывшемся окне в разделе **Центр защиты** выберите компонент **Контроль программ**.
3. Для выбранного компонента нажмите на кнопку **Настройка**.
4. В открывшемся окне на закладке **Персональные данные** откройте окно для добавления ресурсов, перейдя по ссылке **Добавить категорию**.
5. В открывшемся окне **Категория пользовательских ресурсов** введите название новой категории ресурсов.

- *Чтобы добавить защищаемые параметры и ресурсы операционной системы, выполните следующие действия:*

1. Откройте главное окно программы и перейдите по ссылке **Настройка** в верхней части окна.
2. В открывшемся окне в разделе **Центр защиты** выберите компонент **Контроль программ**.
3. Для выбранного компонента нажмите на кнопку **Настройка**.
4. В открывшемся окне на закладке **Операционная система** в раскрывающемся списке **Категория** выберите нужную категорию объектов операционной системы и откройте окно для добавления ресурсов, перейдя по ссылке **Добавить**.

После добавления ресурса его можно изменить или удалить с помощью одноименных кнопок в верхней части закладки. Чтобы отказаться от контроля ресурса или категории, снимите флажок рядом с ним.

Проактивная защита

Проактивная защита обеспечивает защиту от новых угроз, информация о которых отсутствует в базах Kaspersky CRYSTAL.

Превентивные технологии, на которых построена Проактивная защита, позволяют избежать потери времени и обезвредить новую угрозу еще до того, как она нанесет вред вашему компьютеру. В отличие от реактивных технологий, выполняющих анализ на основании записей баз Kaspersky CRYSTAL, превентивные технологии распознают новую угрозу на вашем компьютере по последовательности действий, производимых некоторой программой. Если в результате анализа активности последовательность действий программы вызывает подозрение, Kaspersky CRYSTAL блокирует активность этой программы.

Например, обнаружив такие действия, как самокопирование программы на сетевые ресурсы, в каталог автозапуска и системный реестр, можно с большой долей вероятности предположить, что эта программа –

червь. К опасным последовательностям действий относятся также попытки изменения файла HOSTS, скрытая установка драйверов и т. д. Вы можете отказаться от контроля той или иной опасной активности или изменить правила контроля (см. стр. 142) для нее.

В отличие от Контроля программ, Проактивная защита реагирует именно на определенную последовательность действий программы. Анализ активности производится для всех программ, в том числе и для выделенных в группу **Доверенные** компонентом Контроль программ (на стр. 133).

Вы можете сформировать группу доверенных программ (см. стр. 141) для Проактивной защиты. Уведомления об активности таких программ отображаться не будут.

Если компьютер работает под управлением операционных систем Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista, Microsoft Windows Vista x64, Microsoft Windows 7 или Microsoft Windows 7 x64, то будут контролироваться не все события. Это связано с особенностями перечисленных операционных систем. Так, например, не в полном объеме будут контролироваться отправка данных посредством доверенных программ и подозрительная активность в системе.

В ЭТОМ РАЗДЕЛЕ

Включение и отключение Проактивной защиты 141

Формирование группы доверенных программ 141

Использование списка опасной активности 142

Изменение правила контроля опасной активности 142

Откат действий вредоносной программы 143

Включение и отключение Проактивной защиты

По умолчанию Проактивная защита включена и работает в оптимальном режиме. Вы можете отключить Проактивную защиту при необходимости.

Чтобы включить или отключить Проактивную защиту, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Проактивная защита**.
4. В правой части окна снимите флажок **Включить Проактивную защиту**, если нужно отключить компонент. Установите этот флажок, если компонент нужно включить.

Формирование группы доверенных программ

Программы, которым компонент Контроль программ присвоил статус **Доверенные**, не представляют опасности для системы. Однако их активность также контролируется Проактивной защитой.

Вы можете сформировать группу доверенных программ, активность которых не будет проверяться Проактивной защитой. По умолчанию к числу доверенных относятся программы, имеющие проверенную цифровую подпись, и программы, содержащиеся в базе Kaspersky Security Network.

Чтобы изменить параметры формирования группы доверенных программ, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Проактивная защита**.
4. В правой части окна в блоке **Доверенные программы** установите флажки рядом с нужными параметрами.

Использование списка опасной активности

Список действий, относящихся к опасной активности, отредактировать нельзя. При этом вы можете отказаться от контроля той или иной опасной активности.

Чтобы отказаться от контроля той или иной опасной активности, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Проактивная защита**.
4. В правой части окна нажмите на кнопку **Настройка**.
5. В открывшемся окне **Проактивная защита** снимите флажок, установленный рядом с названием того вида активности, от контроля которого необходимо отказаться.

Изменение правила контроля опасной активности

Действия программ, классифицируемые как опасная активность, отредактировать нельзя. Вы можете выполнить следующие действия:

- отказаться от контроля той или иной активности (см. стр. 142);
- составить список исключений, перечислив программы, активность которых вы не считаете опасной;
- изменить правило, в соответствии с которым действует Проактивная защита при обнаружении опасной активности.

Чтобы изменить правило, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Проактивная защита**.
4. В правой части окна нажмите на кнопку **Настройка**.
5. В открывшемся окне **Проактивная защита** в графе **Событие** выберите нужное событие, для которого необходимо изменить правило.
6. Для выбранного события, используя ссылки в блоке **Описание правила**, задайте необходимые параметры. Например:
   a. Перейдите по ссылке с установленным действием и в открывшемся окне **Выбор действия** выберите нужное действие из предложенных.

b. Нажмите на ссылку с установленным временным интервалом (задается не для всех видов активности) и в открывшемся окне **Обнаружение скрытых процессов** задайте интервал, согласно которому будет проводиться проверка на обнаружение скрытых процессов.

c. Перейдите по ссылке **Вкл. / Выкл.**, чтобы указать необходимость формирования отчета о выполненной операции.

ОТКАТ ДЕЙСТВИЙ ВРЕДОНОСНОЙ ПРОГРАММЫ

Проактивная защита позволяет выполнить откат вредоносной активности в системе.

По умолчанию при работе Kaspersky CRYSTAL в автоматическом режиме откат действий вредоносной программы выполняется автоматически при обнаружении вредоносной активности компонентом Проактивная защита. В интерактивном режиме работы (см. стр. 54) вы можете изменить действие, которое нужно выполнять при обнаружении вредоносной активности.

Процедура отката действий вредоносной программы затрагивает ограниченный набор данных. Она не оказывает негативного влияния на работу операционной системы и целостность информации на вашем компьютере.

Чтобы настроить откат действий, произведенных вредоносной программой, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Проактивная защита**.
4. В правой части окна в блоке **Дополнительно** выберите нужный вариант реакции на действия вредоносной программы.

ЗАЩИТА СЕТИ

Различные компоненты защиты, инструменты и параметры настройки Kaspersky CRYSTAL в комплексе обеспечивают безопасность и контроль вашей работы в сети.

Следующие разделы содержат подробную информацию о принципах работы и настройке Сетевого экрана, Защиты от сетевых атак, мониторинге сетевой активности, проверке защищенных соединений, параметрах прокси-сервера, контроле сетевых портов.

В ЭТОМ РАЗДЕЛЕ

Сетевой экран 144

Защита от сетевых атак 147

Проверка защищенных соединений 150

Мониторинг сети 152

Настройка параметров прокси-сервера 152

Формирование списка контролируемых портов 152

Сетевой экран

Сетевой экран обеспечивает безопасность вашей работы в локальных сетях и интернете.

Компонент фильтрует всю сетевую активность в соответствии с сетевыми правилами контроля программ. Сетевое правило представляет собой действие, которое Сетевой экран совершает при обнаружении попытки соединения с определенным статусом. Статус присваивается каждому сетевому соединению и определяется заданными параметрами: направлением и протоколом передачи данных, адресами и портами, с которыми происходит соединение.

Сетевой экран анализирует параметры сетей, к которым вы подключаете компьютер. Если программа работает в интерактивном режиме, при первом подключении Сетевой экран запрашивает у вас статус подключенной сети. Если интерактивный режим выключен, Сетевой экран определяет статус, ориентируясь на тип сети, диапазоны адресов и другие характеристики. Вы можете изменить статус сетевого соединения вручную.

В этом разделе

Включение и отключение Сетевого экрана 144

Изменение статуса сети 144

Расширение диапазона адресов сети 145

Работа с правилами Сетевого экрана 145

Настройка уведомлений об изменениях сети 146

Дополнительные параметры работы Сетевого экрана 147

Включение и отключение Сетевого экрана

По умолчанию Сетевой экран включен и работает в оптимальном режиме. При необходимости вы можете отключить Сетевой экран.

Чтобы включить или отключить Сетевой экран, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Сетевой экран**.
4. В правой части окна снимите флажок **Включить Сетевой экран**, если нужно отключить компонент. Установите этот флажок, если компонент нужно включить.

Изменение статуса сети

От статуса сетевого соединения зависит набор правил, применяемых для фильтрации сетевой активности данного соединения. При необходимости вы можете изменить статус сети.

Чтобы изменить статус сетевого соединения, выполните следующие действия:

1. Откройте главное окно программы и перейдите по ссылке **Настройка** в верхней части окна.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Сетевой экран**.
3. Для выбранного компонента нажмите на кнопку **Настройка**.
4. В открывшемся окне на закладке **Сети** выберите активное сетевое соединение и перейдите по ссылке **Изменить**.

5. В открывшемся окне на закладке **Свойства** выберите нужный статус из раскрывающегося списка.

РАСШИРЕНИЕ ДИАПАЗОНА АДРЕСОВ СЕТИ

Каждой сети соответствует один или несколько диапазонов IP-адресов. Если вы подключаетесь к сети, доступ к подсетям которой осуществляется через маршрутизатор, вы можете вручную добавить доступные через него подсети.

Пример: Вы подключаетесь к сети одного из офисов вашей компании и хотите, чтобы правила фильтрации для офиса, к которому вы подключены напрямую, и для офисов, доступных через сеть, были одинаковыми.

Узнайте у администратора сети диапазоны адресов сетей этих офисов и добавьте их.

Чтобы расширить диапазон адресов сети, выполните следующие действия:

1. Откройте главное окно программы и перейдите по ссылке **Настройка** в верхней части окна.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Сетевой экран**.
3. Для выбранного компонента нажмите на кнопку **Настройка**.
4. В открывшемся окне на закладке **Сети** выберите активное сетевое соединение и перейдите по ссылке **Изменить**.
5. В открывшемся окне на закладке **Свойства** в блоке **Дополнительные подсети** перейдите по ссылке **Добавить**.
6. В открывшемся окне **IP-адрес** задайте IP-адрес или маску адресов.

РАБОТА С ПРАВИЛАМИ СЕТЕВОГО ЭКРАНА

Сетевой экран работает на основе правил двух видов:

- *Пакетные правила.* Используются для ввода ограничений на пакеты независимо от программы. Чаще всего такие правила ограничивают входящую сетевую активность по определенным портам протоколов TCP и UDP и подвергают фильтрации ICMP-сообщения.
- *Правила программ*. Используются для ввода ограничений сетевой активности конкретной программы. Такие правила позволяют тонко настраивать фильтрацию активности, например, когда определенный тип сетевых соединений запрещен для одних программ, но разрешен для других.

Пакетные правила имеют более высокий приоритет, чем правила программ. Если для одного и того же вида сетевой активности заданы и пакетные правила, и правила программ, то эта сетевая активность будет обрабатываться по пакетным правилам. Кроме того, вы можете установить для каждого правила приоритет выполнения.

СОЗДАНИЕ ПАКЕТНОГО ПРАВИЛА

Пакетные правила состоят из набора условий и действий над пакетами, которые выполняются при соблюдении заданных условий.

При создании пакетных правил помните, что они имеют приоритет перед правилами для программ.

Чтобы создать пакетное правило, выполните следующие действия:

1. Откройте главное окно программы и перейдите по ссылке **Настройка** в верхней части окна.
2. В левой части окна выберите в разделе **Центр защиты** компонент **Сетевой экран**.
3. Для выбранного компонента нажмите на кнопку **Настройка**.
4. В открывшемся окне на закладке **Правила фильтрации** выберите блок **Пакетные правила** и перейдите по ссылке **Добавить**.

5. В открывшемся окне **Сетевое правило** задайте нужные параметры и нажмите на кнопку **ОК**.

6. Назначьте приоритет нового правила, переместив его вверх или вниз по списку с помощью ссылок **Вверх** и **Вниз**.

   После создания правила вы можете внести изменения в его параметры или удалить его с помощью ссылок в нижней части закладки. Чтобы отключить правило, снимите флажок рядом с его названием.

Изменение правил группы

Аналогично компоненту Контроль программ (на стр. 133), по умолчанию Сетевой экран применяет для фильтрации сетевой активности программы правила группы, в которую эта программа помещена.

Сетевые правила группы доверия определяют, какими правами доступа к различным сетям будут обладать программы, помещенные в эту группу. Вы можете изменить предустановленные сетевые правила группы.

Чтобы изменить сетевое правило группы, выполните следующие действия:

1. Откройте главное окно программы и перейдите по ссылке **Настройка** в верхней части окна.

2. В левой части окна выберите в разделе **Центр защиты** компонент **Сетевой экран**.

3. Для выбранного компонента нажмите на кнопку **Настройка правил**.

4. В открывшемся окне выберите группу, по правой клавише мыши откройте контекстное меню для сети и выберите в нем нужное значение: **Разрешить**, **Запретить** или **Запросить действие**.

Изменение правил программы

Вы можете создавать сетевые правила для отдельных программ. Сетевые правила программы имеют более высокий приоритет, чем сетевые правила группы.

При необходимости вы можете создавать сетевые правила программ (см. стр. 137) с помощью компонента Контроль программ.

Чтобы создать правило для программы, выполните следующие действия:

1. Откройте главное окно программы и перейдите по ссылке **Настройка** в верхней части окна.

2. В левой части окна выберите в разделе **Центр защиты** компонент **Сетевой экран**.

3. Для выбранного компонента нажмите на кнопку **Настройка**.

4. В открывшемся окне на закладке **Правила фильтрации** выберите группу правил для программы и перейдите по ссылке **Добавить**.

5. В открывшемся окне **Сетевое правило** задайте параметры сетевого правила.

6. Назначьте приоритет нового правила, переместив его вверх или вниз по списку с помощью ссылок **Вверх** и **Вниз**.

   После создания правила вы можете внести изменения в его параметры или удалить его с помощью ссылок в нижней части закладки. Чтобы отключить правило, снимите флажок рядом с его названием.

Настройка уведомлений об изменениях сети

Параметры сетевых соединений могут меняться в ходе работы. Вы можете получать уведомления об изменениях параметров.

Чтобы настроить уведомления об изменениях параметров сетевого соединения, выполните следующие действия:

1. Откройте главное окно программы и перейдите по ссылке **Настройка** в верхней части окна.

2. В левой части окна выберите в разделе **Центр защиты** компонент **Сетевой экран**.

3. Для выбранного компонента нажмите на кнопку **Настройка**.

4. В открывшемся окне на закладке **Сети** выберите активное сетевое соединение и перейдите по ссылке **Изменить**.

5. В открывшемся окне на закладке **Дополнительно** установите флажки для тех событий, о которых вы хотите получать уведомления.

ДОПОЛНИТЕЛЬНЫЕ ПАРАМЕТРЫ РАБОТЫ СЕТЕВОГО ЭКРАНА

Вы можете задать дополнительные параметры работы Сетевого экрана, такие как разрешение активного режима FTP, блокирование соединения, если нет возможности запроса действия (не загружен интерфейс программы), а также работа до полной остановки системы.

По умолчанию все параметры включены.

Чтобы задать дополнительные параметры работы Сетевого экрана, выполните следующие действия:

1. Откройте главное окно программы и перейдите по ссылке **Настройка** в верхней части окна.

2. В левой части окна выберите в разделе **Центр защиты** компонент **Сетевой экран**.

3. Для выбранного компонента нажмите на кнопку **Настройка**.

4. В открывшемся окне на закладке **Правила фильтрации** нажмите на кнопку **Дополнительно**.

5. В открывшемся окне **Дополнительно** установите / снимите флажки рядом с нужными параметрами.

ЗАЩИТА ОТ СЕТЕВЫХ АТАК

Защита от сетевых атак отслеживает во входящем трафике активность, характерную для сетевых атак. Обнаружив попытку атаки на ваш компьютер, Kaspersky CRYSTAL блокирует любую сетевую активность атакующего компьютера в отношении вашего компьютера.

По умолчанию блокирование происходит на один час. Вы можете изменить параметры блокирования (см. стр. 149). На экран выводится уведомление о том, что была произведена попытка сетевой атаки с указанием информации об атакующем компьютере. Описания известных в настоящее время сетевых атак (см. раздел «Виды обнаруживаемых сетевых атак» на стр. 147) и методов борьбы с ними приведены в базах Kaspersky CRYSTAL. Пополнение списка атак, обнаруживаемых Защитой от сетевых атак, выполняется в процессе обновления (см. раздел «Обновление» на стр. 87) баз.

В ЭТОМ РАЗДЕЛЕ

Виды обнаруживаемых сетевых атак 147

Включение и отключение Защиты от сетевых атак 149

Изменение параметров блокирования 149

ВИДЫ ОБНАРУЖИВАЕМЫХ СЕТЕВЫХ АТАК

В настоящее время существует множество различных видов сетевых атак. Эти атаки используют уязвимости операционной системы, а также иного установленного программного обеспечения системного и прикладного характера.

Чтобы своевременно обеспечивать безопасность компьютера, важно знать, какого рода сетевые атаки могут ему угрожать. Известные сетевые атаки можно условно разделить на три большие группы:

- *Сканирование портов* – этот вид угроз сам по себе не является атакой, но обычно предшествует ей, поскольку это один из основных способов получить сведения об удаленном компьютере. Данный способ заключается в сканировании UDP- / TCP-портов, используемых сетевыми сервисами на интересующем злоумышленника компьютере, для выяснения их состояния (закрытые или открытые порты).

  Сканирование портов позволяет понять, какие типы атак на данную систему могут оказаться удачными, а какие нет. Кроме того, полученная в результате сканирования информация («слепок» системы) даст злоумышленнику представление о типе операционной системы на удаленном компьютере. Это еще более ограничивает круг потенциальных атак и, соответственно, время, затрачиваемое на их проведение, а также позволяет использовать специфические для данной операционной системы уязвимости.

- *DoS-атаки*, или атаки, вызывающие отказ в обслуживании, – это атаки, в результате которых атакуемая система приводится в нестабильное либо полностью нерабочее состояние. Последствиями такого типа атак может стать отсутствие возможности использовать информационные ресурсы, на которые они направлены (например, невозможность доступа в интернет).

  Существует два основных типа DoS-атак:

  - отправка компьютеру-жертве специально сформированных пакетов, не ожидаемых этим компьютером, что приводит к перезагрузке или остановке системы;

  - отправка компьютеру-жертве большого количества пакетов в единицу времени, которые этот компьютер не в состоянии обработать, что приводит к исчерпанию ресурсов системы.

  Яркими примерами данной группы атак могут служить следующие:

  - Атака *Ping of death* – состоит в посылке ICMP-пакета, размер которого превышает допустимое значение в 64 КБ. Эта атака может привести к аварийному завершению работы некоторых операционных систем.

  - Атака *Land* – заключается в передаче на открытый порт вашего компьютера запроса на установление соединения с самим собой. Атака приводит к зацикливанию компьютера, в результате чего сильно возрастает загрузка процессора, а кроме того, возможно аварийное завершение работы некоторых операционных систем.

  - Атака *ICMP Flood* – заключается в отправке на ваш компьютер большого количества ICMP-пакетов. Атака приводит к тому, что компьютер вынужден отвечать на каждый поступивший пакет, в результате чего сильно возрастает загрузка процессора.

  - Атака *SYN Flood* – заключается в отправке на ваш компьютер большого количества запросов на установку соединения. Система резервирует определенные ресурсы для каждого из таких соединений, в результате чего полностью расходует свои ресурсы и перестает реагировать на другие попытки соединения.

- *Атаки-вторжения*, целью которых является «захват» системы. Это самый опасный тип атак, поскольку в случае их успешного выполнения система полностью переходит под контроль злоумышленника.

  Данный тип атак применяется, когда злоумышленнику необходимо получить конфиденциальную информацию с удаленного компьютера (например, номера кредитных карт, пароли) либо просто закрепиться в системе для последующего использования ее вычислительных ресурсов в своих целях (использование захваченной системы в зомби-сетях либо как плацдарма для новых атак).

  В эту группу входит самое большое количество атак. Их можно разделить на три подгруппы в зависимости от установленной на компьютер пользователя операционной системы: атаки на Microsoft Windows, атаки на Unix, а также общая группа для сетевых сервисов, использующихся в обеих операционных системах.

  Наиболее распространенные виды атак, использующих сетевые сервисы операционной системы:

  - *Атаки на переполнение буфера*. Переполнение буфера возникает из-за отсутствия контроля (либо в случае его недостаточности) при работе с массивами данных. Это один из самых старых типов уязвимостей; он наиболее прост для эксплуатации злоумышленником.

- *Атаки, основанные на ошибках форматных строк*. Ошибки форматных строк возникают из-за недостаточного контроля значений входных параметров функций форматного ввода-вывода типа *printf()*, *fprintf()*, *scanf()* и прочих из стандартной библиотеки языка Си. Если подобная уязвимость присутствует в программном обеспечении, то злоумышленник, имеющий возможность посылать специальным образом сформированные запросы, может получить полный контроль над системой.

  Система обнаружения вторжений автоматически анализирует и предотвращает использование подобных уязвимостей в наиболее распространенных сетевых сервисах (FTP, POP3, IMAP), если они функционируют на компьютере пользователя.

- *Атаки, ориентированные на компьютеры с установленной операционной системой Microsoft Windows,* основаны на использовании уязвимостей установленного на компьютере программного обеспечения (например, таких программ, как Microsoft SQL Server, Microsoft Internet Explorer, Messenger, а также системных компонентов, доступных по сети, – DCom, SMB, Wins, LSASS, IIS5).

Кроме того, частными случаями атак-вторжений можно назвать использование различного вида вредоносных скриптов, в том числе скриптов, обрабатываемых Microsoft Internet Explorer, а также разновидности червя Helkern. Суть атаки последнего типа заключается в отправке на удаленный компьютер UDP-пакета специального вида, способного выполнить вредоносный код.

ВКЛЮЧЕНИЕ И ОТКЛЮЧЕНИЕ ЗАЩИТЫ ОТ СЕТЕВЫХ АТАК

По умолчанию Защита от сетевых атак включена и работает в оптимальном режиме. Вы можете отключить Защиту от сетевых атак при необходимости.

Чтобы включить или отключить Защиту от сетевых атак, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Защита от сетевых атак**.
4. В правой части окна снимите флажок **Включить Защиту от сетевых атак**, если нужно отключить компонент. Установите этот флажок, если компонент нужно включить.

ИЗМЕНЕНИЕ ПАРАМЕТРОВ БЛОКИРОВАНИЯ

По умолчанию Защита от сетевых атак блокирует активность атакующего компьютера в течение часа. Вы можете отменить блокирование выбранного компьютера или изменить время блокирования.

Чтобы изменить время блокирования атакующего компьютера, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** компонент **Защита от сетевых атак**.
4. В правой части окна установите флажок **Добавить атакующий компьютер в список блокирования на** и задайте время блокирования.

Чтобы отменить блокирование атакующего компьютера, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Защита компьютера**.

   Откроется окно **Защита компьютера**.

2. В левой части окна выберите **Центр защиты**.
3. В правой части окна в разделе **Работа в сети** по ссылке **Мониторинг сети** откройте окно **Мониторинг сети**.

4. На закладке **Заблокированные компьютеры** выберите заблокированный компьютер и разблокируйте его с помощью ссылки **Разблокировать**.

Проверка защищенных соединений

Соединение с использованием протоколов SSL/TLS обеспечивает защиту канала обмена данными в интернете. Протоколы SSL/TLS позволяют идентифицировать обменивающиеся данными стороны на основе электронных сертификатов, шифровать передаваемые данные и обеспечивать их целостность в процессе передачи.

Эти особенности протокола используются злоумышленниками для распространения вредоносных программ, поскольку большинство антивирусных продуктов не проверяет SSL/TLS-трафик.

Kaspersky CRYSTAL реализует проверку защищенных соединений с помощью сертификата «Лаборатории Касперского».

Если при соединении с сервером обнаружится некорректный сертификат (например, при его подмене злоумышленником), на экран будет выведено уведомление с предложением принять или отвергнуть сертификат.

Если вы уверены в том, что соединение с веб-сайтом всегда безопасно, несмотря на некорректный сертификат, вы можете добавить веб-сайт в список доверенных адресов. Kaspersky CRYSTAL в дальнейшем не будет проверять защищенное соединение с этим веб-сайтом.

Чтобы включить проверку защищенных соединений, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** подраздел **Сеть**.
4. В правой части окна установите флажок **Проверять защищенные соединения** и нажмите на кнопку **Установить сертификат**.
5. В открывшемся окне нажмите на кнопку **Установить сертификат**. Будет запущен мастер, следуя указаниям которого вы установите сертификат.

Автоматическая установка сертификата выполняется только при работе с браузером Microsoft Internet Explorer. Для проверки защищенных соединений в браузерах Mozilla Firefox и Opera установите сертификат «Лаборатории Касперского» вручную.

Проверка защищенных соединений в Mozilla Firefox

Браузер Mozilla Firefox не использует хранилище сертификатов Microsoft Windows. Для проверки SSL-соединений при использовании Firefox необходимо установить сертификат «Лаборатории Касперского» вручную.

Чтобы установить сертификат «Лаборатории Касперского», выполните следующие действия:

1. В меню браузера выберите пункт **Инструменты** → **Настройка**.
2. В открывшемся окне выберите раздел **Дополнительно**.
3. В блоке **Сертификаты** выберите закладку **Безопасность** и нажмите на кнопку **Просмотр сертификатов**.
4. В открывшемся окне выберите закладку **Центры сертификации** и нажмите на кнопку **Восстановить**.
5. В открывшемся окне выберите файл сертификата «Лаборатории Касперского». Путь к файлу сертификата «Лаборатории Касперского»: *%AllUsersProfile%\Application Data\Kaspersky Lab\AVP9\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

6. В открывшемся окне установите флажки, чтобы выбрать действия, для проверки которых будет применяться установленный сертификат. Для просмотра информации о сертификате воспользуйтесь кнопкой **Просмотр**.

Чтобы установить сертификат «Лаборатории Касперского» для Mozilla Firefox версии 3.x, выполните следующие действия:

1. В меню браузера выберите пункт **Инструменты** → **Настройка**.
2. В открывшемся окне выберите раздел **Дополнительно**.
3. На закладке **Шифрование** нажмите на кнопку **Просмотр сертификатов**.
4. В открывшемся окне выберите закладку **Центры сертификации** и нажмите на кнопку **Импортировать**.
5. В открывшемся окне выберите файл сертификата «Лаборатории Касперского». Путь к файлу сертификата «Лаборатории Касперского»: *%AllUsersProfile%\Application Data\Kaspersky Lab\AVP9\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.
6. В открывшемся окне установите флажки, чтобы выбрать действия, для проверки которых будет применяться установленный сертификат. Для просмотра информации о сертификате воспользуйтесь кнопкой **Просмотреть**.

Если ваш компьютер работает под управлением операционной системы Microsoft Windows Vista, то путь к файлу сертификата «Лаборатории Касперского» будет следующим: *%AllUsersProfile%\Kaspersky Lab\AVP9\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

ПРОВЕРКА ЗАЩИЩЕННЫХ СОЕДИНЕНИЙ В OPERA

Браузер Opera не использует хранилище сертификатов Microsoft Windows. Для проверки SSL-соединений при пользовании Opera необходимо установить сертификат «Лаборатории Касперского» вручную.

Чтобы установить сертификат «Лаборатории Касперского», выполните следующие действия:

1. В меню браузера выберите пункт **Инструменты** → **Настройка**.
2. В открывшемся окне выберите раздел **Дополнительно**.
3. В левой части окна выберите закладку **Безопасность** и нажмите на кнопку **Управление сертификатами**.
4. В открывшемся окне выберите закладку **Поставщики** и нажмите на кнопку **Импорт**.
5. В открывшемся окне выберите файл сертификата «Лаборатории Касперского». Путь к файлу сертификата «Лаборатории Касперского»: *%AllUsersProfile%\Application Data\Kaspersky Lab\AVP9\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.
6. В открывшемся окне нажмите на кнопку **Установить**. Сертификат «Лаборатории Касперского» будет установлен. Для просмотра информации о сертификате и выбора действий, при которых будет использоваться сертификат, выберите сертификат в списке и нажмите на кнопку **Просмотреть**.

Чтобы установить сертификат «Лаборатории Касперского» для Opera версии 9.x, выполните следующие действия:

1. В меню браузера выберите пункт **Инструменты** → **Настройка**.
2. В открывшемся окне выберите раздел **Дополнительно**.
3. В левой части окна выберите закладку **Безопасность** и нажмите на кнопку **Управление сертификатами**.

4. В открывшемся окне выберите закладку **Центры сертификации** и нажмите на кнопку **Импорт**.

5. В открывшемся окне выберите файл сертификата «Лаборатории Касперского». Путь к файлу сертификата «Лаборатории Касперского»: *%AllUsersProfile%\Application Data\Kaspersky Lab\AVP9\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

6. В открывшемся окне нажмите на кнопку **Установить**. Сертификат «Лаборатории Касперского» будет установлен.

Если ваш компьютер работает под управлением операционной системы Microsoft Windows Vista, то путь к файлу сертификата «Лаборатории Касперского» будет следующим: *%AllUsersProfile%\Kaspersky Lab\AVP9\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

Мониторинг сети

Мониторинг сети – это инструмент, предназначенный для просмотра информации о сетевой активности в реальном времени.

Чтобы запустить мониторинг сети, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Защита компьютера**.

   Откроется окно **Защита компьютера**.

2. В левой части окна выберите **Центр защиты**.

3. По ссылке **Мониторинг сети** откройте окно **Мониторинг сети**, в котором представлена информация о сетевой активности.

Настройка параметров прокси-сервера

Если выход в интернет осуществляется через прокси-сервер, может возникнуть необходимость настроить параметры подключения к нему. Kaspersky CRYSTAL использует эти параметры в работе некоторых компонентов защиты, а также для обновления баз и программных модулей.

Если в вашей сети установлен прокси-сервер, который использует нестандартный порт, необходимо добавить этот порт в список контролируемых портов (см. раздел «Формирование списка контролируемых портов» на стр. 152).

Чтобы настроить параметры прокси-сервера, выполните следующие действия:

1. Откройте главное окно программы.

2. В верхней части окна перейдите по ссылке **Настройка**.

3. В левой части окна выберите в разделе **Общие параметры** подраздел **Прокси-сервер**.

4. Установите флажок **Использовать прокси-сервер** и отредактируйте параметры подключения к прокси-серверу.

Формирование списка контролируемых портов

При работе таких компонентов защиты, как Почтовый Антивирус, Анти-Спам (см. стр. 113), Веб-Антивирус (на стр. 105) и IM-Антивирус, контролируются потоки данных, передаваемые по определенным протоколам и проходящие через определенные открытые TCP-порты вашего компьютера. Так, например, Почтовый Антивирус

анализирует информацию, передаваемую по SMTP-протоколу, а Веб-Антивирус – по протоколам HTTP, HTTPS и FTP.

Вы можете включить контроль всех или только выбранных сетевых портов. При контроле выбранных портов можно сформировать список программ, для которых требуется контроль всех портов. Рекомендуется включить в этот список программы, которые принимают или передают данные по протоколу FTP.

Чтобы добавить порт в список контролируемых портов, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** подраздел **Сеть**.
4. В правой части окна нажмите на кнопку **Выбрать**.

   Откроется окно **Сетевые порты**.
5. По ссылке **Добавить**, расположенной под списком портов в верхней части окна, откройте окно **Сетевой порт** и введите номер и описание порта.

Чтобы исключить порт из списка контролируемых портов, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** подраздел **Сеть**.
4. В правой части окна нажмите на кнопку **Выбрать**.

   Откроется окно **Сетевые порты**.
5. В списке портов в верхней части окна снимите флажок рядом с описанием порта, который нужно исключить.

Чтобы сформировать список программ, для которых необходимо контролировать все порты, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** подраздел **Сеть**.
4. В правой части окна нажмите на кнопку **Выбрать**.

   Откроется окно **Сетевые порты**.
5. Установите флажок **Контролировать все порты для указанных программ** и в списке программ, расположенном ниже, установите флажки напротив названий программ, для которых нужно контролировать все порты.
6. Если программа отсутствует в списке, добавьте ее следующим образом:

   a. Чтобы выбрать способ добавления программы в список, откройте меню по ссылке **Добавить**, расположенной под списком программ, и выберите в меню один из пунктов:

      - Выберите пункт **Обзор**, чтобы указать местонахождение исполняемого файла программы. После выбора исполняемого файла откроется окно **Программа**.

- Выберите пункт **Программы**, чтобы выбрать одну из программ, работающих в данный момент. После выбора программы откроется окно **Программа**.

7. В окне **Программа** введите описание для выбранной программы.

Доверенная зона

Доверенная зона – это сформированный пользователем перечень объектов, которые не контролируются программой в процессе работы. Иначе говоря, это набор исключений из защиты Kaspersky CRYSTAL.

Доверенная зона формируется на основе списка доверенных программ (см. раздел «Формирование списка доверенных программ» на стр. 155) и правил исключений (см. раздел «Создание правил исключений» на стр. 155) в зависимости от особенностей объектов, с которыми вы работаете, а также от программ, установленных на компьютере. Включение объектов в доверенную зону может потребоваться, например, если Kaspersky CRYSTAL блокирует доступ к какому-либо объекту или программе, в то время как вы уверены, что данный объект / программа абсолютно безвредны.

Например, если вы считаете объекты, используемые стандартной программой Microsoft Windows Блокнот, безопасными и не требующими проверки, то есть доверяете этой программе, добавьте программу Блокнот в список доверенных программ, чтобы исключить проверку объектов, используемых данным процессом.

Кроме того, некоторые действия, классифицируемые как опасные, могут быть безопасны в рамках функциональности ряда программ. Так, перехват текста, вводимого вами с клавиатуры, – штатное действие программ автоматического переключения раскладок клавиатуры (например, Punto Switcher). Чтобы учесть специфику таких программ и отключить контроль их активности, рекомендуется добавить их в список доверенных.

При добавлении программы в список доверенных не будет контролироваться файловая и сетевая активность этой программы (в том числе и подозрительная), а также ее обращения к системному реестру. В то же время исполняемый файл и процесс доверенной программы по-прежнему будут проверяться на вирусы. Для полного исключения программы из проверки следует пользоваться правилами исключений.

Исключение доверенных программ из проверки позволяет избежать проблемы совместимости Kaspersky CRYSTAL с другими программами (например, проблемы двойной проверки сетевого трафика стороннего компьютера Kaspersky CRYSTAL и другой антивирусной программой), а также увеличить производительность компьютера, что особенно важно при использовании серверных программ.

В свою очередь, правила исключений доверенной зоны обеспечивают возможность работы с легальными программами, которые могут быть использованы злоумышленниками для нанесения вреда компьютеру или данным пользователя. Такие программы сами по себе не имеют вредоносных функций, но они могут быть использованы в качестве вспомогательного компонента вредоносной программы. К этой категории относятся программы удаленного администрирования, IRC-клиенты, FTP-серверы, различные утилиты для остановки процессов или сокрытия их работы, клавиатурные шпионы, программы вскрытия паролей, программы автоматического дозвона на платные веб-сайты и другие. В результате работы Kaspersky CRYSTAL такие программы могут быть заблокированы. Чтобы избежать блокирования, для используемых программ можно настроить правила исключения из проверки.

Правило исключения – это набор условий, при которых объект не будет проверяться Kaspersky CRYSTAL. Во всех остальных случаях проверка данного объекта будет осуществляться всеми компонентами защиты в соответствии с установленными для них параметрами защиты.

Правила исключений доверенной зоны могут использоваться некоторыми компонентами программы (например, Файловым Антивирусом (см. раздел «Файловый Антивирус» на стр. 93), Почтовым Антивирусом (см. раздел «Почтовый Антивирус» на стр. 99), Веб-Антивирусом (см. раздел «Веб-Антивирус» на стр. 105)), а также при выполнении задач проверки на вирусы.

В ЭТОМ РАЗДЕЛЕ

Формирование списка доверенных программ 155

Создание правил исключений 155

ФОРМИРОВАНИЕ СПИСКА ДОВЕРЕННЫХ ПРОГРАММ

По умолчанию Kaspersky CRYSTAL проверяет объекты, открываемые, запускаемые или сохраняемые любым программным процессом, а также контролирует активность всех программ и создаваемый ими сетевой трафик. При добавлении программы в список доверенных Kaspersky CRYSTAL исключает ее из проверки.

Чтобы добавить программу в список доверенных, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** подраздел **Угрозы и исключения**.
4. В правой части окна в блоке **Исключения** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Доверенные программы** по ссылке **Добавить** откройте меню выбора программы и выберите в меню один из пунктов:
   - Выберите пункт **Обзор**, чтобы указать местонахождение исполняемого файла программы. После выбора исполняемого файла откроется окно **Исключения для программ**.
   - Выберите пункт **Программы**, чтобы выбрать одну из программ, работающих в данный момент. После выбора программы откроется окно **Исключения для программ**.
6. В открывшемся окне **Исключения для программ** установите флажки для тех видов активности программы, которые не нужно проверять.

Вы можете изменить параметры проверки программы или удалить ее из списка с помощью одноименных ссылок в нижней части списка. Чтобы исключить программу из списка, не удаляя ее, снимите флажок рядом с программой.

СОЗДАНИЕ ПРАВИЛ ИСКЛЮЧЕНИЙ

Если вы используете в своей работе программы, классифицируемые Kaspersky CRYSTAL как легальные программы, которые могут быть использованы злоумышленником для нанесения вреда компьютеру или данным пользователя, рекомендуем вам настроить для них правила исключений.

Чтобы создать правило исключения, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** подраздел **Угрозы и исключения**.
4. В правой части окна в блоке **Исключения** нажмите на кнопку **Настройка**.
5. В открывшемся окне на закладке **Правила исключений** перейдите по ссылке **Добавить**.
6. В открывшемся окне **Правило исключения** задайте параметры правила исключения.

Безопасная среда исполнения программ

Виртуализация представляет собой безопасную, изолированную от основной операционной системы среду для запуска программ, в безопасности которых вы не уверены.

При работе в Безопасной среде реальные объекты операционной системы не подвергаются изменениям. Поэтому, даже если вы запускаете в Безопасной среде зараженную программу, все ее действия будут ограничены виртуальной средой и не окажут воздействия на операционную систему.

Запуск интернет-браузеров в безопасной среде обеспечивает безопасность просмотра веб-ресурсов, в том числе защиту от проникновения на компьютер вредоносных программ и защиту пользовательских данных от несанкционированного изменения и удаления, а также возможность удаления всех объектов, накопленных за сеанс работы в сети Интернет: временные файлы, cookies, история посещения веб-страниц и т. п. Microsoft Internet Explorer включен в список программ, запускаемых в безопасной среде, по умолчанию.

Запуск программы (см. раздел «Запуск программы в безопасной среде» на стр. 157) в безопасной среде осуществляется в соответствии с выбранным режимом. Для быстрого запуска программ в безопасной среде предусмотрена возможность создания ярлыков.

Чтобы при работе в обычной среде были доступны файлы, сохраненные или измененные в безопасной среде, следует пользоваться специально созданной для этого общей папкой безопасной среды, доступной как в безопасной, так и в обычной среде. Файлы, размещенные в этой папке не будут удалены в случае очистки безопасной среды.

На компьютерах под управлением Microsoft Windows XP x64 безопасная среда исполнения программ полностью недоступна.

На компьютерах под управлением Microsoft Windows Vista x64 и Microsoft Windows 7 x64 функциональность некоторых программ при работе в безопасной среде ограничена. При запуске таких программ на экран будет выведено соответствующее сообщение, если установлены уведомления (см. стр. 235) о событии **Функциональность программы в безопасной среде ограничена**.

