Kaspersky CRYSTAL

Руководство пользователя

ВЕРСИЯ ПРОГРАММЫ: 3.0

Уважаемый пользователь!

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

Дата редакции документа: 04.12.2012

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

СОДЕРЖАНИЕ

ОБ ЭТОМ РУКОВОДСТВЕ

Этот документ представляет собой Руководство пользователя Kaspersky CRYSTAL.

Для успешного использования Kaspersky CRYSTAL пользователям нужно быть знакомым с интерфейсом используемой операционной системы, владеть основными приемами работы в ней, уметь работать с электронной почтой и интернетом.

Руководство предназначено для следующих целей:

- Помочь установить Kaspersky CRYSTAL, активировать и использовать программу.
- Обеспечить быстрый поиск информации для решения вопросов, связанных с работой Kaspersky CRYSTAL.
- Рассказать о дополнительных источниках информации о программе и способах получения технической поддержки.

В ЭТОМ РАЗДЕЛЕ

В ЭТОМ РУКОВОДСТВЕ

Этот документ содержит следующие разделы.

Источники информации о программе

Этот раздел содержит описание источников информации о программе и сведения о веб-сайтах, которые вы можете использовать, чтобы обсудить работу программы.

Kaspersky CRYSTAL

Этот раздел содержит описание возможностей программы, а также краткую информацию о функциях и компонентах программы. Вы узнаете о том, из чего состоит комплект поставки и какие услуги доступны зарегистрированным пользователям программы. В разделе приведена информация о том, каким программным и аппаратным требованиям должен отвечать компьютер, чтобы на него можно было установить программу.

Установка и удаление программы

Этот раздел содержит пошаговые инструкции по установке и удалению программы.

Лицензирование программы

Этот раздел содержит информацию об основных понятиях, связанных с активацией программы. Из этого раздела вы узнаете о назначении Лицензионного соглашения, типах лицензии, способах активации программы, а также о продлении срока действия лицензии.

Решение типовых задач

Этот раздел содержит пошаговые инструкции для выполнения основных задач пользователя, которые решает программа.

Обращение в Службу технической поддержки

Этот раздел содержит сведения о способах обращения в Службу технической поддержки «Лаборатории Касперского».

Приложения

Этот раздел содержит информацию, которая дополняет основной текст документа.

Глоссарий

Этот раздел содержит список терминов, которые встречаются в тексте документа, а также определения этих терминов.

ЗАО «Лаборатория Касперского»

Этот раздел содержит информацию о ЗАО «Лаборатория Касперского».

Информация о стороннем коде

Этот раздел содержит информацию о стороннем коде, используемом в программе.

Уведомления о товарных знаках

В этом разделе перечислены товарные знаки сторонних правообладателей, использованные в документе.

Предметный указатель

Этот раздел позволяет быстро найти необходимые сведения в документе.

Условные обозначения

Текст документа сопровождается смысловыми элементами, на которые мы рекомендуем вам обращать особое внимание, – предупреждениями, советами, примерами.

Для выделения смысловых элементов используются условные обозначения. Условные обозначения и примеры их использования приведены в таблице ниже.

Таблица 1. Условные обозначения

Пример текста	Описание условного обозначения
Обратите внимание на то, что...	Предупреждения выделены красным цветом и заключены в рамку. В предупреждениях содержится информация о возможных нежелательных действиях, которые могут привести к потере информации, сбоям в работе оборудования или операционной системы.
Рекомендуется использовать...	Примечания заключены в рамку. Примечания могут содержать полезные советы, рекомендации, особые значения параметров или важные частные случаи в работе программы.

Пример текста	Описание условного обозначения
Пример: ...	Примеры приведены в блоках на желтом фоне под заголовком «Пример».
Обновление – это... Возникает событие *Базы устарели*.	Курсивом выделены следующие смысловые элементы текста: • новые термины; • названия статусов и событий программы.
Нажмите на клавишу **ENTER**. Нажмите комбинацию клавиш **ALT**+**F4**.	Названия клавиш клавиатуры выделены полужирным шрифтом и прописными буквами. Названия клавиш, соединенные знаком + (плюс), означают комбинацию клавиш. Такие клавиши нужно нажимать одновременно.
Нажмите на кнопку **Включить**.	Названия элементов интерфейса программы, например, полей ввода, пунктов меню, кнопок, выделены полужирным шрифтом.
➧ *Чтобы настроить расписание задачи, выполните следующие действия:*	Вводные фразы инструкций выделены курсивом и значком «стрелка».
В командной строке введите текст `help` Появится следующее сообщение: `Укажите дату в формате ДД:ММ:ГГ.`	Специальным стилем выделены следующие типы текста: • текст командной строки; • текст сообщений, выводимых программой на экран; • данные, которые требуется ввести пользователю.
<Имя пользователя>	Переменные заключены в угловые скобки. Вместо переменной требуется подставить соответствующее ей значение, опустив угловые скобки.

ИСТОЧНИКИ ИНФОРМАЦИИ О ПРОГРАММЕ

Этот раздел содержит описание источников информации о программе и сведения о веб-сайтах, которые вы можете использовать, чтобы обсудить работу программы.

Вы можете выбрать наиболее удобный источник информации в зависимости от важности и срочности вопроса.

В ЭТОМ РАЗДЕЛЕ

Источники информации для самостоятельного поиска

Вы можете использовать следующие источники для самостоятельного поиска информации о программе:

- страница на веб-сайте «Лаборатории Касперского»;
- страница на веб-сайте Службы технической поддержки (База знаний);
- электронная справка;
- документация.

Если вы не нашли решения возникшей проблемы самостоятельно, рекомендуем вам обратиться в Службу технической поддержки «Лаборатории Касперского» (см. раздел «Техническая поддержка по телефону« на стр. 80).

Для использования источников информации на веб-сайте «Лаборатории Касперского» необходимо подключение к интернету.

Страница на веб-сайте «Лаборатории Касперского»

Веб-сайт «Лаборатории Касперского» содержит отдельную страницу для каждой программы.

На странице (http://www.kaspersky.ru/kaspersky-crystal) вы можете получить общую информацию о программе, ее возможностях и особенностях работы.

Страница содержит ссылку на интернет-магазин. В нем вы можете приобрести программу или продлить право пользования программой.

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

База знаний – раздел веб-сайта Службы технической поддержки, содержащий рекомендации по работе с программами «Лаборатории Касперского». База знаний состоит из справочных статей, сгруппированных по темам.

На странице программы в Базе знаний (http://support.kaspersky.ru/pure) вы найдете статьи, которые содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании программы.

Статьи могут отвечать на вопросы, которые относятся не только к Kaspersky CRYSTAL, но и к другим программам «Лаборатории Касперского», а также могут содержать новости Службы технической поддержки.

Электронная справка

В состав электронной справки программы входят файлы справки.

Контекстная справка содержит сведения о каждом окне программы: перечень и описание параметров и список решаемых задач.

Полная справка содержит подробную информацию о том, как управлять защитой, настраивать параметры программы и решать основные задачи пользователя.

Документация

Руководство пользователя программы содержит информацию об установке, активации, настройке параметров программы, а также сведения о работе с программой. В документе приведено описание интерфейса программы, предложены способы решения типовых задач пользователя при работе с программой.

Обсуждение программ «Лаборатории Касперского» на форуме

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

На форуме вы можете просматривать опубликованные темы, добавлять свои комментарии, создавать новые темы для обсуждения.

Обращение в Департамент продаж

Если у вас возникли вопросы по выбору, приобретению или продлению срока использования программы, вы можете связаться с нашими специалистами из Департамента продаж одним из следующих способов:

- Позвонив по телефонам нашего центрального офиса в Москве (http://www.kaspersky.ru/contacts).
- Отправив письмо с вопросом по электронному адресу sales@kaspersky.com.

Обслуживание осуществляется на русском и английском языках.

Обращение в Отдел локализации и разработки технической документации

Если у вас возникли вопросы, связанные с документацией к программе, вы можете обратиться к специалистам Группы разработки документации. Например, вы можете присылать нашим специалистам отзывы о документации.

KASPERSKY CRYSTAL

Этот раздел содержит описание возможностей программы, а также краткую информацию о функциях и компонентах программы. Вы узнаете о том, из чего состоит комплект поставки и какие услуги доступны зарегистрированным пользователям программы. В разделе приведена информация о том, каким программным и аппаратным требованиям должен отвечать компьютер, чтобы на него можно было установить программу.

В ЭТОМ РАЗДЕЛЕ

Что нового

В Kaspersky CRYSTAL появились следующие новые возможности:

- Для безопасной работы с сервисами интернет-банкинга и платежных систем, а также оплаты покупок в интернет-магазинах добавлены Безопасные платежи (на стр. 49).
- Улучшена защита от клавиатурных перехватчиков персональной информации, вводимой на веб-сайтах:
  - Добавлена Защита ввода данных с аппаратной клавиатуры (на стр. 53).
  - Программа автоматически добавляет кнопку запуска виртуальной клавиатуры (см. раздел «Использование виртуальной клавиатуры» на стр. 51) в поля ввода паролей на веб-сайтах.
- Добавлена возможность использования Онлайн-хранилища (см. раздел «Использование Онлайн-хранилища» на стр. 67) для сохранения резервных копий файлов. Это позволяет повысить безопасность хранения информации и упростить доступ к данным за счет применения облачных технологий.
- Для защиты от использования злоумышленниками уязвимостей в программном обеспечении в компонент Мониторинг активности добавлена функция защиты от эксплойтов.
- Усовершенствован Менеджер паролей. Теперь вы можете хранить базу паролей на удаленных серверах. С помощью синхронизации актуальные пароли и личные данные доступны на всех ваших ноутбуках и настольных компьютерах, на которых установлен Kaspersky CRYSTAL.
- Усовершенствован интерфейс Kaspersky CRYSTAL: добавлены всплывающие подсказки, содержащие полезные сведения о работе программы.
- Упрощена процедура установки программы (см. раздел «Установка и удаление программы» на стр. 18). Добавлена возможность автоматической установки последней версии Kaspersky CRYSTAL, содержащей набор последних обновлений баз программы.
- Уменьшен размер баз программы, что позволяет сократить объем загружаемых данных и ускорить установку обновлений.

- Усовершенствован эвристический анализ, выполняемый при проверке веб-сайтов на признаки фишинга.

- Адаптированы сообщения, которые Родительский контроль отображает для детей. Повышена точность работы Родительского контроля: теперь этот компонент использует облачную технологию проверки веб-сайтов на наличие нежелательного содержимого.

ОСНОВНЫЕ ФУНКЦИИ ПРОГРАММЫ

Kaspersky CRYSTAL обеспечивает комплексную защиту вашего компьютера. Комплексная защита включает в себя защиту компьютера, защиту данных и защиту пользователей, а также удаленное управление функциями Kaspersky CRYSTAL на компьютерах сети. Для решения задач комплексной защиты в составе Kaspersky CRYSTAL предусмотрены различные функции и компоненты защиты.

Защита компьютера

Компоненты защиты предназначены для защиты компьютера от известных и новых угроз, сетевых атак, мошенничества, спама и нежелательной информации. Каждый тип угроз обрабатывается отдельным компонентом защиты (см. описание компонентов далее в этом разделе). Вы можете включать и выключать компоненты защиты независимо друг от друга, а также настраивать их работу.

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.

Защиту вашего компьютера в реальном времени обеспечивают следующие компоненты защиты:

Ниже описана работа компонентов защиты в режиме работы Kaspersky CRYSTAL, рекомендованном специалистами «Лаборатории Касперского» (то есть при параметрах работы программы, заданных по умолчанию).

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 скриптов, расположенных на веб-сайтах, если эти скрипты представляют угрозу безопасности компьютера. Веб-Антивирус также контролирует весь веб-трафик и 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

Мониторинг сети предназначен для наблюдения за сетевой активностью 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 проверяет все входящие почтовые сообщения на наличие спама. Все письма, содержащие спам, помечаются специальным заголовком. Вы можете настраивать действия Анти-Спама с письмами, содержащими спам (например, автоматическое удаление, помещение в специальную папку).

Анти-Фишинг

Анти-Фишинг позволяет проверять веб-адреса на принадлежность к спискам вредоносных и фишинговых веб-адресов. Этот компонент встроен в Веб-Антивирус, Анти-Спам и IM-Антивирус.

Анти-Баннер

Анти-Баннер блокирует рекламные баннеры, размещенные на веб-сайтах и в интерфейсах программ.

Безопасные платежи

Безопасные платежи обеспечивают защиту конфиденциальных данных при работе с сервисами интернет-банкинга и платежными системами, а также предотвращают кражу платежных средств при проведении платежей онлайн.

Защита информации

Для защиты данных от утери, несанкционированного доступа или кражи предназначены функции Резервное копирование, Шифрование данных и Менеджер 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. 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.

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. Для доступа к данным, хранящимся в зашифрованном контейнере, необходимо ввести пароль.

Менеджер паролей

Для доступа к большинству услуг и ресурсов в интернете требуется регистрация пользователя и ввод учетных данных для аутентификации. В целях безопасности рекомендуется использовать для регистрации на разных веб-сайтах разные учетные записи, а также не записывать свои имя пользователя и пароль.

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 на веб-сайтах. С помощью мастер-пароля вы можете управлять всеми вашими учетными записями на веб-сайтах.

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.

Комплект поставки

Вы можете приобрести программу одним из следующих способов:

- **В коробке**. Распространяется через магазины наших партнеров.
- **Через интернет-магазин**. Распространяется через интернет-магазины «Лаборатории Касперского» (например, http://www.kaspersky.ru, раздел **Интернет-магазин**) или компаний-партнеров.

Если вы приобретаете программу в коробке, в комплект поставки входят следующие компоненты:

- запечатанный конверт с установочным компакт-диском, на котором записаны файлы программы и файлы документации к программе;
- краткое руководство пользователя, содержащее код активации программы;
- Лицензионное соглашение, в котором указано, на каких условиях вы можете пользоваться программой.

Состав комплекта поставки может быть различным в зависимости от региона, в котором распространяется программа.

Если вы приобретаете Kaspersky CRYSTAL через интернет-магазин, вы копируете программу с сайта интернет-магазина. Информация, необходимая для активации программы, высылается вам по электронной почте после оплаты.

За подробной информацией о способах приобретения и комплекте поставки вы можете обратиться в Департамент продаж по адресу sales@kaspersky.com.

Сервис для пользователей

Приобретая лицензию на использование программы, в течение срока действия лицензии вы можете получать следующие услуги:

- обновление баз и предоставление новых версий программы;
- консультации по телефону и электронной почте по вопросам, связанным с установкой, настройкой и использованием программы;
- оповещение о выходе новых программ «Лаборатории Касперского», а также информацию о появлении новых вирусов и вирусных эпидемиях. Для использования этой услуги требуется подписаться на рассылку новостей ЗАО «Лаборатория Касперского» на веб-сайте Службы технической поддержки.

Консультации по работе операционных систем, стороннего программного обеспечения и технологиям не проводятся.

Аппаратные и программные требования

Для функционирования Kaspersky CRYSTAL компьютер должен удовлетворять следующим требованиям:

Общие требования:

- 700 МБ свободного места на жестком диске.
- CD- / DVD-ROM (для установки Kaspersky CRYSTAL с дистрибутивного CD-диска).
- Компьютерная мышь.
- Подключение к интернету (для активации программы, а также обновления баз и программных модулей).
- Microsoft Internet Explorer 8.0 или выше.
- Microsoft Windows® Installer 3.0.

Требования для операционных систем Microsoft Windows XP Home Edition (Service Pack 3 или выше), Microsoft Windows XP Professional (Service Pack 3 или выше), Microsoft Windows XP Professional x64 Edition (Service Pack 2 или выше):

- процессор Intel® Pentium® 800 МГц 32-разрядный (x86) / 64-разрядный (x64) или выше (или совместимый аналог).
- 512 МБ свободной оперативной памяти.