В этом разделе

Запуск программы в безопасной среде 157

Формирование списка программ для запуска в безопасной среде 158

Создание ярлыка для запуска программ 159

Очистка данных безопасной среды 159

Использование общей папки 160

Запуск программы в безопасной среде

Если для программы не установлен режим **Всегда запускать в безопасной среде**, запуск программы в безопасной среде может осуществляться следующими способами:

- из контекстного меню Microsoft Windows;
- из **главного окна Kaspersky CRYSTAL** (см. стр. 39);
- с помощью ранее созданного ярлыка (см. раздел «Создание ярлыка для запуска программ» на стр. 159).

Если для программы установлен режим **Всегда запускать в безопасной среде**, то программа будет запускаться в безопасной среде независимо от способа запуска.

Программы, запущенные в безопасной среде, обозначены зеленой рамкой вокруг окна программы, а также выделены зеленым цветом в списке программ, контролируемых Контролем программ (см. раздел «Контроль программ» на стр. 133).

Установку программ, с которыми в дальнейшем планируете работать в безопасной среде, рекомендуется производить в обычной среде Microsoft Windows.

- *Чтобы запустить программу в безопасной среде из контекстного меню Microsoft Windows, выполните следующие действия:*

  1. По правой клавише мыши откройте контекстное меню для выбранного объекта: ярлыка или исполняемого файла программы.
  2. В раскрывшемся меню выберите пункт **Запустить в безопасной среде**.

- *Чтобы запустить программу в безопасной среде из главного окна Kaspersky CRYSTAL, выполните следующие действия:*

  1. Откройте главное окно программы и нажмите на кнопку **Защита компьютера**.
  2. В открывшемся окне перейдите в раздел **Контроль программ**.
  3. В нижней части окна в поле **Программы, запускаемые в безопасной среде** откройте контекстное меню для нужной программы и выберите пункт **Запустить**.

- *Чтобы запустить программу в безопасной среде с помощью ярлыка, выполните следующие действия:*

  1. Откройте папку, в которой вы создали ярлык.
  2. Запустите программу двойным щелчком мыши на ее ярлыке.

Формирование списка программ для запуска в безопасной среде

В окне **Защита компьютера** (см. стр. 41) можно сформировать список программ для запуска в безопасной среде. Список представлен в разделе **Контроль программ**.

Если вы добавляете в список программу, которая позволяет работать сразу с несколькими своими копиями (например, Windows Internet Explorer), то после добавления в список каждая ее новая копия будет работать в безопасной среде. При добавлении в список программы, которая позволяет пользоваться только одной своей копией, ее необходимо будет перезапустить после добавления.

При добавлении программы в список запускаемых в безопасной среде ей можно назначить режим **Всегда запускать в безопасной среде**. Это означает, что программа будет запускаться в безопасной среде независимо от способа ее запуска: с помощью стандартных средств Microsoft Windows или средствами Kaspersky CRYSTAL.

Не рекомендуется использовать режим **Всегда запускать в безопасной среде** для системных программ и утилит, так как это может привести к некорректной работе операционной системы.

- *Чтобы добавить программу в список для запуска в безопасной среде, выполните следующие действия:*

  1. Откройте главное окно программы и нажмите на кнопку **Защита компьютера**.
  2. В открывшемся окне перейдите в раздел **Контроль программ**.
  3. В нижней части окна в поле **Программы, запускаемые в безопасной среде** по ссылке **Добавить** откройте меню.
  4. В раскрывшемся меню выберите нужную программу. При выборе пункта **Обзор** открывается окно, в котором необходимо указать путь к исполняемому файлу. При выборе пункта **Программы** открывается

список программ, работающих в данный момент. После этого значок программы будет добавлен в список.

Чтобы удалить программу из списка запускаемых в безопасной среде, выберите ее в списке и воспользуйтесь ссылкой **Удалить**.

- *Чтобы программа всегда запускалась в безопасной среде, независимо от способа запуска, выполните следующие действия:*

1. Откройте главное окно программы и нажмите на кнопку **Защита компьютера**.
2. В открывшемся окне перейдите в раздел **Контроль программ**.
3. В нижней части окна в поле **Программы, запускаемые в безопасной среде** откройте контекстное меню для нужной программы и выберите пункт **Всегда запускать в безопасной среде**.

   Рядом с пунктом в меню будет отображен флажок ✔.

СОЗДАНИЕ ЯРЛЫКА ДЛЯ ЗАПУСКА ПРОГРАММ

Для быстрого запуска программ в безопасной среде в Kaspersky CRYSTAL предусмотрена возможность создания ярлыков. Это позволяет запускать нужную программу в безопасной среде, не открывая главного окна программы или контекстного меню Microsoft Windows.

- *Чтобы создать ярлык для запуска программы в безопасной среде, выполните следующие действия:*

1. Откройте главное окно программы и нажмите на кнопку **Защита компьютера**.
2. В открывшемся окне перейдите в раздел **Контроль программ**.
3. В нижней части окна в поле **Программы, запускаемые в безопасной среде** откройте контекстное меню для нужной программы и выберите пункт **Создать ярлык**.
4. В открывшемся окне укажите путь для сохранения ярлыка и его имя. По умолчанию ярлык создается в папке *Мой компьютер* текущего пользователя компьютера с именем, соответствующим процессу программы.

ОЧИСТКА ДАННЫХ БЕЗОПАСНОЙ СРЕДЫ

При запуске программы в безопасной среде все изменения, являющиеся следствием работы программы, производятся только в рамках безопасной среды. По умолчанию при следующем запуске программы все произведенные изменения и сохраненные файлы снова будут доступны в течение сеанса работы в безопасной среде.

Если в данных, сохраненных в безопасной среде, больше нет необходимости или нужно вернуть для всех запускаемых программ текущие параметры в обычной среде Microsoft Windows, используйте очистку безопасной среды.

Если вы не хотите, чтобы для какой-либо программы произведенные изменения были доступны при следующем запуске в безопасной среде, вы можете установить для нее режим **Очищать данные безопасной среды по завершении**. Это означает, что изменения, произведенные за сеанс работы с программой, будут удаляться автоматически по завершении работы программы.

Перед очисткой данных, сохраненных в безопасной среде, следует убедиться в том, что вся информация, которая может понадобиться вам для дальнейшей работы, сохранена в общую папку. В противном случае данные будут удалены без возможности восстановления.

- *Чтобы очистить данные безопасной среды, выполните следующие действия:*

1. Откройте главное окно программы и нажмите на кнопку **Защита компьютера**.

2. В открывшемся окне перейдите в раздел **Контроль программ**.

3. В нижней части окна в поле **Программы, запускаемые в безопасной среде** воспользуйтесь ссылкой **Очистить**.

4. В открывшемся окне подтвердите очистку данных.

Чтобы данные безопасной среды очищались каждый раз по завершении работы программы, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Защита компьютера**.

2. В открывшемся окне перейдите в раздел **Контроль программ**.

3. В нижней части окна в поле **Программы, запускаемые в безопасной среде** откройте контекстное меню для нужной программы и выберите пункт **Очищать данные безопасной среды по завершении**.

   Рядом с пунктом в меню будет отображен флажок ✓ и на значке программы в списке запускаемых в безопасной среде появится значок  .

   Чтобы отменить очистку данных безопасной среды по завершении работы программы, выберите этот пункт повторно.

Использование общей папки

При работе в безопасной среде все изменения, являющиеся следствием работы программы, производятся только в рамках безопасной среды и не сказываются на обычной среде. Таким образом файлы, сохраняемые в безопасной среде не попадают в обычную среду.

Чтобы файлы, с которыми пользователь работал в безопасной среде, были доступны в обычной среде, в Kaspersky CRYSTAL предусмотрена возможность использования *Общей папки безопасной среды*. Все файлы, сохраненные в эту папку при работе в безопасной среде, будут доступны в обычной среде.

Общая папка представляет собой папку на жестком диске, которая создается при установке Kaspersky CRYSTAL.

Общая папка создается в папке *%AllUsersProfile%\Application Data\Kaspersky Lab\SandboxShared* при установке программы, и ее расположение изменять нельзя.

В проводнике Microsoft Windows общая папка обозначена значком  . К папке также можно перейти из главного окна Kaspersky CRYSTAL.

Чтобы открыть общую папку из главного окна Kaspersky CRYSTAL, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Защита компьютера**.

2. В открывшемся окне перейдите в раздел **Контроль программ**.

3. Нажмите на ссылку **Общая папка**. Папка будет открыта в стандартном окне Проводника Microsoft Windows.

Карантин и резервное хранилище

Карантин – это специальное хранилище, в которое помещаются объекты, возможно зараженные вирусами. *Возможно зараженные объекты* **–** это объекты, подозреваемые на заражение вирусами или их модификациями.

Возможно зараженный объект может быть обнаружен и помещен на карантин в процессе проверки на вирусы, а также Файловым Антивирусом, Почтовым Антивирусом и Проактивной защитой.

Объекты помещаются на карантин в следующих случаях:

- Код объекта похож на известную угрозу, но частично изменен, или напоминает по структуре вредоносную программу, однако не зафиксирован в базе. В этом случае объекты помещаются на карантин в результате эвристического анализа в ходе работы Файлового Антивируса и Почтового Антивируса, а также в процессе проверки на вирусы. Механизм эвристического анализа редко приводит к ложным срабатываниям.

- Последовательность совершаемых объектом действий является подозрительной. В этом случае объекты помещаются на карантин в результате анализа их поведения компонентом Проактивная защита.

При помещении объекта на карантин выполняется его перемещение, а не копирование: объект удаляется с диска или из почтового сообщения и сохраняется в карантинном каталоге. Файлы на карантине хранятся в специальном формате и не представляют опасности.

Резервное хранилище предназначено для хранения резервных копий зараженных объектов, которые не удалось вылечить на момент обнаружения.

После очередного обновления баз программы возможна ситуация, когда Kaspersky CRYSTAL сможет однозначно определить угрозу и обезвредить ее. По этой причине программа проверяет объекты на карантине после каждого обновления (см. стр. 91).

В ЭТОМ РАЗДЕЛЕ

Хранение объектов карантина и резервного хранилища 161

Работа с объектами на карантине 162

ХРАНЕНИЕ ОБЪЕКТОВ КАРАНТИНА И РЕЗЕРВНОГО ХРАНИЛИЩА

По умолчанию максимальный срок хранения объектов составляет 30 дней. По истечении этого времени объекты удаляются. Вы можете отменить ограничение по времени или изменить максимальный срок хранения объектов.

Кроме того, вы можете указать максимальный размер карантина и резервного хранилища. При достижении максимального размера содержимое карантина и резервного хранилища заменяется новыми объектами. По умолчанию ограничение максимального размера выключено.

Чтобы настроить максимальный срок хранения объектов, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Общие параметры** подраздел **Отчеты и хранилища**.
4. В правой части окна установите флажок **Хранить объекты не более** и укажите максимальный срок хранения объектов на карантине.

Чтобы настроить максимальный размер карантина и резервного хранилища, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Общие параметры** подраздел **Отчеты и хранилища**.
4. В правой части окна установите флажок **Максимальный размер** и укажите максимальный размер карантина и резервного хранилища.

Работа с объектами на карантине

Карантин Kaspersky CRYSTAL позволяет выполнять следующие операции:

- помещать на карантин файлы, подозреваемые вами на присутствие вируса;
- проверять и лечить все возможно зараженные объекты карантина, используя текущую версию баз Kaspersky CRYSTAL;
- восстанавливать файлы в указанную папку или в исходные папки, откуда они были перенесены на карантин (по умолчанию);
- удалять любой объект карантина или группу объектов;
- отправлять объекты карантина на исследование в «Лабораторию Касперского».

Поместить объект на карантин можно двумя способами:

- с помощью ссылки **Поместить на карантин** в окне **Состояние защиты**;
- с помощью контекстного меню объекта.

Чтобы поместить объект на карантин из окна Состояние защиты, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Защита компьютера**.
2. По ссылке **Карантин**, расположенной в верхней части открывшегося окна, откройте окно **Состояние защиты**.
3. На закладке **Обнаруженные угрозы** перейдите по ссылке **Поместить на карантин**.
4. В открывшемся окне выберите объект, который нужно поместить на карантин.

Чтобы поместить объект на карантин с помощью контекстного меню, выполните следующие действия:

1. Откройте окно Проводника Microsoft Windows и перейдите в папку с объектом, который нужно поместить на карантин.
2. По правой клавише мыши откройте контекстное меню объекта и выберите пункт **Поместить на карантин**.

Чтобы проверить объект карантина, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Защита компьютера**.
2. По ссылке **Карантин**, расположенной в верхней части открывшегося окна, откройте окно **Состояние защиты**.
3. На закладке **Обнаруженные угрозы** выберите объект, который нужно проверить.
4. По правой клавише мыши откройте контекстное меню объекта и выберите в нем пункт **Проверить**.

Чтобы провести лечение всех объектов карантина, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Защита компьютера**.
2. По ссылке **Карантин**, расположенной в верхней части открывшегося окна, откройте окно **Состояние защиты**.
3. На закладке **Обнаруженные угрозы** перейдите по ссылке **Лечить все**.

- *Чтобы восстановить файл из карантина, выполните следующие действия:*

  1. Откройте главное окно программы и нажмите на кнопку **Защита компьютера**.
  2. По ссылке **Карантин**, расположенной в верхней части открывшегося окна, откройте окно **Состояние защиты**.
  3. На закладке **Обнаруженные угрозы** выберите объект, который нужно восстановить.
  4. По правой клавише мыши откройте контекстное меню объекта и выберите в нем пункт **Восстановить**.

- *Чтобы удалить объекты карантина, выполните следующие действия:*

  1. Откройте главное окно программы и нажмите на кнопку **Защита компьютера**.
  2. По ссылке **Карантин**, расположенной в верхней части открывшегося окна, откройте окно **Состояние защиты**.
  3. На закладке **Обнаруженные угрозы** выберите объект, который нужно удалить.
  4. По правой клавише мыши откройте контекстное меню объекта и выберите в нем пункт **Удалить из списка.**

- *Чтобы отправить объект из карантина на исследование в «Лабораторию Касперского», выполните следующие действия:*

  1. Откройте главное окно программы и нажмите на кнопку **Защита компьютера**.
  2. По ссылке **Карантин**, расположенной в верхней части открывшегося окна, откройте окно **Состояние защиты**.
  3. На закладке **Обнаруженные угрозы** выберите объект, который нужно отправить на исследование.
  4. По правой клавише мыши откройте контекстное меню объекта и выберите в нем пункт **Отправить**.

Резервное копирование

В процессе резервного копирования создаются резервные копии выбранных файлов в специальном хранилище.

Хранилищем резервных копий называется специально отведенное дисковое пространство или носитель информации. Хранилища используются задачами резервного копирования для записи резервных копий данных.

В процессе создания хранилища (см. раздел «Создание хранилища» на стр. 164) пользователь выбирает носитель информации, определяет название нового хранилища и параметры хранения резервных копий. Можно также задать пароль для доступа к данным в хранилище. После этого на носитель записывается служебная информация о хранилище.

Для выполнения резервного копирования данных создаются задачи резервного копирования (см. раздел «Создание задачи резервного копирования» на стр. 166). *Задачей резервного копирования* называется предустановленный пользователем набор параметров, определяющий данные для копирования, место хранения резервных копий и условия копирования. Задачи доступны для повторного запуска (вручную или по расписанию).

Резервные копии файлов, созданные в рамках одной задачи, хранятся в *архивах*. Архивы резервных копий помещаются в хранилище и имеют такое же название, как и задача.

При необходимости восстановления данных из резервных копий запускается процедура восстановления (см. раздел «Восстановление данных» на стр. 167) или используется утилита восстановления Kaspersky Restore Utility. Файлы из резервных копий можно восстановить как в исходное место, так и в произвольную папку.

Все события, связанные с резервным копированием, отражаются в отчете (см. раздел «Просмотр отчета о событиях» на стр. 170).

В этом разделе

Создание хранилища 164

Подключение ранее созданного хранилища 165

Очистка хранилища 165

Удаление хранилища 166

Создание задачи резервного копирования 166

Запуск резервного копирования 167

Восстановление данных 167

Поиск резервных копий 168

Просмотр данных резервной копии 169

Просмотр отчета о событиях 170

Создание хранилища

Создание хранилища осуществляется с помощью мастера. Запустить мастер создания хранилища можно двумя способами:

- из главного окна модуля;

- из мастера создания задачи резервного копирования (см. раздел «Создание задачи резервного копирования» на стр. 166).

Мастер состоит из последовательности окон (шагов), переключение между которыми осуществляется при помощи кнопок **Назад** и **Далее**, а завершение работы мастера – при помощи кнопки **Завершить**. Для прекращения работы мастера на любом этапе служит кнопка **Отмена**.

Вы также можете переключаться между пройденными шагами мастера с помощью ссылок навигации в верхней части окна.

Чтобы создать хранилище резервных копий, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Резервное копирование**.
2. В открывшемся окне выберите раздел **Хранилища резервных копий** и нажмите на кнопку **Создать**.
3. Будет запущен мастер создания хранилища резервных копий. Рассмотрим подробнее шаги мастера:
   a. Выберите тип информационного носителя, который будет использоваться в качестве хранилища, в левой части окна **Диск**.

      Для безопасности данных рекомендуется создавать хранилища резервных копий на съемных дисках.

   b. Установите пароль для защиты данных в хранилище от несанкционированного доступа в окне **Защита** (если это необходимо).
   c. Задайте ограничение количества версий файлов, которые будут одновременно находиться в хранилище, а также время хранения версий файлов в окне **Версии файлов** (если это необходимо).
   d. Введите название нового хранилища и подтвердите создание хранилища с указанными параметрами в окне **Сводка**.

ПОДКЛЮЧЕНИЕ РАНЕЕ СОЗДАННОГО ХРАНИЛИЩА

Если вы создали хранилище с помощью Kaspersky CRYSTAL, но на данном компьютере оно недоступно (например, после переустановки системы, или если хранилище было скопировано с другого компьютера), то для работы с данными требуется подключить данное хранилище.

Чтобы подключить ранее созданное хранилище, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Резервное копирование**.
2. В открывшемся окне выберите раздел **Хранилища резервных копий** и нажмите на кнопку **Подключить**.
3. Выберите тип хранилища и укажите требуемые параметры подключения в окне **Подключение хранилища**.

   Если параметры были указаны корректно, хранилище появится в списке.

ОЧИСТКА ХРАНИЛИЩА

Если в хранилище недостаточно свободного места, вы можете удалить устаревшие версии, а также резервные копии файлов, которые отсутствуют на компьютере.

Чтобы очистить хранилище, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Резервное копирование**.

2. В открывшемся окне выберите раздел **Хранилища резервных копий**.

3. Выберите хранилище, которое требуется очистить, и нажмите на кнопку **Очистить**.

4. В открывшемся окне **Очистка хранилища** выберите версии файлов, которые требуется удалить из хранилища.

Удаление хранилища

Для удаления хранилища резервных копий используется мастер удаления хранилища. В процессе удаления определяются действия с данными в удаляемом хранилище и с задачами, использующими хранилище для резервного копирования.

Мастер состоит из последовательности окон (шагов), переключение между которыми осуществляется при помощи кнопок **Назад** и **Далее**, а завершение работы мастера – при помощи кнопки **Завершить**. Для прекращения работы мастера на любом этапе служит кнопка **Отмена**.

Вы также можете переключаться между пройденными шагами мастера с помощью кнопок навигации в верхней части окна.

Чтобы удалить хранилище резервных копий, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Резервное копирование**.

2. В открывшемся окне выберите раздел **Хранилища резервных копий**.

3. Выберите хранилище, которое требуется удалить, и нажмите на кнопку **Удалить**.

4. Будет запущен мастер удаления хранилища резервных копий. Рассмотрим подробнее шаги мастера:

   a. Выберите действие над резервными копиями, находящимися в удаляемом хранилище, в окне **Содержимое**.

   b. Выберите действие над задачами, использующими хранилище для резервного копирования, в окне **Задачи**.

   c. Подтвердите удаление хранилища с указанными параметрами в окне **Сводка**.

Создание задачи резервного копирования

Задачи резервного копирования используются для создания резервных копий файлов и представляют собой набор следующих параметров:

- набор файлов, для которых будут создаваться резервные копии;
- хранилище, в котором будут создаваться резервные копии;
- условия запуска процесса резервного копирования.

Создание задачи осуществляется с помощью мастера.

Мастер состоит из последовательности окон (шагов), переключение между которыми осуществляется при помощи кнопок **Назад** и **Далее**, а завершение работы мастера – при помощи кнопки **Завершить**. Для прекращения работы мастера на любом этапе служит кнопка **Отмена**.

Вы также можете переключаться между пройденными шагами мастера с помощью кнопок навигации в верхней части окна.

Чтобы создать задачу резервного копирования, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Резервное копирование**.
2. В открывшемся окне выберите раздел **Резервное копирование** и нажмите на кнопку **Создать**.
3. Будет запущен мастер создания задачи резервного копирования. Рассмотрим подробнее шаги мастера:
   a. Выберите объекты, для которых будут создаваться резервные копии, в окне **Содержимое**.
   b. Выберите хранилище, в котором будут создаваться резервные копии файлов, в окне **Хранилище**.
   c. Задайте условия запуска задачи в окне **Расписание**.
   d. Введите название новой задачи и подтвердите создание задачи с указанными параметрами в окне **Сводка**.

ЗАПУСК РЕЗЕРВНОГО КОПИРОВАНИЯ

Задачи резервного копирования можно запускать автоматически (по заданному расписанию) или вручную. Текущий режим запуска задачи отображается в списке задач (см. рис. ниже).

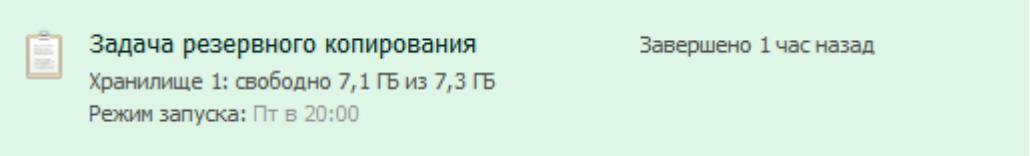


Рисунок 14. Задача резервного копирования

Расписание автоматического запуска настраивается при создании задачи и в дальнейшем может быть изменено.

При необходимости вы можете запустить любую задачу вручную.

Чтобы запустить задачу резервного копирования вручную, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Резервное копирование**.
2. В открывшемся окне выберите раздел **Резервное копирование**.
3. В правой части окна в списке выберите задачу, которую нужно выполнить, и нажмите на кнопку **Выполнить**.

   В строке выбранной задачи отображается время с начала выполнения. Выполнение задачи можно приостановить или отменить, используя соответствующие кнопки в верхней части окна.

   В результате выполнения задачи в хранилище создается архив резервных копий за текущую дату.

ВОССТАНОВЛЕНИЕ ДАННЫХ

При необходимости данные могут быть восстановлены из резервных копий файлов. Процедура восстановления доступна только для подключенных хранилищ. В ходе восстановления данные из резервных копий сохраняются в выбранную папку.

Восстановление файлов можно выполнить разными способами:

- восстановить последнюю версию файла;
- выбрать версию для восстановления по дате.

- *Чтобы восстановить последнюю версию файла, выполните следующие действия:*

1. Откройте главное окно программы и нажмите на кнопку **Резервное копирование**.
2. В открывшемся окне выберите раздел **Восстановление данных**.
3. Выберите хранилище, в котором находятся нужные резервные копии, и нажмите на кнопку **Восстановить**.
4. В верхней части окна **Восстановление данных из хранилища** в раскрывающемся списке **Архив** выберите название задачи, в результате выполнения которой был создан архив с нужными резервными копиями.
5. Выберите файлы, которые нужно восстановить. Для этого установите флажки рядом с нужными файлами в списке. Для выбора всех файлов нажмите на кнопку **Выбрать все** внизу списка. Нажмите на кнопку **Восстановить** в верхней части окна.
6. В открывшемся окне **Восстановление** выберите место сохранения восстановленных файлов и условие сохранения при совпадении имен. Нажмите на кнопку **Восстановить**.

- *Чтобы выбрать нужную версию файла, выполните следующие действия:*

1. Откройте главное окно программы и нажмите на кнопку **Резервное копирование**.
2. В открывшемся окне выберите раздел **Восстановление данных**.
3. Выберите хранилище, в котором находятся нужные резервные копии, и нажмите на кнопку **Восстановить данные**.
4. В верхней части окна **Восстановление данных из хранилища** в раскрывающемся списке **Архив** выберите название задачи, в результате выполнения которой был создан архив с нужными резервными копиями.
5. Выберите файл, версию которого нужно указать. Для этого установите флажок рядом с нужным файлом. Нажмите на кнопку **Версии** в верхней части окна.
6. В открывшемся окне **Версии файла** выберите дату версии, которую нужно восстановить, и нажмите на кнопку **Восстановить**.
7. В открывшемся окне **Восстановление** выберите место сохранения восстановленных файлов и условие сохранения при совпадении имен. Нажмите на кнопку **Восстановить**.

Поиск резервных копий

Для поиска резервных копий в хранилище можно использовать фильтр и строку поиска.

Фильтр резервных копий позволяет отобразить только те копии, которые соответствуют заданным критериям поиска.

С помощью строки поиска можно найти резервную копию в архиве по ее названию.

Чтобы отобразить резервные копии файлов, которые не были включены в список файлов для резервного копирования при последнем выполнении задачи (например, были удалены с компьютера), установите флажок **Показать удаленные файлы**.

- *Чтобы отфильтровать резервные копии, выполните следующие действия:*

1. Откройте главное окно программы и нажмите на кнопку **Резервное копирование**.
2. В открывшемся окне выберите раздел **Восстановление данных**.
3. В правой части окна выберите хранилище и нажмите на кнопку **Восстановить**.

4. В верхней части окна **Восстановление данных из хранилища** выберите критерии поиска в фильтре:

   - В раскрывающемся списке **Архив** выберите название задачи, в результате выполнения которой был создан архив с нужными резервными копиями.
   - В раскрывающемся списке **Дата** выберите дату создания архива с нужными резервными копиями.
   - В раскрывающемся списке **Категория** выберите типы файлов, для которых требуется найти резервные копии.

В результате списке отображаются только те резервные копии, которые соответствуют выбранным условиям.

Чтобы найти резервную копию по ее названию, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Резервное копирование**.
2. В открывшемся окне выберите раздел **Восстановление данных**.
3. В правой части окна выберите хранилище и нажмите на кнопку **Восстановить**.
4. В верхней части окна **Восстановление данных из хранилища** в поле **Поиск** введите название файла целиком или его часть.

В результате в списке отображаются только те резервные копии файлов, названия которых начинаются с введенных символов.

ПРОСМОТР ДАННЫХ РЕЗЕРВНОЙ КОПИИ

Прежде чем восстанавливать данные, можно проверить содержимое выбранной версии резервной копии. Для этого можно сразу открыть последнюю версию или выбрать версию на указанную дату.

Чтобы открыть последнюю версию файла, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Резервное копирование**.
2. В открывшемся окне выберите раздел **Восстановление данных**.
3. Выберите хранилище, в котором находятся нужные резервные копии, и нажмите на кнопку **Восстановить**.
4. В верхней части окна **Восстановление данных из хранилища** в раскрывающемся списке **Архив** выберите название задачи, в результате выполнения которой был создан архив с нужными резервными копиями.
5. В правой части окна в списке выберите нужный файл и нажмите на кнопку **Открыть**.

Чтобы открыть версию файла на определенную дату, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Резервное копирование**.
2. В открывшемся окне выберите раздел **Восстановление данных**.
3. Выберите хранилище, в котором находятся нужные резервные копии, и нажмите на кнопку **Восстановить**.
4. В верхней части окна **Восстановление данных из хранилища** в раскрывающемся списке **Архив** выберите название задачи, в результате выполнения которой был создан архив с нужными резервными копиями.
5. В правой части окна в списке выберите нужный файл и нажмите на кнопку **Версии**.

6. В открывшемся окне **Версии файла** выберите нужную дату и нажмите на кнопку **Открыть**.

Просмотр отчета о событиях

Каждое событие, связанное с резервным копированием и восстановлением данных, фиксируется в отчете.

Чтобы получить отчет о работе модуля резервного копирования, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Резервное копирование**.
2. В открывшемся окне перейдите по ссылке **Отчет** в верхней части окна.
3. В открывшемся окне **Отчет** настройте параметры отображения информации о событиях.

Родительский контроль

Родительский контроль позволяет контролировать действия разных пользователей на компьютере и в сети. Понятие контроля включает возможность ограничивать доступ к ресурсам и программам, а также просматривать отчеты о действиях пользователей.

В настоящее время доступ к компьютеру и интернет-ресурсам получает все большее количество детей и подростков. При этом возникает проблема обеспечения безопасности, так как работа и общение в интернете связаны с рядом угроз. Назовем наиболее распространенные среди них:

- посещение веб-сайтов, которые являются потенциальной причиной потери времени (чаты, игровые ресурсы) или денег (интернет-магазины, аукционы);
- доступ к веб-ресурсам, предназначенным для взрослой аудитории (например, содержащим порнографические, экстремистские материалы, затрагивающим темы оружия, наркотиков, насилия);
- скачивание файлов, зараженных вредоносными программами;
- чрезмерно длительное нахождение за компьютером, что может нанести вред здоровью;
- контакты с незнакомыми людьми, которые под видом сверстников могут получить личную информацию о пользователе (например, настоящее имя, адрес, время, когда никого нет дома).

Родительский контроль позволяет снизить риски, связанные с работой на компьютере и в интернете. Для этого используются следующие функции модуля:

- ограничение использования компьютера и интернета по времени;
- создание списков разрешенных и запрещенных для запуска приложений, а также временное ограничение запуска разрешенных приложений;
- создание списков разрешенных и запрещенных для доступа веб-сайтов, выбор категорий не рекомендованного к просмотру содержимого веб-ресурсов;
- включение режима безопасного поиска с помощью поисковых систем (при этом ссылки на веб-сайты с сомнительным содержимым не отображаются в результатах поиска);
- ограничение загрузки файлов из интернета;
- создание списков контактов, запрещенных или разрешенных для общения через интернет-пейджеры и в социальных сетях;
- просмотр текста переписки через интернет-пейджеры и в социальных сетях;
- запрет пересылки определенных персональных данных;
- поиск заданных ключевых слов в тексте переписки.

Все ограничения включаются по отдельности, что позволяет гибко настраивать Родительский контроль для разных пользователей. Для каждой учетной записи можно просматривать отчеты, в которых регистрируются события контролируемых категорий за выбранный период.

Для управления компонентом требуется ввести пароль администратора (см. раздел «Как ограничить доступ к параметрам Kaspersky CRYSTAL» на стр. 70). Если вы еще не задали пароль для управления Kaspersky CRYSTAL, вам будет предложено это сделать.

В этом разделе

Настройка Родительского контроля пользователя 172

Просмотр отчетов о действиях пользователя 179

Настройка Родительского контроля пользователя

Вы можете включить и настроить Родительский контроль для каждой учетной записи индивидуально, задав разные ограничения для разных пользователей, например в зависимости от возраста. Для пользователей, действия которых контролировать не нужно, вы можете отключить Родительский контроль.

Для управления компонентом требуется пройти процедуру авторизации. После ввода пароля администратора можно включать, приостанавливать или выключать Родительский контроль, а также изменять параметры его работы.

Включение и отключение контроля

Вы можете включать и отключать Родительский контроль отдельно для каждой учетной записи. Например, действия взрослого пользователя с учетной записью администратора компьютера контролировать не нужно – для него Родительский контроль можно отключить. Для остальных пользователей, действия которых нужно контролировать, Родительский контроль нужно включить, а затем настроить – например, загрузив стандартные параметры настройки из шаблона.

Включить и отключить Родительский контроль для текущей учетной записи можно из главного окна и из контекстного меню значка программы

- *Чтобы включить Родительский контроль, выполните следующие действия:*

  1. Откройте главное окно программы и нажмите на кнопку **Родительский контроль**.
  2. В открывшемся окне выберите раздел **Пользователи** и в верхней части окна нажмите на кнопку **Включить**.

- *Чтобы приостановить работу Родительского контроля, выполните следующие действия:*

  1. Откройте главное окно программы и нажмите на кнопку **Родительский контроль**.
  2. В открывшемся окне выберите раздел **Пользователи** и в верхней части окна нажмите на кнопку **Приостановить**.
  3. В окне **Приостановка работы Родительского контроля** выберите режим возобновления работы.

Вы также можете приостановить или возобновить Родительский контроль для текущей учетной записи через главное окно Kaspersky CRYSTAL (см. стр. 39) и из контекстного меню значка программы (см. стр. 38).

См. также:

Сохранение и загрузка параметров Родительского контроля 173

Сохранение и загрузка параметров Родительского контроля

Если вы настроили параметры Родительского контроля для учетной записи, их можно сохранить в отдельный файл. В дальнейшем можно выполнить импорт параметров из этого файла для быстрой настройки. Кроме того, вы можете применить параметры контроля другой учетной записи или использовать шаблон настройки (предустановленный набор правил для разных типов пользователей в зависимости от их возраста, опыта и других характеристик).

После импорта вы всегда можете изменить установленные параметры для отдельной учетной записи.

- *Чтобы сохранить параметры контроля в файл, выполните следующие действия:*

  1. Откройте главное окно программы и нажмите на кнопку **Родительский контроль**.
  2. В открывшемся окне выберите раздел **Пользователи**, выберите учетную запись, параметры контроля которой требуется сохранить, и нажмите на кнопку **Настроить**.
  3. В открывшемся окне перейдите по ссылке **Экспорт параметров** в верхней части окна и сохраните файл настройки.

- *Чтобы загрузить параметры контроля из файла, выполните следующие действия:*

  1. Откройте главное окно программы и нажмите на кнопку **Родительский контроль**.
  2. В открывшемся окне выберите раздел **Пользователи**, выберите учетную запись, для которой требуется загрузить параметры контроля, и нажмите на кнопку **Настроить**.
  3. В открывшемся окне перейдите по ссылке **Импорт параметров** в верхней части окна.
  4. В открывшемся окне **Загрузка параметров контроля** выберите вариант **Файл с ранее сохраненными параметрами** и укажите местонахождение файла.

- *Чтобы применить параметры другой учетной записи, выполните следующие действия:*

  1. Откройте главное окно программы и нажмите на кнопку **Родительский контроль**.
  2. В открывшемся окне выберите раздел **Пользователи**, выберите учетную запись, для которой требуется применить параметры контроля, и нажмите на кнопку **Настроить**.
  3. В открывшемся окне перейдите по ссылке **Импорт параметров** в верхней части окна.
  4. В открывшемся окне **Загрузка параметров контроля** выберите вариант **Другой пользователь** и укажите учетную запись, параметры которой нужно использовать.

- *Чтобы использовать шаблон настройки, выполните следующие действия:*

  1. Откройте главное окно программы и нажмите на кнопку **Родительский контроль**.
  2. В открывшемся окне выберите раздел **Пользователи**, выберите учетную запись, для которой требуется использовать предустановленные параметры контроля, и нажмите на кнопку **Настроить**.
  3. В открывшемся окне перейдите по ссылке **Импорт параметров** в верхней части окна.
  4. В открывшемся окне **Загрузка параметров контроля** выберите вариант **Шаблон** и укажите шаблон, параметры которого нужно использовать.

Отображение учетной записи в Kaspersky CRYSTAL

Вы можете выбрать, под каким псевдонимом и с каким изображением будет отображаться учетная запись пользователя в Kaspersky CRYSTAL.

Чтобы настроить псевдоним и изображение для учетной записи, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Родительский контроль**.
2. В открывшемся окне выберите раздел **Пользователи**, выберите учетную запись, для которой требуется настроить параметры отображения, и нажмите на кнопку **Настроить**.
3. В открывшемся окне в разделе **Дополнительно** выберите компонент **Отображение**. Введите псевдоним для учетной записи и выберите картинку для отображения.

Время работы на компьютере

Вы можете настроить расписание доступа пользователя к компьютеру (дни недели и время в течение дня), а также ограничить суммарное время работы на компьютере в сутки.

За 15 и 5 минут до истечения разрешенного времени работы на компьютере Kaspersky CRYSTAL предупреждает пользователя о том, что компьютер будет выключен. Это позволяет своевременно завершить работу и сохранить нужные данные. По истечении разрешенного времени Kaspersky CRYSTAL показывает уведомление о нарушении графика работы на компьютере и завершает работу.

Чтобы ограничить использование компьютера по времени, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Родительский контроль**.
2. В открывшемся окне выберите раздел **Пользователи**, выберите учетную запись пользователя, для которого требуется задать ограничение, и нажмите на кнопку **Настроить**.
3. В открывшемся окне в разделе **Компьютер** выберите компонент **Использование**.
4. В открывшемся окне **Контроль времени работы за компьютером** установите флажок **Включить контроль** и задайте временные ограничения.

Запуск программ

Вы можете разрешить или запретить запуск определенных программ, а также ограничить запуск разрешенных программ по времени.

Чтобы ограничить запуск программ и игр, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Родительский контроль**.
2. В открывшемся окне выберите раздел **Пользователи**, выберите учетную запись пользователя, для которого требуется задать ограничение, и нажмите на кнопку **Настроить**.
3. В открывшемся окне в разделе **Компьютер** выберите компонент **Запуск программ**.
4. В открывшемся окне **Контроль запускаемых программ** установите флажок **Включить контроль**.
5. На закладках **Разрешенные** и **Запрещенные** создайте списки разрешенных и запрещенных для запуска программ, установите расписание использования разрешенных программ.

Время работы в интернете

Вы можете ограничить время пребывания пользователя в интернете. Для этого можно настроить расписание доступа в интернет (дни недели и время в течение дня, когда доступ разрешен или запрещен), а также ограничить суммарное время пребывания в интернете в сутки.

За 10 минут до истечения разрешенного времени работы в интернете Kaspersky CRYSTAL предупреждает пользователя о том, что соединение будет разорвано. Это позволяет своевременно завершить работу и

сохранить нужные данные. По истечении разрешенного времени Kaspersky CRYSTAL показывает уведомление о нарушении графика работы в интернете и разрывает соединение с интернетом.

Чтобы ограничить использование интернета по времени, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Родительский контроль**.
2. В открывшемся окне выберите раздел **Пользователи**, выберите учетную запись пользователя, для которого требуется задать ограничение, и нажмите на кнопку **Настроить**.
3. В открывшемся окне в разделе **Интернет** выберите компонент **Использование**.
4. В открывшемся окне **Контроль использования интернета** установите флажок **Включить контроль** и задайте временные ограничения.

Посещение веб-сайтов

Вы можете установить ограничения на доступ к определенным веб-ресурсам в зависимости от их содержимого. Для этого можно сформировать списки разрешенных и запрещенных веб-адресов, а также выбрать категории веб-сайтов, доступ к которым должен быть заблокирован.

Чтобы ограничить доступ к веб-ресурсам, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Родительский контроль**.
2. В открывшемся окне выберите раздел **Пользователи**, выберите учетную запись пользователя, для которого требуется задать ограничение и нажмите на кнопку **Настроить**.
3. В открывшемся окне в разделе **Интернет** выберите компонент **Посещение веб-сайтов**.
4. В открывшемся окне **Контроль посещения веб-сайтов** установите флажок **Включить контроль** и задайте ограничения на посещение веб-сайтов.

   На закладках **Запрещенные веб-адреса** и **Разрешенные веб-адреса** можно внести адреса запрещенных и разрешенных для доступа веб-ресурсов. На закладке **Не рекомендуемые** можно выбрать категории веб-сайтов, доступ к которым требуется блокировать.
5. Если вы хотите разрешить доступ только к перечисленным разрешенным веб-сайтам, установите флажок **Запретить посещение всех веб-сайтов кроме списка разрешенных веб-адресов**.

Если вы установили флажок **Запретить посещение всех веб-сайтов кроме списка разрешенных веб-адресов**, то для подключения к интернету через прокси-сервер необходимо добавить адрес прокси-сервера в список **Разрешенные веб-адреса**.

Загрузка файлов из интернета

Вы можете ограничить типы файлов, которые можно загружать из интернета.