Требования для операционных систем Microsoft Windows Vista® Home Basic (Service Pack 2 или выше), Microsoft Windows Vista Home Premium (Service Pack 2 или выше), Microsoft Windows Vista Business (Service Pack 2 или выше), Microsoft Windows Vista Enterprise (Service Pack 2 или выше), Microsoft Windows Vista Ultimate (Service Pack 2 или выше), Microsoft Windows 7 Starter (Service Pack 1 или выше), Microsoft Windows 7 Home Basic (Service Pack 1 или выше), Microsoft Windows 7 Home Premium (Service Pack 1 или выше), Microsoft Windows 7 Professional (Service Pack 1 или выше), Microsoft Windows 7 Ultimate (Service Pack 1 или выше), Microsoft Windows 8, Microsoft Windows 8 Pro, Windows 8 Enterprise и выше (x32 и x64):

- процессор Intel Pentium 1 ГГц 32-разрядный (x86) / 64-разрядный (x64) или выше (или совместимый аналог);
- 1 ГБ свободной оперативной памяти (для 32-разрядной операционной системы); 2 ГБ свободной оперативной памяти (для 64-разрядной операционной системы).

Требования для нетбуков:

- Процессор Intel Atom™ 1,6 МГц (Z520) или совместимый аналог.
- 1 ГБ свободной оперативной памяти.
- Видеокарта Intel GMA950 с видеопамятью объемом не менее 64 МБ (или совместимый аналог).
- Диагональ экрана не менее 10,1 дюйма.

При работе в 64-разрядных версиях операционных систем программа не поддерживает использование Менеджера паролей.

УСТАНОВКА И УДАЛЕНИЕ ПРОГРАММЫ

Этот раздел содержит пошаговые инструкции по установке и удалению программы.

В ЭТОМ РАЗДЕЛЕ

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**.

Если программа будет использована для защиты более чем одного компьютера (максимально допустимое количество компьютеров определяется условиями Лицензионного соглашения), то процедура установки будет одинаковой на всех компьютерах.

- *Чтобы установить Kaspersky CRYSTAL на ваш компьютер,*

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

Для установки Kaspersky CRYSTAL вы также можете использовать дистрибутив, полученный через интернет. При этом для некоторых языков локализации мастер установки отображает несколько дополнительных шагов установки.

В этом разделе

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 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. Начало установки программы

На этом этапе мастер установки предлагает вам установить программу.

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

В зависимости от типа установки и языка локализации на этом этапе мастер установки может предлагать вам ознакомиться с Лицензионным соглашением, которое заключается между вами и «Лабораторией Касперского», а также принять участие в программе Kaspersky Security Network.

Шаг 3. Просмотр Лицензионного соглашения

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

Внимательно прочитайте Лицензионное соглашение и, если вы согласны со всеми его пунктами, нажмите на кнопку **Принять**. Установка программы на ваш компьютер будет продолжена.

Если Лицензионное соглашение не принято, установка программы не производится.

Шаг 4. Положение об использовании Kaspersky Security Network

На этом этапе мастер установки предлагает вам 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, а также информации о системе. При этом сбор, обработка и хранение ваших персональных данных не производятся.

Ознакомьтесь с Положением об использовании Kaspersky Security Network. Если вы согласны со всеми его пунктами, в окне мастера установите флажок **Я хочу участвовать в программе Kaspersky Security Network (KSN)**.

Нажмите на кнопку **Далее**, чтобы продолжить установку программы.

Шаг 5. Установка

Установка программы занимает некоторое время. Дождитесь ее завершения.

По завершении установки мастер автоматически переходит к следующему шагу.

Во время установки Kaspersky CRYSTAL производит ряд проверок. В результате этих проверок могут быть обнаружены следующие проблемы:

- **Несоответствие операционной системы программным требованиям**. Во время установки мастер проверяет соблюдение следующих условий:
  - соответствие операционной системы и пакетов обновлений (Service Pack) программным требованиям;
  - наличие необходимых программ;
  - наличие необходимого для установки свободного места на диске.

Если какое-либо из перечисленных условий не выполнено, на экран будет выведено соответствующее уведомление.

- **Наличие на компьютере несовместимых программ**. При обнаружении несовместимых программ их список будет выведен на экран, и вам будет предложено удалить их. Программы, которые Kaspersky CRYSTAL не может удалить автоматически, необходимо удалить вручную. Во время удаления несовместимых программ потребуется перезагрузка системы, после чего установка Kaspersky CRYSTAL продолжится автоматически.

- **Наличие на компьютере вредоносных приложений**. При обнаружении на компьютере вредоносных приложений, препятствующих установке антивирусных программ, мастер установки предложит загрузить 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, он предложит вам загрузить ее самостоятельно, перейдя по предлагаемой ссылке.

Шаг 6. Завершение установки

На этом этапе мастер информирует вас о завершении установки программы. Чтобы начать работу с Kaspersky CRYSTAL немедленно, убедитесь, что флажок **Запустить Kaspersky CRYSTAL** установлен, и нажмите на кнопку **Готово**.

В некоторых случаях для завершения установки может потребоваться перезагрузка операционной системы. Если флажок **Запустить Kaspersky CRYSTAL** установлен, после перезагрузки программа будет запущена автоматически.

Если перед завершением работы мастера вы сняли флажок **Запустить Kaspersky CRYSTAL**, программу нужно будет запустить вручную.

Шаг 7. Активация программы

На этом этапе мастер установки предлагает вам активировать программу.

Активация – это процедура введения в действие полнофункциональной версии программы на определенный срок.

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. 29), если вы приобрели коммерческую версию программы.

- **Активировать пробную версию**. Выберите этот вариант активации, если вы хотите установить пробную версию программы перед принятием решения о покупке коммерческой версии. Вы сможете использовать программу в режиме полной функциональности в течение срока действия пробной лицензии. По истечении срока действия лицензии возможность повторной активации пробной версии будет недоступна.

Шаг 8. Регистрация пользователя

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

Зарегистрированные пользователи получают возможность отправлять запросы в Службу технической поддержки и Вирусную Лабораторию через Личный кабинет на веб-сайте «Лаборатории Касперского», возможность удобного управления кодами активации, а также оперативную информацию о новых продуктах и специальных предложениях.

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

Шаг 9. Завершение активации

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

В случае использования подписки вместо даты окончания срока действия лицензии приводится информация о статусе подписки.

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

Обновление предыдущей версии Kaspersky CRYSTAL

Если на вашем компьютере установлена предыдущая версия Kaspersky CRYSTAL, вам нужно обновить программу до новой версии Kaspersky CRYSTAL. При наличии действующей лицензии на использование Kaspersky CRYSTAL вам не понадобится активировать программу: мастер установки автоматически получит информацию о лицензии на использование Kaspersky CRYSTAL и применит ее в процессе установки.

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**.

Если программа будет использована для защиты более чем одного компьютера (максимально допустимое количество компьютеров определяется условиями Лицензионного соглашения), то процедура установки будет одинаковой на всех компьютерах.

- *Чтобы установить Kaspersky CRYSTAL на ваш компьютер,*

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

Для установки Kaspersky CRYSTAL вы также можете использовать дистрибутив, полученный через интернет. При этом для некоторых языков локализации мастер установки отображает несколько дополнительных шагов установки.

В этом разделе

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 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. Начало установки программы

На этом этапе мастер установки предлагает вам установить программу.

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

В зависимости от типа установки и языка локализации на этом этапе мастер установки может предлагать вам ознакомиться с Лицензионным соглашением, которое заключается между вами и «Лабораторией Касперского», а также принять участие в программе Kaspersky Security Network.

Шаг 3. Просмотр Лицензионного соглашения

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

Внимательно прочитайте Лицензионное соглашение и, если вы согласны со всеми его пунктами, нажмите на кнопку **Принять**. Установка программы на ваш компьютер будет продолжена.

Если Лицензионное соглашение не принято, установка программы не производится.

Шаг 4. Положение об использовании Kaspersky Security Network

На этом этапе мастер установки предлагает вам 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, а также информации о системе. При этом сбор, обработка и хранение ваших персональных данных не производятся.

Ознакомьтесь с Положением об использовании Kaspersky Security Network. Если вы согласны со всеми его пунктами, в окне мастера установите флажок **Я хочу участвовать в программе Kaspersky Security Network (KSN)**.

Нажмите на кнопку **Далее**, чтобы продолжить установку программы.

Шаг 5. Установка

Установка программы занимает некоторое время. Дождитесь ее завершения.

По завершении установки мастер автоматически переходит к следующему шагу.

Во время установки Kaspersky CRYSTAL производит ряд проверок. В результате этих проверок могут быть обнаружены следующие проблемы:

- **Несоответствие операционной системы программным требованиям**. Во время установки мастер проверяет соблюдение следующих условий:

  - соответствие операционной системы и пакетов обновлений (Service Pack) программным требованиям;

  - наличие необходимых программ;

  - наличие необходимого для установки свободного места на диске.

  Если какое-либо из перечисленных условий не выполнено, на экран будет выведено соответствующее уведомление.

- **Наличие на компьютере несовместимых программ**. При обнаружении несовместимых программ их список будет выведен на экран, и вам будет предложено удалить их. Программы, которые Kaspersky CRYSTAL не может удалить автоматически, необходимо удалить вручную. Во время удаления несовместимых программ потребуется перезагрузка системы, после чего установка Kaspersky CRYSTAL продолжится автоматически.

- **Наличие на компьютере вредоносных приложений**. При обнаружении на компьютере вредоносных приложений, препятствующих установке антивирусных программ, мастер установки предложит загрузить 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, он предложит вам загрузить ее самостоятельно, перейдя по предлагаемой ссылке.

Шаг 6. Завершение установки

Это окно мастера информирует вас о завершении установки программы.

По завершении установки необходимо перезагрузить операционную систему.

Если флажок **Запустить Kaspersky CRYSTAL** установлен, после перезагрузки программа будет запущена автоматически.

Если перед завершением работы мастера вы сняли флажок **Запустить Kaspersky CRYSTAL**, программу нужно запустить вручную.

Удаление программы

В результате удаления Kaspersky CRYSTAL компьютер и ваши личные данные окажутся незащищенными!

Удаление Kaspersky CRYSTAL выполняется с помощью мастера установки.

- *Чтобы запустить мастер,*

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

В этом разделе

Шаг 1. Сохранение данных для повторного использования

На этом шаге вы можете указать, какие используемые программой данные вы хотите сохранить для дальнейшего использования при повторной установке программы (например, ее более новой версии).

Вы можете указать следующие типы данных для повторного использования:

- **Информация о лицензии** – данные, позволяющие в дальнейшем не активировать устанавливаемую программу, а использовать ее по уже действующей лицензии, если срок действия лицензии не истечет к моменту установки.
- **Объекты карантина** – файлы, проверенные программой и помещенные в резервное хранилище и на карантин.

  При удалении Kaspersky CRYSTAL с компьютера файлы на карантине будут недоступны. Для работы с этими файлами нужно установить Kaspersky CRYSTAL.

- **Параметры работы программы** – значения параметров работы программы, установленные в процессе ее настройки.

«Лаборатория Касперского» не гарантирует поддержку параметров предыдущей версии программы. После установки более новой версии программы рекомендуем проверить правильность ее настройки.

- **Данные iChecker** – файлы, содержащие информацию об объектах, уже проверенных с помощью технологии iChecker.
- **Зашифрованные контейнеры (вместе с данными)** – файлы, помещенные в зашифрованные контейнеры с помощью функции Шифрование данных.
- **Базы Менеджера паролей (для всех пользователей)** – учетные записи, личные заметки, закладки и визитные карточки, созданные с помощью функции Менеджер паролей.
- **Базы Анти-Спама** – базы, содержащие образцы спам-сообщений, полученные и сохраненные программой во время работы.

По умолчанию программа предлагает сохранить информацию об активации.

Чтобы сохранить данные для повторного использования,

установите флажки напротив тех данных, которые нужно сохранить.

Шаг 2. Подтверждение удаления

Поскольку удаление программы ставит под угрозу защиту компьютера и ваших личных данных, требуется подтвердить свое намерение удалить программу. Для этого нажмите на кнопку **Удалить**.

Шаг 3. Удаление программы. Завершение удаления

На этом шаге мастер удаляет программу с вашего компьютера. Дождитесь завершения процесса удаления.

В процессе удаления требуется перезагрузка операционной системы. Если вы откажетесь от немедленной перезагрузки, завершение процедуры удаления будет отложено до того момента, когда операционная система будет перезагружена или компьютер будет выключен и включен.

ЛИЦЕНЗИРОВАНИЕ ПРОГРАММЫ

Этот раздел содержит информацию об основных понятиях, связанных с активацией программы. Из этого раздела вы узнаете о назначении Лицензионного соглашения, типах лицензии, способах активации программы, а также о продлении срока действия лицензии.

В ЭТОМ РАЗДЕЛЕ

О Лицензионном соглашении

Лицензионное соглашение – это юридическое соглашение между вами и ЗАО «Лаборатория Касперского», в котором указано, на каких условиях вы можете использовать программу.

Внимательно ознакомьтесь с условиями Лицензионного соглашения перед началом работы с программой.

Считается, что вы принимаете условия Лицензионного соглашения, подтверждая свое согласие с текстом Лицензионного соглашения при установке программы. Если вы не согласны с условиями Лицензионного соглашения, вы должны прервать установку программы или не использовать программу.

О лицензии

Лицензия – это ограниченное по времени право на использование программы, предоставляемое вам на основе Лицензионного соглашения. С лицензией связан уникальный код активации вашего экземпляра Kaspersky CRYSTAL.

Лицензия включает в себя право на получение следующих видов услуг:

- Использование программы на одном или нескольких устройствах.

  Количество устройств, на которых вы можете использовать программу, определяется условиями Лицензионного соглашения.

- Обращение в Службу технической поддержки «Лаборатории Касперского».

- Получение прочих услуг, предоставляемых вам «Лабораторией Касперского» или ее партнерами в течение срока действия лицензии (см. раздел «Сервис для пользователей» на стр. 16).

Объем предоставляемых услуг и срок использования программы зависят от типа лицензии, по которой была активирована программа.

Предусмотрены следующие типы лицензий:

- *Пробная* – бесплатная лицензия, предназначенная для ознакомления с программой.

Пробная лицензия обычно имеет небольшой срок действия. По истечении срока действия пробной лицензии Kaspersky CRYSTAL прекращает выполнять все свои функции. Для продолжения использования программы требуется приобрести коммерческую лицензию.

- *Коммерческая* – платная лицензия, предоставляемая при приобретении программы.

  По истечении срока действия коммерческой лицензии программа продолжает работу, но с ограниченной функциональностью (например, недоступно обновление и использование сервиса Kaspersky Security Network). Вы по-прежнему можете использовать все компоненты программы и выполнять проверку на вирусы и другие программы, представляющие угрозу, но только на основе баз, установленных до даты окончания срока действия лицензии. Для продолжения использования Kaspersky CRYSTAL в режиме полной функциональности требуется продлить срок действия коммерческой лицензии.

  Рекомендуется продлевать срок действия лицензии не позднее даты его окончания, чтобы обеспечить максимальную защиту от всех угроз компьютерной безопасности.

О ПРЕДОСТАВЛЕНИИ ДАННЫХ

Для повышения уровня оперативной защиты, принимая условия Лицензионного соглашения, вы соглашаетесь в автоматическом режиме предоставлять «Лаборатории Касперского» следующую информацию:

- информацию о контрольных суммах обрабатываемых файлов (MD5);
- информацию для определения репутации URL;
- статистику использования продуктовых уведомлений;
- статистические данные для защиты от спама;
- данные об активации и используемой версии Kaspersky CRYSTAL;
- информацию о типах обнаруженных угроз;
- информацию об используемых цифровых сертификатах и информацию, необходимую для проверки их подлинности.