Чтобы ограничить загрузку файлов из интернета, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Родительский контроль**.
2. В открывшемся окне выберите раздел **Пользователи**, выберите учетную запись пользователя, для которого требуется задать ограничение, и нажмите на кнопку **Настроить**.
3. В открывшемся окне в разделе **Интернет** выберите компонент **Загрузка файлов**.
4. В открывшемся окне **Контроль загрузки файлов из интернета** установите флажок **Включить контроль** и выберите категории файлов, загрузка которых разрешена.

Режим безопасного поиска

Некоторые поисковые системы стремятся защитить пользователей от неприемлемого содержимого веб-ресурсов. Для этого при индексации веб-сайтов анализируются ключевые слова и фразы, адреса и категории ресурсов. При включенном режиме безопасного поиска из результатов поиска исключаются сайты, относящиеся к нежелательным категориям (порнография, наркотики, насилие и другие материалы, не рекомендуемые для несовершеннолетних).

Родительский контроль позволяет включать режим безопасного поиска одновременно для поисковых систем Google и Bing.

Чтобы включить режим безопасного поиска, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Родительский контроль**.
2. В открывшемся окне выберите раздел **Пользователи**, выберите учетную запись пользователя, для которого требуется задать ограничение, и нажмите на кнопку **Настроить**.
3. В открывшемся окне в разделе **Интернет** выберите компонент **Безопасный поиск**.
4. В открывшемся окне **Контроль результатов поиска** установите флажок **Включить режим безопасного поиска**.

Переписка через интернет-пейджеры

Контроль переписки через программы мгновенного обмена сообщениями (интернет-пейджеры) заключается в контроле контактов, с которыми разрешено общение, а также содержания переписки. Вы можете сформировать списки разрешенных и запрещенных контактов, задать ключевые слова (см. раздел «Поиск ключевых слов» на стр. 179), наличие которых будет проверяться в сообщениях, а также указать личные данные (см. раздел «Пересылка конфиденциальной информации» на стр. 178), пересылка которых запрещена.

Если переписка с контактом запрещена, то все сообщения, адресованные данному контакту или полученные от него, будут блокироваться. Информация о заблокированных сообщениях, а также о наличии ключевых слов в сообщениях выводится в отчет. В полном отчете можно просмотреть также текст переписки с каждым контактом.

Контроль переписки имеет следующие ограничения:

- Если интернет-пейджер был запущен до включения Родительского контроля, то контроль переписки не будет осуществляться до перезапуска интернет-пейджера.
- При использовании HTTP-прокси контроль переписки осуществляться не будет.

Текущая версия Родительского контроля обеспечивает контроль общения через следующие интернет-пейджеры:

- ICQ;
- QIP
- Windows Live Messenger (MSN);
- Yahoo Messenger;
- GoogleTalk;
- mIRC;
- Mail.Ru Агент;
- Psi;
- Miranda;

- AOL Instant Messenger (AIM);
- Jabber.

Многие интернет-пейджеры используют защищенное соединение. Чтобы контролировать переписку через такие программы, требуется включить проверку защищенных соединений (см. стр. 150).

Чтобы ограничить контакты, доступные для общения через интернет-пейджеры, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Родительский контроль**.
2. В открывшемся окне выберите раздел **Пользователи**, выберите учетную запись пользователя, для которого требуется задать ограничение, и нажмите на кнопку **Настроить**.
3. В открывшемся окне в разделе **Общение** выберите компонент **IM-переписка**.
4. В открывшемся окне **Контроль переписки через интернет-пейджеры** установите флажок **Включить контроль**.
5. На закладках **Разрешенные** и **Запрещенные** создайте списки разрешенных и запрещенных контактов.
6. В раскрывающемся списке **Действие** выберите действие по умолчанию для контактов, не включенных в списки.

Вы также можете разрешить или запретить переписку с выбранным контактом из подробного отчета о событиях для данной учетной записи.

Чтобы просмотреть краткую статистику, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Родительский контроль**.
2. В открывшемся окне выберите раздел **Отчеты** и в раскрывающемся списке справа выберите учетную запись пользователя, для которого требуется отобразить отчет.

   В блоке **Общение** будет отображена краткая статистика переписки через интернет-пейджеры для выбранной учетной записи.

Чтобы получить подробный отчет, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Родительский контроль**.
2. В открывшемся окне выберите раздел **Отчеты** и в раскрывающемся списке справа выберите учетную запись пользователя, для которого требуется отобразить отчет. Перейдите по ссылке **Подробный отчет**.
3. В открывшемся окне в разделе **Общение** выберите компонент **IM-переписка**.

   В открывшемся окне **IM-переписка** будет отображен подробный отчет.

Вы также можете открыть подробный отчет в разделе **Пользователи**, нажав на кнопку **Подробный отчет**.

ПЕРЕПИСКА В СОЦИАЛЬНЫХ СЕТЯХ

Контроль переписки через социальные сети заключается в контроле контактов, с которыми разрешено общение, а также содержания переписки. Вы можете сформировать списки разрешенных и запрещенных контактов, задать ключевые слова (см. раздел «Поиск ключевых слов» на стр. 179), наличие которых будет проверяться в сообщениях, а также указать личные данные (см. раздел «Пересылка конфиденциальной информации» на стр. 178), пересылка которых запрещена.

Если переписка с контактом запрещена, то все сообщения, адресованные данному контакту или полученные от него, будут блокироваться. Информация о заблокированных сообщениях, а также о наличии ключевых слов в сообщениях выводится в отчет. В полном отчете можно просмотреть также текст переписки с каждым контактом.

Некоторые социальные сети, например, Twitter используют защищенное соединение. Чтобы проверять трафик этих сетей, требуется включить проверку защищенных соединений (см. стр. 150).

Текущая версия Родительского контроля обеспечивает контроль общения в следующих социальных сетях:

- Facebook;
- Twitter;
- MySpace.

Чтобы ограничить контакты, доступные для общения через социальные сети, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Родительский контроль**.
2. В открывшемся окне выберите раздел **Пользователи**, выберите учетную запись пользователя, для которого требуется задать ограничение, и нажмите на кнопку **Настроить**.
3. В открывшемся окне в разделе **Общение** выберите компонент **Социальные сети**.
4. В открывшемся окне **Контроль переписки в социальных сетях** установите флажок **Включить контроль**.
5. В раскрывающемся списке **Действие** выберите действие по умолчанию для контактов, не включенных в списки.

   Вы также можете разрешить или запретить переписку с выбранным контактом из подробного отчета о событиях для данной учетной записи.

6. Закройте окно настройки и нажмите на кнопку **Подробный отчет**.
7. В открывшемся окне в разделе **Общение** выберите компонент **Социальные сети**.

   В правой части открывшегося окна отобразится список контактов, от которых было получено или которым было отправлено сообщение.

8. Укажите действие (запретить или разрешить переписку) для выбранных контактов.

   Контакты будут автоматически добавлены в список контролируемых, который можно просмотреть в окне **Настройка** в разделе **Социальные сети**.

Пересылка конфиденциальной информации

Вы можете запретить пересылку данных, содержащих персональную информацию, через интернет-пейджеры, социальные сети и при отправке данных на веб-сайты. Для этого требуется сформировать список записей, которые содержат конфиденциальные данные (например, домашний адрес, номер телефона).

Попытки пересылки данных из списка блокируются, а информация о заблокированных сообщениях выводится в отчет.

Чтобы блокировать пересылку личных данных, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Родительский контроль**.

2. В открывшемся окне выберите раздел **Пользователи**, выберите учетную запись пользователя, для которого требуется задать ограничение, и нажмите на кнопку **Настроить**.

3. В открывшемся окне в разделе **Общение** выберите компонент **Личные данные**.

4. В открывшемся окне **Контроль пересылки личных данных** установите флажок **Включить контроль**. Добавьте запись в список данных, запрещенных к пересылке, по ссылке **Добавить**.

Поиск ключевых слов

Вы можете контролировать наличие определенных слов и словосочетаний в переписке пользователя через интернет-пейджеры, социальные сети и при отправке данных на веб-сайты.

Наличие в пересылаемых сообщениях ключевых слов, входящих в список, отражается в отчете.

Если отключен контроль переписки через интернет-пейджеры, социальные сети или контроль посещения веб-сайтов, поиск ключевых слов не производится.

- *Чтобы контролировать наличие в переписке определенных слов, выполните следующие действия:*

1. Откройте главное окно программы и нажмите на кнопку **Родительский контроль**.

2. В открывшемся окне выберите раздел **Пользователи**, выберите учетную запись пользователя, для которого требуется задать ограничение, и нажмите на кнопку **Настроить**.

3. В открывшемся окне в разделе **Общение** выберите компонент **Ключевые слова**.

4. В открывшемся окне **Контроль употребления ключевых слов** установите флажок **Включить контроль**. Добавьте запись в список ключевых слов, контролируемых в переписке, по ссылке **Добавить**.

Просмотр отчетов о действиях пользователя

Для каждого пользователя, для которого настроен Родительский контроль, вы можете просмотреть краткую статистику и подробный отчет по категориям контролируемых событий.

- *Чтобы просмотреть краткую статистику, выполните следующие действия:*

1. Откройте главное окно программы и нажмите на кнопку **Родительский контроль**.

2. В открывшемся окне выберите раздел **Отчеты** и в раскрывающемся списке справа выберите учетную запись пользователя, для которого требуется отобразить краткую статистику.

3. В окне будет отображена краткая статистика для выбранной учетной записи.

- *Чтобы получить подробный отчет, выполните следующие действия:*

1. Откройте главное окно программы и нажмите на кнопку **Родительский контроль**.

2. В открывшемся окне выберите раздел **Отчеты** и в раскрывающемся списке справа выберите учетную запись пользователя, для которого требуется отобразить отчет. Перейдите по ссылке **Подробный отчет**.

3. В открывшемся окне будет отображен подробный отчет по категориям для выбранной учетной записи.

Вы также можете открыть подробный отчет в разделе **Пользователи**, нажав на кнопку **Подробный отчет**.

Шифрование данных

Шифрование данных служит для защиты конфиденциальной информации от несанкционированного доступа. При этом информация хранится в зашифрованном виде в специальном контейнере.

Контейнер – это зашифрованный объект, созданный пользователем с помощью функции Шифрования данных. В контейнер помещаются файлы и папки. Для доступа к данным, находящимся в контейнере, требуется ввести пароль. Кроме того, на компьютере должна быть установлена программа Kaspersky CRYSTAL.

Для работы с данными в контейнере их требуется расшифровать. При этом Kaspersky CRYSTAL запрашивает пароль для доступа. После успешного ввода пароля контейнер отображается в системе в виде виртуального съемного диска, на который можно копировать или перемещать файлы и папки с данными.

В этом разделе

Создание и подключение ранее созданного контейнера 180

Блокирование и разблокирование доступа к данным в контейнере 181

Добавление файлов в контейнер 182

Настройка параметров контейнера 182

Создание ярлыка для быстрого доступа к контейнеру 183

Создание и подключение ранее созданного контейнера

Для хранения данных в зашифрованном виде требуется создать контейнер. Можно создать контейнер на локальном или съемном диске.

Создание контейнера осуществляется с помощью мастера. При создании контейнера определяется его название, размер, пароль доступа и расположение файла контейнера.

Мастер состоит из последовательности окон (шагов), переключение между которыми осуществляется при помощи кнопок **Назад** и **Далее**, а завершение работы мастера – при помощи кнопки **Завершить**. Для прекращения работы мастера на любом этапе служит кнопка **Отмена**.

Вы также можете переключаться между пройденными шагами мастера с помощью кнопок навигации в верхней части окна.

Кроме того, можно подключить ранее созданный контейнер, если он недоступен на данном компьютере (например, после переустановки системы, или если контейнер был скопирован с другого компьютера). В этом случае контейнер появится в списке, но доступ к данным будет заблокирован. Для работы с данными в контейнере их потребуется расшифровать (см. раздел «Блокирование и разблокирование доступа к данным в контейнере» на стр. 181).

- *Чтобы создать контейнер, выполните следующие действия:*

1. Откройте главное окно программы и нажмите на кнопку **Шифрование данных**.
2. В открывшемся окне нажмите на кнопку **Создать контейнер**.
3. Будет запущен мастер создания зашифрованного контейнера. Рассмотрим подробнее шаги мастера:
   a. Введите название контейнера, размер и пароль доступа в окне **Основные параметры**.
   b. Укажите расположение файла контейнера в окне **Расположение**.

c. Выберите букву виртуального диска для подключения контейнера, задайте дополнительные параметры, если это необходимо, и подтвердите создание контейнера с указанными параметрами в окне **Сводка**.

Чтобы подключить ранее созданный контейнер, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Шифрование данных**.
2. В открывшемся окне нажмите на кнопку **Подключить контейнер**.
3. В открывшемся окне укажите расположение файла контейнера.

БЛОКИРОВАНИЕ И РАЗБЛОКИРОВАНИЕ ДОСТУПА К ДАННЫМ В КОНТЕЙНЕРЕ

После создания контейнера доступ к данным разблокирован. Если был подключен ранее созданный контейнер, то по умолчанию доступ к нему заблокирован. Для работы с данными в контейнере их требуется расшифровать. Это можно сделать через интерфейс Kaspersky CRYSTAL или через контекстное меню Microsoft Windows.

Если контейнер хранится на съемном носителе, вы можете настроить автоматическое разблокирование доступа к данным в контейнере при подключении носителя.

Когда доступ к контейнеру разблокирован, контейнер становится доступен для всех учетных записей компьютера в виде съемного диска в списке устройств, поэтому рекомендуется блокировать доступ (зашифровать данные в контейнере), когда вы не работаете с данными. Зашифровать данные в контейнере можно через интерфейс Kaspersky CRYSTAL или через контекстное меню Microsoft Windows.

Чтобы расшифровать данные в контейнере через интерфейс программы, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Шифрование данных**.
2. В открывшемся окне нажмите на кнопку **Расшифровать данные**.
3. В открывшемся окне введите параметры расшифровки данных и подтвердите разблокировку доступа.

Чтобы расшифровать данные через контекстное меню, выполните следующие действия:

1. По правой клавише мыши откройте контекстное меню файла контейнера или ярлыка для доступа к контейнеру (см. раздел «Создание ярлыка для быстрого доступа к контейнеру» на стр. 183) на рабочем столе.
2. В раскрывшемся меню выберите пункт **Расшифровать данные**.

Чтобы автоматически разблокировать доступ к данным в контейнере при подключении носителя, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Шифрование данных**.
2. В открывшемся окне выберите контейнер, доступ к которому разблокирован, и нажмите на кнопку **Настроить**.
3. В открывшемся окне установите флажок **Расшифровывать при подключении**.

Чтобы зашифровать данные через интерфейс программы, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Шифрование данных**.
2. В открывшемся окне выберите контейнер, доступ к которому разблокирован, и нажмите на кнопку **Зашифровать данные**.

Чтобы зашифровать данные через контекстное меню, выполните следующие действия:

1. По правой клавише мыши откройте контекстное меню файла контейнера, ярлыка для доступа к контейнеру (см. раздел «Создание ярлыка для быстрого доступа к контейнеру» на стр. 183) на рабочем столе или съемного диска.

2. В раскрывшемся меню выберите пункт **Зашифровать данные**.

Добавление файлов в контейнер

После расшифровки данных (см. раздел «Блокирование и разблокирование доступа к данным в контейнере» на стр. 181) контейнер отображается в системе как виртуальный съемный диск и доступен всем пользователям операционной системы. Вы можете открыть контейнер и поместить в него файлы и папки, которые требуется хранить в зашифрованном виде. Для безопасности ваших данных рекомендуется зашифровать данные по окончании работы. После этого для доступа к зашифрованным данным в контейнере потребуется ввести пароль.

Чтобы открыть контейнер через интерфейс программы, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Шифрование данных**.

2. В открывшемся окне выберите контейнер, доступ к которому разблокирован, и откройте его двойным щелчком мыши.

3. Поместите в контейнер данные, которые требуется зашифровать.

Чтобы открыть контейнер через контекстное меню, выполните следующие действия:

1. По правой клавише мыши откройте контекстное меню файла контейнера или ярлыка для доступа к контейнеру (см. раздел «Создание ярлыка для быстрого доступа к контейнеру» на стр. 183) на рабочем столе.

2. В раскрывшемся меню выберите пункт **Открыть контейнер**.

Настройка параметров контейнера

Вы можете изменить название контейнера и пароль доступа к нему.

Изменить параметры можно только для контейнера, доступ к которому заблокирован.

Чтобы переименовать контейнер, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Шифрование данных**.

2. В открывшемся окне выберите контейнер и нажмите на кнопку **Настроить**.

3. В открывшемся окне введите пароль доступа к контейнеру.

4. В открывшемся окне **Параметры контейнера** укажите новое название контейнера.

Чтобы изменить пароль доступа к контейнеру, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Шифрование данных**.

2. В открывшемся окне выберите контейнер и нажмите на кнопку **Настроить**.

3. В открывшемся окне введите пароль доступа к контейнеру.

4. В открывшемся окне **Параметры контейнера** воспользуйтесь ссылкой **Изменить пароль**.

5. В открывшемся окне **Изменение пароля** заполните все поля.

СОЗДАНИЕ ЯРЛЫКА ДЛЯ БЫСТРОГО ДОСТУПА К КОНТЕЙНЕРУ

Для удобства работы с данными можно создать на рабочем столе ярлык для быстрого доступа к контейнеру. С помощью ярлыка вы можете быстро открывать контейнер, расшифровывать и зашифровывать данные независимо от фактического расположения файла контейнера (при наличии доступа к файлу контейнера с вашего компьютера). Вы можете создать ярлык для быстрого доступа в процессе создания контейнера или в любое время после создания.

Создать ярлык можно только для контейнера, доступ к которому заблокирован.

Чтобы создать ярлык для доступа к контейнеру, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Шифрование данных**.
2. В открывшемся окне выберите контейнер, нажмите на кнопку **Настроить**.
3. В открывшемся окне введите пароль доступа к контейнеру.
4. В открывшемся окне **Параметры контейнера** перейдите по ссылке **Создать ярлык на рабочем столе**.

Центр управления

Функции Центра управления предназначены для удаленного управления программой Kaspersky CRYSTAL, установленной на компьютерах домашней сети, с рабочего места администратора.

Через Центр управления администратор сети может выполнять следующие действия:

- анализировать уровень защиты компьютеров в сети;
- проверять всю сеть и отдельные компьютеры на наличие угроз;
- централизованно обновлять антивирусные базы;
- настраивать параметры защиты для компьютеров в сети;
- осуществлять родительский контроль;
- выполнять резервное копирование данных на компьютерах в сети;
- просматривать отчеты о работе подсистем безопасности.

Чтобы запустить Центр управления, выполните следующие действия:

В нижней части главного окна Kaspersky CRYSTAL нажмите на кнопку **Центр управления**.

При первом запуске автоматически запускается мастер настройки удаленного управления (см. раздел «Настройка удаленного управления» на стр. 184). При последующих запусках требуется ввести пароль администратора.

Для удаленного управления программой на компьютерах в сети Центр управления должен быть защищен одинаковым паролем администратора на всех компьютерах.

В этом разделе

Настройка удаленного управления 184

Проверка домашней сети на вирусы и уязвимости 185

Удаленное обновление баз на компьютерах в сети 185

Включение / отключение компонентов защиты на компьютерах в сети 186

Удаленное управление Родительским контролем 186

Запуск резервного копирования на компьютерах в сети 187

Удаленное управление лицензиями на компьютерах в сети 187

Настройка удаленного управления

Настройка удаленного управления осуществляется с помощью мастера. При первом запуске Центра управления мастер настройки запускается автоматически, позже вы сможете запустить мастер настройки вручную.

Мастер состоит из последовательности окон (шагов), переключение между которыми осуществляется при помощи кнопок **Назад** и **Далее**, а завершение работы мастера – при помощи кнопки **Завершить**. Для прекращения работы мастера на любом этапе служит кнопка **Отмена**.

Вы также можете переключаться между пройденными шагами мастера с помощью кнопок навигации в верхней части окна.

Чтобы настроить параметры Центра управления, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Центр управления** в нижней части окна.
2. В открывшемся окне по ссылке **Настройка** в верхней части окна запустите мастер настройки удаленного управления. Рассмотрим подробнее шаги мастера:
   a. Введите или измените пароль администратора в окне **Защита паролем**.
   b. Выберите компьютеры для удаленного управления в окне **Поиск компьютеров**.
   c. Выберите способ обновления баз в окне **Способ обновления**.
   d. Подтвердите выбранные параметры в окне **Сводка**.

ПРОВЕРКА ДОМАШНЕЙ СЕТИ НА ВИРУСЫ И УЯЗВИМОСТИ

Через Центр управления вы можете запустить задачу проверки на вирусы удаленно как для всей сети, так и для отдельного компьютера.

Чтобы проверить на вирусы всю сеть, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Центр управления** в нижней части окна.
2. В открывшемся окне перейдите по ссылке **Выполнить проверку на вирусы** в блоке **Действия для сети** в верхней части окна.
3. В открывшемся окне **Групповой запуск проверки** выберите тип проверки и компьютеры, которые требуется проверить.

Чтобы проверить на вирусы и уязвимости отдельный компьютер, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Центр управления** в нижней части окна.
2. В открывшемся окне выберите компьютер в верхней части окна и перейдите в раздел **Проверка**.
3. В правой части окна выберите нужную задачу проверки.

УДАЛЕННОЕ ОБНОВЛЕНИЕ БАЗ НА КОМПЬЮТЕРАХ В СЕТИ

Через Центр управления можно удаленно управлять обновлением Kaspersky CRYSTAL на компьютерах в сети.

Вы можете выбрать один из следующих способов обновлений:

- Обновление баз на компьютерах независимо друг от друга.
- Загрузка обновлений с выбранного компьютера в сети. При этом один из компьютеров сети требуется назначить сервером обновлений. Остальные компьютеры будут загружать обновления с этого компьютера.

Чтобы изменить способ обновления баз на компьютерах в сети, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Центр управления** в нижней части окна.

2. В открывшемся окне перейдите по ссылке **Настройка** в верхней части окна.

3. В открывшемся мастере настройки Центра управления перейдите к шагу **Способ обновления** и выберите нужный способ обновления.

Чтобы назначить компьютер сервером обновлений, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Центр управления** в нижней части окна.

2. В открывшемся окне выберите компьютер в верхней части окна и перейдите в раздел **Обновление**.

3. Нажмите на кнопку **Назначить сервером обновлений**.

Вы можете запустить задачу обновления удаленно как для всей сети, так и для отдельного компьютера.

Чтобы запустить обновление на всех компьютерах сети, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Центр управления** в нижней части окна.

2. В открывшемся окне перейдите по ссылке **Выполнить обновление** в меню **Действия для сети** в верхней части окна.

3. В открывшемся окне **Групповой запуск обновления** выберите компьютеры, на которые требуется загрузить обновления.

Чтобы запустить обновление на отдельном компьютере, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Центр управления** в нижней части окна.

2. В открывшемся окне выберите компьютер в верхней части окна и перейдите в раздел **Обновление**.

3. В правой части окна нажмите на кнопку **Выполнить обновление**.

Включение / отключение компонентов защиты на компьютерах в сети

Через Центр управления вы можете удаленно включать / отключать различные компоненты защиты на компьютерах сети.

Чтобы удаленно включить / отключить компонент защиты, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Центр управления** в нижней части окна.

2. В открывшемся окне выберите компьютер, для которого требуется управление защитой, и перейдите в раздел **Информация**.

3. В правой части окна выберите пункт **Компоненты защиты**.

4. В открывшемся окне **Компоненты защиты** включите / отключите нужный компонент защиты щелчком мыши по значку статуса справа от названия компонента.

Удаленное управление Родительским контролем

Через Центр управления вы можете удаленно устанавливать ограничения и просматривать статистику событий, связанных с работой пользователей на компьютерах сети и в интернете.

- *Чтобы удаленно настроить родительский контроль, выполните следующие действия:*

  1. Откройте главное окно программы и нажмите на кнопку **Центр управления** в нижней части окна.
  2. В открывшемся окне выберите компьютер в верхней части окна и перейдите в раздел **Родительский контроль**.
  3. В правой части окна выберите учетную запись и нажмите на кнопку **Настроить**.

- *Чтобы просмотреть статистику, выполните следующие действия:*

  1. Откройте главное окно программы и нажмите на кнопку **Центр управления** в нижней части окна.
  2. В открывшемся окне выберите компьютер в верхней части окна и перейдите в раздел **Родительский контроль**.
  3. В правой части окна выберите учетную запись и нажмите на кнопку **Подробный отчет**.

ЗАПУСК РЕЗЕРВНОГО КОПИРОВАНИЯ НА КОМПЬЮТЕРАХ В СЕТИ

Через Центр управления вы можете удаленно выполнять задачи резервного копирования на компьютерах сети, а также просматривать отчет о выполненных задачах резервного копирования и восстановления данных.

- *Чтобы выполнить резервное копирование удаленно, выполните следующие действия:*

  1. Откройте главное окно программы и нажмите на кнопку **Центр управления** в нижней части окна.
  2. В открывшемся окне выберите компьютер в верхней части окна и перейдите в раздел **Резервное копирование**.
  3. В правой части окна выберите задачу резервного копирования и нажмите на кнопку **Выполнить**.

     Вы можете приостановить или отменить выполнение задачи, используя соответствующие кнопки в верхней части окна.

- *Чтобы получить отчет о задачах резервного копирования и восстановления данных, выполните следующие действия:*

  1. Откройте главное окно программы и нажмите на кнопку **Центр управления** в нижней части окна.
  2. В открывшемся окне выберите компьютер в верхней части окна и перейдите в раздел **Резервное копирование**.
  3. Нажмите на кнопку **Посмотреть отчет** в верхней части окна.
  4. В открывшемся окне **Отчет** настройте параметры отображения информации о событиях.

УДАЛЕННОЕ УПРАВЛЕНИЕ ЛИЦЕНЗИЯМИ НА КОМПЬЮТЕРАХ В СЕТИ

Через Центр управления вы можете удаленно проверить статус лицензии на компьютерах сети, продлить срок действия лицензии или активировать программу с новой лицензией.

- *Чтобы управлять лицензией на компьютере сети, выполните следующие действия:*

  1. Откройте главное окно программы и нажмите на кнопку **Центр управления** в нижней части окна.
  2. В открывшемся окне выберите компьютер, для которого требуется отобразить список проблем, и перейдите в раздел **Информация**.

3. В правой части открывшегося окна выберите пункт **Управление лицензиями**.

4. В открывшемся окне **Управление лицензиями** выполните нужные действия.

Менеджер паролей

Менеджер паролей сохраняет и защищает все ваши персональные данные (например, пароли, имена пользователей, номера интернет-пейджеров, контактные данные, номера телефонов и т. д.). Менеджер паролей связывает пароли и учетные записи с программами Microsoft Windows или веб-страницами, для которых они используются. Вся информация в зашифрованном виде хранится в базе паролей, доступ к которой защищен мастер-паролем. Доступ к информации открыт, только если база паролей разблокирована. После запуска веб-страницы или программы Менеджер паролей автоматически вводит пароль, имя пользователя и другие персональные данные. Таким образом, вам достаточно запомнить один пароль и необязательно запоминать остальные.

По умолчанию Менеджер паролей загружается при запуске операционной системы. Компонент встраивается в программы, что позволяет управлять персональными данными непосредственно из окна программ.

Менеджер паролей отслеживает действия программ с паролями и предотвращает перехват и воровство персональной информации. Компонент проверяет программы, которые используют пароли или запрашивают пароль у других программ, а затем предлагает вам разрешить или запретить подозрительное действие.

Кроме того, Менеджер паролей позволяет:

- сохранять и использовать ваши пароли (см. стр. 198);
- искать учетные записи, пароли, имена пользователей и другую персональную информацию в базе паролей (см. стр. 199);
- генерировать надежные пароли (см. стр. 216) при регистрации новых учетных записей;
- хранить все пароли на съемном носителе (см. стр. 217);
- восстановить базу паролей из резервной копии (см. стр. 201);
- защищать пароли от несанкционированного доступа (см. стр. 190).

Чтобы открыть Менеджер паролей из главного окна Kaspersky CRYSTAL,

1. Откройте главное окно программы.
2. В нижней части окна нажмите на кнопку **Менеджер паролей**.

Чтобы открыть Менеджер паролей из контекстного меню,

выберите пункт **Менеджер паролей** в контекстном меню Менеджера паролей.

Вы также можете настроить запуск Менеджера паролей двойным щелчком мыши (см. стр. 215) по значку Менеджера паролей в области уведомления панели задач.

В этом разделе

Управление базой паролей 190

Настройка параметров программы 203

Создание надежных паролей 216

Использование переносной версии Менеджера паролей 217

Управление базой паролей

В базе паролей хранятся все учетные записи программ и веб-страниц с одним или несколькими именами пользователей, а также визитные карточки (содержащие, например, контактные данные, номера телефонов, номера интернет-пейджеров и т. д.).

Работать с базой паролей вы можете в том случае, если она не заблокирована (см. стр. 190). Перед тем как внести любые изменения в базу паролей, рекомендуется настроить параметры резервного копирования базы (см. стр. 209). Если данные были нечаянно изменены или удалены, используйте восстановление базы (см. стр. 201).

Вы можете выполнить следующие действия:

- добавить (см. стр. 191), изменить, удалить (см. стр. 200) персональные данные;
- импортировать / экспортировать (см. стр. 200), восстанавливать (см. стр. 201) базу паролей.

В этом разделе

Доступ к базе паролей 190

Добавление персональных данных 191

Использование персональных данных 198

Поиск паролей 199

Удаление персональных данных 200

Импорт / экспорт данных 200

Резервное копирование / Восстановление базы паролей 201

Доступ к базе паролей

Для доступа к базе паролей можно выбрать один из следующих методов авторизации:

- **Защита мастер-паролем**. Для доступа к базе паролей используется мастер-пароль.
- **USB-устройство**. Для доступа к базе паролей используется устройство с USB-интерфейсом, подключенное к компьютеру. Когда USB-устройство отключено, база паролей будет автоматически заблокирована.
- **Bluetooth-устройство**. Для доступа к базе паролей используется Bluetooth-устройство, подключенное к компьютеру. Когда Bluetooth-устройство отключено, база паролей будет автоматически заблокирована.
- **Без авторизации**. Доступ к базе паролей не защищен.

По умолчанию установлена защита мастер-паролем, что позволяет вам помнить только один пароль и не запоминать все остальные.

Мастер-пароль – это основной метод защиты ваших персональных данных. Если был выбран метод авторизации устройством и в дальнейшем его не оказалось под рукой (или, например, оно было потеряно), вы можете использовать мастер-пароль для доступа к вашим персональным данным.

По умолчанию Менеджер паролей блокирует базу паролей при запуске программы и по истечении заданного времени бездействия компьютера (см. стр. 210). Работа с программой возможна только в том случае, если база паролей не заблокирована.

Вы также можете разблокировать / заблокировать базу паролей следующими способами:

- в окне Менеджер паролей (см. стр. 44);
- посредством USB-, Bluetooth-устройства – используется только для метода авторизации USB-, Bluetooth-устройством;
- двойным щелчком мыши на значке программы (см. стр. 215) – для этого должно быть дополнительно установлено действие по двойному щелчку мыши;
- из контекстного меню Менеджера паролей (см. стр. 45);
- комбинацией клавиш CTRL+ALT+L (см. стр. 207).

Для ввода мастер-пароля вы можете использовать виртуальную клавиатуру, которая позволяет вводить пароли без нажатия клавиш на клавиатуре.

Чтобы заблокировать программу из контекстного меню программы, выполните следующие действия:

1. В области уведомлений панели задач нажмите правой клавишей мыши на значок Менеджера паролей.
2. В открывшемся меню выберите пункт **Заблокировать**.

Чтобы разблокировать базу паролей из контекстного меню, выполните следующие действия:

1. В области уведомлений панели задач нажмите правой клавишей мыши на значок Менеджера паролей.
2. В открывшемся меню выберите пункт **Разблокировать**.
3. В открывшемся окне введите мастер-пароль.

ДОБАВЛЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Добавление персональных данных возможно, если база паролей не заблокирована (см. стр. 190). При запуске программы / веб-страницы новая учетная запись распознается автоматически, если она не была найдена в базе паролей. Тогда после авторизации в программе / на веб-странице Менеджер паролей предлагает добавить персональные данные в базу паролей.

В базе паролей доступны следующие типы персональных данных:

- **Учетная запись**. Комбинация имен пользователей и пароля для авторизации на веб-странице или в программе.
- **Группа учетных записей**. Используется для удобной организации учетных записей в базе паролей.
- **Имя пользователя**. По умолчанию Менеджер паролей предлагает создать учетную запись с одним именем пользователя. Дополнительное имя пользователя используется, когда программы или веб-страницы позволяют создавать несколько имен пользователей для доступа к их ресурсам.
- **Визитка**. Используется для хранения таких данных, как пол, дата рождения, контактная информация, номер телефона, место работы, номер интернет-пейджера, адрес домашней веб-страницы и т д. Чтобы разделить деловую и личную информацию, вы можете создать несколько визиток.
- **Личная заметка**. Используется для хранения любой информации.

Учетная запись

Менеджер паролей автоматически распознает новую учетную запись, если она не была найдена в базе паролей. После завершения авторизации в программе / на веб-странице Менеджер паролей предлагает сохранить данные в базе паролей. Вы также можете вручную добавить новую учетную запись в базу паролей.

Учетная запись содержит следующие данные:

- тип учетной записи (учетная запись программы или учетная запись интернета);
- имя / несколько имен пользователей;
- пароль;
- путь к программе / веб-адрес веб-страницы в интернете (в зависимости от типа учетной записи);
- параметры связи учетной записи с объектом;
- параметры активизации учетной записи;
- комментарий;
- параметры заполнения дополнительных полей на веб-странице.

Менеджер паролей позволяет использовать одну или несколько учетных записей для авторизации в программе или на веб-сайте.

На основе пути к программе или веб-адреса для веб-страницы Менеджер паролей позволяет задать область использования каждой учетной записи.

Перейти к добавлению учетной записи можно несколькими способами:

- по кнопке быстрого запуска – для этого нужно выбрать пункт **Добавить учетную запись** в меню кнопки быстрого запуска;
- из контекстного меню Менеджера паролей – для этого нужно выбрать пункт **Добавить учетную запись** в контекстном меню Менеджера паролей;
- из главного окна Менеджера паролей.

Чтобы добавить новую учетную запись из главного окна, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна нажмите на кнопку **Менеджер паролей**.
3. В открывшемся окне **Менеджер паролей** нажмите на кнопку **База паролей**.
4. В верхней части открывшегося окна нажмите на кнопку **Добавить** и выберите пункт **Добавить учетную запись**.
5. В открывшемся мастере создания учетной записи выберите тип учетной записи (учетная запись интернета, учетная запись программы или пользовательский режим) и нажмите на кнопку **Далее**.
   - Если вы выбрали учетную запись интернета или программы, укажите веб-сайт или программу, для которой будет использоваться учетная запись, и нажмите на кнопку **Далее**.
   - Если вы выбрали расширенный режим, в открывшемся окне на закладке **Связь** укажите путь к программе / веб-странице и задайте параметры использования учетной записи.
6. В верхней части окна в поле **Имя** введите или отредактируйте название новой учетной записи.

7. На закладке **Регистрационные данные** введите имя пользователя и пароль.

   Имя пользователя может состоять из одного или нескольких слов. Чтобы задать ключевые слова (см. стр. 193) для имени пользователя, нажмите на кнопку .

   Чтобы скопировать имя пользователя / пароль в буфер обмена, нажмите на кнопку .

   Чтобы скопировать имя пользователя из другой учетной записи, перейдите по ссылке **Использовать имя пользователя другой учетной записи**.

   Чтобы создать пароль автоматически, перейдите по ссылке **Создать новый пароль** (см. стр. 216).

8. На закладке **Редактирование формы вручную** при необходимости настройте параметры заполнения других полей для веб-страницы.

9. На закладке **Комментарий** при необходимости дополнительно введите поясняющий текст для учетной записи. Чтобы комментарий отображался в уведомлении после активизации учетной записи, установите флажок **Показывать комментарии в уведомлении**.

НАЗНАЧЕНИЕ КЛЮЧЕВЫХ СЛОВ ДЛЯ ПОИСКА

Для быстрого поиска персональных данных в базе паролей вы можете использовать ключевые слова. Они формируются для каждого имени пользователя. Рекомендуется назначать ключевые слова при добавлении учетной записи (см. стр. 192) / имени пользователя (см. стр. 197).

Чтобы задать ключевые слова для имени пользователя, выполните следующие действия:

1. Откройте главное окно программы.

2. В нижней части окна нажмите на кнопку **Менеджер паролей**.

3. В открывшемся окне **Менеджер паролей** нажмите на кнопку **База паролей**.

4. Выберите имя пользователя в списке **Мои пароли** и в верхней части окна нажмите на кнопку **Изменить**.

5. В открывшемся окне нажмите на кнопку рядом с полем **Имя пользователя** и введите ключевые слова в поле **Описание**.

   Если была выбрана учетная запись с одним именем пользователя, в открывшемся окне **Учетная запись с одним именем пользователя** на закладке **Регистрационные данные** нажмите на кнопку .

ДОБАВЛЕНИЕ ПУТИ К ПРОГРАММЕ / ВЕБ-СТРАНИЦЕ

Для связи учетной записи с программой или веб-страницей нужно создать ссылку. Для веб-страницы ссылка представляет собой веб-адрес, а для программы – путь к исполняемому файлу программы на компьютере. Без этих данных учетная запись не будет связана ни с одной программой / веб-страницей.

Связать учетную запись с программой / веб-страницей можно следующими способами:

- выбрав ссылку по кнопке из списка избранных веб-сайтов вашего веб-браузера или из списка программ на вашем компьютере;
- указав вручную путь к программе / веб-странице;
- используя указатель Менеджера паролей.

Чтобы проверить правильность введенного пути, запустите программу / веб-страницу по кнопке .

Чтобы выбрать ссылку из списка, выполните следующие действия:

1. Откройте главное окно программы.

2. В нижней части окна нажмите на кнопку **Менеджер паролей**.

3. В открывшемся окне **Менеджер паролей** нажмите на кнопку **База паролей**.

4. В верхней части окна нажмите на кнопку **Добавить** и выберите пункт **Добавить учетную запись**.

5. В открывшемся окне на закладке **Связи** в поле **Ссылка** нажмите на кнопку  .

6. В открывшемся окне в поле **Ссылка** введите путь для программы / веб-страницы.

   Чтобы указать веб-страницу из списка сохраненных веб-страниц (Избранное), в списке **Закладки** выберите веб-страницу и перейдите по ссылке **Копировать ссылку из Избранного**. Чтобы скопировать путь к веб-странице из окна веб-браузера, нажмите на ссылку **Использовать путь к связанной программе**.

   Чтобы создать ссылку на программу, в поле **Ссылка** нажмите на кнопку  и укажите путь к исполняемому файлу программы.

Чтобы указать путь к программе / веб-странице вручную, выполните следующие действия:

1. Откройте главное окно программы.

2. В нижней части окна нажмите на кнопку **Менеджер паролей**.

3. В открывшемся окне **Менеджер паролей** нажмите на кнопку **База паролей**.

4. В верхней части окна нажмите на кнопку **Добавить** и выберите пункт **Добавить учетную запись**.

5. В открывшемся окне на закладке **Связи** в поле **Ссылка** введите путь к программе / адрес веб-страницы. Адрес веб-страницы должен начинаться с http://www.

Чтобы ввести путь к программе / веб-странице указателем Менеджера паролей, выполните следующие действия:

1. Откройте главное окно программы.

2. В нижней части окна нажмите на кнопку **Менеджер паролей**.

3. В открывшемся окне **Менеджер паролей** нажмите на кнопку **База паролей**.

4. В верхней части окна нажмите на кнопку **Добавить** и выберите пункт **Добавить учетную запись**.

5. В открывшемся окне на закладке **Связи** в поле **Ссылка** введите путь к программе / веб-странице путем наведения указателя Менеджера паролей на окно программы / веб-браузера.

Выбор способа привязки учетной записи

Чтобы определить, данные из какой учетной записи автоматически вводить при запуске программы / веб-страницы, Менеджер паролей использует путь к программе / веб-адрес для веб-страницы.

Поскольку Менеджер паролей позволяет использовать несколько учетных записей для одной программы / веб-сайта, то для каждой учетной записи нужно определить область ее использования.

На основе введенного пути к программе / веб-адреса для веб-страницы Менеджер паролей позволяет сформировать область использования учетной записи. Параметры области настраиваются при создании учетной записи (см. стр. 192). В дальнейшем вы можете изменить их значения.

В зависимости от объекта (программы или веб-сайта) варианты использования учетной записи различаются.

Для программы возможны следующие варианты:

- Использовать учетную запись для программы. Учетная запись будет использоваться для всех окон программы, в которых есть поля для ввода персональных данных.

- Распознавать по заголовку окна. Учетная запись будет использоваться только для указанного окна программы.

  Например, одна программа может использовать несколько учетных записей. Для разных учетных записей в одной программе будут различаться только заголовки окна. Менеджер паролей будет автоматически вводить данные учетной записи на основе заголовка окна программы.

Для веб-страницы возможны следующие варианты использования учетной записи:

- Только для указанной веб-страницы. Менеджер паролей автоматически добавит имя пользователя и пароль в поля идентификации только на веб-странице с данным адресом.

  Например, если учетная запись привязана к веб-странице с адресом http://www.web-site.com/login.html, то для других веб-страниц веб-сайта (например, для веб-страницы http://www.web-site.com/index.php) данная учетная запись действовать не будет.

- Для веб-страниц из директории. Менеджер паролей автоматически добавит имя пользователя и пароль в поля идентификации для всех веб-страниц последней папки.

  Например, если был введен адрес веб-сайта http://www.web-site.com/cgi-bin/login.html, то для всех веб-страниц в папке *cgi-bin* будет использоваться данная учетная запись.

- Для веб-сайта: <название домена от третьего уровня и ниже>. Данная учетная запись используется для любой веб-страницы домена (от домена третьего уровня и ниже).

  Например, Менеджер паролей автоматически добавит идентификационные данные для веб-страниц: http://www.domain1.domain2.web-site.com/login.html или http://www.domain1.domain2.web-site.com/index.php. Однако данная учетная запись не будет использоваться для веб-страниц с адресами, у которых разные домены четвертого уровня: http://www.domain3.domain2.web-site.com/index.php или http://www.domain4.domain2.web-site.com/index.php.

- Для веб-сайта: <название веб-сайта>. Данная учетная запись будет использоваться для всех страниц веб-сайта, на которых имеются поля ввода имени пользователя и пароля.

  Например, Менеджер паролей автоматически добавит идентификационные данные для веб-страниц: http://www.domain1.domain2.web-site.com/login.html, http://www.domain2.domain2.web-site.com/index.php, http://www.domain3.domain2.web-site.com/index.php или http://www.domain4.domain2.web-site.com/index.php.

Чтобы задать параметры использования учетной записи, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна нажмите на кнопку **Менеджер паролей**.
3. В открывшемся окне **Менеджер паролей** нажмите на кнопку **База паролей**.
4. Выберите учетную запись из списка **Мои пароли** и нажмите на кнопку **Изменить**.
5. В открывшемся окне на закладке **Связи** выберите один из вариантов использования учетной записи.

АВТОМАТИЧЕСКАЯ АКТИВИЗАЦИЯ УЧЕТНОЙ ЗАПИСИ

По умолчанию автоматическая активизация для учетной записи включена. Менеджер паролей вводит только имя пользователя и пароль в поля идентификации. Вы можете настроить дополнительные параметры активизации учетной записи (см. стр. 192).

Дополнительно для веб-страницы указывается диапазон веб-адресов, для которого используется автоматическая активизация.

Возможны следующие варианты активизации учетной записи:

- Для выбранной веб-страницы. Учетная запись активируется только для данной веб-страницы.

- Для веб-сайта. Учетная запись активируется на всех веб-страницах веб-сайта.

Чтобы установить автоматическую активизацию учетной записи, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна нажмите на кнопку **Менеджер паролей**.
3. В открывшемся окне **Менеджер паролей** нажмите на кнопку **База паролей**.
4. Выберите учетную запись из списка **Мои пароли** и нажмите на кнопку **Изменить**.
5. В открывшемся окне на закладке **Связи** установите флажок **Автоматическая активизация учетной записи после загрузки**.

   Дополнительно для веб-страницы выберите один из способов активизации учетной записи.

Заполнение дополнительных полей

При авторизации на веб-странице, кроме пароля и имени пользователя, иногда запрашиваются другие данные. Менеджер паролей позволяет использовать автоматическое заполнение дополнительных полей. Вы можете настроить параметры автоматического заполнения дополнительных полей для учетной записи.

Настроить параметры дополнительных полей можно в том случае, если для учетной записи указан путь к программе / адрес веб-страницы.

Для настройки параметров полей Менеджер паролей временно загружает веб-страницу, затем анализирует все поля и кнопки. Поля и кнопки объединены в группы для каждой веб-страницы.

Во время работы с загруженной веб-страницей Менеджер паролей временно сохраняет файлы и рисунки на вашем компьютере.

Чтобы настроить параметры дополнительных полей, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна нажмите на кнопку **Менеджер паролей**.
3. В открывшемся окне **Менеджер паролей** нажмите на кнопку **База паролей**.
4. Выберите учетную запись из списка **Мои пароли** и нажмите **Изменить**.
5. В открывшемся окне на закладке **Редактирование формы вручную** перейдите по ссылке **Нажмите, чтобы изменить значения полей**.
6. В верхней части открывшегося окна **Редактирование формы вручную** установите флажок рядом с нужным полем / кнопкой.
7. Активируйте поле в графе **Значение** для выбранного поля / кнопки двойным щелчком мыши, а затем задайте значение поля.

Создание группы учетных записей

Использование групп учетных записей помогает организовать информацию в базе паролей. Группа состоит из папки с добавленными в нее учетными записями.

Созданные группы отображаются в контекстном меню Менеджера паролей: пункт **Учетные записи** → **<Название группы>**.

Чтобы создать группу учетных записей, выполните следующие действия:

1. Откройте главное окно программы.

2. В нижней части окна нажмите на кнопку **Менеджер паролей**.
3. В открывшемся окне **Менеджер паролей** нажмите на кнопку **База паролей**.
4. В верхней части окна нажмите на кнопку **Добавить** и выберите пункт **Добавить группу**.
5. Введите название для новой группы.
6. Добавьте из списка **Мои пароли** учетные записи путем их перетаскивания в созданную папку.

Имя пользователя

Для работы с некоторыми программами / веб-сайтами часто используются несколько имен пользователей. Менеджер паролей позволяет сохранять для одной учетной записи несколько имен пользователей. Менеджер паролей автоматически распознает новое имя пользователя при первом использовании и предлагает добавить его в учетную запись для данной программы / веб-страницы. Вы можете вручную добавить новое имя пользователя для учетной записи, а затем изменить его. Также вы можете использовать одно и то же имя пользователя для разных учетных записей

Перейти к добавлению нового имени пользователя для учетной записи можно следующими способами:

- По кнопке быстрого запуска. Для этого в меню кнопки быстрого запуска выберите пункт **Изменить учетную запись** → **Добавить имя пользователя**.
- Из главного окна программы.

Чтобы добавить имя пользователя для учетной записи, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна нажмите на кнопку **Менеджер паролей**.
3. В открывшемся окне **Менеджер паролей** нажмите на кнопку **База паролей**.
4. Выберите учетную запись из списка **Мои пароли**, нажмите на кнопку **Добавить** и выберите пункт **Добавить имя пользователя**.
5. В открывшемся окне введите имя пользователя и пароль. Имя пользователя может состоять из одного или нескольких слов. Чтобы задать ключевые слова для имени пользователя, нажмите на кнопку  , затем заполните поле **Описание**.

   Чтобы скопировать имя пользователя / пароль в буфер обмена, воспользуйтесь кнопкой  . Чтобы создать пароль автоматически, воспользуйтесь ссылкой **Создать новый пароль** (см. стр. 216).

   Чтобы скопировать имя пользователя из другой учетной записи, перейдите по ссылке **Использовать имя пользователя другой учетной записи**.

Визитка

Для регистрации на веб-сайте, кроме имени пользователя и пароля, часто используются другие персональные данные, например, ФИО, год рождения, пол, адрес электронной почты, номер телефона, страна проживания и т. д. Все эти данные Менеджер паролей позволяет хранить в зашифрованной базе паролей в виде визиток. При регистрации на новом веб-сайте Менеджер паролей автоматически заполняет регистрационную форму на основе данных из выбранной визитки. Чтобы разделить при хранении деловую и частную информацию, можно использовать несколько визиток. В дальнейшем вы можете изменить параметры визитки.

Чтобы создать визитку, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна нажмите на кнопку **Менеджер паролей**.
3. В открывшемся окне **Менеджер паролей** нажмите на кнопку **База паролей**.

4. В верхней части окна нажмите на кнопку **Добавить визитку**.

5. В открывшемся окне в поле **Имя** введите название визитки.

6. Введите значение для необходимых полей, активируя их двойным щелчком мыши в графе **Значение**.

Личная заметка

Личные заметки предназначены для хранения текстовой информации в зашифрованном виде (например, паспортные данные, номера банковских счетов и т.п.) и для быстрого доступа к сохраненным данным. Для работы с текстом личной заметки Менеджер паролей содержит набор стандартных инструментов текстового редактора. При создании личной заметки можно использовать шаблоны с набором стандартных типов данных (см. стр. 213).

В дальнейшем вы можете изменить параметры личной заметки.

- *Чтобы создать личную заметку с нуля, выполните следующие действия:*

1. Откройте главное окно программы.

2. В нижней части окна нажмите на кнопку **Менеджер паролей**.

3. В открывшемся окне **Менеджер паролей** нажмите на кнопку **База паролей**.

4. В верхней части окна нажмите на кнопку **Добавить личную заметку**.

5. В открывшемся окне в поле **Имя** введите название личной заметки.

6. Введите нужную информацию в текстовом редакторе.

- *Чтобы создать личную заметку на основе шаблона, выполните следующие действия:*

1. Откройте главное окно программы.

2. В нижней части окна нажмите на кнопку **Менеджер паролей**.

3. В открывшемся окне **Менеджер паролей** нажмите на кнопку **База паролей**.

4. В верхней части окна нажмите на кнопку **Добавить личную заметку**.

5. В открывшемся окне в поле **Имя** введите название личной заметки.

6. В нижней части окна нажмите на кнопку **Выбрать шаблон** и выберите нужный шаблон.

7. Заполните требуемые данные и отформатируйте текст при необходимости.

- *Чтобы просмотреть личную заметку,*

  откройте контекстное меню Менеджера паролей и выберите пункт **Личные заметки** → **<название группы>** →**<название личной заметки>**.

Использование персональных данных

Менеджер паролей связывает учетные записи с программами / веб-страницами, для которых они используются. При запуске программы / веб-страницы в базе паролей автоматически происходит поиск связанной учетной записи. Если учетная запись найдена, персональные данные вводятся автоматически. Если в базе паролей нет связанной учетной записи, Менеджер паролей предложит добавить ее в базу паролей (см. стр. 192).

Некоторые программы / веб-сайты могут использовать несколько имен пользователей. Менеджер паролей позволяет сохранить несколько имен пользователей для одной учетной записи. Если во время авторизации было использовано новое имя пользователя, Менеджер паролей предложит добавить его к учетной записи (см. стр. 197) для запущенной программы / веб-страницы. Тогда при запуске программы / веб-страницы рядом с

полями для ввода персональных данных появится окно со списком имен пользователя для данной учетной записи.

Помимо имени пользователя и пароля для регистрации, на веб-сайте часто используются другие персональные данные (например, ФИО, пол, страна, город, телефон, адрес электронной почты и т. д.). Такие данные Менеджер паролей хранит в зашифрованной базе паролей в виде визиток. Чтобы разделить деловую и частную информацию, можно создать несколько визиток (см. стр. 197). Тогда при регистрации в программе / на веб-сайте Менеджер паролей автоматически заполнит поля регистрационной формы на основе данных из выбранной карточки. Использование визиток экономит время при заполнении одинаковых регистрационных форм.

При авторизации в программе / на веб-странице Менеджер паролей автоматически вводит персональные данные, только если база паролей не заблокирована.

Использовать учетную запись можно следующими способами:

- Запустить программу / веб-страницу. Форма авторизации будет заполнена автоматически на основе данных учетной записи.
- Применить указатель Менеджера паролей. Для этого наведите курсор мыши на значок программы в области уведомлений панели задач, а затем активируйте учетную запись путем перетаскивания указателя Менеджера паролей в окно нужной программы / веб-страницы.
- Выбрать учетную запись из списка часто используемых учетных записей. Для этого откройте контекстное меню Менеджера паролей и в блоке часто используемых учетных записей выберите нужную запись.
- Использовать контекстное меню Менеджера паролей. Для этого откройте контекстное меню Менеджера паролей и выберите пункт **Учетные записи** → **<Название учетной записи>**.

Чтобы использовать визитку, выполните следующие действия:

1. В окне программы / веб-браузера в правом верхнем углу нажмите на кнопку быстрого запуска.
2. В открывшемся меню выберите пункт **Визитки** → **<Название визитки>**. Менеджер паролей автоматически заполнит регистрационные поля веб-страницы на основе данных из визитки.

Поиск паролей

Поиск персональных данных может быть затруднен в следующих случаях:

- некоторые пароли не связаны с программами / веб-страницами;
- база паролей содержит большое число учетных записей.

Менеджер паролей позволяет быстро находить пароли по следующим параметрам:

- названию учетной записи;
- имени пользователя;
- ключевым словам (см. стр. 193) (параметры поиска по ключевым словам настраиваются дополнительно для каждого имени пользователя);
- веб-адресу (для веб-страниц).

Поиск производится как по целому названию, так и по начальным буквам и любым символам в названии учетной записи или ссылки.

Чтобы найти учетную запись / пароль, выполните следующие действия:

1. Откройте главное окно программы.

2. В нижней части окна нажмите на кнопку **Менеджер паролей**.
3. В открывшемся окне **Менеджер паролей** нажмите на кнопку **База паролей**.
4. В верхней части окна в строке поиска введите текст.

Удаление персональных данных

Перед внесением любых изменений в персональные данные Менеджер паролей автоматически создает резервную копию базы паролей. Если данные были нечаянно изменены или удалены, используйте восстановление базы паролей (см. стр. 201). Из базы паролей можно удалить один или все элементы.

Чтобы удалить один элемент из базы паролей, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна нажмите на кнопку **Менеджер паролей**.
3. В открывшемся окне **Менеджер паролей** нажмите на кнопку **База паролей**.
4. Выберите элемент из списка **Мои пароли**, нажмите на кнопку **Удалить** и выберите пункт **Удалить**.

Чтобы удалить все элементы из базы паролей, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна нажмите на кнопку **Менеджер паролей**.
3. В открывшемся окне **Менеджер паролей** нажмите на кнопку **База паролей**.
4. Выберите элемент из списка **Мои пароли**, нажмите на кнопку **Удалить** и выберите пункт **Удалить все**.

Импорт / экспорт данных

Менеджер паролей предоставляет возможность импортировать и экспортировать вашу базу паролей, а также отдельные объекты базы паролей (визитки, учетные записи или личные заметки).

Вы можете загрузить пароли из других программ управления паролями (например, из Internet Explorer, Mozilla Firefox, KeePass) и пароли, которые вы ранее сохранили с помощью Менеджера паролей. Импорт паролей осуществляется из файлов, имеющих формат xml, ini.

Менеджер паролей позволяет сохранить базу паролей в файл формата xml, html или txt. Сохранять пароли в файл удобно использовать в случаях, когда нужно открыть пароли в общий доступ, распечатать базу паролей или сохранить резервную копию базы паролей в файл другого формата (отличающегося от формата Менеджера паролей).

Сохраненные пароли хранятся в незашифрованных файлах и не защищены от несанкционированного доступа. Поэтому рекомендуется заранее продумать способы защиты экспортированных данных.

Во время импорта база паролей изменяется. Вы можете выбрать один из следующих вариантов действий с базой паролей:

- **Перезаписать**. Текущая база паролей будет заменена загруженной (все пароли, хранившиеся в базе паролей Менеджера паролей до загрузки, будут удалены).
- **Объединить**. В базу паролей будут добавлены загруженные пароли. При объединении вам предлагается выбрать учетные записи, которые будут загружены в Менеджер паролей.
- **Отмена**. Загрузка паролей будет отменена.

Чтобы загрузить пароли из файла, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна нажмите на кнопку **Менеджер паролей**.
3. В открывшемся окне **Менеджер паролей** нажмите на кнопку **База паролей**.
4. В нижней части окна перейдите по ссылке **Загрузить пароли**.
5. В открывшемся окне **Загрузка паролей** выберите программу, из которой будут импортированы пароли, и нажмите на кнопку **Загрузить пароли**.
6. В открывшемся окне укажите файл с паролями, который вы хотите загрузить, и нажмите на кнопку **Открыть**.
7. В открывшемся окне выберите вариант действия с базой паролей.

Чтобы сохранить базу паролей в файл, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна нажмите на кнопку **Менеджер паролей**.
3. В открывшемся окне **Менеджер паролей** нажмите на кнопку **База паролей**.
4. В нижней части окна перейдите по ссылке **Сохранить пароли**.
5. В открывшемся окне выберите способ сохранения (сохранение всей базы паролей или выбранных объектов) и нажмите на кнопку **Далее**.
6. В открывшемся окне выберите параметры сохранения:
   - Если вы хотите защитить сохраняемые данные, выберите вариант **Безопасное сохранение** и задайте пароль для защиты данных.
   - Если вы хотите сохранить данные в незащищенный файл, выберите вариант **Сохранение без шифрования** и укажите формат файла для сохранения.
   - Чтобы запланировать смену пароля для сохраняемых данных, установите флажок **Запланировать смену пароля для сохраняемых объектов** и выберите дату, при наступлении которой пароль будет сброшен, а Менеджер паролей уведомит вас о необходимости смены пароля.
7. В открывшемся окне укажите путь для сохранения файла и нажмите на кнопку **Далее**.
8. В открывшемся окне проверьте параметры сохранения ваших данных и запустите сохранение.

РЕЗЕРВНОЕ КОПИРОВАНИЕ / ВОССТАНОВЛЕНИЕ БАЗЫ ПАРОЛЕЙ

Перед внесением любых изменений в базу паролей автоматически создается ее резервная копия. Путь сохранения резервных копий задан по умолчанию, но вы можете его изменить (см. стр. 209). Восстановление паролей удобно использовать в следующих случаях:

- если требуется отменить последние изменения;
- если база паролей была перезаписана или удалена;
- если текущая база паролей недоступна / повреждена после аппаратной или системной ошибки.

Все данные в резервной копии хранятся в зашифрованном виде. Менеджер паролей регистрирует все изменения в базе паролей. В программе резервные копии отображаются в списке и отсортированы по дате создания, начиная с последней. Для каждой резервной копии указаны следующие данные:

- место хранения;
- дата и время создания;
- изменения, которые были сделаны относительно предыдущей версии.

Вы можете использовать резервные копии для решения следующих задач:

- восстановления базы паролей из выбранной резервной копии;
- удаления старых версий резервных копий;
- изменения места хранения резервных копий (см. стр. 209).

Чтобы восстановить базу паролей, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна нажмите на кнопку **Менеджер паролей**.
3. В открывшемся окне **Менеджер паролей** нажмите на кнопку **База паролей**.
4. В нижней части окна перейдите по ссылке **Восстановить базу паролей**.
5. В открывшемся окне **Восстановление** выберите дату резервной копии из списка и в верхней части окна нажмите на кнопку **Восстановление**.
6. В открывшемся окне подтвердите восстановление по кнопке **ОК**.

Чтобы удалить ненужные версии резервных копий, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна нажмите на кнопку **Менеджер паролей**.
3. В открывшемся окне **Менеджер паролей** нажмите на кнопку **База паролей**.
4. В нижней части окна перейдите по ссылке **Восстановить базу паролей**.
5. В открывшемся окне **Восстановление** в списке резервных копий выберите версии резервных копий для удаления. Чтобы выбрать несколько версий, удерживайте нажатой клавишу **CTRL**.
6. Нажмите на кнопку **Удалить**.
7. В открывшемся окне подтвердите удаление резервных копий по кнопке **ОК**.

Настройка параметров программы

Настройка параметров программы возможна только, если база паролей не заблокирована (см. стр. 190). Изменяя параметры, вы можете выполнить следующие действия:

- установить время запуска программы;
- включить уведомления (см. стр. 215);
- задать имя пользователя (см. стр. 204), которое будет использоваться по умолчанию при создании новой учетной записи;
- установить время хранения пароля в буфере обмена (см. стр. 214);
- настроить список часто используемых учетных записей (см. стр. 205);
- сформировать список игнорируемых веб-сайтов (см. стр. 206), для которых функции Менеджера паролей не используются;
- сформировать список доверенных веб-сайтов (см. стр. 206), для которых Менеджер паролей разрешит переадресацию;
- настроить комбинацию клавиш для быстрого вызова функций Менеджера паролей (см. стр. 207);
- изменить путь хранения базы паролей (см. стр. 207), резервных копий (см. стр. 209);
- изменить метод шифрования данных (см. стр. 209);
- настроить автоматическую блокировку базы паролей (см. стр. 210);
- изменить мастер-пароль (см. стр. 212);
- настроить доступ к базе паролей (см. стр. 211);
- изменить расположение кнопки быстрого запуска, сформировать список программ, поддерживающих кнопку быстрого запуска (см. стр. 214);
- сформировать список поддерживаемых программ (см. стр. 212).

Чтобы изменить параметры работы Менеджера паролей, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна нажмите на кнопку **Менеджер паролей**.
3. В открывшемся окне нажмите на кнопку **Параметры**.
4. В открывшемся окне выберите нужный раздел для редактирования.
5. В правой части окна для выбранного раздела внесите необходимые изменения в группу параметров.

В этом разделе

Мастер настройки параметров 204

Использование имени пользователя по умолчанию 204

Часто используемые учетные записи 205

Игнорируемые веб-адреса 206

Доверенные веб-адреса 206

Горячие клавиши 207

Расположение файла базы паролей 207

Создание новой базы паролей 208

Расположение резервной копии 209

Выбор метода шифрования 209

Автоматическое блокирование базы паролей 210

Изменение способа авторизации Менеджера паролей 211

Использование USB-, Bluetooth-устройств для авторизации 211

Изменение мастер-пароля 212

Поддерживаемые веб-браузеры 212

Управление шаблонами личных заметок 213

Отображение кнопки быстрого запуска 214

Время хранения пароля в буфере обмена 214

Уведомления 215

Действие по двойному щелчку мыши 215

Мастер настройки параметров

Мастер настройки параметров программы запускается при первом запуске Менеджера паролей. Его задача – помочь вам провести первичную настройку параметров Менеджера паролей в зависимости от ваших личных предпочтений и стоящих перед вами задач.

Мастер состоит из последовательности окон (шагов), переключение между которыми осуществляется нажатием на кнопки **Назад** и **Далее**. Работа мастера завершается нажатием на кнопку **Завершить**. Для прекращения работы мастера на любом этапе следует нажать на кнопку **Отмена**.

Далее мы рассмотрим каждый шаг мастера подробнее.

Использование имени пользователя по умолчанию

Менеджер паролей позволяет задать имя пользователя, которое будет автоматически отображаться в поле **Имя пользователя** при создании новой учетной записи (см. стр. 192).

Чтобы задать имя пользователя по умолчанию, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна нажмите на кнопку **Менеджер паролей**.
3. В открывшемся окне нажмите на кнопку **Параметры**.
4. В левой части открывшегося окна выберите раздел **Основные**.
5. В правой части окна заполните поле **Имя пользователя по умолчанию**.

ЧАСТО ИСПОЛЬЗУЕМЫЕ УЧЕТНЫЕ ЗАПИСИ

Менеджер паролей обеспечивает быстрый доступ к учетным записям. Список часто используемых учетных записей отображается в главном окне программы, а также может отображаться в контекстном меню и в меню кнопки быстрого запуска. Список содержит названия программ / веб-страниц, которые вы запускаете чаще всего. Элементы списка расположены в алфавитном порядке или по частоте использования.

Список часто используемых учетных записей доступен в меню, если база паролей не заблокирована (см. стр. 190).

Вы можете задать следующие параметры списка:

- **Количество элементов в списке** – максимальное количество часто используемых учетных записей, которое отображается в контекстном меню программы;
- **Отображение списка в меню программы** – список часто используемых учетных записей будет доступен в контекстном меню Менеджера паролей;
- **Отображение списка в меню кнопки быстрого запуска** – список часто используемых учетных записей будет доступен в меню кнопки быстрого запуска (из окна программы / веб-браузера).

Чтобы отображать часто используемые учетные записи в контекстном меню, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна нажмите на кнопку **Менеджер паролей**.
3. В открывшемся окне нажмите на кнопку **Параметры**.
4. В левой части окна выберите раздел **Часто используемые учетные записи**.
5. В правой части окна установите флажок **Отображать список в меню программы**.

   Чтобы в меню кнопки быстрого запуска отображался список часто используемых учетных записей, дополнительно установите флажок **Отображать в меню кнопки быстрого запуска**.

   Если флажок **Отображать список в меню программы** не установлен, то остальные параметры списка будут недоступны для изменения.

6. Задайте количество учетных записей в поле **Размер списка**.
7. При необходимости вручную измените состав списка. Чтобы убрать элемент из списка, выберите в нем нужную учетную запись и нажмите на кнопку **Удалить**. Чтобы удалить все элементы из списка, нажмите на кнопку **Очистить**.

Игнорируемые веб-адреса

Вы можете настроить список веб-адресов, для которых функции Менеджера паролей не будут использоваться. Для веб-сайтов из этого списка отключаются функции автоматического ввода пароля и имени пользователя. Кроме того, для них Менеджер паролей не будет автоматически предлагать создание учетной записи (см. стр. 192) / имени пользователя (см. стр. 197).

Чтобы сформировать список игнорируемых веб-сайтов, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна нажмите на кнопку **Менеджер паролей**.
3. В открывшемся окне нажмите на кнопку **Параметры**.
4. В левой части окна выберите раздел **Игнорируемые веб-адреса**.
5. В правой части окна нажмите на кнопку **Добавить**, затем введите веб-адрес и нажмите на клавишу **ENTER**.

   Чтобы изменить веб-адрес, выберите его из списка и нажмите на кнопку **Изменить**. Чтобы удалить веб-адрес из списка, выберите его и нажмите на кнопку **Удалить**.

Доверенные веб-адреса

Менеджер паролей обеспечивает защиту ваших персональных данных от фишинг-атак. Если при попытке авторизоваться вы были переадресованы на другой веб-сайт, программа уведомит вас об этом.

Злоумышленники часто используют переадресацию на веб-сайтах, которые дают доступ к банковским счетам (например, это могут быть страницы интернет-банков, систем оплаты услуг и т. д.). На странице авторизации официального веб-сайта компании устанавливается переадресация на поддельный веб-сайт, визуально похожий на официальную интернет-страницу. Все введенные на поддельной странице данные попадают в руки злоумышленников.

Часто переадресация бывает официально установлена на веб-сайтах. Чтобы Менеджер паролей не считал данную переадресацию фишинг-атакой, вы можете сформировать список доверенных веб-адресов. В список доверенных веб-адресов входят веб-сайты, на которые передаются введенные персональные данные. При авторизации Менеджер паролей не будет уведомлять о передаче персональных данных на доверенный веб-сайт.

Менеджер паролей разрешает пересылать персональные данные с других веб-сайтов на доверенный веб-сайт. Перед добавлением веб-сайта в список доверенных, убедитесь в его полной надежности.

Добавить веб-сайт в список доверенных веб-адресов можно следующими способами:

- непосредственно во время авторизации на веб-сайте;
- вручную из окна **Настройка Менеджера паролей**.

Чтобы добавить веб-сайт в список доверенных веб-адресов во время авторизации на веб-сайте, дождитесь переадресации с одного веб-сайта на другой и затем в открывшемся окне Менеджера паролей установите флажок **Всегда доверять <название веб-сайта>**.

Чтобы вручную сформировать список доверенных веб-адресов, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна нажмите на кнопку **Менеджер паролей**.
3. В открывшемся окне нажмите на кнопку **Параметры**.

4. В левой части окна выберите раздел **Доверенные веб-адреса**.

5. В правой части окна нажмите на кнопку **Добавить**. Поле в списке **Доверенные веб-адреса** станет доступным. Затем введите веб-адрес и нажмите на клавишу **ENTER**.

   Чтобы изменить веб-адрес, выберите его в списке и нажмите на кнопку **Изменить**. Чтобы удалить веб-адрес из списка, выберите его в списке и нажмите на кнопку **Удалить**.

Горячие клавиши

Для быстрого запуска различных функций программы удобно использовать комбинацию клавиш на клавиатуре.

Вы можете задать комбинацию клавиш для следующих действий:

- Блокировать / разблокировать Менеджер паролей (см. стр. 190).
- Ввести пароль.

Для быстрого вызова функции можно задать одну клавишу или комбинацию из двух или трех клавиш.

Не назначайте для вызова функций Менеджера паролей те комбинации клавиш, которые используются в Microsoft Windows.

Чтобы назначить комбинации клавиш, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна нажмите на кнопку **Менеджер паролей**.
3. В открывшемся окне нажмите на кнопку **Параметры**.
4. В левой части окна выберите раздел **Горячие клавиши**.
5. В правой части окна задайте нужную комбинацию клавиш для каждого действия.

Расположение файла базы паролей

База паролей Менеджера паролей – это зашифрованный файл (см. стр. 209), в котором хранятся все ваши персональные данные (учетные записи, имена пользователей, пароли и визитки).

По умолчанию для разных версий Microsoft Windows путь к базе паролей следующий:

- для Microsoft Windows XP: C:\Documents and Settings\User_name\My Documents\Passwords Database\;
- для Microsoft Windows Vista: C:\Users\User_name\Documents\Passwords Database\;
- для Microsoft Windows 7: C:\Users\User_name\My Documents\Passwords Database\.

В качестве хранилища вашей базы паролей вы можете использовать разные накопители: съемный диск, локальный диск или сетевой диск.

При изменении пути к базе паролей или ее названия возможны следующие варианты действий:

- **Копировать** – будет создана копия базы паролей по указанному пути. Копия станет активной базой паролей.
- **Переместить** – активная база паролей будет сохранена по указанному пути.
- **Создать новую базу паролей** – будет создана пустая копия базы паролей, которая станет активной.

Чтобы переместить базу паролей и изменить ее имя, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна нажмите на кнопку **Менеджер паролей**.
3. В открывшемся окне нажмите на кнопку **Параметры**.
4. В левой части окна выберите раздел **Мои пароли**.
5. В правой части окна в блоке **Расположение** нажмите на кнопку  , расположенную в правой части поля **Путь**.
6. В открывшемся окне **Выбор базы паролей** задайте путь к файлу и его имя, затем нажмите на кнопку **Открыть**.
7. В открывшемся окне **Расположение базы паролей** выберите нужное действие с базой паролей.
8. В открывшемся окне **Менеджер паролей** введите мастер-пароль для подтверждения изменений.

Чтобы изменить текущую базу паролей, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна нажмите на кнопку **Менеджер паролей**.
3. В открывшемся окне нажмите на кнопку **Параметры**.
4. В левой части окна выберите раздел **Мои пароли**.
5. В правой части окна в блоке **Расположение** нажмите на кнопку  , расположенную в правой части поля **Путь**.
6. В открывшемся окне **Выбор базы паролей** выберите файл базы паролей и нажмите на кнопку **Открыть**.
7. В открывшемся окне **Менеджер паролей** введите мастер-пароль для доступа к выбранной базы паролей.

Создание новой базы паролей

Менеджер паролей позволяет последовательно работать с несколькими базами паролей. Создание новой базы паролей позволяет разделить ваши персональные данные, сохраняя их в двух и более базах паролей. При необходимости старую базу паролей можно восстановить. Менеджер паролей предложит создать новую базу паролей, если текущая база паролей повреждена или восстановление из резервной копии невозможно.

Чтобы создать новую базу паролей, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна нажмите на кнопку **Менеджер паролей**.
3. В открывшемся окне нажмите на кнопку **Параметры**.
4. В левой части окна выберите раздел **Мои пароли**.
5. В правой части окна в блоке **Расположение** нажмите на кнопку  , расположенную в правой части поля **Путь**.

6. В открывшемся окне **Выбор базы паролей** укажите место хранения и имя файла базы паролей, затем нажмите на кнопку **Открыть**.

7. В открывшемся окне **Расположение базы паролей** выберите действие **Создать новую базу паролей**.

8. В окне **Новая база паролей** в блоке **Пароль** задайте пароль для доступа к новой базе и введите его повторно в поле **Подтверждение пароля**.

   Если при подтверждении пароль введен неверно, он будет выделен красным цветом.

   В блоке **Алгоритм шифрования** выберите криптопровайдера и нужный метод шифрования (см. стр. 209).

9. В открывшемся окне введите новый мастер-пароль, чтобы подтвердить создание новой базы паролей.

РАСПОЛОЖЕНИЕ РЕЗЕРВНОЙ КОПИИ

Перед сохранением любых изменений ваших персональных данных Менеджер паролей автоматически делает резервные копии базы паролей. Это позволяет избежать потери данных в случае системных или технических сбоев. Менеджер паролей создает полную копию базы паролей на момент, предшествующий внесению последних изменений. Если база паролей была повреждена, вы можете восстановить данные из последней резервной копии базы паролей (см. стр. 201).

В качестве хранилища резервной копии базы паролей можно использовать локальный диск, съемный диск или сетевой диск.

По умолчанию в зависимости от операционной системы резервная копия сохраняется по следующему пути:

- Microsoft Windows XP: C:\Documents and Settings\User_name\My Documents\Passwords Database\;
- Microsoft Windows Vista: C:\Users\User_name\Documents\Passwords Database\;
- Microsoft Windows 7: C:\Users\User_name\My Documents\Passwords Database\.

Чтобы изменить путь сохранения резервных копий, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна нажмите на кнопку **Менеджер паролей**.
3. В открывшемся окне нажмите на кнопку **Параметры**.
4. В левой части окна выберите раздел **Мои пароли**.
5. В правой части окна в блоке **Резервное копирование** нажмите на кнопку  , расположенную в правой части поля **Путь**.
6. В открывшемся окне **Обзор папок** выберите папку назначения для резервной копии базы паролей.

ВЫБОР МЕТОДА ШИФРОВАНИЯ

Задача криптографии – защитить информацию от несанкционированного доступа и распространения. Основное назначение шифра – передавать зашифрованное сообщение по незащищенным каналам.

Для функций шифрования и дешифровки необходимы ключи. Ключ – это обязательный параметр шифра. Если для функций шифрования и дешифровки используется один ключ, алгоритм называется симметричным, если два ключа – асимметричным. Симметричные шифры, в свою очередь, могут быть блочными и поточными. Любая информация (вне зависимости от формата исходных данных) интерпретируется в бинарный код. Блочный шифр

подразумевает, что все данные будут разбиты на блоки, а затем к каждому из них будет применено независимое преобразование. В поточном шифре алгоритм применяется к каждому биту информации.

Менеджер паролей предлагает следующие симметричные алгоритмы шифрования:

- **DES**. Блочный шифр со стандартным размером ключа в 56 бит. По сегодняшним меркам, DES не обладает высоким уровнем защиты. Алгоритм используется в тех случаях, когда надежность не является основным требованием.

- **3DES**. Блочный алгоритм, созданный на основе DES. В нем устранен главный недостаток предыдущего алгоритма – малый размер ключа. Размер ключа 3DES втрое превышает аналогичный показатель DES (56*3=168 бит). Скорость работы в три раза ниже, чем у DES, но безопасность значительно выше. 3DES используется чаще, поскольку DES недостаточно устойчив к современным технологиям «взлома» шифра.

- **3DES TWO KEY**. Блочный алгоритм, созданный на основе DES. Это алгоритм 3DES, в котором размер ключа равен 112 битам (56*2).

- **RC2**. Блочный алгоритм шифрования с переменной длиной ключа быстро обрабатывает большой объем информации. Это более быстрый алгоритм, чем DES. По надежности и устойчивости он сравним с 3DES.

- **RC4**. Поточный шифр с переменной длиной ключа. Размер ключа может составлять от 40 до 256 бит. Преимущества алгоритма – высокая скорость работы и переменный размер ключа. Менеджер паролей по умолчанию использует RC4 для шифрования данных.

- **AES**. Симметричный алгоритм блочного шифрования с ключами длиной 128, 192, 256 бит. Алгоритм гарантирует высокий уровень безопасности и относится к числу самых распространенных.

Чтобы в операционной системе Microsoft Windows выполнялись криптографические операции, используется криптопровайдер. Каждый криптопровайдер поддерживает несколько алгоритмов шифрования с определенной длиной ключа. Менеджер паролей использует следующие встроенные в Microsoft Windows криптопровайдеры:

- Microsoft Base Cryptographic Provider;

- Microsoft Enhanced Cryptographic Provider;

- Microsoft Enhanced RSA and AES Cryptographic Provider (Prototype);

- Microsoft RSA/Schannel Cryptographic Provider;

- Microsoft Strong Cryptographic Provider.

Чтобы изменить алгоритм шифрования, выполните следующие действия:

1. Откройте главное окно программы.

2. В нижней части окна нажмите на кнопку **Менеджер паролей**.

3. В открывшемся окне нажмите на кнопку **Параметры**.

4. В левой части окна выберите раздел **Мои пароли**.

5. В правой части окна в блоке **Шифрование** нажмите на кнопку **Изменить**.

6. В открывшемся окне **Алгоритм шифрования** задайте параметры шифрования.

Автоматическое блокирование базы паролей

Менеджер паролей автоматически блокирует базу паролей после запуска программы и по окончании заданного интервала, в течение которого компьютер не использовался. Вы можете задать время, по истечении которого база паролей будет заблокирована. Значение интервала варьируется от 1 до 60 минут. Рекомендуется

установить блокировку базы паролей после 5-20 минут бездействия компьютера. Вы можете также отключить автоматическую блокировку базы паролей.

Менеджер паролей автоматически блокирует базу паролей после определенного времени бездействия компьютера. Если автоматическая блокировка компьютера отключена, ваши персональные данные не будут защищены в случае, если вы отойдете от компьютера, не заблокировав его вручную.

Чтобы изменить время, после которого база паролей блокируется, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна нажмите на кнопку **Менеджер паролей**.
3. В открывшемся окне нажмите на кнопку **Параметры**.
4. В левой части окна выберите раздел **Мои пароли**.
5. В правой части окна в блоке **Автоматическое блокирование** выберите из раскрывающегося списка время бездействия компьютера, по истечении которого база паролей будет заблокирована.

   Чтобы отключить блокировку базы паролей, выберите значение **Никогда**.

Изменение способа авторизации Менеджера паролей

Авторизация позволяет контролировать доступ к вашим персональным данным. Способ авторизации вы выбираете при первом запуске Менеджера паролей, но при необходимости способ авторизации можно изменить.

Чтобы изменить способ авторизации, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна нажмите на кнопку **Менеджер паролей**.
3. В открывшемся окне нажмите на кнопку **Параметры**.
4. В левой части окна выберите раздел **Способ авторизации**.
5. В правой части окна в блоке **Способ авторизации** выберите из раскрывающегося списка один из вариантов авторизации.

См. также:

Использование USB-, Bluetooth-устройств для авторизации 211

Использование USB-, Bluetooth-устройств для авторизации

Для доступа к базе паролей (см. стр. 211) Менеджер паролей позволяет использовать различные USB- и Bluetooth-устройства.

Чтобы использовать USB-устройство для доступа к базе паролей, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна нажмите на кнопку **Менеджер паролей**.
3. В открывшемся окне нажмите на кнопку **Параметры**.

4. В левой части окна выберите раздел **Способ авторизации**.

5. В правой части окна в блоке **Способ авторизации** выберите из раскрывающегося списка значение **USB-устройство**.

6. Подключите переносное устройство к компьютеру.

7. Выберите одно устройство из списка **Дисковые устройства** и нажмите на кнопку **Установить**. Рядом с выбранным устройством появится значок  . Если подключенного устройства в списке не оказалось, установите флажок **Показать дополнительные устройства**. При необходимости вы можете изменить устройство для авторизации, нажав на кнопку **Сбросить**.