Если компьютер оборудован модулем TPM (Trusted Platform Module), то вы также соглашаетесь предоставлять «Лаборатории Касперского» отчет TPM о загрузке операционной системы компьютера и информацию, необходимую для проверки подлинности отчета. При возникновении ошибки установки Kaspersky CRYSTAL вы соглашаетесь в автоматическом режиме предоставить «Лаборатории Касперского» информацию о коде ошибки, используемом дистрибутиве и компьютере.

При участии в программе Kaspersky Security Network в «Лабораторию Касперского» автоматически передается следующая информация, полученная в результате работы Kaspersky CRYSTAL на компьютере:

- информация об установленном аппаратном и программном обеспечении;
- информация о состоянии антивирусной защиты компьютера, а также обо всех потенциально вредоносных объектах и действиях и принятых решений относительно этих объектов и действий;
- информация о загружаемых и запускаемых программах;
- информация об ошибках и использовании пользовательского интерфейса Kaspersky CRYSTAL;
- информация о версии используемых баз программы;
- статистика обновлений и соединений с серверами «Лаборатории Касперского»;
- статистика фактического времени, которое затрачивают компоненты программы на проверку объектов.

Также для дополнительной проверки в «Лабораторию Касперского» могут отправляться файлы (или их части), в отношении которых существует риск использования их злоумышленником для нанесения вреда компьютеру или данным.

Полученная информация защищается «Лабораторией Касперского» в соответствии с установленными законом требованиями. «Лаборатория Касперского» использует полученную информацию только в виде общей статистики. Данные общей статистики формируются автоматически из исходной полученной информации и не содержат персональных данных и иной конфиденциальной информации. Исходная полученная информация хранится в зашифрованном виде и уничтожается по мере накопления (два раза в год). Данные общей статистики хранятся бессрочно.

О коде активации

Код активации – это код, который вы получаете, приобретая коммерческую лицензию на использование Kaspersky CRYSTAL. Этот код необходим для активации программы.

Код активации представляет собой уникальную последовательность из двадцати латинских букв и цифр в формате xxxxx-xxxxx-xxxxx-xxxxx.

В зависимости от способа приобретения программы возможны следующие варианты получения кода активации:

- Если вы приобрели коробочную версию Kaspersky CRYSTAL, код активации указан в документации или на коробке, в которой находится установочный компакт-диск.

- Если вы приобрели Kaspersky CRYSTAL в интернет-магазине, код активации высылается по адресу электронной почты, указанному вами при заказе.

Отсчет срока действия лицензии начинается с даты активации программы. Если вы приобрели лицензию, допускающую использование Kaspersky CRYSTAL на нескольких устройствах, то отсчет срока действия лицензии начинается с даты первого применения кода активации.

Если код активации был потерян или случайно удален после активации программы, то для его восстановления обратитесь в Службу технической поддержки «Лаборатории Касперского».

РЕШЕНИЕ ТИПОВЫХ ЗАДАЧ

Этот раздел содержит пошаговые инструкции для выполнения основных задач пользователя, которые решает программа.

В этом разделе

Активация программы

Для того чтобы пользоваться функциями программы и связанными с программой дополнительными услугами, нужно активировать программу.

Если вы не активировали программу во время установки, вы можете сделать это позже. О необходимости активировать программу вам будут напоминать уведомления Kaspersky CRYSTAL, появляющиеся в области уведомлений панели задач. Активация Kaspersky CRYSTAL выполняется с помощью мастера активации.

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

- Перейдите по ссылке **Активировать** 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 **Лицензирование** нажмите на кнопку **Активировать программу**.

Во время работы мастера активации программы требуется указать ряд параметров.

Шаг 1. Ввод кода активации

Введите код активации (см. раздел «О коде активации» на стр. 29) в соответствующее поле и нажмите на кнопку **Далее**.

Шаг 2. Запрос на активацию

При успешном выполнении запроса на активацию мастер автоматически переходит к следующему шагу.

Шаг 3. Ввод регистрационных данных

Зарегистрированные пользователи получают следующие возможности:

- отправлять запросы в Службу технической поддержки и Вирусную Лабораторию через Личный кабинет на веб-сайте «Лаборатории Касперского»;

- управлять кодами активации;

- получать информацию о новых продуктах и специальных предложениях «Лаборатории Касперского».

Укажите ваши данные для регистрации, затем нажмите на кнопку **Далее**.

Шаг 4. Активация

Если активация программы прошла успешно, мастер автоматически переходит к следующему окну.

Шаг 5. Завершение работы мастера

В этом окне мастера отображается информация о результатах активации.

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

ПРИОБРЕТЕНИЕ ЛИЦЕНЗИИ ИЛИ ПРОДЛЕНИЕ СРОКА ЕЕ ДЕЙСТВИЯ

Если вы установили Kaspersky CRYSTAL, не имея коммерческой лицензии, вы можете приобрести лицензию после установки программы. При приобретении коммерческой лицензии вы получите код активации, с помощью которого нужно активировать программу (см. раздел «Активация программы» на стр. 32).

Когда срок действия лицензии подходит к концу, вы можете его продлить. Для этого вы можете указать в программе резервный код активации, не дожидаясь истечения срока действия лицензии. По истечении срока действия лицензии Kaspersky CRYSTAL будет автоматически активирован с помощью резервного кода активации.

Чтобы приобрести лицензию, выполните следующие действия:

1. Откройте главное окно программы.
2. По ссылке **Лицензия**, расположенной в нижней части главного окна, откройте окно **Лицензирование**.
3. В открывшемся окне нажмите на кнопку **Купить код активации**.

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

Чтобы ввести резервный код активации, выполните следующие действия:

1. Откройте главное окно программы.
2. По ссылке **Лицензия**, расположенной в нижней части главного окна, откройте окно **Лицензирование**.
3. В открывшемся окне нажмите на кнопку **Активировать программу**.

   Откроется окно мастера активации программы.
4. Введите код активации в соответствующие поля и нажмите на кнопку **Далее**.

   Kaspersky CRYSTAL отправит данные на сервер активации для проверки. Если проверка завершится успешно, мастер активации автоматически перейдет на следующий шаг.
5. По завершении работы мастера нажмите на кнопку **Завершить**.

РАБОТА С УВЕДОМЛЕНИЯМИ 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 для обеспечения безопасности компьютера (например, об обнаружении вредоносного объекта или опасной активности в системе). Окна критических уведомлений и всплывающих сообщений – красные.
- *Важные* – информируют о событиях, потенциально важных для обеспечения безопасности компьютера (например, об обнаружении возможно зараженного объекта или подозрительной активности в системе). Окна важных уведомлений и всплывающих сообщений – желтые.
- *Информационные* – информируют о событиях, не имеющих первостепенной важности для обеспечения безопасности компьютера. Окна информационных уведомлений и всплывающих сообщений – зеленые.

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

Анализ состояния защиты компьютера и устранение проблем безопасности

О появлении проблем в защите компьютера сигнализирует цветовая индикация главного окна Kaspersky CRYSTAL (см. рис. ниже). 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. Рекомендуется немедленно решать проблемы безопасности и немедленно устранять угрозы.

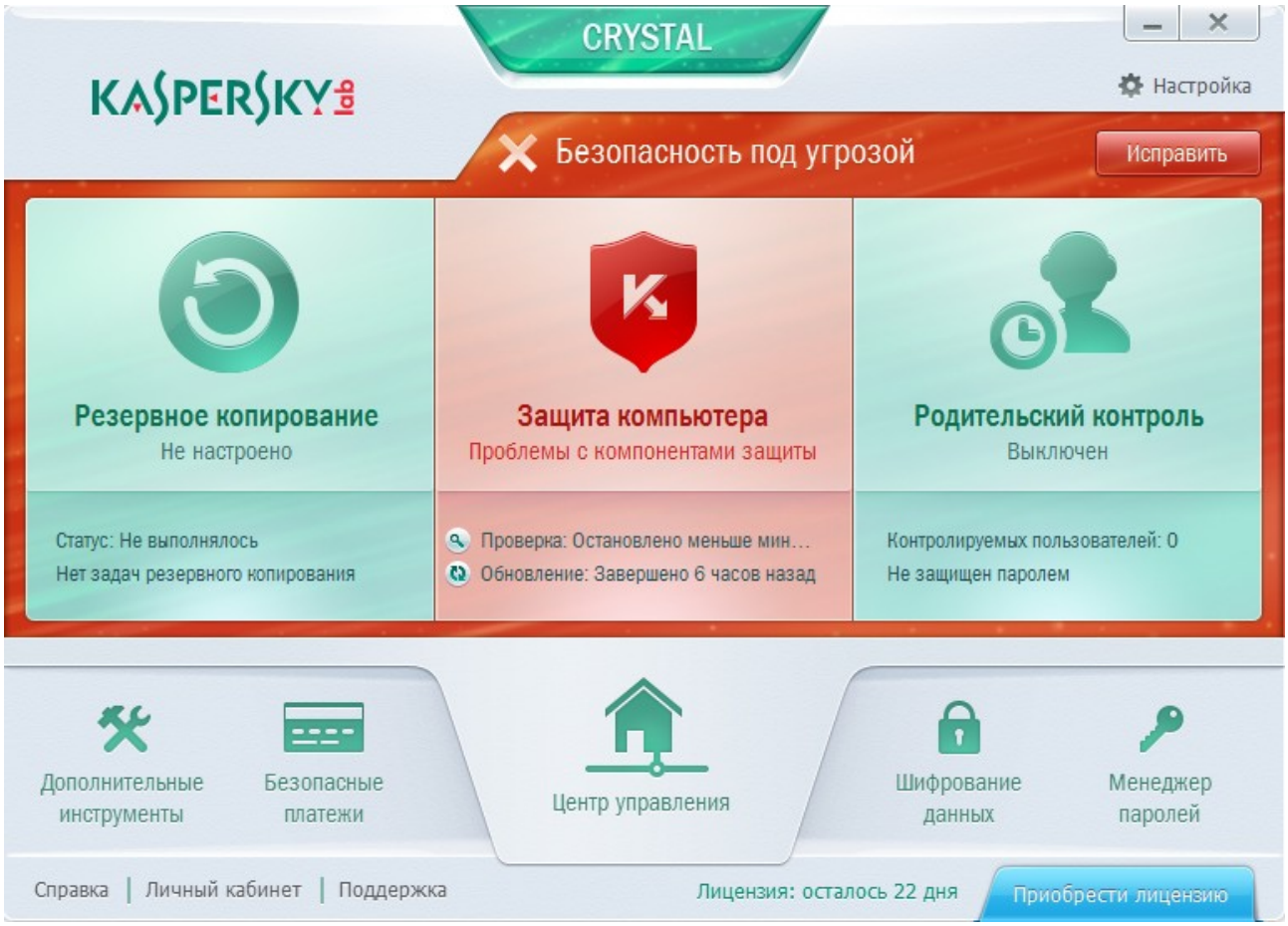

Рисунок 1. Красная цветовая индикация главного окна

При наличии проблем безопасности компьютера на индикаторе состояния защиты в правой верхней части главного окна программы отображается кнопка **Исправить** (см. рис. выше). Нажав на кнопку **Исправить**, вы можете открыть окно **Проблемы безопасности** (см. рис. ниже), в котором приведена подробная информация о состоянии защиты компьютера и предложены варианты действий для решения проблем безопасности и устранения угроз.

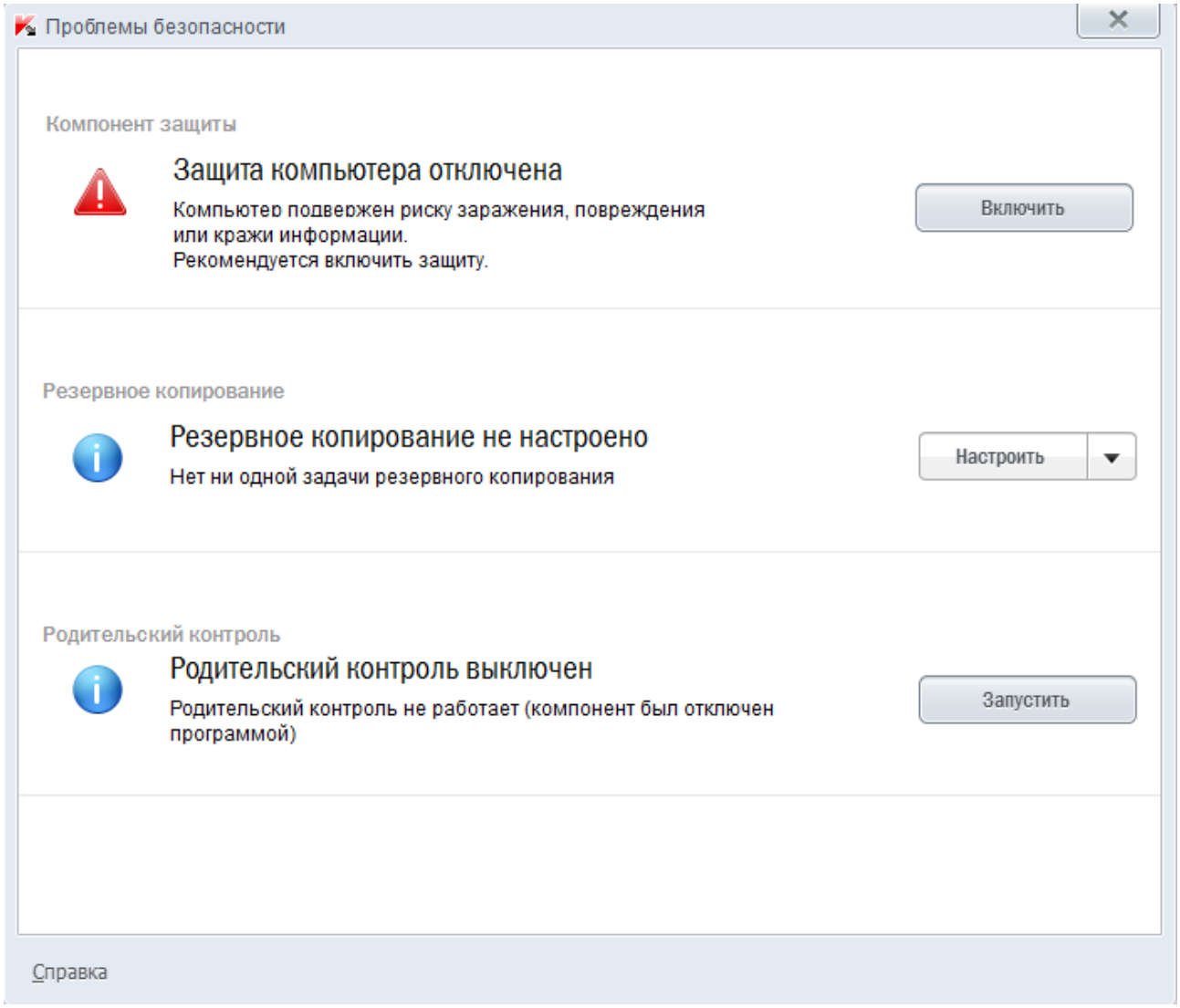

*Рисунок 2. Окно **Проблемы безопасности***

Проблемы в защите сгруппированы по категориям, к которым они относятся. Для каждой проблемы приведены действия, которые вы можете предпринять, чтобы решить проблему.

Проверить состояние защиты на других компьютерах домашней сети можно с помощью Центра управления (см. раздел «Удаленное управление защитой домашней сети» на стр. 45).