Чтобы использовать Bluetooth-устройство для доступа к базе паролей, выполните следующие действия:

1. Откройте главное окно программы.

2. В нижней части окна нажмите на кнопку **Менеджер паролей**.

3. В открывшемся окне нажмите на кнопку **Параметры**.

4. В левой части окна выберите раздел **Способ авторизации**.

5. В правой части окна в блоке **Способ авторизации** выберите из раскрывающегося списка значение **Bluetooth-устройство**.

6. Включите функцию Bluetooth на вашем компьютере, а затем на устройстве.

7. Выберите одно устройство из списка **Телефоны и модемы**, затем нажмите на кнопку **Установить**. Рядом с выбранным устройством появится значок  . При необходимости можно изменить устройство для авторизации, нажав на кнопку **Сбросить**.

Изменение мастер-пароля

Мастер-пароль создается при первом запуске Менеджера паролей. В дальнейшем вы можете его изменить.

При изменении мастер-пароля Менеджер паролей требует подтверждение введенного пароля (повторный ввод нового пароля). Без подтверждения новый пароль сохранить невозможно. Если введенный и подтвержденный пароли не совпадают, подтвержденный пароль будет выделен красным цветом. Тогда при попытке сохранить новый пароль появится предупреждающее сообщение.

Чтобы изменить мастер-пароль, выполните следующие действия:

1. Откройте главное окно программы.

2. В нижней части окна нажмите на кнопку **Менеджер паролей**.

3. В открывшемся окне нажмите на кнопку **Параметры**.

4. В левой части окна выберите раздел **Способ авторизации**.

5. В правой части окна в блоке **Защита паролем** нажмите на кнопку **Изменить**.

6. В открывшемся окне **Защита паролем** введите новый пароль в поля **Пароль** и **Подтверждение пароля**.

Поддерживаемые веб-браузеры

Чтобы функции автоматической активизации учетной записи и кнопки быстрого запуска (см. стр. 214) работали корректно, для некоторых веб-браузеров и почтовых программ Менеджер паролей запрашивает установку дополнительных расширений (плагинов). По умолчанию установка расширений происходит при первичном запуске Менеджера паролей. Вы можете дополнительно установить нужный плагин.

Менеджер паролей содержит список веб-браузеров и почтовых программ, в котором каждой программе присвоен статус **Установлено** / **Не установлено** в зависимости от того, установлен для нее плагин или нет.

Рекомендуется закрыть все программы, для которых вы будете устанавливать плагины.

Чтобы установить плагин для веб-браузера или почтовой программы, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна нажмите на кнопку **Менеджер паролей**.
3. В открывшемся окне нажмите на кнопку **Параметры**.
4. В левой части окна выберите раздел **Поддерживаемые веб-браузеры**.
5. В правой части окна выберите программу из списка **Поддерживаемые веб-браузеры и доступные расширения**, затем нажмите на кнопку **Установить**.
6. Следуйте подсказкам **Мастера установки**. Когда плагин будет установлен, название программы автоматически переместится в группу **Установленные**. Ей будет присвоен статус **Установлено**. Вы можете удалить установленное расширение по кнопке **Удалить**.

УПРАВЛЕНИЕ ШАБЛОНАМИ ЛИЧНЫХ ЗАМЕТОК

Вы можете отредактировать предустановленные шаблоны личных заметок (см. стр. 198), создать новые шаблоны, а также использовать в качестве шаблона существующую личную заметку.

Чтобы изменить предустановленный шаблон личной заметки, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна нажмите на кнопку **Менеджер паролей**.
3. В открывшемся окне нажмите на кнопку **Параметры**.
4. В левой части окна выберите раздел **Управление шаблонами**.
5. В правой части окна выберите шаблон в списке и нажмите на кнопку **Изменить**.
6. Выполните нужные изменения в текстовом редакторе.

Чтобы создать шаблон личной заметки, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна нажмите на кнопку **Менеджер паролей**.
3. В открывшемся окне нажмите на кнопку **Параметры**.
4. В левой части окна выберите раздел **Управление шаблонами**.
5. В правой части окна нажмите на кнопку **Добавить**.
6. В открывшемся окне в поле **Имя** введите название нового шаблона личной заметки.
7. Введите нужную информацию в текстовом редакторе.

Чтобы использовать существующую личную заметку в качестве шаблона, выполните следующие действия.

1. Откройте главное окно программы.
2. В нижней части окна нажмите на кнопку **Менеджер паролей**.
3. В открывшемся окне **Менеджер паролей** нажмите на кнопку **База паролей**.
4. В открывшемся окне выберите нужную личную заметку в списке и в верхней части окна нажмите на кнопку **Изменить**.
5. В нижней части открывшегося окна нажмите на кнопку **Сохранить как шаблон**.
6. В открывшемся окне в поле **Имя** введите название нового шаблона личной заметки.

Отображение кнопки быстрого запуска

Если в программу, с которой вы работаете, встроено меню не только Менеджер паролей, но и меню других программ, вы можете задать позицию кнопки быстрого запуска относительно других кнопок. Кроме того, можно вручную сформировать список веб-браузеров, для которых используется кнопка быстрого запуска (см. стр. 47).

Чтобы изменить параметры отображения кнопки быстрого запуска, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна нажмите на кнопку **Менеджер паролей**.
3. В открывшемся окне нажмите на кнопку **Параметры**.
4. В левой части окна выберите раздел **Кнопка быстрого запуска**.
5. В правой части окна в блоке **Отображение кнопки быстрого запуска** настройте нужные параметры в зависимости от задачи:
   - чтобы изменить расположение кнопки быстрого запуска, в поле **Переместить кнопку влево** введите номер позиции кнопки (сколько кнопок справа будет расположено до кнопки быстрого запуска);
   - чтобы при блокировании базы паролей кнопка быстрого запуска не отображалась, установите флажок **Не отображать, если Менеджер паролей заблокирован**;
   - чтобы сформировать список веб-браузеров, в которых доступна кнопка быстрого запуска, в блоке **Отображать кнопку быстрого запуска в следующих веб-браузерах** установите флажок рядом с нужным веб-браузером из списка.

Время хранения пароля в буфере обмена

Менеджер паролей позволяет копировать пароль в буфер обмена на заданный промежуток времени. Это удобно для быстрых действий с паролями (например, когда вам необходимо использовать созданный пароль при регистрации на веб-сайте / в программе). Вы можете задать время, в течение которого пароль будет храниться в буфере обмена. По истечении этого времени пароль автоматически будет удален из буфера обмена. Это предотвратит перехват и воровство паролей, поскольку после заданного времени пароль будет невозможно скопировать из буфера обмена.

Чтобы изменить время хранения пароля в буфере обмена, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна нажмите на кнопку **Менеджер паролей**.

3. В открывшемся окне нажмите на кнопку **Параметры**.

4. В левой части окна выберите раздел **Основные**.

5. В правой части окна в блоке **Буфер обмена** задайте время в секундах.

Уведомления

В процессе работы Менеджера паролей возникают различного рода события, которые обычно носят информационный характер. Чтобы быть в курсе событий, воспользуйтесь сервисом уведомлений. Для уведомления пользователя служат подсказки и всплывающие сообщения.

В программе реализованы уведомления следующих типов:

- **Запуск программы**. Сообщение появляется при повторном запуске программы, когда программа уже запущена и база паролей не заблокирована.

- **Активизация учетной записи**. Сообщение появляется, когда учетная запись активирована.

- **Очистка буфера обмена**. Менеджер паролей позволяет временно сохранять пароль в буфере обмена. Это удобно, когда необходимо скопировать данные, а затем вставить их в выбранное поле. По истечении установленного времени (см. стр. 214) пароль из буфера обмена будет удален.

- **Автоматическая блокировка Менеджера паролей**. Сообщение появляется, когда Менеджер паролей автоматически блокирует базу паролей. По умолчанию база паролей автоматически блокируется после запуска операционной системы и после заданного времени (см. стр. 210), в течение которого компьютер не использовался.

- **Экспорт данных в незащищенный файл**. Предупреждающее сообщение о том, что по результатам экспорта ваши пароли будут сохранены в незашифрованном файле, и как следствие, будут доступны любому пользователю, работающему на вашем компьютере. Рекомендуем перед экспортом данных заранее продумать способ защиты файла, содержащего пароли.

- **Редактирование формы вручную**. Чтобы настроить параметры дополнительных полей, программа запрашивает разрешение на использование установленного по умолчанию веб-браузера. Сообщение предупреждает, что изображения и системные файлы (cookies) будут сохранены на вашем компьютере.

- **Проблемы при заполнении имени пользователя для учетной записи**. Сообщение предупреждает о том, что невозможно автоматически ввести персональные данные при авторизации.

Чтобы получать уведомления, выполните следующие действия:

1. Откройте главное окно программы.

2. В нижней части окна нажмите на кнопку **Менеджер паролей**.

3. В открывшемся окне нажмите на кнопку **Параметры**.

4. В левой части окна выберите раздел **Основные**.

5. В правой части окна в блоке **Основные** нажмите на кнопку **Настройка уведомлений**.

6. В открывшемся окне установите / снимите флажок рядом с нужными типами уведомлений.

Действие по двойному щелчку мыши

Менеджер паролей позволяет выбрать действие, которое будет выполняться по двойному щелчку мыши на значке программы в области уведомлений панели задач Microsoft Windows (см. стр. 44). Можно выбрать одно из следующих действий:

- открыть главное окно Менеджера паролей (см. стр. 44);
- заблокировать / разблокировать Менеджер паролей (действие установлено по умолчанию).

Чтобы изменить запуск задачи двойным щелчком мыши на значке программы в области уведомлений панели задач, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна нажмите на кнопку **Менеджер паролей**.
3. В открывшемся окне нажмите на кнопку **Параметры**.
4. В левой части окна выберите раздел **Основные**.
5. В правой части окна из раскрывающегося списка **Двойным щелчком мыши по значку** выберите действие.

Создание надежных паролей

Безопасность данных напрямую зависит от надежности паролей. Данные могут быть подвержены риску в следующих случаях:

- один пароль используется для всех учетных записей;
- простой пароль;
- в качестве пароля используется информация, которую легко угадать (например, имена членов семьи или даты их рождения).

Для обеспечения безопасности данных Менеджер паролей позволяет создавать уникальные надежные пароли для учетных записей с помощью генератора паролей.

Пароль считается надежным, если он состоит более чем из четырех символов с использованием специальных символов и цифр, прописных и строчных букв.

Надежность пароля определяют следующие параметры:

- **Длина** – количество символов в пароле. Это значение может составлять от 4 до 99 символов. Считается, что чем длиннее пароль, тем он надежнее.
- **А-Я** – использование прописных букв.
- **а-я** – использование строчных букв.
- **0-9** – использование цифр.
- **Специальные символы** – использование специальных символов.
- **Не использовать символ дважды** – запрет на использование в пароле одинаковых символов.

Чтобы создать надежный пароль с помощью генератора паролей, выполните следующие действия:

1. Откройте контекстное меню Менеджера паролей и выберите пункт **Генератор паролей**.
2. В открывшемся окне **Генератор паролей** в поле **Длина пароля** задайте количество символов в пароле.
3. При необходимости настройте дополнительные параметры генератора паролей, для чего в блоке **Дополнительные параметры** установите / снимите флажок рядом с нужными параметрами.

4. Нажмите на кнопку **Генерировать**. В поле **Пароль** отобразится созданный пароль. Чтобы посмотреть созданный пароль, установите флажок **Показать пароль**.

5. Скопируйте пароль в буфер обмена по кнопке  , затем вставьте пароль в поле ввода пароля в программе / на веб-странице по нажатию на клавиши **CTRL+V**. Созданный пароль сохраняется в буфере обмена.

6. Чтобы установленные параметры сохранились для последующего использования, установите флажок **По умолчанию**.

Использование переносной версии Менеджера паролей

Менеджер паролей позволяет хранить все ваши пароли на съемном носителе (например, на флеш-карте или в мобильном телефоне, если он используется как флеш-карта). Для этого необходимо создать переносную версию Менеджера паролей на съемном носителе. Переносная версия программы создается на том компьютере, где установлена полная версия Менеджер паролей. Переносная версия программы обладает всей функциональностью Менеджера паролей.

Переносная версия позволяет использовать Менеджер паролей на общедоступном компьютере (например, в интернет-кафе, библиотеке), где Менеджер паролей не установлен. При подключении съемного устройства к компьютеру, Менеджер паролей запустится автоматически. Как только съемный носитель будет отключен, Менеджер паролей автоматически закроется и на общедоступном компьютере не останется ваших данных.

Кроме того, с помощью переносной версии вы можете синхронизировать ваши базы паролей, если Менеджера паролей установлен и параллельно используется на разных компьютерах (например, на домашнем и рабочем компьютере).

В этом разделе

Создание и подключение переносной версии 217

Синхронизация базы паролей 218

Создание и подключение переносной версии

Для корректной работы переносной версии Менеджера паролей на общедоступном компьютере рекомендуется установить дополнительные плагины для веб-браузера.

Плагин можно установить одним из следующих способов:

- Из окна мастера установки плагина. Для этого следуйте шагам мастера установки плагина при первом запуске переносной версии Менеджера паролей.

- Из меню кнопки быстрого запуска в окне веб-браузера. Для этого в меню кнопки быстрого запуска выберите пункт **Плагин автозаполнения не установлен**.

При первом запуске на общедоступном компьютере автоматически запускается мастер установки переносной версии Менеджера паролей. Вам предлагается установить следующие дополнительные параметры использования переносной версии программы:

- создать ярлык переносной версии на рабочем столе – позволяет в дальнейшем запускать программу с рабочего стола на текущем компьютере;

- использовать виртуальную клавиатуру – открывает виртуальную клавиатуру для ввода персональных данных.

Чтобы создать переносную версию Менеджера паролей, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна нажмите на кнопку **Менеджер паролей**.
3. В открывшемся окне нажмите на кнопку **Переносная версия**.
4. В открывшемся окне выберите устройство, на которое вы хотите установить переносную версию Менеджера паролей, и нажмите на кнопку **Далее**.
5. В открывшемся окне установите параметры переносной версии:
   - Чтобы не вводить мастер-пароль для доступа к переносной версии Менеджера паролей, установите флажок **Никогда не запрашивать мастер-пароль**.
   - Чтобы переносная версия запускалась автоматически при подключении съемного носителя к компьютеру, установите флажок **Включить автозапуск Менеджера паролей с переносного устройства**.
6. Нажмите на кнопку **Выполнить**. По окончании установки нажмите на кнопку **Готово**.

Чтобы использовать переносную версию программы, выполните следующие действия:

1. Подключите съемное устройство к компьютеру.
2. Запустите переносную версию Менеджера паролей с выбранного съемного диска, если она не запустилась автоматически при подключении носителя.
3. При первом запуске переносной версии вам будет предложено установить плагины автозаполнения, а также отключить встроенные менеджеры паролей для установленных на вашем компьютере веб-браузеров.
4. В открывшемся окне введите мастер-пароль.

   Переносная версия Менеджера паролей готова к использованию.

Синхронизация базы паролей

Если вы используете Менеджер паролей на разных компьютерах, то возникает необходимость поддерживать все базы паролей в актуальном состоянии. С помощью переносной версии программы вы сможете синхронизировать данные и использовать актуальную базу паролей на всех компьютерах, где установлен Менеджер паролей. Для этого синхронизируйте базу паролей переносной версии с базой паролей на одном из компьютеров, а затем повторите синхронизацию на другом компьютере.

Чтобы синхронизировать базу паролей переносной версии с базой паролей на одном из компьютеров, выполните следующие действия:

1. Подключите съемное устройство к компьютеру.
2. Откройте главное окно программы.
3. В нижней части окна нажмите на кнопку **Менеджер паролей**.
4. В открывшемся окне нажмите на кнопку **Переносная версия**.
5. В открывшемся окне выберите устройство, на котором установлена переносная версия Менеджера паролей, и нажмите на кнопку **Далее**.
6. В открывшемся окне выберите способ синхронизации базы паролей:

- Чтобы добавить данные из базы Менеджера паролей, установленного на компьютере, в базу паролей переносной версии, выберите вариант **Объединить базы паролей**.

  При этом база Менеджера паролей, установленного на компьютере, не будет изменена. Чтобы внести в нее объединенные данные, повторите синхронизацию, выбрав вариант **Использовать базу паролей переносной версии**.

- Чтобы заменить базу паролей переносной версии базой Менеджера паролей, установленного на компьютере, в переносной версии, выберите вариант **Использовать базу Менеджера паролей, установленного на этом компьютере**.

- Чтобы заменить базу Менеджера паролей, установленного на компьютере, базой паролей переносной версии, выберите вариант **Использовать базу паролей переносной версии**.

7. Нажмите на кнопку **Далее**.

8. В открывшемся окне установите параметры переносной версии:

   - Чтобы не вводить мастер-пароль для доступа к переносной версии Менеджера паролей, установите флажок **Никогда не запрашивать мастер-пароль**.

   - Чтобы переносная версия запускалась автоматически при подключении съемного носителя к компьютеру, установите флажок **Включить автозапуск Менеджера паролей с переносного устройства**.

9. Нажмите на кнопку **Выполнить**. По окончании синхронизации нажмите на кнопку **Готово**.

ПРОИЗВОДИТЕЛЬНОСТЬ И СОВМЕСТИМОСТЬ С ДРУГИМИ ПРОГРАММАМИ

Под производительностью Kaspersky CRYSTAL подразумевается спектр обнаруживаемых угроз, а также потребление энергии и ресурсов компьютера.

Kaspersky CRYSTAL позволяет гибко настраивать спектр защиты и выбирать различные категории угроз (см. раздел «Выбор категорий обнаруживаемых угроз» на стр. 220), которые программа будет обнаруживать в ходе работы.

При работе на портативных компьютерах потребление программами энергоресурсов имеет особое значение. Зачастую проверка компьютера на вирусы и обновление баз Kaspersky CRYSTAL требуют значительного количества ресурсов. Специальный режим работы Kaspersky CRYSTAL на портативном компьютере (см. стр. 222) позволяет автоматически откладывать задачи проверки и обновления по расписанию при питании от аккумулятора и экономить тем самым его заряд.

Потребление ресурсов компьютера Kaspersky CRYSTAL может сказываться на производительности других программ. Для решения проблем совместной работы при увеличении нагрузки на центральный процессор и дисковые подсистемы Kaspersky CRYSTAL может приостанавливать выполнение задач проверки и уступать ресурсы другим программам (см. стр. 221), работающим на компьютере.

В режиме игрового профиля автоматически отключается показ уведомлений о работе Kaspersky CRYSTAL при запуске других программ в полноэкранном режиме.

Процедура расширенного лечения в случае активного заражения системы требует обязательной перезагрузки компьютера, что также может влиять на работу других программ. При необходимости вы можете отключить применение технологии лечения активного заражения (см. стр. 220), чтобы избежать нежелательной перезагрузки компьютера.

В этом разделе

Выбор категорий обнаруживаемых угроз 220

Технология лечения активного заражения 220

Распределение ресурсов компьютера при проверке на вирусы 221

Параметры программы при работе в полноэкранном режиме. Игровой профиль 221

Энергосбережение при работе от аккумулятора 222

Выбор категорий обнаруживаемых угроз

Угрозы, обнаруживаемые Kaspersky CRYSTAL, подразделяются на категории по различным признакам. Программа всегда обнаруживает вирусы, троянские программы и вредоносные утилиты. Эти программы могут нанести значительный вред вашему компьютеру. Для обеспечения большей безопасности компьютера можно расширить список обнаруживаемых угроз, включив контроль за действиями легальных программ, которые могут быть использованы злоумышленником для нанесения вреда компьютеру или данным пользователя.

Чтобы выбрать категории обнаруживаемых угроз, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Центр защиты** подраздел **Угрозы и исключения**.
4. В правой части окна в блоке **Угрозы** нажмите на кнопку **Настройка**.
5. В открывшемся окне **Угрозы** установите флажки для категорий угроз, которые необходимо обнаруживать.

Технология лечения активного заражения

Современные вредоносные программы могут внедряться на самые нижние уровни операционной системы, что делает их удаление практически невозможным. При обнаружении вредоносной активности в системе Kaspersky CRYSTAL предлагает провести специальную расширенную процедуру лечения, в результате которой угроза будет обезврежена и удалена с компьютера.

По окончании процедуры будет произведена обязательная перезагрузка компьютера. После перезагрузки компьютера рекомендуется запустить полную проверку на вирусы (см. раздел «Как выполнить полную проверку компьютера на вирусы» на стр. 61).

Чтобы Kaspersky CRYSTAL применял процедуру расширенного лечения, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Общие параметры** подраздел **Совместимость**.
4. В правой части окна установите флажок **Применять технологию активного лечения**.

РАСПРЕДЕЛЕНИЕ РЕСУРСОВ КОМПЬЮТЕРА ПРИ ПРОВЕРКЕ НА ВИРУСЫ

Для ограничения нагрузки на центральный процессор и дисковые подсистемы вы можете отложить выполнение задач проверки на вирусы.

Выполнение задач проверки увеличивает нагрузку на центральный процессор и дисковые подсистемы, тем самым замедляя работу других программ. По умолчанию при возникновении такой ситуации Kaspersky CRYSTAL приостанавливает выполнение задач проверки и высвобождает ресурсы системы для программ пользователя.

Однако существует ряд программ, которые запускаются в момент высвобождения ресурсов процессора и работают в фоновом режиме. Чтобы проверка не зависела от работы таких программ, не следует уступать им ресурсы системы.

Обратите внимание на то, что данный параметр можно настраивать индивидуально для каждой задачи проверки. В этом случае настройка параметров, произведенная для конкретной задачи, имеет более высокий приоритет.

- *Чтобы Kaspersky CRYSTAL откладывал выполнение задач проверки при замедлении работы других программ, выполните следующие действия:*

  1. Откройте главное окно программы.
  2. В верхней части окна перейдите по ссылке **Настройка**.
  3. В левой части окна выберите в разделе **Общие параметры** подраздел **Совместимость**.
  4. В правой части окна установите флажок **Уступать ресурсы другим программам**.

ПАРАМЕТРЫ ПРОГРАММЫ ПРИ РАБОТЕ В ПОЛНОЭКРАННОМ РЕЖИМЕ. ИГРОВОЙ ПРОФИЛЬ

Использование некоторых программ (особенно компьютерных игр) в полноэкранном режиме плохо совместимо с некоторыми функциями Kaspersky CRYSTAL: например, в этом режиме неуместны окна уведомлений. Зачастую такие программы требуют также значительных системных ресурсов, поэтому выполнение некоторых задач Kaspersky CRYSTAL может привести к замедлению работы этих программ.

Чтобы вручную не отключать уведомления и не приостанавливать задачи каждый раз при переходе в полноэкранный режим, в Kaspersky CRYSTAL предусмотрена возможность временного изменения параметров с помощью игрового профиля. Когда игровой профиль используется, при переходе в полноэкранный режим автоматически изменяются параметры всех компонентов таким образом, чтобы обеспечить оптимальную работу в этом режиме. При выходе из полноэкранного режима параметрам программы возвращаются значения, которые были установлены до перехода в полноэкранный режим.

- *Чтобы включить использование игрового профиля, выполните следующие действия:*

  1. Откройте главное окно программы.
  2. В верхней части окна перейдите по ссылке **Настройка**.
  3. В левой части окна выберите в разделе **Общие параметры** подраздел **Игровой профиль**.
  4. В правой части окна установите флажок **Использовать Игровой профиль** и в блоке **Параметры профиля** ниже укажите необходимые параметры использования игрового профиля.

Энергосбережение при работе от аккумулятора

В целях экономии питания аккумулятора портативного компьютера вы можете отложить выполнение задач проверки на вирусы и обновления по расписанию. По мере необходимости можно обновлять Kaspersky CRYSTAL или запускать проверку на вирусы вручную.

Чтобы включить режим энергосбережения при работе от аккумулятора, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Общие параметры** подраздел **Энергосбережение**.
4. В правой части окна установите флажок **Не запускать задачи проверки по расписанию при работе от аккумуляторов**.

Самозащита Kaspersky CRYSTAL

Поскольку Kaspersky CRYSTAL обеспечивает безопасность компьютера от вредоносных программ, попадающее на компьютер вредоносное программное обеспечение пытается заблокировать работу Kaspersky CRYSTAL или даже удалить программу с компьютера.

Стабильность системы безопасности вашего компьютера обеспечивают реализованные в Kaspersky CRYSTAL механизмы самозащиты и защиты от удаленного воздействия.

Самозащита Kaspersky CRYSTAL предотвращает изменение и удаление собственных файлов на диске, процессов в памяти, записей в системном реестре. Защита от удаленного воздействия позволяет блокировать все попытки удаленного управления сервисами программы.

Под управлением 64-разрядных операционных систем и Microsoft Windows Vista доступно только управление механизмом самозащиты Kaspersky CRYSTAL от изменения или удаления собственных файлов на диске, а также от изменения или удаления записей в системном реестре.

В этом разделе

Включение и отключение самозащиты 222

Защита от внешнего управления 223

Включение и отключение самозащиты

По умолчанию самозащита Kaspersky CRYSTAL включена. При необходимости вы можете отключить самозащиту.

Чтобы включить или отключить самозащиту Kaspersky CRYSTAL, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Общие параметры** подраздел **Самозащита**.

4. В правой части окна снимите флажок **Включить самозащиту**, если нужно отключить самозащиту Kaspersky CRYSTAL. Установите этот флажок, если самозащиту нужно включить.

ЗАЩИТА ОТ ВНЕШНЕГО УПРАВЛЕНИЯ

По умолчанию защита от удаленного воздействия включена. При необходимости вы можете отключить защиту.

Нередко возникают ситуации, когда при использовании защиты от удаленного воздействия возникает необходимость применить программы удаленного администрирования (например, RemoteAdmin). Для обеспечения работы этих программ необходимо добавить их в список доверенных программ (см. раздел «Формирование списка доверенных программ» на стр. 155) и включить для них параметр **Не контролировать активность программы**.

Чтобы отключить защиту от внешнего управления, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Общие параметры** подраздел **Самозащита**.
4. В правой части окна в блоке **Внешнее управление** снимите флажок **Отключить возможность внешнего управления системной службой**.

ВНЕШНИЙ ВИД ПРОГРАММЫ

Вы можете изменять внешний вид Kaspersky CRYSTAL, используя альтернативные графические оболочки. Возможна также настройка использования активных элементов интерфейса (значка программы в области уведомлений панели задач Microsoft Windows и всплывающих сообщений).

В ЭТОМ РАЗДЕЛЕ

Активные элементы интерфейса 223

Графическая оболочка Kaspersky CRYSTAL 224

Новостной агент 224

АКТИВНЫЕ ЭЛЕМЕНТЫ ИНТЕРФЕЙСА

Вы можете настроить отображение активных элементов интерфейса: например, окон уведомлений, значка Kaspersky CRYSTAL в панели задач.

Чтобы настроить активные элементы интерфейса, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Общие параметры** подраздел **Вид**.
4. В правой части окна в блоке **Значок в панели задач** установите или снимите соответствующие флажки.

Графическая оболочка Kaspersky CRYSTAL

Все используемые в интерфейсе Kaspersky CRYSTAL цвета, шрифты, пиктограммы, тексты могут быть изменены. Вы можете создавать собственные графические оболочки для программы, а также локализовать интерфейс программы на другой язык.

Чтобы использовать другую графическую оболочку, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Общие параметры** подраздел **Вид**.
4. В правой части окна установите флажок **Использовать альтернативную графическую оболочку**, чтобы подключить графическую оболочку. В поле ввода укажите каталог с параметрами графической оболочки или нажмите на кнопку **Обзор**, чтобы найти этот каталог.

Новостной агент

С помощью *новостного агента* «Лаборатория Касперского» информирует вас обо всех важных событиях, касающихся Kaspersky CRYSTAL и защиты от компьютерных угроз в целом.

Программа будет уведомлять вас о появлении новостей с помощью всплывающего сообщения в области уведомлений панели задач. Значок программы в этом случае видоизменяется (см. ниже).

Прочитать новости вы можете одним из следующих способов:

- нажмите на значок  в области уведомлений панели задач;
- перейдите по ссылке **Читать новости** во всплывающем сообщении о новостях.

Чтобы отключить получение новостей, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Общие параметры** подраздел **Вид**.
4. В правой части окна в блоке **Значок в панели задач** снимите флажок **Уведомлять о новостях**.

Дополнительные инструменты

Для решения специфических задач по обеспечению безопасности компьютера используются мастеры и инструменты, включенные в состав Kaspersky CRYSTAL:

- Мастер создания диска аварийного восстановления – предназначен для создания Диска аварийного восстановления, который позволяет восстановить работоспособность системы после вирусной атаки с помощью загрузки со съемных носителей. Диск аварийного восстановления применяется при такой степени заражения, когда не представляется возможным вылечить компьютер с помощью антивирусных программ или утилит лечения.

- Мастер устранения следов активности – предназначен для поиска и устранения следов активности пользователя в системе, а также параметров операционной системы, способствующих накоплению информации об активности пользователя.

- Мастер удаления неиспользуемой информации - предназначен для поиска и удаления временных и неиспользуемых файлов на вашем компьютере и оптимизации работы системы.

- Мастер восстановления системы – предназначен для устранения повреждений системы и следов пребывания вредоносных объектов в системе.

- Мастер настройки браузера – предназначен для анализа и настройки параметров браузера Microsoft Internet Explorer с целью устранения его потенциальных уязвимостей.

- Инструмент для необратимого удаления данных - обеспечивает уничтожение конфиденциальных данных без возможности их дальнейшего восстановления.

Все проблемы, обнаруживаемые мастерами (кроме Мастера создания диска аварийного восстановления), группируются в зависимости от опасности, которую они представляют для системы. Для каждой группы проблем специалисты «Лаборатории Касперского» предлагают набор действий, выполнение которых поможет устранить уязвимости и проблемные места в системе. Всего выделено три группы проблем и, соответственно, действий при их обнаружении:

- *Настоятельно рекомендуемые действия* помогут избавиться от проблем, представляющих серьезную угрозу безопасности. Рекомендуем вам своевременно выполнять все действия этой группы для устранения угрозы.

- *Рекомендуемые действия* направлены на устранение проблем, которые могут представлять потенциальную опасность. Действия этой группы также рекомендуется выполнять для обеспечения оптимальной защиты.

- *Дополнительные действия* предназначены для устранения неопасных в данный момент проблем, которые в будущем могут поставить безопасность компьютера под угрозу. Выполнение этих действий обеспечивает полноценную защиту вашего компьютера, но в некоторых случаях может привести к удалению пользовательских параметров (например, файлов cookies).

В этом разделе

Необратимое удаление данных 226

Устранение следов активности 227

Удаление неиспользуемой информации 228

Настройка браузера 230

Необратимое удаление данных

Безопасность данных обеспечивается не только защитой от вирусов, троянов и других вредоносных программ, но и защитой от несанкционированного восстановления удаленной информации.

Удаление данных стандартными методами Microsoft Windows не обеспечивает надежности и защиты от возможного восстановления. При удалении данные не исчезают с жесткого диска: просто занятые ими секторы диска будут отмечены как свободные. Удаляется лишь запись о файле в файловой таблице. Форматирование носителей информации (например, жесткого диска, флеш- или USB-карт) тоже не дает гарантии безвозвратного удаления данных. Считается, что только после многократной перезаписи данные исчезают навсегда. Но даже в этом случае информацию удается восстановить с помощью мощных программных средств.

В состав Kaspersky CRYSTAL входит мастер необратимого удаления данных. Этот мастер позволяет удалить конфиденциальные данные без возможности их дальнейшего восстановления и использования злоумышленниками. Необратимое удаление данных исключает варианты, которые позволяют восстановить информацию обычными программными средствами. Мастер применим для объектов как малого, так и большого размера (в несколько гигабайт).

Мастер поддерживает удаление данных со следующих носителей информации:

- Локальные диски. Удаление возможно, если у пользователя есть права на запись и удаление информации.

- Съемные диски или другие устройства, которые распознаются как съемные диски (например, дискеты, флеш-, USB-карты или мобильные телефоны). Удаление с флеш-карт возможно, если механически не включен режим защиты от записи (Lock-режим).

Перед процедурой безвозвратного удаления программа выясняет, возможно ли удаление данных с выбранного носителя информации. Процедура удаления будет выполнена только, если на выбранном носителе информации поддерживается удаление данных. В противном случае безвозвратно удалить данные будет невозможно.

Вы можете удалить только те данные, доступ к которым разрешен под вашей учетной записью. Перед удалением данных убедитесь, что файл или папка не открыты или не используются другими программами.

Возможно удаление таких объектов, как файл и папка. Для предотвращения случайного удаления нужных файлов за один раз вы можете выбрать для удаления только один объект (при этом выбранная для удаления папка может содержать несколько файлов или вложенных папок).

В выбранной для удаления папке могут находиться системные файлы, отсутствие которых может вызвать сбои в работе системы. При обнаружении системных файлов и папок среди выбранных данных, мастер запрашивает дополнительное подтверждение для их удаления.

Методы необратимого удаления персональных данных стандартизованы. Все они основаны на многократной перезаписи удаляемой информации нулями, единицами или случайными символами. В зависимости от количества циклов скорость и качество удаления различаются.

Чтобы удалить данные без возможности восстановления, выполните следующие действия:

1. Откройте главное окно программы.

2. В нижней части окна нажмите на кнопку **Дополнительные инструменты**.

3. В открывшемся окне нажмите на кнопку **Необратимое удаление данных**.

4. В открывшемся окне **Необратимое удаление данных** выберите объект по кнопке **Обзор**, затем в открывшемся окне **Выбор папки** выберите объект для удаления.

   В раскрывающемся списке **Метод удаления данных** выберите нужный алгоритм удаления данных.

5. В открывшемся окне подтвердите удаление данных по кнопке **ОК**. Если некоторые файлы не были удалены, в открывшемся окне повторите удаление по кнопке **Повторить**. Чтобы выбрать другой объект для удаления, нажмите на кнопку **Завершить**.

УСТРАНЕНИЕ СЛЕДОВ АКТИВНОСТИ

При работе на компьютере действия пользователя регистрируются в системе. При этом сохраняются данные о введенных пользователем поисковых запросах и посещенных им сайтах, о запуске программ и открытии и сохранении файлов, записи в системном журнале Microsoft Windows, временные файлы и многое другое.

Все эти источники информации об активности пользователя могут содержать конфиденциальные данные (в том числе пароли) и могут оказаться доступными для анализа злоумышленниками. В то же время пользователь зачастую не обладает достаточными знаниями для того, чтобы предотвратить хищение информации из этих источников.

В состав Kaspersky CRYSTAL входит Мастер устранения следов активности. Этот мастер производит поиск как следов активности пользователя в системе, так и параметров операционной системы, способствующих накоплению информации об этой активности.

Следует помнить о том, что накопление информации об активности пользователя в системе происходит постоянно. Запуск любого файла или открытие документа фиксируется в истории, системный журнал Microsoft Windows регистрирует множество событий, происходящих в системе. Это приводит к тому, что повторный запуск Мастера устранения следов активности может обнаружить следы активности, удаленные во время предыдущего запуска мастера. Некоторые файлы, например файл журнала Microsoft Windows, могут оказаться активно используемыми системой в момент их удаления мастером. Чтобы удалить эти файлы, мастер предложит перезагрузить систему. Однако в ходе перезагрузки такие файлы могут быть созданы заново, что приведет к их повторному обнаружению как следов активности

Мастер состоит из последовательности окон (шагов), переключение между которыми осуществляется нажатием на кнопки **Назад** и **Далее**. Работа мастера завершается нажатием на кнопку **Завершить**. Для прекращения работы мастера на любом этапе следует нажать на кнопку **Отмена**.

Чтобы запустить Мастер устранения следов активности, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна нажмите на кнопку **Дополнительные инструменты**.
3. В открывшемся окне нажмите на кнопку **Устранение следов активности**.

Рассмотрим подробнее шаги мастера.

Шаг 1. Начало работы мастера

Убедитесь, что выбран вариант **Диагностика следов активности пользователя**, и нажмите на кнопку **Далее**, чтобы начать работу мастера.

Шаг 2. Поиск следов активности

Мастер осуществляет поиск следов активности на вашем компьютере. Поиск может занять некоторое время. По завершении поиска мастер автоматически перейдет к следующему шагу.

Шаг 3. Выбор действий для устранения следов активности

По завершении поиска мастер сообщает о найденных следах активности и предлагаемых действиях для их устранения. Отчет о работе мастера представлен в виде списка (см. раздел «Дополнительные инструменты» на стр. 225).

Для просмотра действий, включенных в группу, нажмите на значок **+**, расположенный слева от названия группы.

Чтобы мастер выполнил какое-либо действие, установите флажок слева от названия действия. По умолчанию выполняются все рекомендуемые и настоятельно рекомендуемые действия. Если вы не хотите выполнять какое-либо действие, снимите флажок рядом с ним.

Настоятельно не рекомендуется снимать флажки, установленные по умолчанию, поскольку в результате этого действия безопасность вашего компьютера останется под угрозой.

Сформировав набор действий для выполнения мастером, нажмите на кнопку **Далее**.

Шаг 4. Устранение следов активности

Мастер выполняет действия, выбранные на предыдущем шаге. Устранение следов активности может занять некоторое время. Для устранения некоторых следов активности может потребоваться перезагрузка компьютера, о чем мастер вас уведомит.

По завершении устранения следов активности мастер автоматически перейдет к следующему шагу.

Шаг 5. Завершение работы мастера

Если вы хотите, чтобы устранение следов активности в дальнейшем выполнялось автоматически при завершении работы Kaspersky CRYSTAL, на завершающем шаге работы мастера установите флажок **Выполнять устранение следов активности при каждом завершении работы Kaspersky CRYSTAL**. Если вы планируете самостоятельно устранять следы активности с помощью мастера, не устанавливайте этот флажок.

Нажмите на кнопку **Завершить**, чтобы завершить работу мастера.

Удаление неиспользуемой информации

Со временем в операционной системе накапливаются временные и неиспользуемые файлы, что снижает эффективность работы системы. Такие файлы могут занимать большой объем памяти, а также они могут использоваться вредоносными программами.

Временные файлы создаются при запуске любых программ или операционных систем. По завершении работы не все временные файлы автоматически удаляются.

К неиспользуемой информации относятся следующие файлы:

- журналы событий системы, куда записываются названия всех открытых программ;
- журналы событий разных программ (например, Microsoft Office, Microsoft Visio, Macromedia Flash Player) или утилит обновления (например, Windows Updater, Adobe Updater);
- журналы системных соединений;
- временные файлы веб-браузеров (cookies);
- временные файлы, которые остаются после установки / удаления программ;
- содержимое корзины;
- файлы папки TEMP, объем которой иногда достигает нескольких гигабайт.

В состав Kaspersky CRYSTAL входит мастер удаления неиспользуемой информации. Задача мастера – помочь оптимизировать работу системы. Помимо удаления из системы ненужных файлов, мастер стирает те файлы, в которых могли сохраниться конфиденциальные данные (пароли, имена пользователей и информация с регистрационных форм). Тем не менее, для полного удаления таких данных рекомендуется использовать мастер устранения следов активности (см. стр. 227).

В момент очистки системы некоторые файлы (например, файл журнала Microsoft Windows, журнал событий Microsoft Office) могут использоваться системой. Чтобы удалить эти файлы, мастер предложит перезагрузить систему.

Мастер состоит из последовательности окон (шагов), переключение между которыми осуществляется нажатием на кнопки **Назад** и **Далее**. Работа мастера завершается нажатием на кнопку **Завершить**. Для прекращения работы мастера на любом этапе следует нажать на кнопку **Отмена**.

Чтобы запустить Мастер удаления неиспользуемой информации, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна нажмите на кнопку **Дополнительные инструменты**.
3. В открывшемся окне нажмите на кнопку **Удаление неиспользуемой информации**.

Рассмотрим подробнее шаги мастера.

Шаг 1. Начало работы мастера

Нажмите на кнопку **Далее**, чтобы начать работу мастера.

Шаг 2. Поиск неиспользуемой информации

Мастер осуществляет поиск временных и неиспользуемых файлов на вашем компьютере. Поиск может занять некоторое время. По завершении поиска мастер автоматически перейдет к следующему шагу.

Шаг 3. Выбор действий для удаления неиспользуемых файлов

По завершении поиска мастер сообщает о найденных неиспользуемых файлах и предлагаемых действиях для их удаления. Отчет о работе мастера представлен в виде списка (см. раздел «Дополнительные инструменты» на стр. 225).

Для просмотра действий, включенных в группу, нажмите на значок **+**, расположенный слева от названия группы.

Чтобы мастер выполнил какое-либо действие, установите флажок слева от названия действия. По умолчанию выполняются все рекомендуемые и настоятельно рекомендуемые действия. Если вы не хотите выполнять какое-либо действие, снимите флажок рядом с ним.

Настоятельно не рекомендуется снимать флажки, установленные по умолчанию, поскольку в результате этого действия безопасность вашего компьютера останется под угрозой.

Сформировав набор действий для выполнения мастером, нажмите на кнопку **Далее**.

Шаг 4. Удаление неиспользуемой информации

Мастер выполняет действия, выбранные на предыдущем шаге. Удаление неиспользуемой информации может занять некоторое время. Для удаления некоторых файлов может потребоваться перезагрузка компьютера, о чем мастер вас уведомит.

По завершении удаления неиспользуемой информации мастер автоматически перейдет к следующему шагу.

Шаг 5. Завершение работы мастера

Нажмите на кнопку **Завершить**, чтобы завершить работу мастера.

Настройка браузера

Браузер Microsoft Internet Explorer в некоторых случаях требует специального анализа и настройки, поскольку некоторые значения параметров, заданные пользователем или установленные по умолчанию, могут приводить к возникновению проблем в безопасности.

Приведем примеры объектов и параметров, используемых браузером и представляющих собой потенциальные угрозы безопасности:

- **Кеш работы Microsoft Internet Explorer**. В кеше хранятся данные, загруженные из интернета, что позволяет в дальнейшем не загружать их повторно. Это сокращает время загрузки веб-страниц и уменьшает интернет-трафик. Вместе с тем кеш содержит конфиденциальные данные и предоставляет возможность узнать, какие ресурсы посещал пользователь. Многие вредоносные объекты при сканировании диска сканируют также и кеш, в результате чего злоумышленники могут получить, например, почтовые адреса пользователей. Для усиления защиты рекомендуется очищать кеш после завершения работы браузера.

- **Отображение расширений для файлов известных форматов**. Для удобства редактирования имен файлов можно не отображать их расширения. Однако для пользователя иногда полезно видеть реальное расширение файла. В именах файлов многих вредоносных объектов используются сочетания символов, имитирующие дополнительное расширение перед реальным расширением (например, example.txt.com). Если реальное расширение файла не отображается, пользователь видит только часть названия файла с имитацией расширения и может принять вредоносный объект за безопасный файл. Для усиления защиты рекомендуется включать отображение расширений для файлов известных форматов.

- **Список доверенных веб-сайтов**. Для корректной работы некоторых веб-сайтов их нужно добавлять в список доверенных. В то же время вредоносные объекты могут добавлять в такой список ссылки на веб-сайты, созданные злоумышленниками.

Следует учитывать, что некоторые значения параметров могут привести к проблемам в отображении некоторых веб-сайтов (например, в случае использования ими ActiveX-элементов). Решить проблему поможет включение подобных веб-сайтов в доверенную зону.

Анализ и настройка браузера выполняются Мастером настройки браузера. В ходе работы мастер проверяет, установлены ли последние обновления для браузера и не делают ли установленные значения параметров браузера систему уязвимой для действий злоумышленников. По окончании работы мастера формируется отчет, который может быть отправлен в «Лабораторию Касперского» для анализа.

Мастер состоит из последовательности окон (шагов), переключение между которыми осуществляется нажатием на кнопки **Назад** и **Далее**. Работа мастера завершается нажатием на кнопку **Завершить**. Для прекращения работы мастера на любом этапе следует нажать на кнопку **Отмена**.

Перед началом диагностики закройте все окна браузера Microsoft Internet Explorer.

Чтобы запустить Мастер настройки браузера, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна нажмите на кнопку **Дополнительные инструменты**.
3. В открывшемся окне нажмите на кнопку **Настройка браузера для безопасной работы**.

Рассмотрим подробнее шаги мастера.

Шаг 1. Начало работы мастера

Убедитесь, что выбран вариант **Диагностика Microsoft Internet Explorer**, и нажмите на кнопку **Далее**, чтобы начать работу мастера.

Шаг 2. Анализ параметров Microsoft Internet Explorer

Мастер осуществляет анализ параметров браузера Microsoft Internet Explorer. Поиск проблем в параметрах браузера может занять некоторое время. По завершении поиска мастер автоматически перейдет к следующему шагу.

Шаг 3. Выбор действий для настройки браузера

Все найденные на предыдущем шаге проблемы группируются в зависимости от опасности, которую они представляют для системы (см. раздел «Дополнительные инструменты» на стр. 225).

Для просмотра действий, включенных в группу, нажмите на значок **+**, расположенный слева от названия группы.

Чтобы мастер выполнил какое-либо действие, установите флажок слева от названия действия. По умолчанию выполняются все рекомендуемые и настоятельно рекомендуемые действия. Если вы не хотите выполнять какое-либо действие, снимите флажок рядом с ним.

Настоятельно не рекомендуется снимать флажки, установленные по умолчанию, поскольку в результате этого действия безопасность вашего компьютера останется под угрозой.

Сформировав набор действий для выполнения мастером, нажмите на кнопку **Далее**.

Шаг 4. Настройка браузера

Мастер выполняет действия, выбранные на предыдущем шаге. Настройка браузера может занять некоторое время. После выполнения настройки мастер автоматически перейдет к следующему шагу.

Шаг 5. Завершение работы мастера

Нажмите на кнопку **Завершить**, чтобы завершить работу мастера.

Отчеты

События, происходящие в ходе работы компонентов защиты или выполнения задач Kaspersky CRYSTAL, фиксируются в отчетах. Вы можете сформировать подробный отчет для каждого компонента защиты или задачи и настроить представление данных в удобном виде. Кроме того, вы можете фильтровать данные (см. раздел «Фильтрация данных» на стр. 232), а также выполнять поиск (см. раздел «Поиск событий» на стр. 233) по всем событиям в отчете.

При необходимости вы можете сохранить данные отчета (см. раздел «Сохранение отчета в файл» на стр. 234) в текстовый файл. Вы также можете очистить отчеты (см. раздел «Очистка отчетов» на стр. 235), данные которых больше не нужны, и настроить параметры формирования (см. раздел «Запись некритических событий» на стр. 235) и хранения (см. раздел «Хранение отчетов» на стр. 234) отчетов.

В этом разделе

Формирование отчета для выбранного компонента 232

Фильтрация данных 232

Поиск событий 233

Сохранение отчета в файл 234

Хранение отчетов 234

Очистка отчетов 235

Запись некритических событий 235

Настройка напоминания о готовности отчета 235

Формирование отчета для выбранного компонента

Вы можете получить подробный отчет о событиях, произошедших в ходе работы каждого компонента или задачи Kaspersky CRYSTAL.

Для удобства работы с отчетами вы можете изменять представление данных на экране: группировать события по различным параметрам, выбирать отчетный период, сортировать события по каждой графе или по важности, а также скрывать графы таблицы.

Чтобы получить отчет для компонента или задачи, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Защита компьютера**.

   Откроется окно **Защита компьютера**.

2. По ссылке **Отчет** перейдите к окну отчетов Kaspersky CRYSTAL.

3. В открывшемся окне на закладке **Отчет** нажмите на кнопку **Подробный отчет**.

   Откроется окно **Подробный отчет**.

4. В раскрывающемся списке в левой верхней части окна выберите компонент или задачу, для которой нужно сформировать отчет. При выборе пункта **Центр защиты** отчет будет сформирован для всех компонентов защиты.

Фильтрация данных

В отчетах Kaspersky CRYSTAL вы можете отфильтровать события по одному или нескольким значениям в графах таблицы, а также задать сложные условия фильтрации данных.

Чтобы отфильтровать события по значениям, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Защита компьютера**.

   Откроется окно **Защита компьютера**.

2. По ссылке **Отчет** перейдите к окну отчетов Kaspersky CRYSTAL.

3. В открывшемся окне на закладке **Отчет** нажмите на кнопку **Подробный отчет**.

Откроется окно **Подробный отчет**.

4. В правой части окна наведите курсор на верхний левый угол заголовка графы таблицы и по левой клавише мыши откройте меню фильтра.

5. В меню фильтра выберите значение, по которому нужно отфильтровать данные.

6. При необходимости повторите процедуру для другой графы таблицы.

Чтобы задать сложное условие фильтрации, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Защита компьютера**.

   Откроется окно **Защита компьютера**.

2. По ссылке **Отчет** перейдите к окну отчетов Kaspersky CRYSTAL.

3. В открывшемся окне на закладке **Отчет** нажмите на кнопку **Подробный отчет**.

   Откроется окно **Подробный отчет**.

4. В правой части окна по правой клавише мыши откройте контекстное меню нужной графы отчета и выберите в нем пункт **Фильтр**.

5. В открывшемся окне **Сложный фильтр** задайте условия фильтрации:

   a. В правой части окна задайте границу выборки.

   b. В левой части окна в раскрывающемся списке **Условие** выберите условие выборки (например, больше или меньше, равно или не равно значению, указанному в качестве границы выборки).

   c. При необходимости добавьте второе условие, используя логические операции конъюнкции (логическое И) и дизъюнкции (логическое ИЛИ). Если вы хотите, чтобы выборка данных удовлетворяла обоим заданным условиям, выберите **И**. Если достаточно хотя бы одного условия, выберите **ИЛИ**.

Поиск событий

Вы можете выполнить поиск нужного события в отчете по ключевому слову через поисковую строку или с помощью специального окна поиска.

Чтобы найти событие, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Защита компьютера**.

   Откроется окно **Защита компьютера**.

2. По ссылке **Отчет** перейдите к окну отчетов Kaspersky CRYSTAL.

3. В открывшемся окне на закладке **Отчет** нажмите на кнопку **Подробный отчет**.

   Откроется окно **Подробный отчет**.

4. По правой клавише мыши откройте контекстное меню заголовка нужной графы и выберите в нем пункт **Поиск**.

5. В открывшемся окне **Поиск** задайте критерии поиска:

   a. В поле **Строка** введите ключевое слово для поиска.

b. В раскрывающемся списке **Графа** выберите название графы, в которой нужно искать заданное ключевое слово.

c. При необходимости установите флажки для дополнительных параметров поиска.

6. Нажмите на кнопку **Искать дальше**.

Сохранение отчета в файл

Полученный отчет можно сохранить в текстовом файле.

Чтобы сохранить отчет в файле, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Защита компьютера**.

   Откроется окно **Защита компьютера**.

2. По ссылке **Отчет** перейдите к окну отчетов Kaspersky CRYSTAL.

3. В открывшемся окне на закладке **Отчет** нажмите на кнопку **Подробный отчет**.

   Откроется окно **Подробный отчет**.

4. Сформируйте необходимый отчет и нажмите на кнопку **Сохранить**.

5. В открывшемся окне укажите папку, в которую следует сохранить файл отчета, и введите название файла.

Хранение отчетов

По умолчанию максимальный срок хранения отчетов о событиях составляет 30 дней. По истечении этого времени данные удаляются. Вы можете отменить ограничение по времени или изменить максимальный срок хранения отчетов.

Кроме того, вы можете указать максимальный размер файла отчета. По умолчанию максимальный размер составляет 1024 МБ. При достижении максимального размера содержимое файла заменяется новыми записями. Вы можете отменить ограничение размера отчета или установить другое значение.

Чтобы настроить максимальный срок хранения отчетов, выполните следующие действия:

1. Откройте главное окно программы.

2. В верхней части окна перейдите по ссылке **Настройка**.

3. В левой части окна выберите в разделе **Общие параметры** подраздел **Отчеты и хранилища**.

4. В правой части окна в блоке **Хранение** установите флажок **Хранить отчеты не более** и укажите максимальный срок хранения отчетов.

Чтобы настроить максимальный размер файла отчета, выполните следующие действия:

1. Откройте главное окно программы.

2. В верхней части окна перейдите по ссылке **Настройка**.

3. В левой части окна выберите в разделе **Общие параметры** подраздел **Отчеты и хранилища**.

4. В правой части окна в блоке **Хранение** установите флажок **Максимальный размер файла** и укажите максимальный размер файла отчета.

ОЧИСТКА ОТЧЕТОВ

Вы можете очистить отчеты, данные которых вам больше не нужны.

Чтобы очистить отчеты, *выполните следующие действия*:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Общие параметры** подраздел **Отчеты и хранилища**.
4. В правой части окна в блоке **Очистка отчетов** нажмите на кнопку **Очистить**.
5. В открывшемся окне **Удаление информации из отчетов** установите флажки для тех отчетов, которые вы хотите очистить.

ЗАПИСЬ НЕКРИТИЧЕСКИХ СОБЫТИЙ

По умолчанию записи о некритических событиях, событиях реестра и файловой системы в отчет не добавляются. Вы можете включить такие записи в отчеты о защите.

Чтобы включить запись в отчет некритических событий, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Общие параметры** подраздел **Отчеты и хранилища**.
4. В правой части окна в блоке **События, включаемые в отчеты** установите флажки напротив типов событий, которые нужно включать в отчет.

НАСТРОЙКА НАПОМИНАНИЯ О ГОТОВНОСТИ ОТЧЕТА

Вы можете сформировать расписание, согласно которому Kaspersky CRYSTAL будет напоминать вам о готовности отчета.

Чтобы сформировать расписание, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Защита компьютера**.

   Откроется окно **Защита компьютера**.

2. По ссылке **Отчет** перейдите к окну отчетов Kaspersky CRYSTAL.
3. В открывшемся окне на закладке **Отчет** установите флажок **Напоминать об отчете** и откройте окно настройки расписания, перейдя по ссылке с установленным временем.
4. В открывшемся окне **Отчет: расписание** задайте параметры расписания.

УВЕДОМЛЕНИЯ

По умолчанию при возникновении событий в процессе работы Kaspersky CRYSTAL уведомляет вас об этом. Если от вас требуется выбор дальнейших действий, то на экран выводятся окна уведомлений (см. раздел «Окна уведомлений и всплывающие сообщения» на стр. 49). О событиях, не требующих выбора действий, программа

уведомляет с помощью звукового оповещения, почтовых сообщений и всплывающих сообщений в области уведомлений панели задач (см. раздел «Окна уведомлений и всплывающие сообщения» на стр. 49).

Вы можете выбрать способы уведомления (см. раздел «Настройка способа уведомления» на стр. 236) о событиях, не требующих выбора действия, а также отключить доставку уведомлений (см. раздел «Включение и отключение уведомлений» на стр. 236).

См. также:

Настройка способа уведомления 236

Включение и отключение уведомлений

По умолчанию Kaspersky CRYSTAL уведомляет вас о значимых событиях, связанных с работой программы, различными способами (см. раздел «Настройка способа уведомления» на стр. 236). Вы можете отключить доставку уведомлений.

Вне зависимости от того, включена или отключена доставка уведомлений, информация о событиях, возникающих в ходе работы Kaspersky CRYSTAL, записывается в отчет о работе программы.

Когда вы отключаете доставку уведомлений, это не влияет на отображение окон уведомлений. Чтобы на экране отображалось минимальное количество окон уведомлений, используйте автоматический режим защиты (см. раздел «Использование интерактивного режима защиты» на стр. 54).

Чтобы включить или отключить доставку уведомлений, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Общие параметры** подраздел **Уведомления**.
4. В правой части окна снимите флажок **Уведомлять о событиях**, если нужно отключить доставку уведомлений. Установите этот флажок, если доставку уведомлений нужно включить.

Настройка способа уведомления

Программа уведомляет вас о событиях следующими способами:

- всплывающими сообщениями в области уведомлений панели задач;
- звуковым оповещением;
- сообщениями электронной почты.

Вы можете настроить способы доставки уведомлений индивидуально для каждого типа событий.

По умолчанию критические уведомления и уведомления о нарушениях в работе программы сопровождаются звуковым сигналом. В качестве звукового сопровождения используется звуковая схема Microsoft Windows. Вы можете изменить использующуюся схему или отключить звуковое оповещение.

Чтобы настроить способы доставки уведомлений для разных типов событий, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.

3. В левой части окна выберите в разделе **Общие параметры** подраздел **Уведомления**.

4. В правой части окна установите флажок **Уведомлять о событиях** и нажмите на кнопку **Настройка**, расположенную правее.

5. В открывшемся окне **Уведомления** установите флажки в соответствии с тем, какими способами вы хотите получать уведомления о различных событиях: по электронной почте, в виде всплывающего сообщения или с помощью звукового оповещения. Чтобы не получать никаких уведомлений для определенного типа событий, снимите все флажки в строке этого события.

   Чтобы Kaspersky CRYSTAL мог уведомлять вас о событиях по почте, необходимо настроить параметры электронной почты для доставки уведомлений.

- *Чтобы настроить параметры электронной почты для доставки уведомлений, выполните следующие действия:*

1. Откройте главное окно программы.

2. В верхней части окна перейдите по ссылке **Настройка**.

3. В левой части окна выберите в разделе **Общие параметры** подраздел **Уведомления**.

4. В правой части окна установите флажок **Отправлять почтовые сообщения о событиях** и нажмите на кнопку **Настройка**, расположенную правее.

5. В открывшемся окне **Настройка почтовых уведомлений** задайте параметры доставки.

- *Чтобы изменить звуковую схему уведомлений, выполните следующие действия:*

1. Откройте главное окно программы.

2. В верхней части окна перейдите по ссылке **Настройка**.

3. В левой части окна выберите в разделе **Общие параметры** подраздел **Уведомления**.

4. В правой части окна установите флажок **Использовать стандартную звуковую схему Windows Default** и отредактируйте использующуюся схему операционной системы.

   Если флажок снят, в качестве звукового сопровождения будет использоваться звуковая схема предыдущих версий программы.

- *Чтобы отключить звуковое сопровождение уведомлений, выполните следующие действия:*

1. Откройте главное окно программы.

2. В верхней части окна перейдите по ссылке **Настройка**.

3. В левой части окна выберите в разделе **Общие параметры** подраздел **Уведомления**.

4. В правой части окна снимите флажок **Включить звуковое сопровождение уведомлений**.

УЧАСТИЕ В KASPERSKY SECURITY NETWORK

Каждый день в мире появляется множество новых угроз. Для оперативного сбора информации о типах и источниках новых угроз, а также для ускорения разработки способов их нейтрализации вы можете присоединиться к Kaspersky Security Network.

Kaspersky Security Network (KSN) – это инфраструктура онлайн-служб и сервисов, предоставляющая доступ к оперативной базе знаний «Лаборатории Касперского» о репутации файлов, интернет-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции

Kaspersky CRYSTAL на новые виды угроз, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

При участии в Kaspersky Security Network статистика, полученная в результате работы Kaspersky CRYSTAL на вашем компьютере, автоматически отправляется в «Лабораторию Касперского».

Сбор, обработка и хранение персональных данных пользователя не производится.

Участие в Kaspersky Security Network добровольное. Решение об участии вы принимаете на этапе установки Kaspersky CRYSTAL, но можете изменить его в любой момент.

Чтобы включить использование Kaspersky Security Network, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В левой части окна выберите в разделе **Общие параметры** подраздел **Обратная связь**.
4. В правой части окна установите флажок **Я согласен участвовать в Kaspersky Security Network**.

ПРОВЕРКА КОРРЕКТНОСТИ НАСТРОЙКИ KASPERSKY CRYSTAL

После установки и настройки Kaspersky CRYSTAL вы можете проверить с помощью тестового «вируса» и его модификаций, правильно ли выполнена настройка параметров. Проверку следует выполнять для каждого компонента защиты / протокола отдельно.

В ЭТОМ РАЗДЕЛЕ

Тестовый «вирус» EICAR и его модификации 239

Тестирование защиты HTTP-трафика 240

Тестирование защиты SMTP-трафика 241

Проверка корректности настройки Файлового Антивируса 241

Проверка корректности настройки задачи проверки на вирусы 242

Проверка корректности настройки защиты от нежелательной почты 242

Тестовый «вирус» EICAR и его модификации

Тестовый «вирус» специально разработан организацией EICAR (The European Institute for Computer Antivirus Research) для проверки работы антивирусных продуктов.

Тестовый «вирус» НЕ ЯВЛЯЕТСЯ вредоносным программным обеспечением и не содержит программного кода, который мог бы нанести ущерб вашему компьютеру. Тем не менее большинство продуктов антивирусных компаний-производителей идентифицируют EICAR как вирус.

Никогда не используйте в качестве проверки работоспособности антивирусного продукта настоящие вирусы!

Загрузить тестовый «вирус» можно с официального веб-сайта организации EICAR: http://www.eicar.org/anti_virus_test_file.htm.

Перед загрузкой необходимо приостановить антивирусную защиту, поскольку тестовый «вирус», загружаемый со страницы anti_virus_test_file.htm, будет идентифицирован и обработан программой как зараженный объект, передаваемый по HTTP-протоколу.

Файл, загруженный с веб-сайта компании EICAR, программа идентифицирует как зараженный объект, содержащий не подлежащий лечению вирус, и выполняет действие, установленное для такого объекта.

Вы можете также использовать модификации стандартного тестового «вируса» для проверки работы программы. Для этого следует изменить содержание стандартного тестового «вируса», добавив к нему один из префиксов (см. таблицу далее). Для создания модификаций тестового «вируса» может использоваться любой текстовый или гипертекстовый редактор, например Microsoft Блокнот или UltraEdit32.

В первой графе таблицы (см. ниже) приведены префиксы, которые следует добавить в начало строки стандартного тестового «вируса» для создания его модификаций. Во второй графе перечислены все возможные значения статуса, присваиваемого объекту по результатам проверки программой. Третья графа содержит информацию об обработке программой объектов с указанным статусом. Обращаем ваше внимание на то, что действия над объектами определяются значениями параметров программы.

После добавления префикса к тестовому «вирусу» сохраните полученный файл под именем, дающим представление о модификации «вируса»: например, добавив префикс DELE-, сохраните полученный файл под именем eicar_dele.com.

Не забудьте возобновить антивирусную защиту после загрузки тестового «вируса» и создания его модификаций.

Таблица 2. Модификации тестового вируса

Префикс	Статус объекта	Информация об обработке объекта
Префикс отсутствует, стандартный тестовый «вирус».	**Зараженный**. Объект содержит код известного вируса. Лечение невозможно.	Программа идентифицирует данный объект как вирус, не подлежащий лечению. При попытке лечения объекта возникает ошибка; применяется действие, установленное для неизлечимых объектов.
CORR-	**Поврежденный**.	Программа получила доступ к объекту, но не смогла проверить его, поскольку объект поврежден (например, нарушена структура объекта, неверный формат файла). Информацию о том, что объект был обработан, вы можете найти в отчете о работе программы.
WARN-	**Подозрительный**. Объект содержит код неизвестного вируса. Лечение невозможно.	Объект признан подозрительным. На момент обнаружения базы программы не содержат описания процедуры лечения данного объекта. Вы получите уведомление при обнаружении такого объекта.
SUSP-	**Подозрительный**. Объект содержит модифицированный код известного вируса. Лечение невозможно.	Программа обнаружила частичное совпадение участка кода объекта с участком кода известного вируса. На момент обнаружения базы программы не содержат описания процедуры лечения данного объекта. Вы получите уведомление при обнаружении такого объекта.
ERRO-	**Ошибка проверки**.	При проверке объекта возникла ошибка. Программа не смогла получить доступ к объекту: нарушена целостность объекта (например, нет конца многотомного архива) либо отсутствует связь с ним (если проверяется объект на сетевом ресурсе). Информацию о том, что объект был обработан, вы можете найти в отчете о работе программы.
CURE-	**Зараженный**. Объект содержит код известного вируса. Излечим.	Объект содержит вирус, который может быть вылечен. Программа выполняет лечение объекта, при этом текст тела вируса изменяется на CURE. Вы получите уведомление при обнаружении такого объекта.
DELE-	**Зараженный**. Объект содержит код известного вируса. Лечение невозможно.	Программа идентифицирует данный объект как вирус, не подлежащий лечению. При попытке лечения объекта возникает ошибка; применяется действие, установленное для неизлечимых объектов. Вы получите уведомление при обнаружении такого объекта.

Тестирование защиты HTTP-трафика

- *Чтобы проверить обнаружение вирусов в потоке данных, передаваемых по HTTP-протоколу:*

  попытайтесь загрузить тестовый «вирус» с официального сайта организации **EICAR**: http://www.eicar.org/anti_virus_test_file.htm.

При попытке загрузить тестовый «вирус» Kaspersky CRYSTAL обнаружит объект, идентифицирует как зараженный неизлечимый и выполнит действие, установленное в параметрах проверки HTTP-трафика для такого объекта. По умолчанию при попытке загрузить тестовый «вирус» соединение с ресурсом будет разорвано, и в окне браузера будет выведено сообщение о том, что данный объект заражен вирусом EICAR-Test-File.

ТЕСТИРОВАНИЕ ЗАЩИТЫ SMTP-ТРАФИКА

Для проверки обнаружения вирусов в потоке данных, передаваемых по SMTP-протоколу, вы можете использовать почтовую систему, в которой передача данных осуществляется по этому протоколу.

Рекомендуется протестировать обнаружение вирусов в различных частях исходящей почты: как в теле сообщения, так и во вложениях. Для тестирования используйте файл тестового вируса EICAR (см. раздел «Тестовый “вирус” EICAR и его модификации» на стр. 239).

Чтобы протестировать обнаружение вирусов в потоке данных, отправляемых по протоколу SMTP, выполните следующие действия:

1. Создайте письмо в формате «Обычный текст» с помощью установленного на компьютере почтового клиента.

   Письмо, содержащее в теле тестовый «вирус» и сформированное в формате RTF и HTML, проверено не будет!

2. В зависимости от того, в какой части письма программа должна обнаружить вирус, выполните следующие действия:

   - для обнаружения вируса в теле письма поместите текст стандартного или модифицированного тестового «вируса» EICAR в начало письма;
   - для обнаружения вируса во вложениях присоедините к письму файл, содержащий тестовый «вирус» EICAR.

3. Отправьте письмо на адрес администратора.

Программа обнаружит объект, идентифицирует его как зараженный и заблокирует отправку письма.

ПРОВЕРКА КОРРЕКТНОСТИ НАСТРОЙКИ ФАЙЛОВОГО АНТИВИРУСА

Чтобы проверить, насколько корректно настроен Файловый Антивирус, выполните следующие действия:

1. Создайте папку на диске, скопируйте в нее тестовый «вирус», загруженный с официального сайта организации **EICAR** (http://www.eicar.org/anti_virus_test_file.htm), а также созданные вами модификации тестового «вируса».

2. Разрешите запись в отчет всех событий, чтобы в файле отчета сохранялись данные о поврежденных объектах или объектах, не проверенных в результате сбоя.

3. Запустите файл тестового «вируса» или его модификацию на выполнение.

Файловый Антивирус перехватит обращение к файлу, проверит его и выполнит действие, заданное в параметрах. Выбирая различные варианты действий над обнаруженным объектом, вы сможете проверить работу компонента полностью.

Полную информацию о результате работы Файлового Антивируса можно посмотреть в отчете о работе компонента.

Проверка корректности настройки задачи проверки на вирусы

Чтобы проверить, насколько корректно настроена задача проверки на вирусы, выполните следующие действия:

1. Создайте папку на диске, скопируйте в нее тестовый «вирус», загруженный с официального сайта организации **EICAR** (http://www.eicar.org/anti_virus_test_file.htm), а также созданные вами модификации тестового «вируса».

2. Создайте новую задачу проверки на вирусы и в качестве объекта проверки выберите папку, содержащую набор тестовых «вирусов».

3. Разрешите запись в отчет всех событий, для того чтобы в файле отчета сохранялись данные о поврежденных объектах или объектах, не проверенных в результате сбоя.

4. Запустите задачу проверки на вирусы на выполнение.

При проверке по мере обнаружения подозрительных или зараженных объектов будут выполняться действия, заданные в параметрах задачи. Выбирая различные варианты действий над обнаруженным объектом, вы сможете проверить работу компонента полностью.

Полную информацию о результат выполнения задачи проверки на вирусы можно посмотреть в отчете по работе компонента.

Проверка корректности настройки защиты от нежелательной почты

Для проверки защиты от нежелательной почты вы можете использовать тестовое сообщение, которое идентифицируется программой как спам.

Тестовое сообщение должно содержать в теме письма строку:

```
Spam is bad do not send it
```

После поступления данного сообщения на компьютер Kaspersky CRYSTAL проверит его, присвоит сообщению статус спама и выполнит над ним действие, установленное для объекта данного типа.

ОБРАЩЕНИЕ В СЛУЖБУ ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ

Если при использовании Kaspersky CRYSTAL возникли проблемы, прежде всего проверьте, не описан ли метод их решения в документации, справке, в Базе знаний на веб-сайте Службы технической поддержки «Лаборатории Касперского» или на Форуме пользователей.

Если вы не нашли решения возникшей проблемы, обратитесь в Службу технической поддержки «Лаборатории Касперского» одним из следующих способов:

- отправьте запрос из Личного кабинета на веб-сайте Службы технической поддержки;
- позвоните по телефону.

Специалисты Службы технической поддержки ответят на ваши вопросы об установке, активации и использовании программы. Если ваш компьютер был заражен, они помогут устранить последствия работы вредоносных программ.

Прежде чем обращаться в Службу технической поддержки, пожалуйста, ознакомьтесь с правилами поддержки (http://support.kaspersky.ru/support/rules).

При обращении в Службу технической поддержки специалисты службы могут попросить вас сформировать отчет о состоянии системы и файл трассировки и отправить их в Службу технической поддержки. В результате анализа присланных вами данных специалисты Службы технической поддержки могут создать и отправить вам скрипт AVZ, с помощью которого вы можете устранить возникшие проблемы.

В ЭТОМ РАЗДЕЛЕ

Личный кабинет 243

Техническая поддержка по телефону 244

Создание отчета о состоянии системы 244

Создание файла трассировки 245

Отправка файлов данных 245

Выполнение скрипта AVZ 246

Личный кабинет

Личный кабинет – это ваш персональный раздел на сайте Службы технической поддержки. В нем вы можете выполнять следующие действия:

- отправлять запросы в Службу технической поддержки и Вирусную лабораторию;
- переписываться со Службой технической поддержки без использования электронной почты;
- отслеживать состояние ваших запросов в реальном времени;
- просматривать полную историю ваших обращений в Службу технической поддержки.

Чтобы открыть страницу входа в Личный кабинет, воспользуйтесь одним из следующих способов:

- перейдите по ссылке **Личный кабинет** в главном окне Kaspersky CRYSTAL;
- введите в адресную строку браузера адрес https://my.kaspersky.ru.

Если вы еще не зарегистрированы в Личном кабинете, можно пройти регистрацию на странице регистрации https://my.kaspersky.com/ru/registration. Здесь вам нужно указать адрес электронной почты и пароль для доступа в Личный кабинет. Для отправки запросов об использовании Kaspersky CRYSTAL вам понадобится код активации программы.

Обратите внимание на то, что некоторые запросы нужно направлять не в Службу технической поддержки, а в Вирусную лабораторию. Это запросы следующих типов:

- неизвестная вредоносная программа – вы подозреваете, что некоторый объект является вредоносным, но Kaspersky CRYSTAL не идентифицирует его таким образом;
- ложное срабатывание антивируса – Kaspersky CRYSTAL определяет некий файл как вирус, но вы уверены, что файл не является вирусом;
- запрос на описание вредоносной программы – вы хотите получить описание какого-то вируса.

Чтобы направить запрос в Вирусную лабораторию, код активации не нужен.

Вы также можете направлять запросы в Вирусную лабораторию, не регистрируясь в Личном кабинете, со страницы с формой запроса (http://support.kaspersky.ru/virlab/helpdesk.html).

Техническая поддержка по телефону

Если возникла неотложная проблема, вы можете позвонить в Службу технической поддержки в вашем городе. Перед обращением к специалистам русскоязычной (http://support.kaspersky.ru/support/support_local) или интернациональной (http://support.kaspersky.ru/support/international) технической поддержки, пожалуйста, соберите информацию (http://support.kaspersky.ru/support/details) о своем компьютере и установленном на нем антивирусном приложении. Это позволит нашим специалистам быстрее помочь вам.

Создание отчета о состоянии системы

При решении ваших проблем специалистам Службы технической поддержки «Лаборатории Касперского» может понадобиться отчет о состоянии системы. Этот отчет содержит подробную информацию о запущенных процессах, загружаемых модулях и драйверах, модулях расширения Microsoft Internet Explorer и Проводника Microsoft Windows, открытых портах, обнаруженных подозрительных объектах и т.п.

В процессе создания отчета о состоянии системы сбор персональных данных пользователя не производится.

Чтобы создать отчет о состоянии системы, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна программы перейдите по ссылке **Поддержка**.
3. В открывшемся окне **Поддержка** перейдите по ссылке **Трассировки**.
4. В открывшемся окне **Информация для поддержки** нажмите на кнопку **Создать отчет о состоянии системы**.

Отчет о состоянии системы формируется в форматах HTML и XML и сохраняется в архиве sysinfo.zip. По окончании процесса сбора информации о системе вы можете просмотреть отчет.

Чтобы просмотреть отчет, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна программы перейдите по ссылке **Поддержка**.
3. В открывшемся окне **Поддержка** перейдите по ссылке **Трассировки**.
4. В открывшемся окне **Информация для поддержки** нажмите на кнопку **Просмотр**.
5. Откройте архив sysinfo.zip, содержащий файлы отчета.

Создание файла трассировки

После установки Kaspersky CRYSTAL могут возникнуть сбои в работе операционной системы или отдельных программ. В этом случае, скорее всего, имеет место конфликт Kaspersky CRYSTAL с программным обеспечением, установленным на вашем компьютере, или с драйверами комплектующих вашего компьютера. Для успешного решения этой проблемы специалисты Службы технической поддержки «Лаборатории Касперского» могут попросить вас создать файл трассировки.

Чтобы создать файл трассировки, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна программы перейдите по ссылке **Поддержка**.
3. В открывшемся окне **Поддержка** перейдите по ссылке **Трассировки**.
4. В открывшемся окне **Информация для поддержки** в блоке **Трассировка** выберите уровень трассировки в раскрывающемся списке.

   Требуемый уровень трассировки рекомендуется уточнить у специалиста Службы технической поддержки. При отсутствии указаний Службы технической поддержки рекомендуется устанавливать уровень трассировки **500**.
5. Чтобы запустить процесс трассировки, нажмите на кнопку **Включить**.
6. Воспроизведите ситуацию, в которой возникает ваша проблема.
7. Чтобы остановить процесс трассировки, нажмите на кнопку **Выключить**.

Вы можете перейти к загрузке результатов трассировки (см. раздел «Отправка файлов данных» на стр. 245) на сервер «Лаборатории Касперского».

Отправка файлов данных

После создания файлов трассировки и отчета о состоянии системы их необходимо отправить специалистам Службы технической поддержки «Лаборатории Касперского».

Чтобы загрузить файлы данных на сервер Службы технической поддержки, вам понадобится номер запроса. Этот номер доступен в вашем Личном кабинете на веб-сайте Службы технической поддержки при наличии активного запроса.

Чтобы загрузить файлы данных на сервер Службы поддержки, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна программы перейдите по ссылке **Поддержка**.

3. В открывшемся окне **Поддержка** перейдите по ссылке **Трассировки**.

4. В открывшемся окне **Информация для поддержки** в блоке **Действия** нажмите на кнопку **Загрузить информацию для поддержки на сервер**.

5. В открывшемся окне **Загрузка информации для поддержки на сервер** установите флажки рядом с теми файлами, которые вы хотите отправить в Службу технической поддержки, и нажмите на кнопку **Отправить**.

6. В открывшемся окне **Номер запроса** укажите номер, присвоенный вашему запросу при заполнении электронной формы на сайте Службы технической поддержки.

Выбранные файлы данных будут упакованы и отправлены на сервер Службы технической поддержки.

Если связаться со Службой технической поддержки по какой-либо причине невозможно, вы можете сохранить файлы данных на вашем компьютере и впоследствии отправить их из Личного кабинета.

Чтобы сохранить файлы данных на диск, выполните следующие действия:

1. Откройте главное окно программы.

2. В нижней части окна программы перейдите по ссылке **Поддержка**.

3. В открывшемся окне **Поддержка** перейдите по ссылке **Трассировки**.

4. В открывшемся окне **Информация для поддержки** в блоке **Действия** нажмите на кнопку **Загрузить информацию для поддержки на сервер**.

5. В открывшемся окне **Загрузка информации для поддержки на сервер** установите флажки рядом с теми файлами, которые вы хотите отправить в Службу технической поддержки, и нажмите на кнопку **Отправить**.

6. В открывшемся окне **Номер запроса** нажмите на кнопку **Отмена** и в открывшемся окне подтвердите сохранение файлов на диске, нажав на кнопку **Да**.

7. В открывшемся окне задайте имя архива и подтвердите сохранение.

Созданный архив вы можете отправить в Службу технической поддержки через Личный кабинет.

Выполнение скрипта AVZ

Специалисты «Лаборатории Касперского» анализируют вашу проблему на основе файлов трассировки и отчета о состоянии системы. Результатом анализа является последовательность действий, направленных на устранение обнаруженных проблем. Количество этих действий может оказаться очень большим.

Для упрощения процедуры устранения проблем используются скрипты AVZ. Скрипт AVZ представляет собой набор инструкций, позволяющих редактировать ключи реестра, помещать на карантин файлы, производить поиск классов с возможностью карантина связанных с ними файлов, выполнять блокирование перехватчиков UserMode и KernelMode и т. д.

Для запуска скриптов в состав программы включен *мастер Выполнения скриптов AVZ*.

Мастер состоит из последовательности окон (шагов), переключение между которыми осуществляется нажатием на кнопки **Назад** и **Далее**. Работа мастера завершается нажатием на кнопку **Завершить**. Для прекращения работы мастера на любом этапе следует нажать на кнопку **Отмена**.

Не рекомендуется вносить изменения в текст скрипта, присланного вам специалистами «Лаборатории Касперского». В случае возникновения проблем в ходе выполнения скрипта обращайтесь в Службу поддержки.

Чтобы запустить мастер, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна программы перейдите по ссылке **Поддержка**.
3. В открывшемся окне **Поддержка** перейдите по ссылке **Трассировки**.
4. В открывшемся окне **Информация для поддержки** нажмите на кнопку **Выполнить скрипт AVZ**.

В случае успешного выполнения скрипта работа мастера завершается. Если во время выполнения скрипта возникнет сбой, мастер выведет на экран соответствующее сообщение.

ПРИЛОЖЕНИЯ

Этот раздел содержит справочную информацию, которая дополняет основной текст документа.

В ЭТОМ РАЗДЕЛЕ

Статусы подписки 248

Работа с программой из командной строки 249

Список уведомлений Kaspersky CRYSTAL 259

Статусы подписки

Состояние подписки характеризуется одним из следующих статусов:

- *Определяется*. Запрос на активацию подписки еще не обработан (для обработки запроса на сервере требуется некоторое время). Kaspersky CRYSTAL работает в полнофункциональном режиме. Если по окончании определенного периода запрос на подписку не будет обработан, вы получите уведомление о том, что обновление статуса подписки не выполнено. При этом перестанут обновляться базы программы (для лицензии с подпиской на обновление), перестанет осуществляться защита компьютера (для лицензии с подпиской на обновление и защиту).

- *Активирована*. Подписка была активирована бессрочно или на определенное время (дата окончания подписки определена).

- *Продлена*. Подписка была продлена бессрочно или на определенное время.

- *Ошибка*. При обновлении статуса подписки произошла ошибка.

- *Истекла. Действует льготный период.* Истек срок действия подписки или срок для обновления статуса. Если истек срок для обновления статуса, обновите статус подписки вручную. Если истек срок действия подписки, вы можете продлить подписку, связавшись с онлайн-магазином, где вы приобрели Kaspersky CRYSTAL. Чтобы воспользоваться другим кодом активации, следует сначала удалить используемую подписку.