Обновление баз и модулей программы

По умолчанию Kaspersky CRYSTAL автоматически проверяет наличие обновлений на серверах обновлений «Лаборатории Касперского». Если на сервере содержится набор последних обновлений, Kaspersky CRYSTAL загружает и устанавливает их в фоновом режиме. Вы можете в любой момент запустить обновление Kaspersky CRYSTAL вручную из главного окна программы или из контекстного меню значка программы в области уведомлений панели задач.

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

- *Чтобы запустить обновление из контекстного меню значка программы в области уведомлений панели задач,*

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

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

  1. Откройте главное окно программы.
  2. В блоке **Защита компьютера** по ссылке **Обновление** запустите обновление баз.

Проверка важных областей компьютера на вирусы

Под проверкой важных областей подразумевается проверка следующих объектов:

- объектов, которые загружаются при запуске операционной системы;
- системной памяти;
- загрузочных секторов диска.

- *Чтобы запустить проверку важных областей 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 **Проверка важных областей** нажмите на кнопку  .

Полная проверка компьютера на вирусы

Во время полной проверки по умолчанию Kaspersky CRYSTAL проверяет следующие объекты:

- системную память;
- объекты, которые загружаются при старте операционной системы;
- резервное хранилище системы;
- жесткие и съемные диски.

Рекомендуется выполнить полную проверку сразу после установки Kaspersky CRYSTAL на компьютер.

- *Чтобы запустить полную проверку из главного окна программы, выполните следующие действия:*

  1. Откройте главное окно программы.
  2. В блоке **Защита компьютера** по ссылке **Проверка** откройте список задач проверки.
  3. По ссылке **Полная проверка** запустите полную проверку.

ПРОВЕРКА НА ВИРУСЫ ФАЙЛА, ПАПКИ, ДИСКА ИЛИ ДРУГОГО ОБЪЕКТА

Проверить на вирусы отдельный объект вы можете следующими способами:

- из контекстного меню объекта;
- из главного окна программы.

Чтобы запустить проверку 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. рис. ниже) и выберите пункт **Проверить на вирусы**.

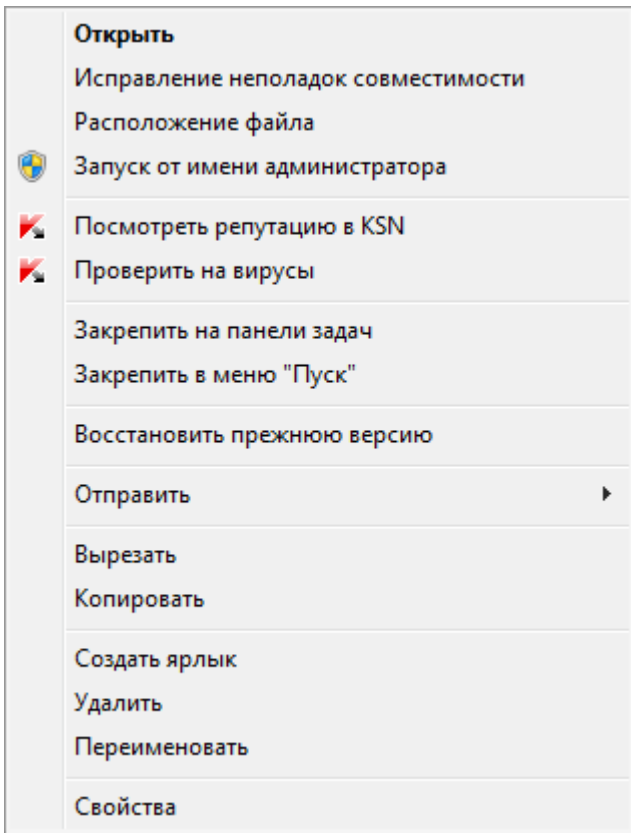

Рисунок 3. Контекстное меню исполняемого файла

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. Укажите объект, который нужно проверить, одним из следующих способов:
   - По ссылке **укажите**, расположенной в нижней правой части окна, откройте окно **Выборочная проверка** и установите флажки напротив папок и дисков, которые нужно проверить.

     Если в окне отсутствует объект, который требуется проверить, выполните следующие действия:

a. По ссылке **Добавить** в левой нижней части окна откройте окно **Выбор объекта для проверки**.

b. В открывшемся окне **Выбор объекта для проверки** выберите объект для проверки.

- Перетащите объект для проверки в предназначенную для этого область (см. рисунок ниже).

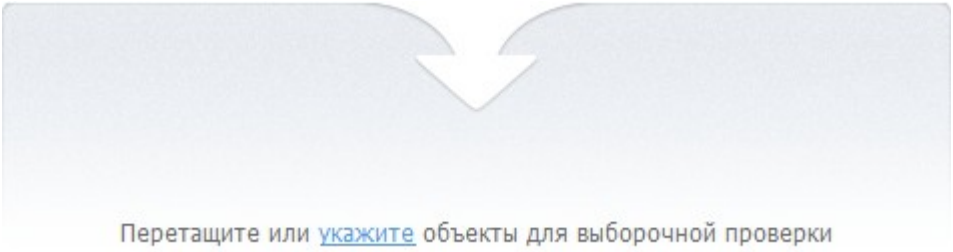

*Рисунок 4. Область раздела **Проверка**, в которую нужно перетащить объект для проверки*

Проверка компьютера 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 уязвимостей позволяет найти такие «слабые места» в защите компьютера. Найденные уязвимости рекомендуется устранить.

Чтобы запустить поиск уязвимостей 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 открывшемся окне в блоке **Поиск уязвимостей** нажмите на кнопку  .

Восстановление удаленного или вылеченного программой файла

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

Для восстановления удаленного или вылеченного файла используется его резервная копия, созданная программой в ходе проверки файла.

Чтобы восстановить удаленный или вылеченный программой файл, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Защита компьютера**.
2. В левой части открывшегося окна перейдите по ссылке **Карантин: <количество файлов>** (см. рис. ниже).

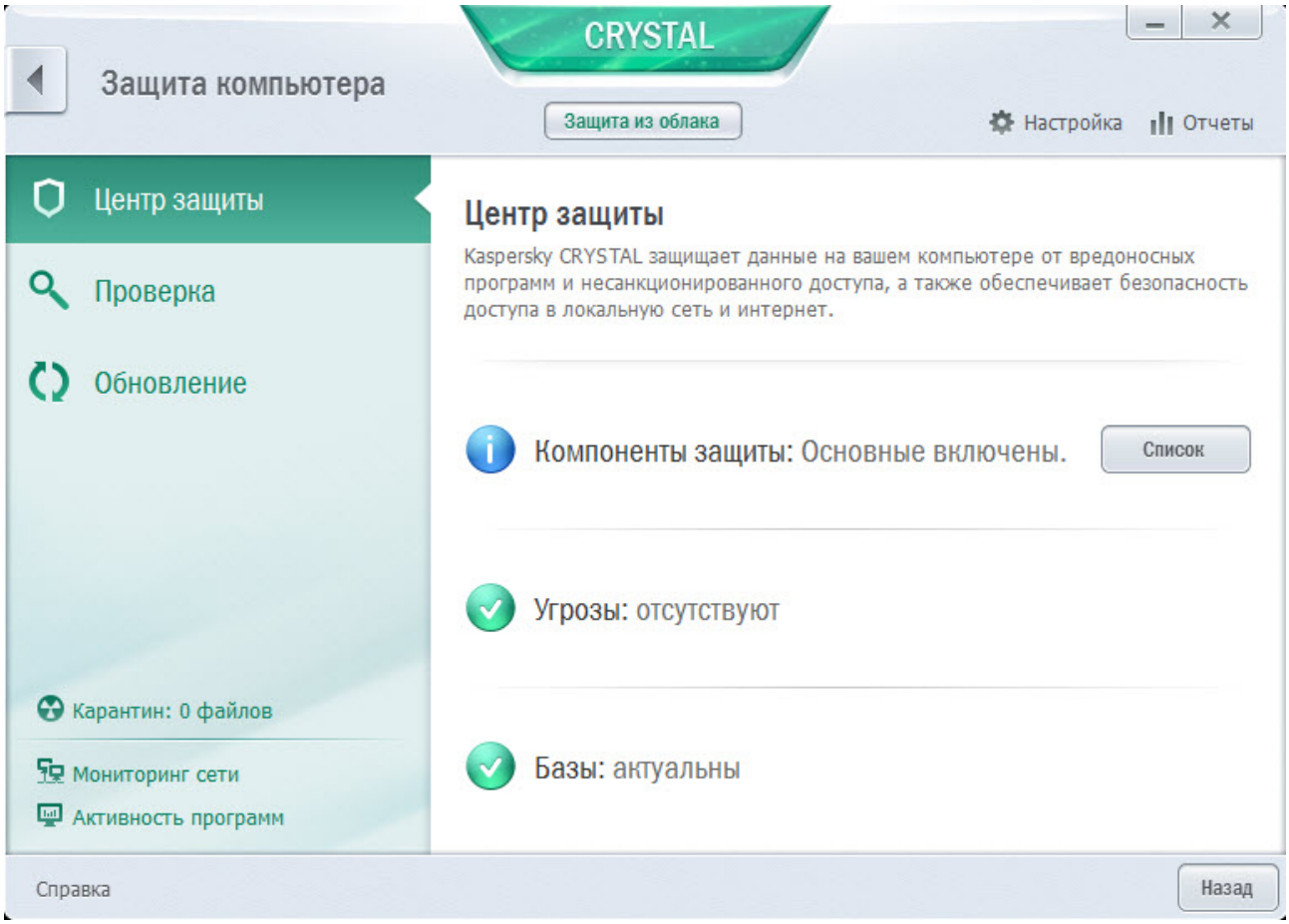

*Рисунок 5. Окно **Защита компьютера***

3. В открывшемся окне **Карантин** выберите нужный файл в списке и нажмите на кнопку **Восстановить** (см. рис. ниже).

Kaspersky CRYSTAL восстанавливает указанный файл в папку, в которой находился удаленный и вылеченный программой файл.

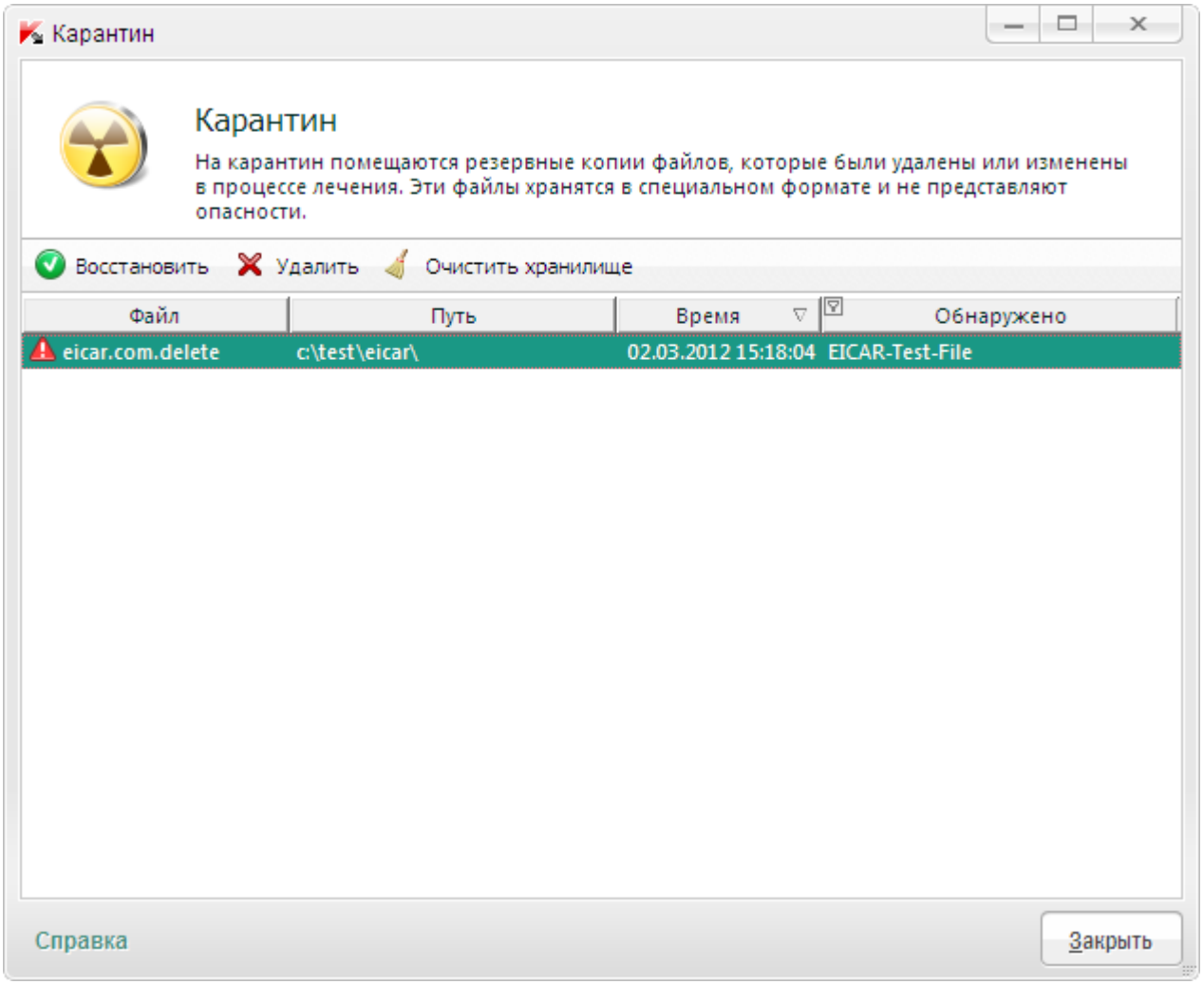

*Рисунок 6. Окно **Карантин***

Восстановление операционной системы после заражения

Если вы подозреваете, что операционная система вашего компьютера была повреждена или изменена в результате действий вредоносных программ или системного сбоя, используйте м*астер восстановления после заражения*, 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 тому подобное. Причины появления таких повреждений различны. Это могут быть активность вредоносных программ, неправильная настройка системы, системные сбои или применение неправильно работающих программ – оптимизаторов системы.

После 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.

Чтобы запустить мастер восстановления системы, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна выберите раздел **Дополнительные инструменты**.
3. В открывшемся окне в блоке **Восстановление после заражения** нажмите на кнопку **Выполнить**.

   Откроется окно мастера восстановления системы.

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**.

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 завершении 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 специалисты «Лаборатории Касперского» предлагают 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 представляют 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 действия, выбранные на предыдущем шаге. 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.

Блокирование нежелательной почты (спама)

Если вы получаете большое количество нежелательной почты (спама), включите компонент Анти-Спам и установите для него рекомендуемый уровень безопасности.

- *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 **Защита** компонент **Анти-Спам**.
4. В правой части окна установите флажок **Включить Анти-Спам**.
5. Убедитесь, что в блоке **Уровень безопасности** установлен уровень безопасности **Рекомендуемый**.

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

Проверка почты и фильтрация вложений в почтовых сообщениях

Kaspersky CRYSTAL позволяет проверять сообщения электронной почты на наличие в них опасных объектов с помощью Почтового Антивируса. Почтовый Антивирус запускается при старте операционной системы, постоянно находится в оперативной памяти компьютера и проверяет почтовые сообщения, получаемые или отправляемые по протоколам POP3, SMTP, IMAP, MAPI и NNTP (в том числе через защищенные соединения (SSL) по протоколам POP3, SMTP и IMAP).

По умолчанию Почтовый Антивирус проверяет как входящие, так и исходящие сообщения. При необходимости вы можете включить проверку только входящих сообщений.

- *Чтобы проверять только входящие сообщения, 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 нажмите на кнопку **Настройка**.