- *Истекла. Льготный период истек.* Истек срок действия подписки или льготный период для ее продления. Обратитесь к поставщику подписки для приобретения новой или возобновления текущей подписки.

  Если срок действия подписки истек и истек льготный период, в течение которого доступно ее продление (статус подписки – *Истекла*), Kaspersky CRYSTAL уведомляет вас об этом и прекращает попытки автоматического продления подписки. Для лицензии с подпиской на обновление функциональность программы сохраняется, за исключением обновления баз программы. Для лицензии с подпиской на обновление и защиту перестанут обновляться базы программы, осуществляться защита компьютера и запускаться задачи проверки.

- *Отказ от подписки*. Вы отказались от подписки на автоматическое продление лицензии.

- *Требуется обновление*. Статус подписки по каким-либо причинам не был обновлен вовремя.

  Если подписка не была продлена вовремя (например, компьютер был выключен весь период, когда было доступно продление лицензии), вы можете обновить ее статус вручную в окне управления лицензиями (см. раздел «Просмотр информации о лицензии» на стр. 35). До момента продления подписки Kaspersky CRYSTAL прекращает обновление баз программы (для лицензии с подпиской на

обновление), а также прекращает осуществлять защиту компьютера и запускать задачи проверки (для лицензии с подпиской на обновление и защиту).

- *Приостановлена*. Подписка на автоматическое продление лицензии приостановлена.
- *Возобновлена*. Подписка возобновлена.

> В некоторых случаях для лицензии с подпиской возможно отображение дополнительной информации о статусе подписки.

Работа с программой из командной строки

Вы можете работать с Kaspersky CRYSTAL с помощью командной строки. При этом предусмотрена возможность выполнения следующих операций:

- активация программы;
- запуск и остановка программы;
- запуск и остановка работы компонентов программы;
- запуск и остановка задач;
- получение информации о текущем статусе компонентов и задач и их статистики;
- запуск и остановка выполнения задач проверки на вирусы;
- проверка выбранных объектов;
- обновление баз и программных модулей, откат обновления;
- экспорт и импорт параметров защиты;
- вызов справки по синтаксису командной строки в целом и отдельных команд.

Синтаксис командной строки:

```
avp.com <команда> [параметры]
```

Обращаться к программе через командную строку следует из каталога установки продукта либо с указанием полного пути к avp.com.

Перечень команд, используемых для управления программой и ее компонентами, приведен в таблице ниже.

START	Запуск компонента или задачи
STOP	Остановка работы компонента или задачи (выполнение команды возможно только с вводом пароля, заданного через интерфейс Kaspersky CRYSTAL)
STATUS	Вывод на экран текущего статуса компонента или задачи
STATISTICS	Вывод на экран статистики работы компонента или задачи
HELP	Вывод на экран списка команд, а также информации о синтаксисе команды
SCAN	Проверка объектов на присутствие вирусов

UPDATE	Запуск обновления программы
ROLLBACK	Откат последнего произведенного обновления Kaspersky CRYSTAL (выполнение команды возможно только с вводом пароля, заданного через интерфейс программы)
EXIT	Завершение работы с программой (выполнение команды возможно только с вводом пароля, заданного через интерфейс программы)
IMPORT	Импорт параметров защиты Kaspersky CRYSTAL (выполнение команды возможно только с вводом пароля, заданного через интерфейс программы)
EXPORT	Экспорт параметров защиты программы

Каждой команде соответствует собственный набор параметров, специфичный для конкретного компонента программы.

В этом разделе

Активация программы 250

Запуск программы 251

Остановка программы 251

Управление компонентами и задачами программы 251

Проверка на вирусы 253

Обновление программы 255

Откат последнего обновления 256

Экспорт параметров защиты 256

Импорт параметров защиты 257

Получение файла трассировки 257

Просмотр справки 257

Коды возврата командной строки 258

Активация программы

Активировать Kaspersky CRYSTAL можно с помощью файла ключа.

Синтаксис команды:

```
avp.com ADDKEY <имя_файла>
```

Описание параметров выполнения команды приведено в таблице ниже.

<имя_файла>	Имя файла ключа к программе с расширением .key

Пример:

```
avp.com ADDKEY 1AA111A1.key
```

Запуск программы

Синтаксис команды:

```
avp.com
```

Остановка программы

Синтаксис команды:

```
avp.com EXIT /password=<ваш_пароль>
```

Описание параметров приведено в таблице ниже.

<ваш_пароль>	Пароль к программе, заданный в интерфейсе

Обратите внимание на то, что без ввода пароля команда выполняться не будет.

Управление компонентами и задачами программы

Синтаксис команды:

```
avp.com <команда> <профайл|имя_задачи> [/R[A]:<файл_отчета>]
avp.com STOP <профайл|имя_задачи> /password=<ваш_пароль> [/R[A]:<файл_отчета>]
```

Описание команд и параметров приведено в таблице ниже.

<команда>	Управление компонентами и задачами Kaspersky CRYSTAL из командной строки выполняется с помощью следующего набора команд: START – запуск компонента защиты или задачи. STOP – остановка работы компонента защиты или задачи. STATUS – вывод на экран текущего статуса компонента защиты или задачи. STATISTICS – вывод на экран статистики по работе компонента защиты или задачи. Обратите внимание, что без ввода пароля команда STOP выполняться не будет.
<профайл|имя_задачи>	В качестве значений для параметра **<профайл>** вы можете указать любой из компонентов защиты Kaspersky CRYSTAL, а также модули, входящие в состав компонентов, сформированные задачи проверки по требованию или обновления (используемые программой стандартные значения приводятся в таблице ниже). В качестве значений для параметра **<имя_задачи>** может быть указано имя любой сформированной пользователем задачи проверки по требованию либо обновления.
<ваш_пароль>	Пароль к программе, заданный в интерфейсе.
/R[A]:<файл_отчета>	**/R:<файл_отчета>** – фиксировать в отчете только важные события. **/RA:<файл_отчета>** – записывать в отчет все события. Допускается использование абсолютного или относительного пути к файлу. Если параметр не указан, результаты проверки выводятся на экран, отображаются все события.

В качестве параметра **<профайл>** указывается одно из значений, приведенных в следующей таблице.

RTP	Все компоненты защиты. Команда **avp.com START RTP** запускает все компоненты защиты, если защита была полностью отключена. В случае если компонент был выключен командой **STOP** командной строки, он не будет запущен командой **avp.com START RTP**. Для этого необходимо выполнить команду **avp.com START <профайл>**, где для параметра **<профайл>** используется значение для конкретного компонента защиты, например, **avp.com START FM**.
FW	Сетевой экран.
HIPS	Контроль программ.
pdm	Проактивная защита.
FM	Файловый Антивирус.
EM	Почтовый Антивирус.
WM	Веб-Антивирус. Значения для подкомпонентов Веб-Антивируса: **httpscan (HTTP)** – проверка HTTP-трафика; **sc** – проверка скриптов.
IM	IM-Антивирус.
AB	Анти-Баннер.
AS	Анти-Спам.
PC	Родительский контроль.
AP	Анти-Фишинг.
ids	Защита от сетевых атак.
Updater	Обновление.
Rollback	Откат последнего обновления.
Scan_My_Computer	Проверка компьютера.
Scan_Objects	Проверка объектов.
Scan_Quarantine	Проверка карантина.
Scan_Startup (STARTUP)	Проверка объектов автозапуска.
Scan_Vulnerabilities (SECURITY)	Поиск уязвимостей.

Компоненты и задачи, запущенные из командной строки, выполняются с параметрами, установленными в интерфейсе программы.

Примеры:

- *Чтобы включить Файловый Антивирус, введите команду:*

```
avp.com START FM
```

Чтобы остановить проверку компьютера, введите команду:

```
avp.com STOP Scan_My_Computer /password=<ваш_пароль>
```

Проверка на вирусы

Командная строка запуска проверки некоторой области на присутствие вирусов, а также запуска обработки вредоносных объектов имеет следующий общий вид:

```
avp.com SCAN [<объект проверки>] [<действие>] [<типы файлов>] [<исключения>]
[<конфигурационный файл>] [<параметры отчета>] [<дополнительные параметры>]
```

Для проверки объектов вы также можете воспользоваться сформированными в программе задачами, запустив нужную из командной строки. При этом задача будет выполнена с параметрами, установленными в интерфейсе Kaspersky CRYSTAL.

Описание параметров приведено в таблице ниже.

<объект проверки> – параметр задает перечень объектов, которые будут проверены на присутствие вредоносного кода. Параметр может включать несколько значений из представленного списка, разделенных пробелом.	
<files>	Список путей к файлам и папкам для проверки. Допускается ввод абсолютного или относительного пути. Разделительный символ для элементов списка – пробел. Замечания: • если имя объекта содержит пробел, оно должно быть заключено в кавычки; • если указан конкретный каталог, проверяются все содержащиеся в нем файлы.
/MEMORY	Объекты оперативной памяти.
/STARTUP	Объекты автозапуска.
/MAIL	Почтовые ящики.
/REMDRIVES	Все съемные диски.
/FIXDRIVES	Все локальные диски.
/NETDRIVES	Все сетевые диски.
/QUARANTINE	Объекты на карантине.
/ALL	Полная проверка компьютера.
/@:<filelist.lst>	Путь к файлу со списком объектов и каталогов, включаемых в проверку. Допускается ввод абсолютного или относительного пути к файлу со списком. Путь указывается без кавычек, даже если в нем содержится символ пробела. Файл со списком объектов должен иметь текстовый формат. Каждый объект проверки необходимо указывать с новой строки. Рекомендуется указывать в файле абсолютные пути к объектам проверки. При указании относительного пути указывается путь относительно исполняемого файла программы, а не относительно файла со списком проверяемых объектов.

<действие> – параметр определяет действия над вредоносными объектами, обнаруженными в ходе проверки. Если параметр не задан, по умолчанию выполняется действие, соответствующее значению **/i8**. Если вы работаете в автоматическом режиме, то Kaspersky CRYSTAL будет автоматически применять рекомендуемое специалистами «Лаборатории Касперского» действие при обнаружении опасных объектов. Действие, соответствующее значению параметра **<действие>**, будет игнорироваться.	
/i0	Не совершать над объектом никаких действий, фиксировать информацию о нем в отчете.
/i1	Лечить зараженные объекты; если лечение невозможно – пропустить.
/i2	Лечить зараженные объекты; если лечение невозможно – удалять; не удалять зараженные объекты из контейнеров (составных объектов); удалять контейнеры с исполняемым заголовком (sfx-архивы).
/i3	Лечить зараженные объекты; если лечение невозможно – удалять; удалять объекты-контейнеры полностью, если невозможно удалить вложенные зараженные файлы.
/i4	Удалять зараженные объекты; удалять объекты-контейнеры полностью, если невозможно удалить вложенные зараженные файлы.
/i8	Запрашивать действие у пользователя при обнаружении зараженного объекта.
/i9	Запрашивать действие у пользователя по окончании проверки.
<типы файлов> – параметр определяет типы файлов, которые будут подвергаться антивирусной проверке. По умолчанию, если параметр не задан, проверяются только заражаемые файлы по содержимому.	
/fe	Проверять только заражаемые файлы по расширению.
/fi	Проверять только заражаемые файлы по содержимому.
/fa	Проверять все файлы.
<исключения> – параметр определяет объекты, исключаемые из проверки. Параметр может включать несколько значений из представленного списка, разделенных пробелом.	
-e:a	Не проверять архивы.
-e:b	Не проверять почтовые базы.
-e:m	Не проверять почтовые сообщения в формате plain text.
-e:<filemask>	Не проверять объекты по маске.
-e:<seconds>	Пропускать объекты, которые проверяются дольше указанного параметром **<seconds>** времени.
-es:<size>	Пропускать объекты, размер которых (в мегабайтах) превышает значение, заданное параметром **<size>**. Параметр применим только к составным файлам (например, архивам).
<конфигурационный файл> – определяет путь к конфигурационному файлу, содержащему параметры работы программы при проверке. Конфигурационный файл представляет собой файл текстового формата, содержащий набор параметров командной строки для антивирусной проверки. Допускается ввод абсолютного или относительного пути к файлу. Если параметр не задан, используются значения, установленные в интерфейсе программы.	
/C:<имя_файла>	Использовать значения параметров, заданные в конфигурационном файле **<имя_файла>**.

<параметры отчета> – параметр определяет формат отчета о результатах проверки. Допускается использование абсолютного или относительного пути к файлу. Если параметр не указан, результаты проверки выводятся на экран, отображаются все события.	
/R:<файл_отчета>	Записывать в указанный файл отчета только важные события.
/RA:<файл_отчета>	Записывать в указанный файл отчета все события.
<дополнительные параметры> – параметр, определяющий использование технологий антивирусной проверки.	
/iChecker=<on|off>	Включить / отключить использование технологии iChecker.
/iSwift=<on|off>	Включить / отключить использование технологии iSwift.

Примеры:

- *Запустить проверку оперативной памяти, объектов автозапуска, почтовых ящиков, а также каталогов My Documents, Program Files и файла test.exe:*

```
avp.com SCAN /MEMORY /STARTUP /MAIL "C:\Documents and Settings\All Users\My Documents" "C:\Program Files" "C:\Downloads\test.exe"
```

- *Проверить объекты, список которых приведен в файле object2scan.txt. Использовать для работы конфигурационный файл scan_settings.txt. По результатам проверки сформировать отчет, в котором зафиксировать все события:*

```
avp.com SCAN /MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

Пример конфигурационного файла:

```
/MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

Обновление программы

Команда для обновления модулей Kaspersky CRYSTAL и программных баз имеет следующий синтаксис:

```
avp.com UPDATE [<источник_обновлений>] [/R[A]:<файл_отчета>] [/C:<имя_файла>]
```

Описание параметров приведено в таблице ниже.

<источник_обновлений>	HTTP-, FTP-сервер или сетевой каталог для загрузки обновлений. В качестве значения для данного параметра может быть указан полный путь к источнику обновлений либо URL-адрес. Если путь не указан, источник обновлений будет взят из параметров сервиса обновления программы.
/R[A]:<файл_отчета>	**/R:<файл_отчета>** – фиксировать в отчете только важные события. **/RA:<файл_отчета>** – записывать в отчет все события. Допускается использование абсолютного или относительного пути к файлу. Если параметр не указан, результаты проверки выводятся на экран; отображаются все события.
/C:<имя_файла>	Путь к конфигурационному файлу, содержащему параметры работы Kaspersky CRYSTAL при обновлении. Конфигурационный файл представляет собой файл текстового формата, содержащий набор параметров командной строки для обновления программы. Допускается ввод абсолютного или относительного пути к файлу. Если параметр не задан, используются значения параметров, установленные в интерфейсе программы.

Примеры:

- *Обновить базы программы, зафиксировав все события в отчете:*

```
avp.com UPDATE /RA:avbases_upd.txt
```

- *Обновить модули Kaspersky CRYSTAL, используя параметры конфигурационного файла updateapp.ini:*

```
avp.com UPDATE /C:updateapp.ini
```

Пример конфигурационного файла:

```
"ftp://my_server/kav updates" /RA:avbases_upd.txt
```

Откат последнего обновления

Синтаксис команды:

```
avp.com ROLLBACK [/R[A]:<файл_отчета>][/password=<ваш_пароль>]
```

Описание параметров приведено в таблице ниже.

/R[A]:<файл_отчета>	**/R:<файл_отчета>** – фиксировать в отчете только важные события. **/RA:<файл_отчета>** – записывать в отчет все события. Допускается использование абсолютного или относительного пути к файлу. Если параметр не указан, результаты проверки выводятся на экран; отображаются все события.
<ваш_пароль>	Пароль к программе, заданный в интерфейсе.

Обратите внимание на то, что без ввода пароля команда выполняться не будет.

Пример:

```
avp.com ROLLBACK /RA:rollback.txt /password=<ваш_пароль>
```

Экспорт параметров защиты

Синтаксис команды:

```
avp.com EXPORT <профайл> <имя_файла>
```

Описание параметров выполнения команды приведено в таблице ниже.

<профайл>	Компонент или задача, для которых выполняется экспорт параметров. В качестве значения параметра **<профайл>** может быть использовано любое значение, указанное в разделе справки «Управление компонентами программы и задачами».
<имя_файла>	Путь к файлу, в который экспортируются параметры Kaspersky CRYSTAL. Может быть указан абсолютный или относительный путь. Конфигурационный файл сохраняется в бинарном формате (dat), если не указан иной формат либо формат не задан, и далее может использоваться для переноса параметров программы на другие компьютеры. Кроме того, вы можете сохранить конфигурационный файл в текстовом формате, для этого в имени файла укажите расширение txt. Обратите внимание, что импорт параметров защиты из текстового файла не поддерживается, данный файл может использоваться только для просмотра основных параметров работы Kaspersky CRYSTAL.

Пример:

```
avp.com EXPORT RTP c:\settings.dat
```

Импорт параметров защиты

Синтаксис команды:

```
avp.com IMPORT <имя_файла> [/password=<ваш_пароль>]
```

Описание параметров выполнения команды приведено в таблице ниже.

<имя_файла>	Путь к файлу, из которого импортируются параметры Kaspersky CRYSTAL. Может быть указан абсолютный или относительный путь.
<ваш_пароль>	Пароль к Kaspersky CRYSTAL, заданный в интерфейсе программы. Импорт параметров защиты возможен только из файла в бинарном формате.

Обратите внимание на то, что без ввода пароля команда выполняться не будет.

Пример:

```
avp.com IMPORT c:\settings.dat /password=<ваш_пароль>
```

Получение файла трассировки

Создание файла трассировки может потребоваться при возникновении проблем в работе Kaspersky CRYSTAL. Это поможет специалистам Службы технической поддержки более точно диагностировать проблемы.

Рекомендуется включать создание файлов трассировки только для диагностики конкретной проблемы. Постоянное включение трассировки может привести к потере производительности работы компьютера и переполнению жесткого диска.

Синтаксис команды:

```
avp.com TRACE [file] [on|off] [<уровень_трассировки>]
```

Описание параметров приведено в таблице ниже.

[on|off]	Включить / отключить создание файла трассировки.
[file]	Получить трассировку в виде файла.
<уровень_трассировки>	Для данного параметра допустимо указывать числовое значение в диапазоне от 0 (минимальный уровень, только критические сообщения) до 700 (максимальный уровень, все сообщения). При обращении в Службу технической поддержки специалист должен указать необходимый уровень трассировки. Если уровень не был указан, рекомендуется устанавливать значение 500.

Примеры:

- *Отключить создание файлов трассировки:*

  ```
  avp.com TRACE file off
  ```

- *Создать файл трассировки для отправки в Службу технической поддержки с максимальным уровнем трассировки равным 500:*

  ```
  avp.com TRACE file on 500
  ```

Просмотр справки

Для просмотра справочной информации о синтаксисе командной строки предусмотрена команда:

```
avp.com [ /? | HELP ]
```

Для получения справочной информации о синтаксисе конкретной команды вы можете воспользоваться одной из следующих команд:

```
avp.com <команда> /?
avp.com HELP <команда>
```

Коды возврата командной строки

В этом разделе приведено описание кодов возврата командной строки (в таблице ниже). Общие коды могут быть возвращены любой командой командной строки. К кодам возврата задач относятся общие коды, а также коды, специфичные для конкретного типа задачи.

Общие коды возврата	
0	Операция выполнена успешно
1	Неверное значение параметра
2	Неизвестная ошибка
3	Ошибка выполнения задачи
4	Выполнение задачи отменено
Коды возврата задач проверки на вирусы	
101	Все опасные объекты обработаны
102	Обнаружены опасные объекты

Список уведомлений Kaspersky CRYSTAL

В этом разделе приведен список уведомлений, которые могут выводиться на экран в процессе работы Kaspersky CRYSTAL.

В этом разделе

Лечение объекта невозможно 259

Недоступный сервер обновлений 260

Обнаружен вредоносный объект 260

Обнаружен опасный объект на трафике 261

Обнаружен подозрительный объект 261

Обнаружена опасная активность в системе 262

Обнаружен скрытый процесс 262

Обнаружена попытка доступа к системному реестру 263

Обнаружена сетевая активность программы 264

Обнаружена новая сеть 264

Обнаружена попытка фишинг-атаки 265

Обнаружена подозрительная ссылка 265

Обнаружен некорректный сертификат 266

Ограничение времени использования программы 266

Ошибка восстановления данных 266

Требуется специальная процедура лечения 266

Лечение объекта невозможно

В некоторых случаях лечение вредоносного объекта невозможно. Например, если файл поврежден настолько, что удалить из него вредоносный код и восстановить целостность не удается. Кроме того, процедура лечения не применима к некоторым видам вредоносных объектов, например, троянским программам.

В данных случаях на экран выводится специальное уведомление, которое содержит:

- Вид угрозы (например, *вирус*, *троянская программа*) и имя вредоносного объекта, как оно представлено в Вирусной энциклопедии «Лаборатории Касперского». Имя вредоносного объекта оформлено в виде ссылки на ресурс www.viruslist.ru, где вы можете получить подробную информацию о том, угроза какого рода обнаружена на вашем компьютере.

- Полное имя вредоносного объекта и путь к нему.

Вам предлагается выбрать одно из следующих действий над объектом:

- **Удалить** – удалить вредоносный объект. Перед удалением формируется резервная копия объекта на тот случай, если возникнет необходимость восстановить его или картину его заражения.

- **Пропустить** – заблокировать доступ к объекту, но не выполнять над ним никаких действий, лишь зафиксировать информацию о нем в отчете.

  Позже вы можете вернуться к обработке пропущенных вредоносных объектов из окна отчета (возможность отложенной обработки недоступна только для объектов, обнаруженных в электронных сообщениях).

Чтобы применить выбранное действие ко всем объектам с тем же статусом, обнаруженным в текущем сеансе работы компонента защиты или задачи, установите флажок **Применить во всех подобных случаях**. Текущим сеансом работы считается время работы компонента от момента его запуска до момента выключения либо перезапуска программы, а также время выполнения задачи проверки на вирусы от момента запуска до завершения.

Недоступный сервер обновлений

Если один или несколько компьютеров в сети используют в качестве сервера обновлений недоступный в данный момент компьютер, то своевременное обновление Kaspersky CRYSTAL невозможно. В таком случае безопасность сети находится под угрозой, и Kaspersky CRYSTAL отображает соответствующее сообщение в отчете о состоянии защиты сети.

Для безопасной работы требуется включить недоступный компьютер или назначить другой источник обновлений.

Обнаружен вредоносный объект

При обнаружении Файловым Антивирусом, Почтовым Антивирусом или задачей проверки на вирусы вредоносного объекта на экране открывается специальное уведомление.

Оно содержит:

- Вид угрозы (например, *вирус*, *троянская программа*) и имя вредоносного объекта, как оно представлено в Вирусной энциклопедии «Лаборатории Касперского». Имя вредоносного объекта оформлено в виде ссылки на ресурс www.viruslist.ru, где вы можете получить подробную информацию о том, угроза какого рода обнаружена на вашем компьютере.

- Полное имя вредоносного объекта и путь к нему.

Вам предлагается выбрать одно из следующих действий над объектом:

- **Лечить** – пытаться лечить вредоносный объект. Перед лечением формируется резервная копия объекта на тот случай, если возникнет необходимость восстановить его или картину его заражения.

- **Удалить** – удалить вредоносный объект. Перед удалением формируется резервная копия объекта на тот случай, если возникнет необходимость восстановить его или картину его заражения.

- **Пропустить** – заблокировать доступ к объекту, но не выполнять над ним никаких действий, а лишь зафиксировать информацию о нем в отчете.

  Позже вы можете вернуться к обработке пропущенных вредоносных объектов из окна отчета (возможность отложенной обработки недоступна только для объектов, обнаруженных в электронных сообщениях).

Чтобы применить выбранное действие ко всем объектам с тем же статусом, обнаруженным в текущем сеансе работы компонента защиты или задачи, установите флажок **Применить во всех подобных случаях**. Текущим сеансом работы считается время работы компонента от момента его запуска до момента выключения либо перезапуска программы, а также время выполнения задачи поиска вирусов от момента запуска до завершения.

Обнаружен опасный объект на трафике

При обнаружении Веб-Антивирусом опасного объекта на трафике на экране открывается специальное уведомление.

Уведомление содержит:

- Вид угрозы (например, *модификация вируса*) и имя опасного объекта, как оно представлено в Вирусной энциклопедии «Лаборатории Касперского». Имя объекта оформлено в виде ссылки на ресурс www.viruslist.ru, где вы можете получить подробную информацию о том, угроза какого рода обнаружена.

- Полное имя опасного объекта и путь к веб-ресурсу.

Вам предлагается выбрать одно из следующих действий над объектом:

- **Разрешить** – продолжить загрузку объекта.

- **Запретить** – заблокировать загрузку объекта с веб-ресурса.

Чтобы применить выбранное действие ко всем объектам с тем же статусом, обнаруженным в текущем сеансе работы компонента защиты или задачи, установите флажок **Применить во всех подобных случаях**. Текущим сеансом работы считается время работы компонента от момента его запуска до момента выключения либо перезапуска программы, а также время выполнения задачи поиска вирусов от момента запуска до завершения.

Обнаружен подозрительный объект

При обнаружении Файловым Антивирусом, Почтовым Антивирусом или задачей проверки на вирусы объекта, содержащего код неизвестного вируса либо модифицированный код известного вируса, на экране открывается специальное уведомление.

Оно содержит:

- Вид угрозы (например, *вирус*, *троянская программа*) и имя объекта, как оно представлено в Вирусной энциклопедии «Лаборатории Касперского». Имя вредоносного объекта оформлено в виде ссылки на ресурс www.viruslist.ru, где вы можете получить подробную информацию о том, угроза какого рода обнаружена на вашем компьютере.

- Полное имя объекта и путь к нему.

Вам предлагается выбрать одно из следующих действий над объектом:

- **Карантин** – поместить объект на карантин. При помещении объекта на карантин выполняется его перемещение, а не копирование: объект удаляется с диска или из почтового сообщения и сохраняется в карантинном каталоге. Файлы на карантине хранятся в специальном формате и не представляют опасности.

  При последующих проверках карантина с обновленными сигнатурами угроз статус объекта может измениться. Например, объект может быть идентифицирован как зараженный и обработан с помощью обновленных баз – либо может получить статус *не заражен*, и тогда его можно будет восстановить.

  > Если вручную поместить на карантин файл, который при последующей проверке окажется незараженным, его статус после проверки не сразу будет изменен на *ок*. Это произойдет только если проверка производилась (не менее чем через три дня) после помещения файла на карантин.

- **Удалить** – удалить объект. Перед удалением формируется резервная копия объекта на тот случай, если впоследствии возникнет необходимость восстановить его или картину его заражения.

- **Пропустить** – заблокировать доступ к объекту, но не выполнять над ним никаких действий, а лишь зафиксировать информацию о нем в отчете.

  Позже вы можете вернуться к обработке пропущенных объектов из окна отчета (возможность отложенной обработки недоступна только для объектов, обнаруженных в электронных сообщениях).

Чтобы применить выбранное действие ко всем объектам с тем же статусом, обнаруженным в текущем сеансе работы компонента защиты или задачи, установите флажок **Применить во всех подобных случаях**. Текущим сеансом работы считается время работы компонента от момента его запуска до момента выключения либо перезапуска программы, а также время выполнения задачи поиска вирусов от момента запуска до завершения.

Если вы уверены, что обнаруженный объект не является вредоносным, рекомендуется, во избежание повторных срабатываний программы при работе с этим объектом, добавить его в доверенную зону.

Обнаружена опасная активность в системе

При обнаружении Проактивной защитой опасной активности какой-либо программы в системе на экран выводится специальное уведомление, в котором содержится:

- Название угрозы, как оно представлено в Вирусной энциклопедии «Лаборатории Касперского». Имя угрозы оформлено в виде ссылки на ресурс www.viruslist.ru, где вы можете получить подробную информацию о том, угроза какого рода обнаружена.

- Полное имя файла процесса, инициирующего опасную активность, и путь к нему.

- Набор возможных действий:

  - **Карантин** – завершить процесс и поместить исполняемый файл процесса на карантин. При помещении объекта на карантин выполняется его перемещение, а не копирование. Файлы на карантине хранятся в специальном формате и не представляют опасности.

    При последующих проверках карантина с обновленными сигнатурами угроз статус объекта может измениться. Например, объект может быть идентифицирован как зараженный и обработан с помощью обновленных баз, либо получить статус *не заражен*, и тогда его можно будет восстановить.

    Если вручную поместить на карантин файл, который при последующей проверке окажется незараженным, его статус после проверки не сразу будет изменен на *ок*. Это произойдет только если проверка производилась (не менее чем через три дня) после помещения файла на карантин.

  - **Завершить** – завершить процесс.

  - **Разрешить** – разрешить выполнение процесса.

Чтобы применить выбранное действие ко всем объектам с тем же статусом, обнаруженным в текущем сеансе работы компонента защиты или задачи, установите флажок **Применить во всех подобных случаях**. Текущим сеансом работы считается время работы компонента от момента его запуска до момента выключения либо перезапуска программы, а также время выполнения задачи поиска вирусов от момента запуска до завершения.

Если вы уверены, что обнаруженная программа не является опасной, во избежание повторных срабатываний Kaspersky CRYSTAL при ее обнаружении, рекомендуется добавить программу в доверенную зону.

Обнаружен скрытый процесс

При обнаружении Проактивной защитой скрытого процесса в системе на экран выводится специальное уведомление, в котором содержится:

- Название угрозы, как оно представлено в Вирусной энциклопедии «Лаборатории Касперского». Имя угрозы оформлено в виде ссылки на ресурс www.viruslist.ru, где вы можете получить подробную информацию о том, угроза какого рода обнаружена.

- Полное имя файла скрытого процесса и путь к нему.

- Набор возможных действий:

  - **Карантин** – поместить исполняемый файл процесса на карантин. При помещении объекта на карантин выполняется его перемещение, а не копирование. Файлы на карантине хранятся в специальном формате и не представляют опасности.

    При последующих проверках карантина с обновленными сигнатурами угроз статус объекта может измениться. Например, объект может быть идентифицирован как зараженный и обработан с помощью обновленных баз, либо получить статус *не заражен*, и тогда его можно будет восстановить.

    Если вручную поместить на карантин файл, который при последующей проверке окажется незараженным, его статус после проверки не сразу будет изменен на *ок*. Это произойдет только если проверка производилась через некоторое время (не менее трех дней) после помещения файла на карантин.

  - **Завершить** – завершить процесс.

  - **Разрешить** – разрешить выполнение процесса.

Чтобы применить выбранное действие ко всем объектам с тем же статусом, обнаруженным в текущем сеансе работы компонента защиты или задачи, установите флажок **Применить во всех подобных случаях**. Текущим сеансом работы считается время работы компонента от момента его запуска до момента выключения либо перезапуска программы, а также время выполнения задачи поиска вирусов от момента запуска до завершения.

Если вы уверены, что обнаруженная программа не является опасной, рекомендуется, во избежание повторных срабатываний Kaspersky CRYSTAL при ее обнаружении, добавить программу в доверенную зону.

Обнаружена попытка доступа к системному реестру

При обнаружении Проактивной защитой попытки доступа к ключам системного реестра на экран выводится специальное уведомление, в котором содержится:

- Ключ реестра, к которому осуществляется попытка доступа.

- Полное имя файла процесса, инициирующего попытку доступа к ключам реестра, и путь к нему.

- Набор возможных действий:

  - **Разрешить** – однократно разрешить выполнение опасного действия;

  - **Запретить** – однократно запретить выполнение опасного действия.

Чтобы выбранное вами действие выполнялось автоматически каждый раз, когда такая активность будет инициироваться на вашем компьютере, установите флажок **Создать правило**.

Если вы считаете, что любая активность программы, которая инициировала обращение к ключам системного реестра, не является опасной, добавьте эту программу в список доверенных.

Обнаружена сетевая активность программы

При обнаружении сетевой активности программы (по умолчанию для программ, входящих в группы **Слабые ограничения** или **Сильные ограничения**) на экран будет выведено уведомление.

Уведомление будет выведено, если Kaspersky CRYSTAL работает в интерактивном режиме (см. раздел «Использование интерактивного режима защиты» на стр. 54) и если для программы, сетевая активность которой была обнаружена, не создано пакетное правило.

Уведомление содержит следующую информацию:

- название программы и краткую характеристику соединения, которое она инициирует;
- информацию о соединении (тип соединения, локальный и удаленный порты, адрес, с которым выполняется соединение);
- последовательность запуска программы.

Вам предлагается выбрать одно из следующих действий:

- **Разрешить сейчас**.
- **Запретить сейчас**.
- **Создать правило**. При выборе этого варианта открывается окно **Сетевой экран**, в котором вы можете создать правило, регулирующее сетевую активность программы.

Вы можете разрешить или запретить сетевую активность программы единожды или на более продолжительный срок. Для этого выполните одно из следующих действий:

- Чтобы единожды разрешить или запретить сетевую активность программы, выберите действие **Разрешить сейчас** или **Запретить сейчас**.
- Чтобы запомнить выбранное действие на сессию работы программы, проявившей сетевую активность, выберите **Разрешить сейчас** или **Запретить сейчас** и установите флажок **Запомнить на сессию работы программы**.

  Если в окне отображается флажок **Запомнить навсегда**, установите его, затем по ссылке **навсегда** измените название на **Запомнить на сессию работы программы**.
- Чтобы запомнить выбранное для программы действие навсегда, выберите действия **Разрешить сейчас** или **Запретить сейчас** и установите флажок **Запомнить навсегда**.

  Если в окне отображается флажок **Запомнить на сессию работы программы**, установите его, затем по ссылке **на сессию работы программы** измените название на **Запомнить навсегда**.

Обнаружена новая сеть

При каждом подключении компьютера к новой зоне (сети) на экран будет выведено специальное уведомление.

В верхней части уведомления приведено краткое описание сети с указанием IP-адреса и маски подсети.

В нижней части окна вам предлагается присвоить обнаруженной зоне статус, на основании которого будет разрешена та или иная сетевая активность:

- **Публичная сеть (запретить доступ к компьютеру извне)**. Сеть с высокой степенью риска, при работе в которой компьютер подвержен любым возможным типам угроз. Данный статус также рекомендуется выбирать для сетей, не защищенных какими-либо антивирусными программами, сетевыми экранами,

фильтрами и т.д. При выборе этого статуса обеспечивается максимальная безопасность работы компьютера в данной зоне.

- **Локальная сеть (разрешить доступ к файлам и принтерам)**. Рекомендуется применять этот статус для зон со средней степенью риска работы в них (например, для внутренней корпоративной сети).

- **Доверенная сеть (разрешить любую сетевую активность)**. Этот статус рекомендуется применять только для абсолютно безопасной, по вашему мнению, зоны, при работе в которой компьютер не подвергается атакам и попыткам несанкционированного доступа к данным.

Обнаружена попытка фишинг-атаки

При обнаружении Kaspersky CRYSTAL попытки открытия фишинг-сайта на экран будет выведено специальное уведомление.

В уведомлении содержится:

- Название угрозы – *фишинг-атака*, выполненная в виде ссылки на Вирусную энциклопедию «Лаборатории Касперского» с подробным описанием угрозы.

- Веб-адрес фишинг-сайта в интернете.

- Набор возможных действий:

  - **Разрешить** – продолжить загрузку фишинг-сайта.

  - **Запретить** – заблокировать загрузку фишинг-сайта.

Чтобы применить выбранное действие ко всем объектам с тем же статусом, обнаруженным в текущем сеансе работы компонента защиты или задачи, установите флажок ☑ **Применить во всех подобных случаях**. Текущим сеансом работы считается время работы компонента от момента его запуска до момента выключения либо перезапуска программы, а также время выполнения задачи поиска вирусов от момента запуска до завершения.

Обнаружена подозрительная ссылка

При обнаружении Kaspersky CRYSTAL попытки открытия веб-сайта, адрес которого содержится в списке подозрительных веб-адресов, на экран будет выведено специальное уведомление.

В уведомлении содержится:

- Веб-адрес сайта в интернете.

- Набор возможных действий:

  - **Разрешить** – продолжить загрузку веб-сайта.

  - **Запретить** – заблокировать загрузку веб-сайта.

Чтобы применить выбранное действие ко всем объектам с тем же статусом, обнаруженным в текущем сеансе работы компонента защиты или задачи, установите флажок ☑ **Применить во всех подобных случаях**. Текущим сеансом работы считается время работы компонента от момента его запуска до момента выключения либо перезапуска программы, а также время выполнения задачи поиска вирусов от момента запуска до завершения.

Обнаружен некорректный сертификат

Проверка безопасности соединения по протоколу SSL производится с помощью установленного сертификата. При попытке соединения с сервером с использованием некорректного сертификата (например, в случае его подмены злоумышленниками), на экран будет выведено специальное уведомление.

В уведомлении будет приведена информация о возможных причинах ошибки, а также удаленные порт и адрес. Вам будет предложено принять решение о необходимости соединения в условиях использования некорректного сертификата:

- **Принять сертификат** – продолжить соединение с веб-ресурсом;
- **Отклонить сертификат** – разорвать соединение с веб-ресурсом;
- **Просмотреть сертификат** – воспользоваться возможностью просмотреть информацию о сертификате.

Ограничение времени использования программы

Если в Родительском контроле установлено временное ограничение на использование программы, то по истечении разрешенного времени на экран будет выведено специальное уведомление.

В уведомлении отображается следующая информация:

- название программы;
- время, оставшееся до завершения работы программы, или причина завершения работы.

Ошибка восстановления данных

Если при восстановлении файла из резервной копии в выбранной для восстановления папке уже существует файл с таким же именем или отсутствует доступ к файлу, то на экран будет выведено специальное уведомление.

В верхней части уведомления приведено имя и расположение файла.

В нижней части окна вам предлагается выбрать действие для решения проблемы. Предлагаемые варианты действий различаются в зависимости от типа проблемы:

- **Заменить**. Восстанавливаемый файл заменит существующий. Действие доступно, когда файл с таким именем уже существует.
- **Повторить**. Будет выполнена повторная попытка записи в указанный файл. Действие доступно, когда нет доступа к файлу.
- **Пропустить**. Будет сохранена текущая версия файла.
- **Сохранить оба файла**. Восстанавливаемому файлу будет присвоено другое имя. Действие доступно, когда файл с таким именем уже существует.
- **Прекратить**. Задача восстановления данных будет прервана. Действие доступно, когда нет доступа к файлу.

Требуется специальная процедура лечения

При обнаружении угрозы, которая в данный момент активна в системе (например, вредоносного процесса в оперативной памяти или объектах автозапуска), на экран выводится запрос о проведении специальной расширенной процедуры лечения.

Специалисты «Лаборатории Касперского» настоятельно рекомендуют согласиться с проведением расширенной процедуры лечения. Для этого нажмите на кнопку **ОК**. Однако обратите внимание, что по ее окончании будет произведена перезагрузка компьютера, поэтому перед выполнением процедуры рекомендуется сохранить результаты текущей работы и закрыть все программы.

В процессе выполнения процедуры лечения не разрешается запускать почтовые клиенты и редактировать реестр операционной системы. После перезагрузки компьютера рекомендуется запустить полную проверку на вирусы.

ГЛОССАРИЙ ТЕРМИНОВ

B

Boot-вирус (загрузочный)

Вирус, поражающий загрузочные секторы дисков компьютера. Вирус «заставляет» систему при ее перезапуске считывать в память и отдавать управление не оригинальному коду загрузчика, а коду вируса.

O

OLE-объект

Присоединенный или встроенный в другой файл объект. Программа «Лаборатории Касперского» позволяет проверять на присутствие вирусов OLE-объекты. Например, если вы вставите какую-либо таблицу Microsoft Office Excel в документ Microsoft Office Word, данная таблица будет проверяться как OLE-объект.

S

SOCKS

Протокол прокси-сервера, позволяющий реализовать двухточечное соединение между компьютерами внутренней и внешней сетей.

A

Активация программы

Перевод программы в полнофункциональный режим. Для активации программы пользователю необходима лицензия.

Активная лицензия

Лицензия, используемая в данный временной период для работы программы «Лаборатории Касперского». Лицензия определяет срок действия полной функциональности и лицензионную политику в отношении программы. В программе не может быть больше одной лицензии со статусом «активная».