   Откроется окно **Почтовый Антивирус**.
5. В открывшемся окне на закладке **Общие** в блоке **Область защиты** выберите вариант **Только входящие сообщения**.

Если угрозы в почтовом сообщении не обнаружены или зараженные объекты были успешно вылечены, почтовое сообщение становится доступным для работы. Если зараженный объект вылечить не удалось, Почтовый Антивирус переименовывает или удаляет объект из сообщения и помещает в тему сообщения уведомление о том, что оно обработано Kaspersky CRYSTAL. В случае удаления объекта Kaspersky CRYSTAL создает его резервную копию и помещает на карантин.

Вредоносные программы могут распространяться в виде вложений в почтовые сообщения. Вы можете включить фильтрацию вложений в почтовых сообщениях. Фильтрация позволяет автоматически переименовывать или удалять вложенные файлы указанных вами типов.

Чтобы включить фильтрацию вложений в почтовых 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 **Почтовый Антивирус**.
4. В правой части окна нажмите на кнопку **Настройка**.

   Откроется окно **Почтовый Антивирус**.
5. В открывшемся окне на закладке **Фильтр вложений** выберите режим фильтрации вложений (**Переименовывать вложения указанных типов** или **Удалять вложения указанных типов**).
6. В списке типов файлов (расширений) выберите типы вложений, которые нужно фильтровать.

   Если вы хотите добавить маску нового типа файлов, выполните следующие действия:

   a. По ссылке **Добавить** в нижней части окна откройте окно **Маска имени файла**.

   b. В открывшемся окне введите нужную маску типа файлов.
7. В окне **Настройка** нажмите на кнопку **Применить**.

ОПРЕДЕЛЕНИЕ БЕЗОПАСНОСТИ ВЕБ-САЙТА

Kaspersky CRYSTAL позволяет проверить безопасность веб-сайта, прежде чем перейти по ссылке на этот веб-сайт. Для этого используется *модуль проверки ссылок*.

Модуль проверки ссылок недоступен в браузере Microsoft Internet Explorer 10 в стиле Metro, а также в браузере Miscrosoft Internet Explorer 10, если в параметрах браузера установлен флажок **Включить расширенный защищенный режим** (Enhanced Protected Mode).

Модуль проверки ссылок встраивается в браузеры Microsoft Internet Explorer, Google Chrome™ и Mozilla™ Firefox™ и проверяет ссылки на открытой в браузере веб-странице. Рядом с каждой ссылкой Kaspersky CRYSTAL отображает один из следующих значков:

-  – если веб-страница, которая открывается по ссылке, безопасна по данным «Лаборатории Касперского»;
-  – если нет информации о безопасности веб-страницы, которая открывается по ссылке;
-  – если веб-страница, которая открывается по ссылке, опасна по данным «Лаборатории Касперского».

При наведении курсора мыши на значок отображается всплывающее окно с более подробным описанием ссылки.

По умолчанию Kaspersky CRYSTAL проверяет ссылки только в результатах поиска. Вы можете включить проверку ссылок на любом веб-сайте.

Чтобы включить проверку ссылок на любом веб-сайте, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В открывшемся окне **Настройка** в разделе **Центр защиты** выберите подраздел **Веб-Антивирус** и нажмите на кнопку **Настройка**.

   Откроется окно **Веб-Антивирус**.
4. В открывшемся окне на закладке **Веб-фильтр** в блоке **Модуль проверки ссылок** нажмите на кнопку **Настройка**.

   Откроется окно **Настройка модуля проверки ссылок**.
5. В открывшемся окне в блоке **Режим проверки** выберите вариант **Любые ссылки**.
6. В окне **Настройка** нажмите на кнопку **Применить**.

Блокирование доступа к веб-сайтам разных регионов

По статистике «Лаборатории Касперского» уровень зараженности веб-сайтов в разных странах различается. Kaspersky CRYSTAL позволяет запретить доступ к веб-сайтам, принадлежащим к региональным доменам с высокой степенью зараженности, с помощью компонента Гео-фильтр.

При включенном Гео-фильтре Kaspersky CRYSTAL в зависимости от вашего выбора разрешает или запрещает доступ к региональному домену, либо запрашивает разрешение на доступ.

Чтобы включить и настроить Гео-фильтр, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В открывшемся окне **Настройка** в разделе **Центр защиты** выберите подраздел **Веб-Антивирус** и нажмите на кнопку **Настройка**.

   Откроется окно **Веб-Антивирус**.
4. В открывшемся окне на закладке **Гео-фильтр** установите флажок **Включить фильтрацию по региональным доменам**.
5. В нижней части окна в списке контролируемых доменов укажите, к каким доменам следует разрешать или запрещать доступ, либо запрашивать разрешение на доступ.
6. В окне **Настройка** нажмите на кнопку **Применить**.

Удаленное управление защитой домашней сети

Для удаленного управления программой Kaspersky CRYSTAL, установленной на компьютерах домашней сети, с рабочего места администратора предназначен компонент Центр управления.

С помощью Центра управления вы можете решать следующие задачи по обеспечению безопасности домашней сети:

- просматривать перечень проблем безопасности на отдельном компьютере сети и удаленно устранять некоторые из них;
- проверять на вирусы одновременно несколько компьютеров домашней сети;
- обновлять базы одновременно на нескольких компьютерах домашней сети.

Чтобы просмотреть перечень проблем безопасности на отдельном компьютере сети, выполните следующие действия:

1. Откройте главное окно программы и в нижней части окна нажмите на кнопку **Центр управления**.
2. В верхней части открывшегося окна **Центр управления** выберите компьютер, для которого нужно показать список проблем, и перейдите в раздел **Информация**.
3. В правой части окна в разделе **Проблемы** нажмите на кнопку **Список**.

   Откроется окно **Проблемы безопасности**, в котором отображается информация о проблемах безопасности на выбранном компьютере.

Чтобы проверить на вирусы несколько компьютеров сети, выполните следующие действия:

1. Откройте главное окно программы и в нижней части окна нажмите на кнопку **Центр управления**.

   Откроется окно **Центр управления**.
2. По ссылке **Проверить на вирусы** откройте окно **Групповой запуск проверки**.
3. В окне **Групповой запуск проверки** выберите закладку с нужным типом проверки (**Полная проверка** или **Проверка важных областей**).
4. Выберите компьютеры, которые вы хотите проверить, и нажмите на кнопку **Запустить проверку**.

Чтобы обновить базы одновременно на нескольких компьютерах сети, выполните следующие действия:

1. Откройте главное окно программы и в нижней части окна нажмите на кнопку **Центр управления**.

   Откроется окно **Центр управления**.
2. По ссылке **Обновить базы** откройте окно **Групповой запуск обновления**.
3. В окне **Групповой запуск обновления** выберите компьютеры, на которых вы хотите обновить базы, и нажмите на кнопку **Запустить обновление**.

Работа с неизвестными программами

С помощью Kaspersky CRYSTAL вы сможете снизить риски, связанные с использованием неизвестных программ (например, риски заражения компьютера вирусами и нежелательного изменения параметров операционной системы).

В состав Kaspersky CRYSTAL входят компоненты и инструменты, позволяющие проверить репутацию программы и запустить программу в безопасной среде, изолированной от операционной системы.

Контроль действий программы на компьютере и в сети

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 активность, от которой может зависеть безопасность компьютера, в том числе доступ программ к защищаемым ресурсам (например, файлам, папкам, ключам реестра, сетевым адресам).

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 (Доверенные, Недоверенные, Сильные ограничения или Слабые ограничения). Группа определяет правила, которые Kaspersky CRYSTAL будет применять для контроля активности этой программы.

Вы можете изменить правила контроля действий программы вручную.

Чтобы изменить правила контроля программы вручную, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В открывшемся окне **Настройка** в разделе **Центр защиты** выберите подраздел **Контроль программ**.
4. В правой части окна в блоке **Настройка правил для программ, защита персональных данных и других ресурсов** нажмите на кнопку **Программы**.
5. В открывшемся окне **Программы** выберите нужную программу в списке и нажмите на кнопку **Изменить**.
6. В открывшемся окне **Правила программы** задайте правила контроля программы:
   - Чтобы настроить правила доступа программы к ресурсам операционной системы, выполните следующие действия:
     a. На закладке **Файлы и системный реестр** выберите нужную категорию ресурсов.
     b. По правой клавише мыши в графе с возможным действием над ресурсом (**Чтение**, **Запись**, **Удаление** или **Создание**) откройте контекстное меню и выберите в нем нужное значение (**Разрешить**, **Запретить** или **Запросить действие**).
   - Чтобы настроить права программы на выполнение различных действий в операционной системе, выполните следующие действия:
     a. На закладке **Права** выберите нужную категорию прав.
     b. По правой клавише мыши в графе **Разрешение** откройте контекстное меню и выберите в нем нужное значение (**Разрешить**, **Запретить** или **Запросить действие**).

- Чтобы настроить права программы на выполнение различных действий в сети, выполните следующие действия:

  a. На закладке **Сетевые правила** нажмите на кнопку **Добавить**.

     Откроется окно **Сетевое правило**.

  b. В открывшемся окне задайте нужные параметры правила и нажмите на кнопку **ОК**.

  c. Назначьте приоритет нового правила, переместив его вверх или вниз по списку с помощью кнопок **Вверх** и **Вниз**.

- Чтобы исключить некоторые действия из проверки Контролем программ, на закладке **Исключения** установите флажки для действий, которые не нужно контролировать.

  Все исключения, созданные в правилах программ, доступны в окне настройки программы в разделе **Угрозы и исключения**.

7. В окне **Настройка** нажмите на кнопку **Применить**.

ПРОВЕРКА РЕПУТАЦИИ ПРОГРАММЫ

Kaspersky CRYSTAL позволяет проверять репутацию программ у пользователей во всем мире. В состав репутации программы входят следующие показатели:

- название производителя;
- информация о цифровой подписи (доступно при наличии цифровой подписи);
- информация о группе, в которую программа помещена Контролем программ или большинством пользователей Kaspersky Security Network;
- количество пользователей Kaspersky Security Network, использующих программу (доступно, если программа отнесена к группе Доверенные в базе Kaspersky Security Network);
- время, когда программа стала известна в Kaspersky Security Network;
- страны, в которых программа наиболее всего распространена.

Проверка репутации программ доступна, если вы согласились участвовать в Kaspersky Security Network.

Чтобы узнать репутацию программы,

в контекстном меню исполняемого файла программы выберите пункт **Посмотреть репутацию в KSN** (см. рис. ниже).

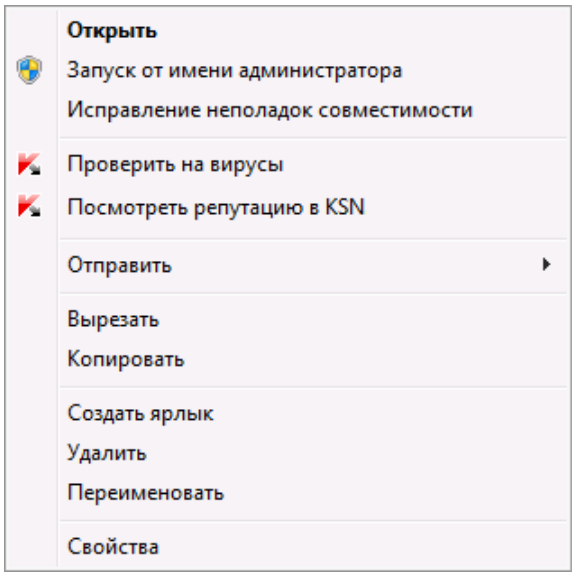

Рисунок 7. Контекстное меню исполняемого файла в Microsoft Windows

Откроется окно со сведениями о репутации программы в KSN.

Защита личных данных от кражи

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

- 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 данных при использовании сервисов интернет-банкинга и при оплате покупок в интернет-магазинах предназначены функции Безопасных платежей.

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, Защита ввода данных с аппаратной клавиатуры и Менеджер паролей.

Для защиты файлов от несанкционированного доступа предназначено Шифрование данных.

Для удаления информации о действиях пользователя на компьютере предназначен мастер устранения следов активности.

В ЭТОМ РАЗДЕЛЕ

БЕЗОПАСНЫЕ ПЛАТЕЖИ

Для защиты конфиденциальных данных, которые вы вводите на веб-сайтах банков и платежных систем (например, номера банковской карты, пароля для доступа к сервисам интернет-банкинга), а также для предотвращения кражи платежных средств при проведении платежей онлайн Kaspersky CRYSTAL предлагает открывать такие веб-сайты в защищенном браузере.

Запуск защищенного браузера невозможен, если снят флажок **Включить самозащиту** в разделе **Дополнительные параметры**, подраздел **Самозащита** окна настройки программы.

Вы можете настроить Безопасные платежи для автоматического определения веб-сайтов банков и платежных систем.

Безопасные платежи недоступны в браузере Microsoft Internet Explorer 10 в стиле Metro, а также в браузере Microsoft Internet Explorer 10, если в параметрах браузера установлен флажок **Включить расширенный защищенный режим** (Enhanced Protected Mode). Вы можете запустить режим безопасного браузера из интерфейса Kaspersky CRYSTAL.

Чтобы настроить Безопасные платежи, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В открывшемся окне **Настройка** в разделе **Центр защиты** выберите подраздел **Безопасные платежи**.
4. Установите флажок **Включить Безопасные платежи**.
5. Чтобы включить уведомление об уязвимостях, обнаруженных в операционной системе перед запуском защищенного браузера, установите флажок **Уведомлять об уязвимостях в операционной системе**.
6. Чтобы настроить Безопасные платежи для определенного веб-сайта, выполните следующие действия:

   a. В списке **Веб-сайты банков и платежных систем** нажмите на кнопку **Добавить**.

      Откроется окно **Веб-сайт для Безопасных платежей**.

b. В открывшемся окне в поле **Веб-сайт банка или платежной системы** введите адрес веб-сайта, который нужно открывать в защищенном браузере.

> Перед адресом веб-сайта должен быть указан протокол https://, по умолчанию используемый защищенным браузером.

c. При необходимости в поле **Описание** введите название или описание этого веб-сайта.

d. Выберите способ запуска защищенного браузера при открытии этого веб-сайта:

- Если вы хотите, чтобы Kaspersky CRYSTAL предлагал запустить безопасный браузер каждый раз при открытии этого веб-сайта, выберите вариант **Запрашивать действие**.
- Если вы хотите, чтобы Kaspersky CRYSTAL автоматически открывал этот веб-сайт в защищенном браузере, выберите вариант **Запускать защищенный браузер автоматически**.
- Если вы хотите выключить Безопасные платежи для этого веб-сайта, выберите вариант **Не запускать защищенный браузер**.

7. В окне **Настройка** нажмите на кнопку **Применить**.

Защита от фишинга

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

Вы можете настроить дополнительные параметры защиты от фишинга при работе компонентов Веб-Антивирус и IM-Антивирус.

Чтобы настроить защиту от фишинга при работе Веб-Антивируса, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В открывшемся окне **Настройка** в разделе **Защита** выберите подраздел **Веб-Антивирус** и нажмите на кнопку **Настройка**.

   Откроется окно **Веб-Антивирус**.
4. В открывшемся окне на закладке **Общие** в блоке **Проверка ссылок** установите флажок **Проверять веб-страницы на наличие фишинга**.
5. Если вы хотите, чтобы Анти-Фишинг использовал эвристический анализ при проверке веб-страниц, нажмите на кнопку **Дополнительно**.

   Откроется окно **Настройка Анти-Фишинга**.
6. В открывшемся окне установите флажок **Использовать эвристический анализ для проверки веб-страниц на наличие фишинга** и задайте уровень детализации проверки.
7. В окне **Настройка** нажмите на кнопку **Применить**.