Альтернативные потоки NTFS

Потоки данных файловой системы NTFS (alternate data streams), предназначенные для размещения дополнительных атрибутов или информации к файлу.

Каждый файл в файловой системе NTFS представляет собой набор потоков (streams). В одном из них находится содержимое файла, которое мы сможем увидеть, открыв файл, остальные (альтернативные) предназначены для размещения метаинформации и обеспечивают, например, совместимость системы NTFS с другими системами, такими как старая файловая система Macintosh – Hierarchical File System (HFS). Потоки можно создавать, удалять, сохранять отдельно, переименовывать и даже запускать как процесс.

Альтернативные потоки могут использоваться злоумышленниками для скрытой передачи или получения данных с компьютера.

Аппаратный порт

Разъем на каком-либо элементе аппаратного обеспечения компьютера, в который подключается кабель или вилка (LPT-порт, последовательный порт, USB).

Архив

Файл, «содержащий» в себе один или несколько других объектов, которые в свою очередь также могут быть архивами.

Б

База подозрительных веб-адресов

Список адресов веб-ресурсов, содержимое которых может быть расценено как потенциально опасное. Список сформирован специалистами «Лаборатории Касперского», регулярно обновляется и входит в поставку программы «Лаборатории Касперского».

База фишинговых веб-адресов

Список адресов веб-ресурсов, которые определены специалистами «Лаборатории Касперского» как фишинговые. База регулярно обновляется и входит в поставку программы «Лаборатории Касперского».

Базы

Базы данных, формируемые специалистами «Лаборатории Касперского» и содержащие подробное описание всех существующих на текущий момент угроз компьютерной безопасности, способов их обнаружения и обезвреживания. Базы постоянно обновляются в «Лаборатории Касперского» по мере появления новых угроз.

Блокирование объекта

Запрет доступа к объекту со стороны внешних программ. Заблокированный объект не может быть прочитан, выполнен, изменен или удален.

В

Вирусная атака

Ряд целенаправленных попыток заразить компьютер вирусом.

Возможно зараженный объект

Объект, код которого содержит либо модифицированный код известного вируса, либо код, напоминающий вирус, но пока не известный «Лаборатории Касперского». Возможно зараженные файлы обнаруживаются с помощью эвристического анализатора.

Восстановление

Перемещение оригинального объекта из карантина или резервного хранилища в папку его исходного расположения, где объект хранился до его помещения на карантин, лечения или удаления, либо другую папку, указанную пользователем.

Д

Двухканальный шлюз

Компьютер, снабженный двумя сетевыми адаптерами, каждый из которых подключен к разным сетям, пересылающий информацию из одной сети в другую.

Доверенный процесс

Программный процесс, файловые операции которого не контролируется программой «Лаборатории Касперского» в режиме постоянной защиты. То есть все объекты, запускаемые, открываемые и сохраняемые доверенным процессом, не проверяются.

Дополнительная лицензия

Лицензия, добавленная для работы программы «Лаборатории Касперского», но не активированная. Дополнительная лицензия начинает действовать по окончании срока действия активной лицензии.

Доступное обновление

Пакет обновлений модулей программы «Лаборатории Касперского», в состав которого включены набор срочных обновлений, собранных за некоторый период, и изменения в архитектуре программы.

З

Заголовок

Информация, которая содержится в начале файла или сообщения и состоит из низкоуровневых данных о статусе и обработке файла (сообщения). В частности, заголовок сообщения электронной почты содержит такие сведения, как данные об отправителе, получателе и дату.

Загрузочный сектор диска

Загрузочный сектор — это особый сектор на жёстком диске компьютера, дискете или другом устройстве хранения информации. Содержит сведения о файловой системе диска и программу-загрузчик, отвечающую за запуск операционной системы.

Существует ряд вирусов, поражающих загрузочные секторы дисков, которые так и называются – загрузочные вирусы (boot-вирусы). Программа «Лаборатории Касперского» позволяет проверять загрузочные секторы на присутствие вирусов и лечить их в случае заражения.

Задача

Функции, выполняемые программой «Лаборатории Касперского», реализованы в виде задач, например: **Постоянная защита файлов**, **Полная проверка компьютера**, **Обновление баз**.

Зараженный объект

Объект, внутри которого содержится вредоносный код: при проверке объекта было обнаружено полное совпадение участка кода объекта с кодом известной угрозы. Специалисты «Лаборатории Касперского» не рекомендуют вам работать с такими объектами, поскольку это может привести к заражению вашего компьютера.

И

Исключение

Исключение – объект, исключаемый из проверки программой «Лаборатории Касперского». Исключать из проверки можно файлы определенного формата, файлы по маске, некоторую область (например, папку или программу), процессы программ или объекты по типу угрозы согласно классификации Вирусной энциклопедии. Для каждой задачи могут быть заданы свои исключения.

К

Карантин

Определенная папка, куда помещаются все возможно зараженные объекты, обнаруженные во время проверки или в процессе функционирования постоянной защиты.

Контейнер

Зашифрованный объект, предназначенный для хранения конфиденциальной информации. Контейнер представляет собой защищенный паролем виртуальный съемный диск, в который помещаются файлы и папки.

Для работы с контейнерами на компьютере должна быть установлена программа Kaspersky CRYSTAL.

Контролируемый объект

Файл, перемещаемый по протоколам HTTP, FTP или SMTP через межсетевой экран и направляемый на проверку программе «Лаборатории Касперского».

Л

Лечение объектов

Способ обработки зараженных объектов, в результате которого происходит полное или частичное восстановление данных, либо принимается решение о невозможности лечения объектов. Лечение объектов выполняется на основе записей баз. В процессе лечения часть данных может быть потеряна.

Лечение объектов при перезагрузке

Способ обработки зараженных объектов, используемых в момент лечения другими программами. Заключается в создании копии зараженного объекта, лечении созданной копии и замене при следующей перезагрузке исходного зараженного объекта его вылеченной копией.

Ложное срабатывание

Ситуация, когда незараженный объект определяется программой «Лаборатории Касперского» как зараженный ввиду того, что его код напоминает код вируса.

М

Маска подсети

Маска подсети (также именуемая сетевой маской) и сетевой адрес определяют адреса входящих в состав сети компьютеров.

Маска файла

Представление имени и расширения файла общими символами. Двумя основными символами, используемыми в масках файлов, являются ***** и **?** (где ***** – любое число любых символов, а **?** – любой один символ). При помощи данных знаков можно представить любой файл. Обратите внимание, что имя и расширение файла всегда пишутся через точку.

Н

Неизвестный вирус

Новый вирус, информации о котором нет в базах. Как правило, неизвестные вирусы обнаруживаются программой в объектах при помощи эвристического анализатора, и таким объектам присваивается статус возможно зараженных.

Несовместимая программа

Антивирусная программа стороннего производителя или программа «Лаборатории Касперского», не поддерживающая управление через Kaspersky CRYSTAL.

Нецензурное сообщение

Электронное сообщение, содержащее ненормативную лексику.

О

Обновление

Процедура замены / добавления новых файлов (баз или программных модулей), получаемых с серверов обновлений «Лаборатории Касперского».

Обновление баз

Одна из функций, выполняемых программой «Лаборатории Касперского», которая позволяет поддерживать защиту в актуальном состоянии. При этом происходит копирование баз с серверов обновлений «Лаборатории Касперского» на компьютер и автоматическое подключение их к программе.

Объекты автозапуска

Набор программ, необходимых для запуска и корректной работы установленных на вашем компьютере операционной системы и программного обеспечения. Каждый раз при старте операционная система запускает эти объекты. Существуют вирусы, способные поражать именно такие объекты, что может привести, например, к блокированию запуска операционной системы.

Опасный объект

Объект, внутри которого содержится вирус. Не рекомендуется работать с такими объектами, поскольку это может привести к заражению компьютера. При обнаружении зараженного объекта рекомендуется лечить его с помощью программы «Лаборатории Касперского» или удалить, если лечение невозможно.

П

Пакет обновлений

Пакет файлов для обновления программного обеспечения, который копируется из интернета и устанавливается на вашем компьютере.

Параметры задачи

Параметры работы программы, специфичные для каждого типа задач.

Параметры программы

Параметры работы программы, общие для всех типов ее задач и отвечающие за работу программы в целом, например, параметры производительности программы, параметры ведения отчетов, параметры резервного хранилища.

Перехватчик

Подкомпонент программы, отвечающий за проверку определенных типов почтовых сообщений. Набор подлежащих установке перехватчиков зависит от того, в какой роли или в какой комбинации ролей развернута программа.

Подозрительное сообщение

Сообщение, которое нельзя однозначно классифицировать как спам, но при проверке оно вызвало подозрение (например, некоторые виды рассылок и рекламных сообщений).

Подозрительный объект

Объект, код которого содержит либо модифицированный код известного вируса, либо код, напоминающий вирус, но пока не известный «Лаборатории Касперского». Подозрительные объекты обнаруживаются при помощи эвристического анализатора.

Помещение объектов на карантин

Способ обработки возможно зараженного объекта, при котором доступ к объекту блокируется, и он перемещается из исходного местоположения в папку карантина, где сохраняется в закодированном виде, что исключает угрозу заражения.

Порог вирусной активности

Максимально допустимое количество событий заданного типа в течение ограниченного времени, превышение которого будет считаться повышением вирусной активности и возникновением угрозы вирусной атаки. Данная характеристика имеет большое значение в периоды вирусных эпидемий и позволяет администратору своевременно реагировать на возникающие угрозы вирусных атак.

Порт ввода-вывода

Используется в микропроцессорах (например, Intel) при обмене данными с аппаратным обеспечением. Порт ввода-вывода сопоставляется с тем или иным устройством и позволяет программам обращаться к нему для обмена данными.

Постоянная защита

Режим работы программы, в котором осуществляется проверка объектов на присутствие вредоносного кода в режиме реального времени.

Программа перехватывает все попытки открыть какой-либо объект на чтение, запись и исполнение и проверяет объект на наличие угроз. Незараженные объекты пропускаются пользователю, объекты, содержащие угрозы или подозреваемые на наличие угрозы, обрабатываются в соответствии с параметрами задачи (лечатся, удаляются, помещаются на карантин).

Потенциально заражаемый объект

Объект, который в силу своей структуры или формата может быть использован злоумышленниками в качестве «контейнера», для размещения и распространения вредоносного объекта. Как правило, это исполняемые

файлы, например, с расширением com, exe, dll и др. Риск внедрения в такие файлы вредоносного кода достаточно высок.

Почтовые базы

Базы, включающие почтовые сообщения, хранящиеся на вашем компьютере и имеющие специальный формат. Каждое входящее / исходящее письмо помещается в почтовую базу после его получения / отправки. Такие базы проверяются во время полной проверки компьютера.

Входящие и исходящие почтовые сообщения в момент их получения и отправки анализируются на присутствие вирусов в реальном времени, если включена постоянная защита.

Проверка трафика

Проверка в режиме реального времени с использованием информации текущей (последней) версии баз объектов, передаваемых по всем протоколам (например, HTTP, FTP и пр.).

Программные модули

Файлы, входящие в состав дистрибутива программы «Лаборатории Касперского» и отвечающие за реализацию его основных задач. Каждому типу задач, реализуемых программой (Постоянная защита, Проверка по требованию, Обновление), соответствует свой исполняемый модуль. Запуская из главного окна полную проверку вашего компьютера, вы инициируете запуск модуля этой задачи.

Прокси-сервер

Служба в компьютерных сетях, позволяющая клиентам выполнять косвенные запросы к другим сетевым службам. Сначала клиент подключается к прокси-серверу и запрашивает какой-либо ресурс (например, файл), расположенный на другом сервере. Затем прокси-сервер либо подключается к указанному серверу и получает ресурс у него, либо возвращает ресурс из собственного кеша (в случаях, если прокси имеет свой кеш). В некоторых случаях запрос клиента или ответ сервера может быть изменён прокси-сервером в определённых целях.

Протокол

Четко определенный и стандартизованный набор правил, регулирующих взаимодействие между клиентом и сервером. К ряду хорошо известных протоколов и связанных с ними служб относятся: HTTP (WWW), FTP и NNTP (новости).

Протокол интернета (IP)

Базовый протокол сети интернет, используемый без изменений со времени его разработки в 1974 г. Он осуществляет основные операции передачи данных с одного компьютера на другой и служит в качестве основы для протоколов более высокого уровня, таких как TCP и UDP. Он управляет соединением и обработкой ошибок. Такие технологии как NAT и маскарад делают возможным скрытие больших частных сетей за небольшим числом IP-адресов (или даже одним адресом), что позволяет удовлетворить запросы постоянно растущего интернета, используя относительно ограниченное адресное пространство IPv4.

Р

Резервное копирование

Создание резервной копии файла перед его лечением или удалением и размещение этой копии в резервном хранилище с возможностью последующего восстановления файла, например, для его проверки с помощью обновленных баз.

Резервное хранилище

Специальное хранилище, предназначенное для сохранения резервных копий объектов, создаваемых перед их первым лечением или удалением.

Рекомендуемый уровень

Уровень безопасности, базирующийся на параметрах работы программы, рекомендуемых экспертами «Лаборатории Касперского» и обеспечивающих оптимальную защиту вашего компьютера. Данный уровень установлен для использования по умолчанию.

С

Серверы обновлений «Лаборатории Касперского»

Список HTTP- и FTP-серверов «Лаборатории Касперского», с которых программа копирует базы и обновления модулей на ваш компьютер.

Сертификат Сервера администрирования

Сертификат, на основании которого осуществляется аутентификация Сервера администрирования при подключении к нему Консоли администрирования и обмене информацией с клиентскими компьютерами. Сертификат Сервера администрирования создается при установке Сервера администрирования и хранится во вложенной папке **Cert** папки установки программы.

Сетевой порт

Параметр протоколов TCP и UDP, определяющий назначение пакетов данных в IP-формате, передаваемых на хост по сети и позволяющий различным программам, выполняемым на одном хосте, получать данные независимо друг от друга. Каждая программа обрабатывает данные, поступающие на определённый порт (иногда говорят, что программа «слушает» этот номер порта).

Обычно за некоторыми распространёнными сетевыми протоколами закреплены стандартные номера портов (например, веб-серверы обычно принимают данные по протоколу HTTP на TCP-порт 80), хотя в общем случае программа может использовать любой протокол на любом порте. Возможные значения: от 1 до 65535.

Скрипт

Небольшая компьютерная программа или независимая часть программы (функция), как правило, написанная для выполнения небольшой конкретной задачи. Наиболее часто применяется при использовании программ, встраиваемых в гипертекст. Скрипты запускаются, например, когда вы открываете некоторый веб-сайт.

Если включена постоянная защита, программа отслеживает запуск скриптов, перехватывает их и проверяет на присутствие вирусов. В зависимости от результатов проверки вы можете запретить или разрешить выполнение скрипта.

Служба имен доменов (DNS)

Распределенная система преобразования имени хоста (компьютера или другого сетевого устройства) в IP-адрес. DNS работает в сетях TCP/IP. Как частный случай, DNS может хранить и обрабатывать и обратные запросы, определения имени хоста по его IP (PTR-записи). Разрешение имен DNS обычно осуществляется сетевыми программами, а не самими пользователями.

Состояние защиты

Текущее состояние защиты, характеризующее степень защищенности компьютера.

Спам

Несанкционированная массовая рассылка электронных сообщений, чаще всего рекламного характера.

Список доверенных веб-адресов

Список масок и адресов веб-ресурсов, содержимому которых доверяет пользователь. Программа «Лаборатории Касперского» не проверяет веб-страницы, соответствующие какому-либо элементу списка, на присутствие вредоносных объектов.

Список запрещенных веб-адресов

Список масок и адресов веб-ресурсов, доступ к которым блокируется программой «Лаборатории Касперского». Список адресов формируется пользователем при настройке параметров программы.

Список запрещенных отправителей

(также «Черный» список адресов)

Список электронных адресов, входящие сообщения с которых блокируются программой «Лаборатории Касперского» независимо от их содержания.

Список проверяемых веб-адресов

Список масок и адресов веб-ресурсов, которые проверяются программой «Лаборатории Касперского» на присутствие вредоносных объектов в обязательном порядке.

Список разрешенных веб-адресов

Список масок и адресов веб-ресурсов, доступ к которым не блокируется программой «Лаборатории Касперского». Список адресов формируется пользователем при настройке параметров программы.

Список разрешенных отправителей

(также «Белый» список адресов)

Список электронных адресов, входящие сообщения с которых не проверяются программой «Лаборатории Касперского».

Срок действия лицензии

Период, в течение которого вам предоставляется возможность использовать полную функциональность программы «Лаборатории Касперского». Срок действия лицензии, как правило, составляет календарный год со дня ее установки. После окончания срока действия лицензии функциональность программы сокращается: вы не сможете обновлять базы программы.

Срочное обновление

Критическое обновление модулей программы «Лаборатории Касперского».

Счетчик вирусной эпидемии

Шаблон, на основании которого проводится оповещение об угрозе возникновении вирусной эпидемии. Счетчик вирусной эпидемии содержит набор параметров, определяющих порог вирусной активности, способ распространения и текст рассылаемых сообщений.

Т

Технология iChecker

Технология, позволяющая увеличить скорость антивирусной проверки за счет исключения тех объектов, которые не были изменены с момента предыдущей проверки, при условии, что параметры проверки (антивирусные базы и настройки) не были изменены. Информация об этом хранится в специальной базе. Технология применяется как в режиме постоянной защиты, так и в режиме проверки по требованию.

Например, у вас есть файл архива, который был проверен программой «Лаборатории Касперского» и ему был присвоен статус *незаражен*. В следующий раз этот архив будет исключен из проверки, если он не был изменен и не менялись параметры проверки. Если вы изменили состав архива, добавив в него новый объект, изменили параметры проверки, обновили антивирусные базы, архив будет проверен повторно.

Ограничения технологии **iChecker**:

- технология не работает с файлами больших размеров, так как в этом случае проверить весь файл быстрее, чем вычислять был ли он изменен с момента последней проверки;
- технология поддерживает ограниченное число форматов (**exe, dll, lnk, ttf, inf, sys, com, chm, zip, rar**).

У

Удаление объекта

Способ обработки объекта, при котором происходит его физическое удаление с того места, где он был обнаружен программой (жесткий диск, папка, сетевой ресурс). Такой способ обработки рекомендуется применять к опасным объектам, лечение которых по тем или иным причинам невозможно.

Удаление сообщения

Способ обработки электронного сообщения, при котором происходит его физическое удаление. Такой способ рекомендуется применять к сообщениям, однозначно содержащим спам или вредоносный объект. Перед удалением сообщения его копия сохраняется в резервном хранилище (если данная функциональность не отключена).

Упакованный файл

Файл архива, который содержит в себе некоторую программу-распаковщик и инструкции операционной системе для ее выполнения.

Уровень безопасности

Под уровнем безопасности понимается предустановленный набор параметров работы компонента.

Уровень важности события

Характеристика события, зафиксированного в работе программы «Лаборатории Касперского». Существуют четыре уровня важности:

- **Критическое событие**.
- **Отказ функционирования**.
- **Предупреждение**.
- **Информационное сообщение**.

События одного и того же типа могут иметь различные уровни важности, в зависимости от ситуации, при которой событие произошло.

Установка с помощью сценария входа

Метод удаленной установки программ «Лаборатории Касперского», который позволяет закрепить запуск задачи удаленной установки за конкретной учетной записью пользователя (нескольких пользователей). При регистрации пользователя в домене предпринимается попытка провести установку программы на клиентском компьютере, с которого пользователь зарегистрировался. Данный метод рекомендуется для установки программ компании на компьютеры, работающие под управлением операционных систем Microsoft Windows 98 / Me.

Ф

Файл ключа

Файл с расширением *.key, который является вашим личным «ключом», необходимым для работы с программой «Лаборатории Касперского». Файл ключа входит в комплект поставки продукта, если вы приобрели его у дистрибьюторов «Лаборатории Касперского», или присылается вам по почте, если продукт был приобретен в интернет-магазине.

Ч

Черный список файлов ключей

База данных, содержащая информацию о заблокированных «Лабораторией Касперского» файлах ключей. Содержимое файла с «черным» списком обновляется вместе с базами.

Ш

Шаблон уведомления

Шаблон, на основании которого проводится оповещение об обнаруженных при проверке зараженных объектах. Шаблон уведомления содержит набор параметров, определяющих порядок уведомления, способ распространения и текст рассылаемых сообщений.

Э

Эвристический анализатор

Технология обнаружения угроз, неопределяемых с помощью баз программ «Лаборатории Касперского». Позволяет находить объекты, которые подозреваются на заражение неизвестным вирусом или новой модификацией известного.

С помощью эвристического анализатора обнаруживаются до 92% новых угроз. Этот механизм достаточно эффективен и очень редко приводит к ложным срабатываниям.

Файлы, обнаруженные с помощью эвристического анализатора, признаются подозрительными.

ЗАО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

«Лаборатория Касперского» была основана в 1997 году. Сегодня это самый известный в России разработчик широкого спектра программных продуктов для обеспечения информационной безопасности: систем защиты от вирусов, нежелательной почты (спама) и хакерских атак.

«Лаборатория Касперского» – международная компания. Центральный офис находится в России, открыты локальные офисы в Великобритании, Франции, Германии, Японии, в странах Бенилюкса, Китае, Польше, Румынии и США (Калифорния). Во Франции открыто новое отделение компании – Европейский центр антивирусных исследований. Наша партнерская сеть объединяет более 500 компаний по всему миру.

«Лаборатория Касперского» сегодня – это более тысячи высококвалифицированных специалистов, десять из которых имеют дипломы MBA, шестнадцать – степени кандидатов наук. Ведущие вирусные аналитики «Лаборатории Касперского» являются членами престижной организации Computer Anti-virus Researcher's Organization (CARO).

Главная ценность компании – уникальные знания и опыт, накопленные ее сотрудниками в течение более чем четырнадцати лет непрерывной борьбы с вирусами. Благодаря постоянному анализу вирусной активности мы умеем предугадывать тенденции развития вредоносных программ и заблаговременно обеспечиваем пользователей надежной защитой от новых видов атак. Это преимущество – основа продуктов и услуг «Лаборатории Касперского». Мы всегда на шаг впереди конкурентов и предоставляем нашим заказчикам наилучшую защиту.

Годы упорной работы позволили компании стать лидером в разработке технологий защиты от вирусов. «Лаборатория Касперского» первой разработала многие современные стандарты антивирусных программ. Основной продукт компании, Антивирус Касперского, обеспечивает надежную защиту всех объектов вирусных атак: рабочих станций, файловых серверов, почтовых систем, сетевых экранов и интернет-шлюзов, карманных компьютеров. Удобные средства управления дают пользователям возможность максимально автоматизировать антивирусную защиту компьютеров и корпоративных сетей. Многие мировые разработчики используют в своих продуктах программное ядро Антивируса Касперского, например, такие как: Nokia ICG (США), Aladdin (Израиль), Sybari (США), G Data (Германия), Deerfield (США), Alt-N (США), Microworld (Индия), BorderWare (Канада).

Клиенты «Лаборатории Касперского» обеспечиваются широким спектром дополнительных услуг, гарантирующих бесперебойную работу продуктов и точное соответствие любым специфическим бизнес-требованиям. Мы проектируем, внедряем и сопровождаем корпоративные антивирусные комплексы. Наши базы обновляются каждый час. Мы обеспечиваем наших пользователей технической поддержкой на нескольких языках.

Если у вас возникнут какие-либо вопросы, вы можете обратиться к нашим дистрибьюторам или непосредственно в ЗАО «Лаборатория Касперского». Вам всегда будут предоставлены подробные консультации по телефону или электронной почте. На все ваши вопросы вы получите полные и исчерпывающие ответы.

Веб-сайт «Лаборатории Касперского»:	http://www.kaspersky.ru
Вирусная энциклопедия:	http://www.securelist.com/ru/
Антивирусная лаборатория:	newvirus@kaspersky.com (только для отправки подозрительных объектов в архивированном виде) http://support.kaspersky.ru/virlab/helpdesk.html (для запросов вирусным аналитикам)
Веб-форум «Лаборатории Касперского»:	http://forum.kaspersky.com

ИНФОРМАЦИЯ О СТОРОННЕМ КОДЕ

Для создания программы использовался код сторонних производителей.

В ЭТОМ РАЗДЕЛЕ

Программный код 279

Другая информация 302

Программный код

Информация о программном коде сторонних производителей, использованном при создании программы.

В этом разделе

AGG (ANTI-GRAIN GEOMETRY) 2.4 280
BISON PARSER SKELETON 2.3 281
BOOST 1.30.0, 1.39.0, 1.43.0 281
BZIP2/LIBBZIP2 1.0.5 282
EXPAT 1.2, 2.0.1 282
FASTSCRIPT 1.9 282
GECKO SDK 1.8 282
INFO-ZIP 5.51 282
LIBJPEG 6B 283
LIBNKFM 2.0.5 284
LIBPNG 1.2.8, 1.2.29 284
LIBSPF2 1.2.9 284
LIBUNGIF 3.0 285
LIBXDR 285
NDIS INTERMEDIATE MINIPORTDRIVER SAMPLE 285
NDIS SAMPLE NDIS LIGHTWEIGHT FILTER DRIVER 286
NETWORK CONFIGURATION SAMPLE 286
OPENSSL 0.9.8D 286
PCRE 3.0, 7.4, 7.7 287
PROTOCOL BUFFER 288
QT 4.6.1 288
RFC1321-BASED (RSA-FREE) MD5 LIBRARY 294
TINICONV 1.0.0 294
WINDOWS TEMPLATE LIBRARY 7.5 299
WINDOWS TEMPLATE LIBRARY 8.0 302
ZLIB 1.2, 1.2.2 302

AGG (ANTI-GRAIN GEOMETRY) 2.4

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 2004 Alberto Demichelis

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

BISON PARSER SKELETON 2.3

Copyright (C) GNU Project

---

http://ftp.gnu.org/gnu/bison/

As a special exception, you may create a larger work that containspart or all of the Bison parser skeleton and distribute that work under terms of your choice, so long as that work isn't itself a parser generator using the skeleton or a modified version thereof as a parser skeleton. Alternatively, if you modify or redistribute the parser skeleton itself, you may (at your option) remove this special exception, which will cause the skeleton and the resulting Bison output files to be licensed under the GNU General Public License without this special exception.

BOOST 1.30.0, 1.39.0, 1.43.0

Copyright (C) Beman Dawes

BZIP2/LIBBZIP2 1.0.5

Copyright (C) 1996-2007, Julian R Seward

EXPAT 1.2, 2.0.1

Copyright (C) 1998, 1999, 2000, Thai Open Source Software Center Ltd

---

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the «Software»), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED «AS IS», WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

FASTSCRIPT 1.9

Copyright (C) Fast Reports Inc

GECKO SDK 1.8

Copyright (C) Mozilla Foundation

---

http://www.mozilla.org/MPL/MPL-1.1.html

INFO-ZIP 5.51

Copyright (C) 1990-2007, Info-ZIP

This software is provided «as is», without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the above disclaimer and the following restrictions:

1. Redistributions of source code (in whole or in part) must retain the above copyright notice, definition, disclaimer, and this list of conditions.

2. Redistributions in binary form (compiled executables and libraries) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.

3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, versions with modified or added functionality, and dynamic, shared, or static library versions not from Info-ZIP--must be plainly marked as such and must not be misrepresented as being the original source or, if binaries, compiled from the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names «Info-ZIP» (or any variation thereof, including, but not limited to, different capitalizations), «Pocket UnZip,» «WiZ» or «MacZip» without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or the Info-ZIP URL(s), such as to imply Info-ZIP will provide support for the altered versions.

4. Info-ZIP retains the right to use the names «Info-ZIP,» «Zip,» «UnZip, “UnZipSFX,” “WiZ,” “Pocket UnZip,” “Pocket Zip,” and “MacZip” for its own source and binary releases.

LIBJPEG 6B

Copyright (C) 1991-2009, Thomas G. Lane, Guido Vollbeding

LEGAL ISSUES

In plain English:

We don't promise that this software works. (But if you find any bugs, please let us know!)

You can use this software for whatever you want. You don't have to pay us.

You may not pretend that you wrote this software. If you use it in a program, you must acknowledge somewhere in your documentation that you've used the IJG code.

In legalese:

The authors make NO WARRANTY or representation, either express or implied, with respect to this software, its quality, accuracy, merchantability, or fitness for a particular purpose. This software is provided “AS IS”, and you, its user, assume the entire risk as to its quality and accuracy.

Permission is hereby granted to use, copy, modify, and distribute this software (or portions thereof) for any purpose, without fee, subject to these conditions:

(1) If any part of the source code for this software is distributed, then this README file must be included, with this copyright and no-warranty notice unaltered; and any additions, deletions, or changes to the original files must be clearly indicated in accompanying documentation.

(2) If only executable code is distributed, then the accompanying documentation must state that “this software is based in part on the work of the Independent JPEG Group”.

(3) Permission for use of this software is granted only if the user accepts full responsibility for any undesirable consequences; the authors accept NO LIABILITY for damages of any kind.

These conditions apply to any software derived from or based on the IJG code, not just to the unmodified library. If you use our work, you ought to acknowledge us.

Permission is NOT granted for the use of any IJG author's name or company name in advertising or publicity relating to this software or products derived from it. This software may be referred to only as “the Independent JPEG Group's software”.

We specifically permit and encourage the use of this software as the basis of commercial products, provided that all warranty or liability claims are assumed by the product vendor.

ansi2knr.c is included in this distribution by permission of L. Peter Deutsch, sole proprietor of its copyright holder, Aladdin Enterprises of Menlo Park, CA. ansi2knr.c is NOT covered by the above copyright and conditions, but instead by the usual distribution terms of the Free Software Foundation; principally, that you must include source code if you redistribute it. (See the file ansi2knr.c for full details.) However, since ansi2knr.c is not needed as part of any program generated from the IJG code, this does not limit you more than the foregoing paragraphs do.

The Unix configuration script “configure” was produced with GNU Autoconf. It is copyright by the Free Software Foundation but is freely distributable. The same holds for its supporting scripts (config.guess, config.sub, ltconfig, ltmain.sh). Another support script, install-sh, is copyright by M.I.T. but is also freely distributable.

It appears that the arithmetic coding option of the JPEG spec is covered by patents owned by IBM, AT&T, and Mitsubishi. Hence arithmetic coding cannot legally be used without obtaining one or more licenses. For this reason, support for arithmetic coding has been removed from the free JPEG software.

(Since arithmetic coding provides only a marginal gain over the unpatented Huffman mode, it is unlikely that very many implementations will support it.) So far as we are aware, there are no patent restrictions on the remaining code.

The IJG distribution formerly included code to read and write GIF files. To avoid entanglement with the Unisys LZW patent, GIF reading support has been removed altogether, and the GIF writer has been simplified to produce “uncompressed GIFs”. This technique does not use the LZW algorithm; the resulting GIF files are larger than usual, but are readable by all standard GIF decoders.

We are required to state that “The Graphics Interchange Format(c) is the Copyright property of CompuServe Incorporated. GIF(sm) is a Service Mark property of CompuServe Incorporated.”

LIBNKFM 2.0.5

Copyright (C) KUBO Takehiro

LIBPNG 1.2.8, 1.2.29

Copyright (C) 2004, 2006-2008, Glenn Randers-Pehrson

LIBSPF2 1.2.9

Copyright (C) 2005, Shevek and Wayne Schlitt

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,

STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

LIBUNGIF 3.0

Copyright (C) 1997, Eric S. Raymond

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

LIBXDR

Copyright (C) Sun Microsystems, Inc

Sun RPC is a product of Sun Microsystems, Inc. and is provided for unrestricted use provided that this legend is included on all tape media and as a part of the software program in whole or part.

Users may copy or modify Sun RPC without charge, but are not authorized to license or distribute it to anyone else except as part of a product or program developed by the user.

SUN RPC IS PROVIDED AS IS WITH NO WARRANTIES OF ANY KIND INCLUDING THE WARRANTIES OF DESIGN, MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE.

Sun RPC is provided with no support and without any obligation on the part of Sun Microsystems, Inc. to assist in its use, correction, modification or enhancement.

SUN MICROSYSTEMS, INC. SHALL HAVE NO LIABILITY WITH RESPECT TO THE INFRINGEMENT OF COPYRIGHTS, TRADE SECRETS OR ANY PATENTS BY SUN RPC OR ANY PART THEREOF.

In no event will Sun Microsystems, Inc. be liable for any lost revenue or profits or other special, indirect and consequential damages, even if Sun has been advised of the possibility of such damages.

Sun Microsystems, Inc.

2550 Garcia Avenue

Mountain View, California 94043

NDIS INTERMEDIATE MINIPORTDRIVER SAMPLE

Copyright (C) 1992-2000, Microsoft Corporation

NDIS SAMPLE NDIS LIGHTWEIGHT FILTER DRIVER

NETWORK CONFIGURATION SAMPLE

OPENSSL 0.9.8D

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)”

4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com). Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:»This product includes cryptographic software written byEric Young (eay@cryptsoft.com)» The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: “This product includes software written by Tim Hudson (tjh@cryptsoft.com)»

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence

[including the GNU Public Licence.]

PCRE 3.0, 7.4, 7.7

Copyright (C) University of Cambridge

PCRE is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language.

Release 5 of PCRE is distributed under the terms of the “BSD» licence, as specified below. The documentation for PCRE, supplied in the “doc» directory, is distributed under the same terms as the software itself.

Written by: Philip Hazel <ph10@cam.ac.uk>

University of Cambridge Computing Service,

Cambridge, England. Phone: +44 1223 334714.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the University of Cambridge nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS» AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

PROTOCOL BUFFER

Copyright (C) 2008, Google Inc

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS» AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Code generated by the Protocol Buffer compiler is owned by the owner of the input file used when generating it. This code is not standalone and requires a support library to be linked with it. This support library is itself covered by the above license.

QT 4.6.1

Copyright (C) 2009, Nokia Corporation and/or its subsidiary(-ies)

GNU LESSER GENERAL PUBLIC LICENSE v.2.1

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the “Lesser» General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a “work based on the library» and a “work that uses the library». The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called “this License»). Each licensee is addressed as “you».

A “library» means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The “Library», below, refers to any such software library or work which has been distributed under these terms. A “work based on the Library» means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term “modification».)

“Source code» for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a “work that uses the Library». Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a “work that uses the Library» with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a “work that uses the library». The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a “work that uses the Library» uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a “work that uses the Library» with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable “work that uses the Library», as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the “work that uses the Library» must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and “any later version», you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY “AS IS» WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the “copyright» line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>

Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA. Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a “copyright disclaimer» for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990

Ty Coon, President of Vice

That's all there is to it!

RFC1321-BASED (RSA-FREE) MD5 LIBRARY

Copyright (C) 1999, 2002, Aladdin Enterprises

TINICONV 1.0.0

Copyright (C) Free Software Foundation, Inc

---

http://sourceforge.net/projects/tiniconv/

GNU LESSER GENERAL PUBLIC LICENSE v.2.1

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the “Lesser» General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a “work based on the library» and a “work that uses the library». The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called “this License»). Each licensee is addressed as “you».

A “library» means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The “Library», below, refers to any such software library or work which has been distributed under these terms. A “work based on the Library» means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term “modification».)

“Source code» for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a “work that uses the Library». Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a “work that uses the Library» with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a “work that uses the library». The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a “work that uses the Library» uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a “work that uses the Library» with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable “work that uses the Library», as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the “work that uses the Library» must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and “any later version», you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY “AS IS» WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the “copyright» line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>

Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA. Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a “copyright disclaimer» for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990

Ty Coon, President of Vice

That's all there is to it!

WINDOWS TEMPLATE LIBRARY 7.5

Copyright (C) 2005, Microsoft Corporation

Common Public License Version 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE (“AGREEMENT»). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. DEFINITIONS

“Contribution» means:

a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and

b) in the case of each subsequent Contributor:

i) changes to the Program, and

ii) additions to the Program;

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

“Contributor» means any person or entity that distributes the Program.

“Licensed Patents « mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

“Program” means the Contributions distributed in accordance with this Agreement.

“Recipient” means anyone who receives the Program under this Agreement, including all Contributors.

2. GRANT OF RIGHTS

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. REQUIREMENTS

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. COMMERCIAL DISTRIBUTION

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. NO WARRANTY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. DISCLAIMER OF LIABILITY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. GENERAL

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

WINDOWS TEMPLATE LIBRARY 8.0

Copyright (C) Microsoft Corporation

ZLIB 1.2, 1.2.2

Copyright (C) Jean-loup Gailly and Mark Adler

Другая информация

Дополнительная информация о стороннем коде.

Для проверки электронной цифровой подписи используется программная библиотека защиты информации (ПБЗИ) “Агава-С”, разработанная ООО “Р-Альфа”.

Данный продукт содержит или может содержать программы, которые лицензируются (или сублицензируются) пользователю в соответствии с общедоступной лицензией GNU или иными аналогичными лицензиями Open Source, которые помимо прочих прав разрешают пользователю копировать, модифицировать, перераспределять определенные программы или их части и получать доступ к исходному коду (“ПО с открытым исходным кодом”). Если такая лицензия предусматривает предоставление исходного кода пользователям, которым предоставляется ПО в формате исполняемого двоичного кода, исходный код делается доступным при осуществлении запроса на адрес source@kaspersky.com или сопровождается с продуктом.

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

А

Анти-Баннер
  список разрешенных адресов баннеров 131
Анти-Спам
  расширение Microsoft Office Outlook 128
  расширение Microsoft Outlook Express 128
  расширение The Bat! 129
  расширение Thunderbird 130
  список разрешенных отправителей 122
  список разрешенных фраз 120
  фильтрация писем на сервере 126

Б

Безопасная среда
  выбор режима 159
  создание ярлыка 159

В

Выбор режима
  безопасная среда 159

Д

Диспетчер писем
  Анти-Спам 126
Дополнительные инструменты
  мастер устранения следов активности 227
  настройка браузера 230
  необратимое удаление данных 226
  удаление неиспользуемой информации 228

З

Зараженный объект 270
Защита от сетевых атак
  виды обнаруживаемых сетевых атак 147

К

Категории обнаруживаемых угроз 220
Контроль программ
  наследование прав 138
  правила Контроля программ 136

Л

Лицензия 276
  активная 268
  лицензионное соглашение 34
  получение файла ключа 276

М

Менеджер паролей
  быстрый запуск функций 207
  визитка 197
  генератор паролей 216
  группа учетных записей 196
  доступ к базе паролей 190

изменение мастер-пароля....212
импорт / экспорт паролей....200
имя пользователя....197
кнопка быстрого запуска....214
метод шифрования....209
переносная версия....217
персональные данные....198
поиск паролей....199
учетная запись....192

Н

Наследование прав
Контроль программ....138

О

Обновление
из локальной папки....90
источник обновлений....88
откат последнего обновления....91
по расписанию....90
прокси-сервер....92
региональные настройки....89
Обновление программы....87
Отчеты....231

П

Правила Контроля программ
Контроль программ....136

Р

Резервное копирование....273
восстановление данных....167
запуск задачи резервного копирования....167
очистка хранилища....165
подключение хранилища....165
поиск резервных копий....168
просмотр данных резервной копии....169
просмотр отчета о событиях....170
создание задачи резервного хранилища....166
создание хранилища....164
удаление хранилища....166
Родительский контроль
включение и настройка параметров....172
загрузка файлов из интернета....175
запуск программ и игр....174
ограничение использования интернета по времени....174
ограничение использования компьютера....174
отправка персональной информации....178
переписка через интернет-пейджеры....176
поиск ключевых слов....179
посещение веб-сайтов....175
режим безопасного поиска....176
экспорт / импорт параметров....173

С

Сетевой экран
Мастер создания правила....146
расширение диапазона адресов сети....145
Создание ярлыка
безопасная среда....159

Ц

Центр управления
анализ безопасности сети ... 62
настройка удаленного управления ... 184
обновление ... 185
проверка на вирусы и уязвимости ... 185
резервное копирование ... 187
управление компонентами защиты ... 186
управление лицензиями ... 187
управление родительским контролем ... 186

Ш

Шифрование данных
добавление файлов в контейнер ... 182
настройка параметров контейнера ... 182
подключение и отключение контейнера ... 181
создание контейнера ... 180