Чтобы настроить защиту от фишинга при работе IM-Антивируса, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.

3. В открывшемся окне **Настройка** в разделе **Защита** выберите подраздел **IM-Антивирус**.

4. В правой части окна в блоке **Методы проверки** установите флажок **Проверять ссылки по базе фишинговых веб-адресов**.

5. В окне **Настройка** нажмите на кнопку **Применить**.

ИСПОЛЬЗОВАНИЕ ВИРТУАЛЬНОЙ КЛАВИАТУРЫ

При работе в интернете часто возникают ситуации, когда необходимо указать персональные данные, а также имя пользователя и пароль. Это происходит, например, при регистрации на веб-сайтах, при совершении покупок в интернет-магазинах, при использовании интернет-банкинга.

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

Виртуальная клавиатура позволяет избежать перехвата данных, вводимых с клавиатуры.

Виртуальная клавиатура защищает от перехвата персональной информации только при работе с интернет-браузерами Microsoft Internet Explorer, Mozilla Firefox и Google Chrome. При работе с другими интернет-браузерами виртуальная клавиатура не защищает вводимые персональные данные от перехвата.

Виртуальная клавиатура недоступна в браузере Microsoft Internet Explorer 10 в стиле Metro, а также в браузере Miscrosoft Internet Explorer 10, если в параметрах браузера установлен флажок **Включить расширенный защищенный режим** (Enhanced Protected Mode). В этом случае рекомендуется вызывать виртуальную клавиатуру из интерфейса Kaspersky CRYSTAL.

Виртуальная клавиатура не может защитить ваши персональные данные в случае взлома веб-сайта, требующего ввода таких данных, поскольку в этом 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 экрана.

Виртуальная клавиатура не предотвращает снятие снимков экрана с помощью нажатия клавиши **Print Screen** и других комбинаций клавиш, заданных в параметрах операционной системы, а также снятие снимков экрана с помощью технологии DirectX.

Виртуальная клавиатура имеет следующие особенности:

- На клавиши виртуальной клавиатуры нужно нажимать с помощью мыши.

- В отличие от настоящей клавиатуры, на виртуальной клавиатуре невозможно одновременно нажать несколько клавиш. Поэтому, чтобы использовать комбинации клавиш (например, **ALT**+**F4**), нужно сначала нажать на первую клавишу (например, **ALT**), затем на следующую (например, **F4**), а затем повторно нажать на первую клавишу. Повторное нажатие заменяет отпускание клавиши на настоящей клавиатуре.

- На виртуальной клавиатуре язык ввода переключается с помощью того же сочетания клавиш, которое установлено в параметрах операционной системы для обычной клавиатуры. При этом на вторую клавишу нужно нажимать правой клавишей мыши (например, если в параметрах операционной системы для переключения языка ввода задана комбинация **LEFT ALT**+**SHIFT**, то на клавишу **LEFT ALT** нужно нажимать левой клавишей мыши, а на клавишу **SHIFT** нужно нажимать правой клавишей мыши).

Для защиты данных, вводимых с помощью виртуальной клавиатуры, после установки Kaspersky CRYSTAL необходимо перезагрузить компьютер.

Открыть виртуальную клавиатуру можно следующими способами:

- из контекстного меню значка программы в области уведомлений;
- из главного окна программы;
- из окна браузера Microsoft Internet Explorer, Mozilla Firefox или Google Chrome;
- с помощью значка быстрого вызова виртуальной клавиатуры в поле ввода на веб-сайтах;

  Отображение значка быстрого вызова в полях ввода на веб-сайтах можно настроить.

- с помощью комбинации клавиш аппаратной клавиатуры.

Чтобы открыть виртуальную клавиатуру из контекстного меню значка программы в области уведомлений,

выберите пункт **Инструменты** → **Виртуальная клавиатура** в контекстном меню значка программы (см. рис. ниже).

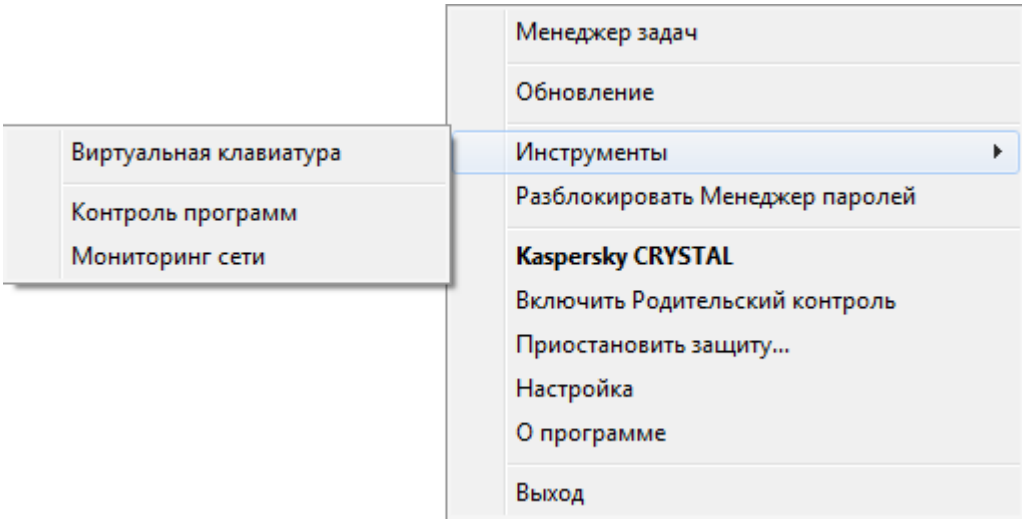

Рисунок 8. Контекстное меню значка Kaspersky CRYSTAL

Чтобы открыть виртуальную клавиатуру из главного окна программы, выполните следующие действия:

1. В нижней части главного окна программы выберите раздел **Менеджер паролей**.
2. В нижней части открывшегося окна нажмите на кнопку **Виртуальная клавиатура**.

Чтобы открыть виртуальную клавиатуру из окна браузера,

нажмите на кнопку  **Виртуальная клавиатура** в панели инструментов браузера Microsoft Internet Explorer, Mozilla Firefox или Google Chrome.

Чтобы открыть виртуальную клавиатуру с помощью компьютерной клавиатуры,

нажмите комбинацию клавиш **CTRL**+**ALT**+**SHIFT**+**P**.

Чтобы настроить отображение значка быстрого вызова виртуальной клавиатуры в полях ввода на веб-сайтах, выполните следующие действия:

1. Откройте главное окно программы.

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

3. В открывшемся окне **Настройка** в разделе **Центр защиты** выберите подраздел **Безопасный ввод данных**.

4. В правой части окна в блоке **Виртуальная клавиатура** установите флажок **Показывать значок быстрого вызова в полях ввода** и нажмите на кнопку **Настройка**.

   Откроется окно **Виртуальная клавиатура**.

5. В открывшемся окне задайте правила отображения значка быстрого вызова:

   - На закладке **Категории** установите флажки для категорий веб-сайтов, на которых нужно отображать значок быстрого вызова в полях ввода.

   - Если вы хотите, чтобы значок быстрого вызова отображался в полях ввода на тех веб-сайтах, которые открываются в защищенном браузере при работе в режиме Безопасных платежей, на закладке **Категории** установите флажок **Показывать значок быстрого вызова в полях ввода Безопасных платежей**.

   - Если вы хотите включить отображение значка быстрого вызова в полях ввода на определенном веб-сайте, выполните следующие действия:

     a. На закладке **Исключения** в списке **Показывать значок быстрого вызова на веб-сайтах** нажмите на кнопку **Добавить**.

        Откроется окно **Показывать значок быстрого вызова**.

     b. В открывшемся окне введите адрес веб-сайта в поле **Веб-адрес** и выберите один из вариантов отображения значка быстрого вызова на этом веб-сайте (**Показывать значок только на указанной веб-странице** или **Показывать значок на всем веб-сайте**).

6. В окне **Настройка** нажмите на кнопку **Применить**.

ЗАЩИТА ВВОДА ДАННЫХ С АППАРАТНОЙ КЛАВИАТУРЫ

При работе в интернете часто возникают ситуации, когда необходимо указать персональные данные, а также имя пользователя и пароль. Это происходит, например, при регистрации на веб-сайтах, совершении покупок в интернет-магазинах, использовании интернет-банкинга.

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

Защита ввода данных с аппаратной клавиатуры позволяет избежать перехвата данных, вводимых с клавиатуры.

Защита ввода данных с аппаратной клавиатуры работает только в интернет-браузерах Microsoft Internet Explorer, Mozilla Firefox и Google Chrome. При работе с другими интернет-браузерами данные, вводимые с аппаратной клавиатуры, не защищаются от перехвата.

Защита ввода данных недоступна в браузере Microsoft Internet Explorer 10 в стиле Metro, а также в браузере Microsoft Internet Explorer 10, если в параметрах браузера установлен флажок **Включить расширенный защищенный режим** (Enhanced Protected Mode).

Защита ввода данных с аппаратной клавиатуры не может защитить ваши персональные данные в случае взлома веб-сайта, требующего ввода таких данных, поскольку в этом случае информация попадет непосредственно в руки злоумышленников.

Вы можете настроить защиту ввода данных с клавиатуры на разных веб-сайтах. После того как защита ввода данных с клавиатуры настроена, не требуется выполнять дополнительные действия при вводе данных.

Для защиты ввода данных с аппаратной клавиатуры после установки Kaspersky CRYSTAL необходимо перезагрузить компьютер.

Чтобы настроить защиту ввода данных с клавиатуры, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В открывшемся окне **Настройка** в разделе **Центр защиты** выберите подраздел **Безопасный ввод данных**.
4. В правой части окна в блоке **Защита ввода данных с аппаратной клавиатуры** установите флажок **Защищать ввод данных с аппаратной клавиатуры** и нажмите на кнопку **Настройка**.

   Откроется окно **Защита ввода с клавиатуры**.
5. В открывшемся окне задайте область защиты ввода данных с аппаратной клавиатуры:

   - На закладке **Категории** установите флажки для категорий веб-сайтов, на которых нужно защищать данные, вводимые с клавиатуры.
   - Если вы хотите, чтобы ввод данных с клавиатуры был защищен на тех веб-сайтах, которые открываются в защищенном браузере в режиме Безопасных платежей, на закладке **Категории** установите флажок **Защищать ввод данных с клавиатуры для Безопасных платежей**.
   - Если вы хотите, чтобы ввод данных с клавиатуры был защищен в полях для ввода паролей на всех веб-сайтах, на закладке **Категории** установите флажок **Защищать поля для ввода паролей на всех веб-сайтах**.
   - Если вы хотите включить защиту ввода данных с клавиатуры на определенном веб-сайте, выполните следующие действия:

     a. На закладке **Исключения** в списке **Защищать ввод данных с клавиатуры на веб-сайтах** нажмите на кнопку **Добавить**.

        Откроется окно **Защищаемый веб-сайт**.

     b. В открывшемся окне введите адрес веб-сайта в поле **Веб-адрес** и выберите один из вариантов защиты ввода данных на этом веб-сайте (**Включить защиту только на указанной веб-странице** или **Включить защиту на всем веб-сайте**).
6. В окне **Настройка** нажмите на кнопку **Применить**.

Защита паролей

Kaspersky CRYSTAL сохраняет и защищает ваши персональные данные (например, пароли, имена пользователей, контактные данные, финансовую информацию). Kaspersky CRYSTAL связывает пароли и учетные записи с приложениями или веб-сайтами, для авторизации на которых они используются. Персональные данные содержатся в зашифрованном виде в хранилище, доступ к которому защищен мастер-паролем. Если хранилище разблокировано, вы легко можете получить доступ к своим паролям и данным. Kaspersky CRYSTAL позволяет быстро и удобно вводить пароль, имя пользователя и другие персональные данные при авторизации на веб-сайтах или в приложениях, а также производить автоматическую авторизацию.

Вы можете получить доступ к своим персональным данным с любого из ваших устройств, на котором установлена программа и есть подключение к интернету. Если устройство не подключено к интернету, вы можете сохранять ваши пароли и данные на устройстве. Когда устройство получит доступ к интернету, Kaspersky CRYSTAL предложит вам синхронизировать ваши пароли и данные с хранилищем паролей на удаленных серверах.

Кроме того, вы можете использовать следующие функции Kaspersky CRYSTAL:

- создавать надежные пароли для учетных записей, используя Генератор паролей;
- синхронизировать актуальные пароли и личные данные на всех ваших устройствах, на которых установлен Kaspersky CRYSTAL.

В ЭТОМ РАЗДЕЛЕ

ДОБАВЛЕНИЕ УЧЕТНЫХ ДАННЫХ ДЛЯ АВТОМАТИЧЕСКОЙ АВТОРИЗАЦИИ

С помощью программы вы можете выполнять автоматическую авторизацию (ввод логина и пароля) на веб-сайтах и в приложениях. Для автоматической авторизации программа использует учетные записи.

Вы можете создавать учетные записи двух типов:

- учетные записи интернета, которые используются для авторизации на веб-сайтах;
- учетные записи приложений, которые используются для авторизации в приложениях, например, в почтовом клиенте.

Чтобы добавить новую учетную запись интернета из главного окна Kaspersky CRYSTAL, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Менеджер паролей**.

   Откроется окно Менеджера паролей.

2. Нажмите на кнопку **Пароли и данные**.

   Отобразится содержимое хранилища паролей и данных.

3. Откройте раздел **Интернет** окна Менеджера паролей.

   В правой части окна появятся поля для указания данных учетной записи.

4. В верхней части окна в поле **Название учетной записи** введите название учетной записи. Нажмите на кнопку  .

   Название учетной записи будет сохранено.

5. В поле **Ссылка** укажите адрес веб-сайта, для авторизации на котором будет использоваться учетная запись.

6. В поле **Логин** введите логин для авторизации на веб-сайте.

7. В поле **Пароль** введите пароль учетной записи. Чтобы создать пароль автоматически, перейдите по ссылке **Генератор паролей**.

8. В нижней части окна нажмите на кнопку **Добавить**.

   Созданная учетная запись отобразится в списке учетных записей в разделе **Интернет**.

Чтобы добавить новую учетную запись приложения, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Менеджер паролей**.

   Откроется окно Менеджера паролей.

2. Нажмите на кнопку **Пароли и данные**.

   Отобразится содержимое хранилища паролей и данных.

3. Откройте раздел **Приложения**. Нажмите на кнопку **Добавить учетную запись приложения**.

4. В верхней части окна в поле **Название учетной записи** введите название учетной записи. Нажмите на кнопку  .

   Название учетной записи будет сохранено.

5. В поле **Приложение** укажите путь к исполняемому файлу приложения, для авторизации в котором будет использоваться учетная запись.

6. В поле **Логин** введите логин для авторизации в приложении.

7. В поле **Пароль** введите пароль учетной записи. Чтобы создать пароль автоматически, перейдите по ссылке **Генератор паролей**.

8. В нижней части окна нажмите на кнопку **Добавить**.

   Созданная учетная запись будет отображаться в списке учетных записей в разделе **Приложения**.

Использование генератора паролей

Безопасность данных напрямую зависит от надежности паролей. Данные могут быть подвержены риску в следующих случаях:

- для всех учетных записей используется один пароль;
- используются слишком простые пароли;
- в качестве пароля используется информация, которую легко угадать (например, имена членов семьи или даты их рождения).

Для обеспечения безопасности данных Kaspersky CRYSTAL 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.

Чтобы создать надежный пароль с помощью генератора паролей, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Менеджер паролей**.

   Откроется окно Менеджера паролей.

2. Нажмите на кнопку **Генератор паролей**.

   Также вы можете воспользоваться генератором паролей непосредственно во время указания пароля для учетной записи. Для вызова генератора паролей воспользуйтесь ссылкой **Генератор паролей** в области управления учетной записью рядом с полем ввода пароля.

3. В открывшемся окне **Генератор паролей** в поле **Длина пароля** задайте количество символов в пароле.

Длина пароля может составлять от 4 до 99 символов. Считается, что чем длиннее пароль, тем он надежнее.

4. При необходимости настройте дополнительные параметры генератора паролей, для чего в блоке **Дополнительные параметры** установите / снимите флажки рядом с нужными параметрами.

5. Нажмите на кнопку **Генерировать**.

   В поле **Пароль** отобразится созданный пароль.

ДОБАВЛЕНИЕ НОВОЙ ПАРЫ ЛОГИН-ПАРОЛЬ

Иногда требуется использовать несколько разных пар логин-пароль для авторизации на одном и том же веб-сайте / приложении. Например, вы можете использовать несколько почтовых ящиков на одном и том же почтовом сервере или нескольким пользователям одного компьютера может требоваться доступ к своим страницам в социальной сети. В этих случаях Kaspersky CRYSTAL позволяет создать одну учетную запись, связанную с нужным веб-сайтом или приложением, и указать для этой учетной записи несколько пар логин-пароль.

При загрузке указанного приложения или веб-сайта Kaspersky CRYSTAL предлагает выбрать нужную пару логин-пароль для заполнения полей регистрации.

Kaspersky CRYSTAL автоматически распознает новый логин при первом использовании и предлагает добавить его в учетную запись для этого приложения / веб-сайта. Вы можете вручную добавить новую пару логин-пароль для учетной записи, а затем изменить ее. Также вы можете использовать одну и ту же пару логин-пароль для разных учетных записей.

Чтобы добавить новую пару логин-пароль для учетной записи, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Менеджер паролей**.

   Откроется окно Менеджера паролей.

2. Нажмите на кнопку **Пароли и данные**.

   Отобразится содержимое хранилища паролей и данных.

3. Откройте раздел **Интернет** или **Приложения**, в зависимости от того, к какой учетной записи вы хотите добавить логин и пароль.

4. Выберите в списке нужную учетную запись и нажмите на кнопку  .

5. В открывшемся меню выберите пункт **Добавить логин**.

6. Введите логин в поле **Логин** и пароль в поле **Пароль**.

   Если вам нужно добавить логин и пароль, которые уже используются в других учетных записях, нажмите на кнопку  в поле **Логин**. В открывшемся окне **Выбор учетных записей для связывания** выберите учетную запись, содержащую нужный логин, и нажмите на кнопку **Связать**.

7. Если вы хотите, чтобы Менеджер паролей автоматически подставлял добавляемые логин и пароль на веб-сайте или в приложении, установите флажок **Автоматический вход** в нижней части области управления учетной записью.

   Если вам не нужно, чтобы Менеджер паролей автоматически подставлял логин и пароль в поля авторизации, снимите флажок **Автоматический вход**. В этом случае для использования автозаполнения вам нужно будет выбрать добавленные логин и пароль в контекстном меню значка программы или кнопки быстрого запуска.

8. В нижней части окна нажмите на кнопку **Добавить**.

   Количество логинов, добавленных в учетную запись, отобразится в списке учетных записей.

Шифрование данных

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

По умолчанию после установки Kaspersky CRYSTAL вам доступен один предустановленный контейнер со стандартными параметрами. Для работы с этим контейнером нужно задать пароль. Вы можете создавать контейнеры с нужными параметрами.

Для защиты данных нужно поместить их в контейнер и зашифровать. После этого для доступа к данным в контейнере нужно будет вводить 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** (см. рис. ниже).

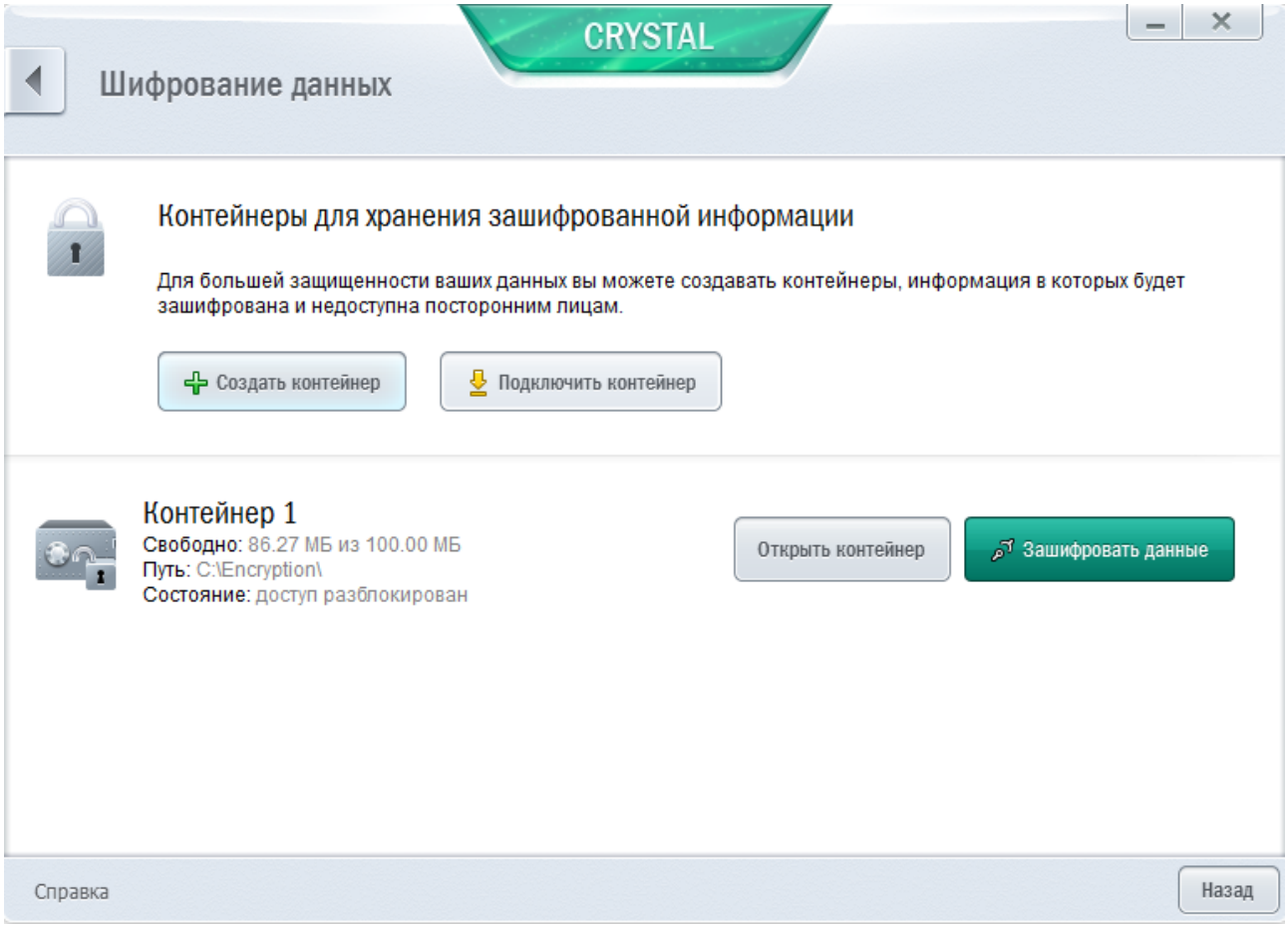

*Рисунок 9. Окно **Шифрование данных***

3. В открывшемся окне **Создание зашифрованного контейнера** задайте параметры нового контейнера.
4. Нажмите на кнопку **ОК**.

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**.

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 контейнер**.

УДАЛЕНИЕ НЕИСПОЛЬЗУЕМЫХ ДАННЫХ

Со временем в операционной системе накапливаются временные и неиспользуемые файлы. Эти файлы могут занимать большой объем памяти, что снижает эффективность работы системы, а также могут использоваться вредоносными программами.

Временные файлы создаются при запуске любых программ или операционных систем. По завершении работы не все временные файлы автоматически удаляются. В состав Kaspersky CRYSTAL входит мастер удаления неиспользуемых данных.

Мастер удаления неиспользуемых данных позволяет найти и удалить следующие файлы:

- журналы событий системы, куда записываются названия всех открытых программ;
- журналы событий разных программ или утилит обновления (например, Windows 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.

Помимо удаления из системы ненужных файлов, мастер удаляет 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. 63).

Чтобы запустить мастер удаления неиспользуемых данных, выполните следующие действия:

1. Откройте главное окно программы.

2. В нижней части окна нажмите на кнопку **Дополнительные инструменты**.

Откроется окно **Дополнительные инструменты** (см. рис. ниже).

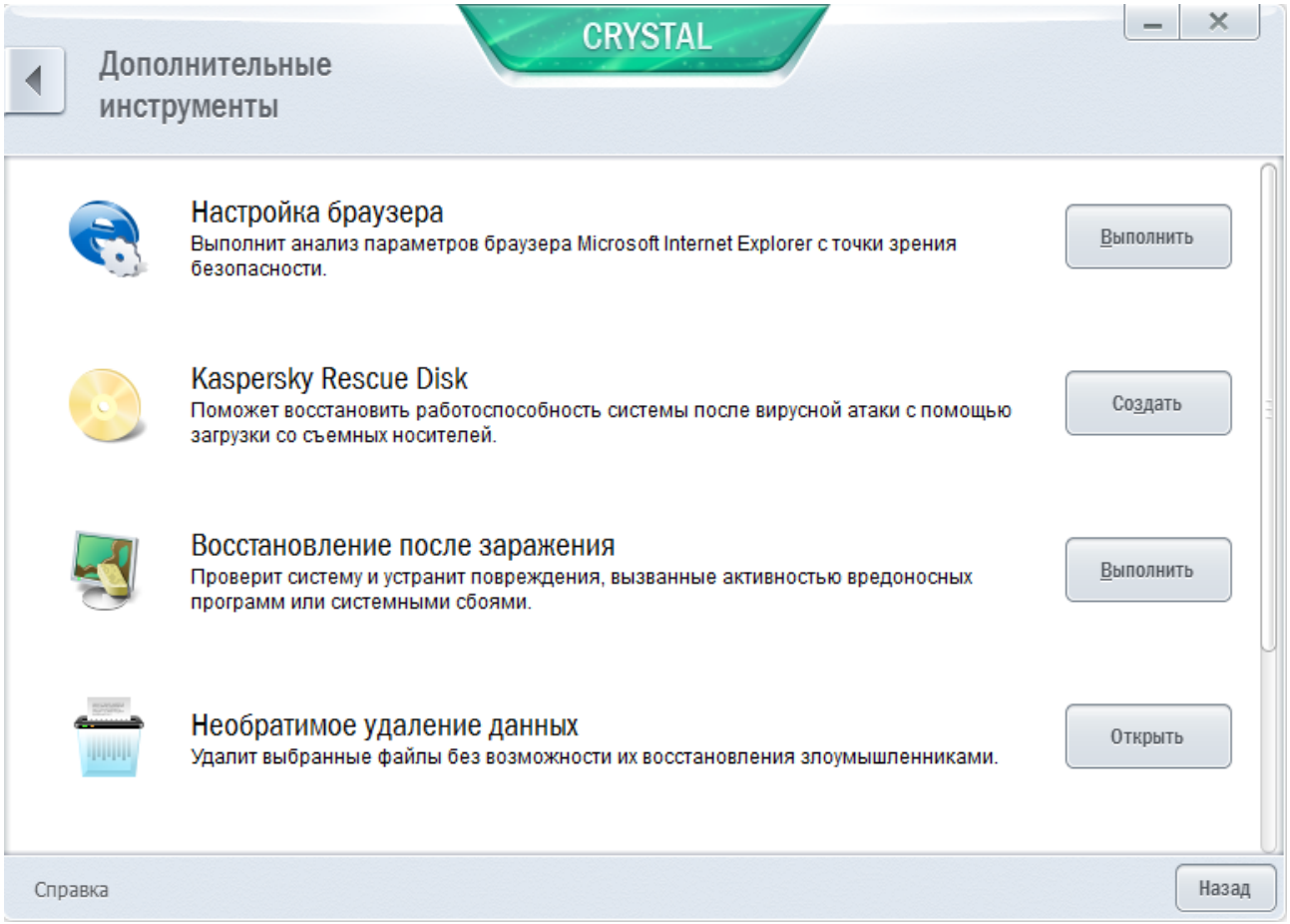

*Рисунок 10. Окно **Дополнительные инструменты***

3. В открывшемся окне в блоке **Удаление неиспользуемых данных** нажмите на кнопку **Выполнить**.

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**.

Рассмотрим подробнее шаги мастера.

Шаг 1. Начало работы мастера

В первом окне мастера представлена информация об удалении неиспользуемых данных.

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

Шаг 2. Поиск неиспользуемых данных

Мастер осуществляет поиск неиспользуемых данных на вашем компьютере. Поиск может занять некоторое время. По завершении поиска мастер автоматически перейдет к следующему шагу.

Шаг 3. Выбор действий для удаления неиспользуемых данных

По завершении поиска неиспользуемых данных мастер отображает список действий, которые можно выполнить с этими данными.

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.

Не рекомендуется снимать флажки, установленные по умолчанию. В результате этого действия безопасность вашего компьютера может оказаться 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.

После удаления неиспользуемой информации мастер автоматически перейдет к следующему шагу.

Во время работы мастера некоторые файлы (например, файл журнала Microsoft Windows, журнал событий Microsoft Office) могут использоваться системой. Чтобы удалить эти файлы, мастер предложит перезагрузить систему.

Шаг 5. Завершение работы мастера

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

НЕОБРАТИМОЕ УДАЛЕНИЕ ДАННЫХ

Дополнительная безопасность личных данных обеспечивается защитой от несанкционированного восстановления удаленной информации злоумышленниками.

В состав Kaspersky CRYSTAL входит инструмент для необратимого удаления данных без возможности их восстановления обычными программными средствами.

Kaspersky CRYSTAL позволяет удалять данные без возможности восстановления 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-карты, USB-карты или мобильные телефоны). Удаление данных с флеш-карт возможно, если на них механически не включен режим защиты от записи.

Вы можете удалять те данные, доступ к которым разрешен под вашей учетной записью. Перед удалением данных убедитесь, что эти данные не используются работающими программами.

➡ *Чтобы удалить данные без возможности восстановления, выполните следующие действия:*

1. Откройте главное окно программы.
2. В нижней части окна нажмите на кнопку **Дополнительные инструменты**.

Откроется окно **Необратимое удаление данных** (см. рис. ниже).

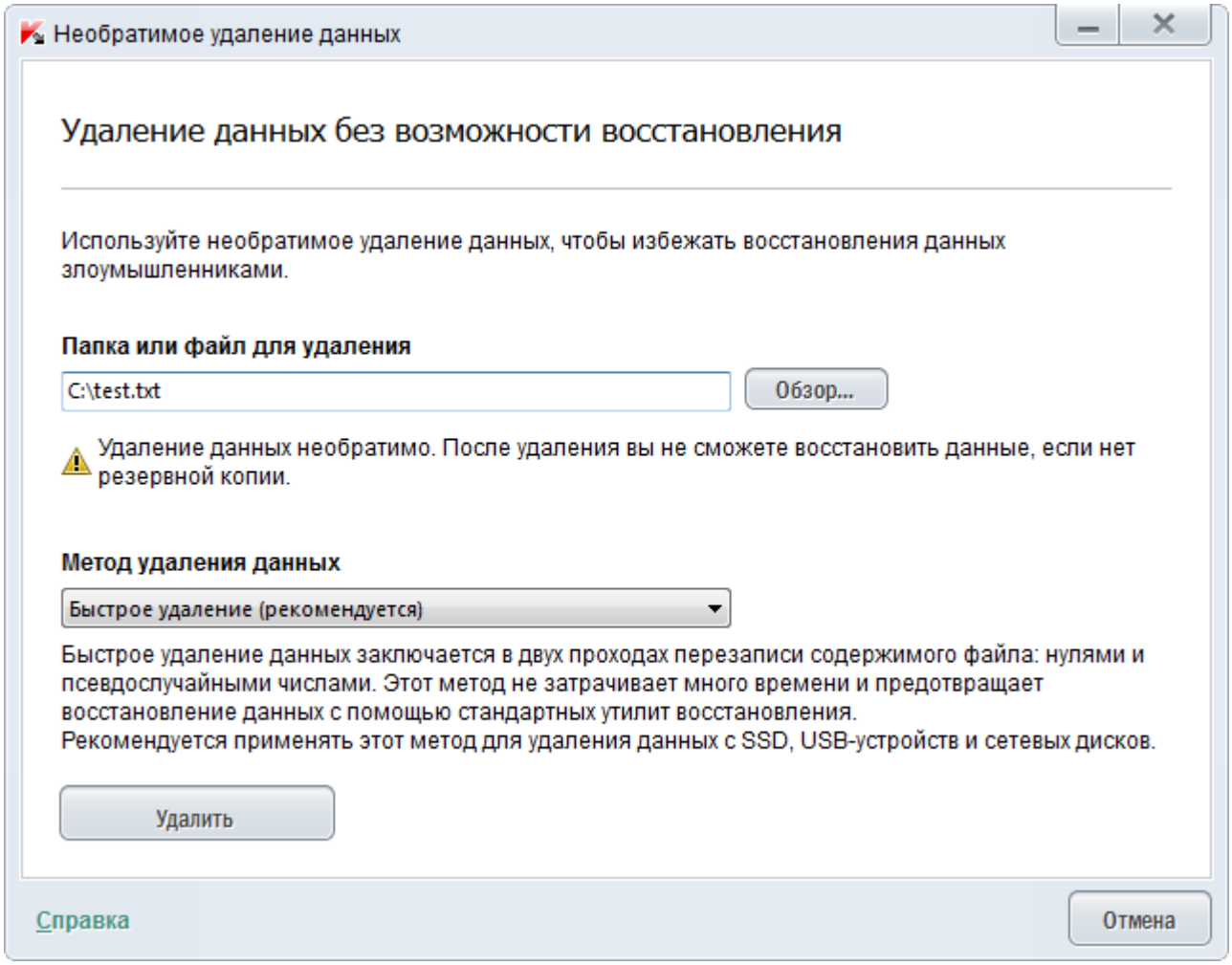

*Рисунок 11. Окно **Необратимое удаление данных***

3. В открывшемся окне в блоке **Необратимое удаление данных** нажмите на кнопку **Открыть**.

4. В открывшемся окне **Необратимое удаление данных** нажмите на кнопку **Обзор** и в открывшемся окне **Выбор файла или папки** выберите файл или папку для необратимого удаления.

   Удаление системных файлов может вызвать сбои в работе операционной системы. Если для удаления будут выбраны системные файлы или папки, программа запросит у вас дополнительное подтверждение для их удаления.

5. В раскрывающемся списке **Метод удаления данных** выберите нужный алгоритм удаления данных.

   Для удаления данных с SSD, USB-устройств и сетевых дисков рекомендуется применять методы Быстрое удаление или ГОСТ Р 50739-95. Остальные алгоритмы удаления могут нанести вред сетевому или съемному устройству.

6. 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 операционной системе. При этом сохраняется следующая информация:

- данные о введенных пользователем поисковых запросах и посещенных веб-сайтах;
- сведения о запуске программ, открытии и сохранении файлов;
- записи в системном журнале Microsoft Windows;
- другая информация о действиях пользователя.

Сведения о действиях пользователя, содержащие конфиденциальную информацию, могут оказаться доступными злоумышленникам и посторонним лицам.

В состав Kaspersky CRYSTAL входит мастер устранения следов активности пользователя в системе.

Чтобы запустить мастер устранения следов активности, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна выберите раздел **Дополнительные инструменты**.
3. В открывшемся окне в блоке **Устранение следов активности** нажмите на кнопку **Выполнить**.

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**.

Рассмотрим подробнее шаги мастера.

Шаг 1. Начало работы мастера

Убедитесь, что выбран вариант **Провести диагностику 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 переходит 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 (см. рис. ниже).

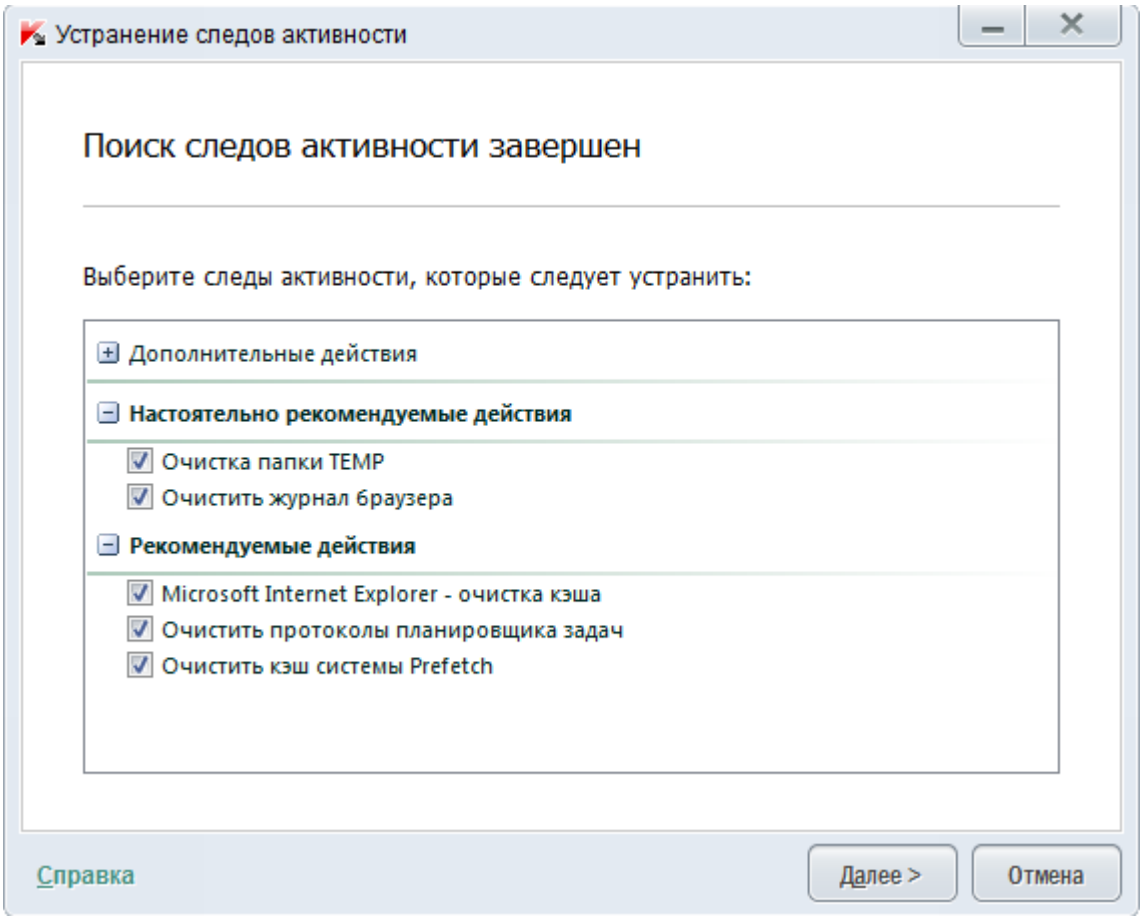

Рисунок 12. Найденные следы активности и рекомендации по их устранению

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.

Не рекомендуется снимать флажки, установленные по умолчанию. В результате этого действия безопасность вашего компьютера может оказаться 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.

После 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.

РЕЗЕРВНОЕ КОПИРОВАНИЕ

Основной способ защиты важных данных от потери – создание резервных копий данных на надежном носителе. Kaspersky CRYSTAL позволяет автоматически создавать резервные копии выбранных данных в указанном хранилище по заданному расписанию или вручную.

С помощью Центра управления (см. раздел «Удаленное управление защитой домашней сети» на стр. 45) вы можете запускать задачи резервного копирования на компьютерах домашней сети, а также отслеживать статус выполнения этих задач.

Для создания резервных копий вы можете использовать следующие типы хранилищ:

- локальный диск;
- съемный диск (например, внешний жесткий диск);
- сетевой диск;
- FTP-сервер;
- Онлайн-хранилище.

В ЭТОМ РАЗДЕЛЕ

РЕЗЕРВНОЕ КОПИРОВАНИЕ ДАННЫХ

Чтобы выполнить резервное копирование, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Резервное копирование**.
2. В открывшемся окне **Резервное копирование** нажмите на кнопку **Создать задачу резервного копирования**.

   Будет запущен мастер создания задачи резервного копирования.

   Рассмотрим подробнее шаги мастера:

   a. В окне выбора типа данных выполните одно из следующих действий:

      - Для быстрой настройки выберите один из предустановленных типов данных (файлы из папок Мои документы и Рабочий стол, видео, фотографии, музыкальные файлы).

- Выберите вариант **Выборочные файлы**, чтобы вручную выбрать файлы, для которых нужно создавать резервные копии.

b. Если на предыдущем шаге вы выбрали вариант **Выборочные файлы**, то в окне выбора файлов укажите файлы или категории файлов, для которых нужно создать резервные копии.

При создании резервной копии с использованием Онлайн-хранилища Kaspersky CRYSTAL не создает резервные копии тех типов данных, на которые наложены ограничения правилами использования Dropbox (см. раздел «Использование Онлайн-хранилища» на стр. 67).

c. В окне выбора хранилища выполните одно из следующих действий:

- Выберите одно из предустановленных хранилищ, в котором будут создаваться резервные копии.

  По умолчанию Kaspersky CRYSTAL позволяет создавать резервные копии на локальных и съемных дисках, а также в Онлайн-хранилище.

  Перед тем как использовать Онлайн-хранилище для создания резервных копий ваших данных, требуется активировать Онлайн-хранилище (см. раздел «Использование Онлайн-хранилища» на стр. 67).

- Выберите существующее сетевое хранилище.

- Нажмите на кнопку **Добавить хранилище**, чтобы создать новое сетевое хранилище.

  Для безопасности данных рекомендуется использовать Онлайн-хранилище или создавать хранилища резервных копий на съемных дисках.

d. В окне расписания задайте условия запуска задачи.

Если вы хотите выполнить однократное резервное копирование, не устанавливайте флажок **Запускать автоматически согласно расписанию**.

e. В окне **Сводная информация** введите название новой задачи, установите флажок **Запустить задачу по завершении работы мастера** и нажмите на кнопку **Завершить**.

Восстановление информации из резервной копии

Чтобы восстановить данные из резервной копии, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Резервное копирование**.

2. Выберите раздел **Восстановление данных**.

3. Выберите хранилище, в котором находятся нужные резервные копии, и нажмите на кнопку **Восстановить данные**.

   Откроется окно **Восстановление данных из хранилища**.

4. В открывшемся окне выполните следующие действия:

   a. В раскрывающемся списке **Задача резервного копирования** выберите задачу, в процессе выполнения которой были созданы нужные резервные копии.

   b. В раскрывающемся списке **Дата** выберите дату и время создания нужных резервных копий.

c. В раскрывающемся списке **Категория** выберите тип файлов, которые нужно восстановить.

5. В списке файлов в нижней части окна выберите файлы, которые нужно восстановить. Для этого установите флажки рядом с нужными файлами в списке.

Kaspersky CRYSTAL не позволяет восстановить данные из Онлайн-хранилища, если эти данные были удалены через веб-интерфейс Dropbox.

6. Нажмите на кнопку **Восстановить данные**.

Откроется окно **Восстановление**.

7. В окне **Восстановление** укажите место сохранения восстановленных файлов (в исходную папку или в указанную папку).

8. Нажмите на кнопку **Восстановить выбранные данные**.

Выбранные для восстановления файлы будут восстановлены и сохранены в указанной папке.

В случае обнаружения другой версии какого-либо из файлов, выбранных для восстановления, программа предлагает заменить существующий файл резервной копией либо сохранить оба файла.

ИСПОЛЬЗОВАНИЕ ОНЛАЙН-ХРАНИЛИЩА

Онлайн-хранилище позволяет сохранять резервные копии ваших данных на удаленном сервере, используя веб-сервис Dropbox.

Для использования Онлайн-хранилища требуется создать учетную запись на веб-сайте поставщика услуг резервного копирования Dropbox.

Вы можете использовать одну и ту же учетную запись Dropbox для сохранения в единое Онлайн-хранилище резервных копий данных с разных устройств, на которых установлен Kaspersky CRYSTAL.

Стандартная учетная запись Dropbox позволяет использовать до двух гигабайт свободного пространства на удаленном диске. При необходимости вы можете увеличить объем Онлайн-хранилища на условиях, определяемых поставщиком услуг резервного копирования. Более подробную информацию об условиях использовании веб-сервиса вы можете получить на сайте Dropbox.

Перед тем как использовать Онлайн-хранилище для создания резервных копий ваших данных, требуется активировать Онлайн-хранилище.

Чтобы активировать Онлайн-хранилище, выполните следующие действия:

1. Откройте главное окно программы и нажмите на кнопку **Резервное копирование**.

2. В открывшемся окне **Резервное копирование** нажмите на кнопку **Создать задачу резервного копирования**.

Будет запущен мастер создания задачи резервного копирования.

3. В окне выбора типа данных выберите категорию данных или вручную укажите файлы, для которых нужно создавать резервные копии.

4. В окне выбора хранилища выберите Онлайн-хранилище и нажмите на кнопку **Активировать сейчас**.

Откроется окно входа в учетную запись Dropbox.

5. В открывшемся окне выполните одно из следующих действий

a. Если вы еще не зарегистрированы на сайте Dropbox, пройдите процедуру регистрации.

b. Если вы уже зарегистрированы на сайте Dropbox, войдите в учетную запись Dropbox.

Для завершения активации Онлайн-хранилища подтвердите, что Kaspersky CRYSTAL может использовать вашу учетную запись Dropbox для выполнения резервного копирования и восстановления информации. Kaspersky CRYSTAL будет помещать резервные копии сохраняемых данных в отдельную папку, которая создается в папке хранения приложений Dropbox.

После завершения активации Онлайн-хранилища откроется окно выбора хранилища. Онлайн-хранилище будет доступно для выбора. Для активированного Онлайн-хранилища отображается объем занятого пространства и объем свободного пространства, доступного для записи информации.

Защита паролем доступа к параметрам Kaspersky CRYSTAL

На одном компьютере могут работать несколько пользователей с разным опытом и уровнем компьютерной грамотности. Неограниченный доступ разных пользователей к управлению Kaspersky CRYSTAL и настройке его параметров может привести к снижению уровня защищенности компьютера.

Чтобы ограничить доступ к программе, вы можете задать пароль администратора и указать действия, при выполнении которых этот пароль должен запрашиваться:

- настройка параметров программы;
- управление Резервным копированием;
- удаленное управление безопасностью на компьютерах домашней сети (пароль должен быть одинаковым на всех компьютерах);
- управление Родительским контролем;
- завершение работы программы;
- удаление программы.

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

1. Откройте главное окно программы.
2. В правом верхнем углу окна перейдите по ссылке **Настройка**.

   Откроется окно настройки программы.

3. В верхней части окна настройки программы выберите закладку **Пароль** (см. рис ниже).

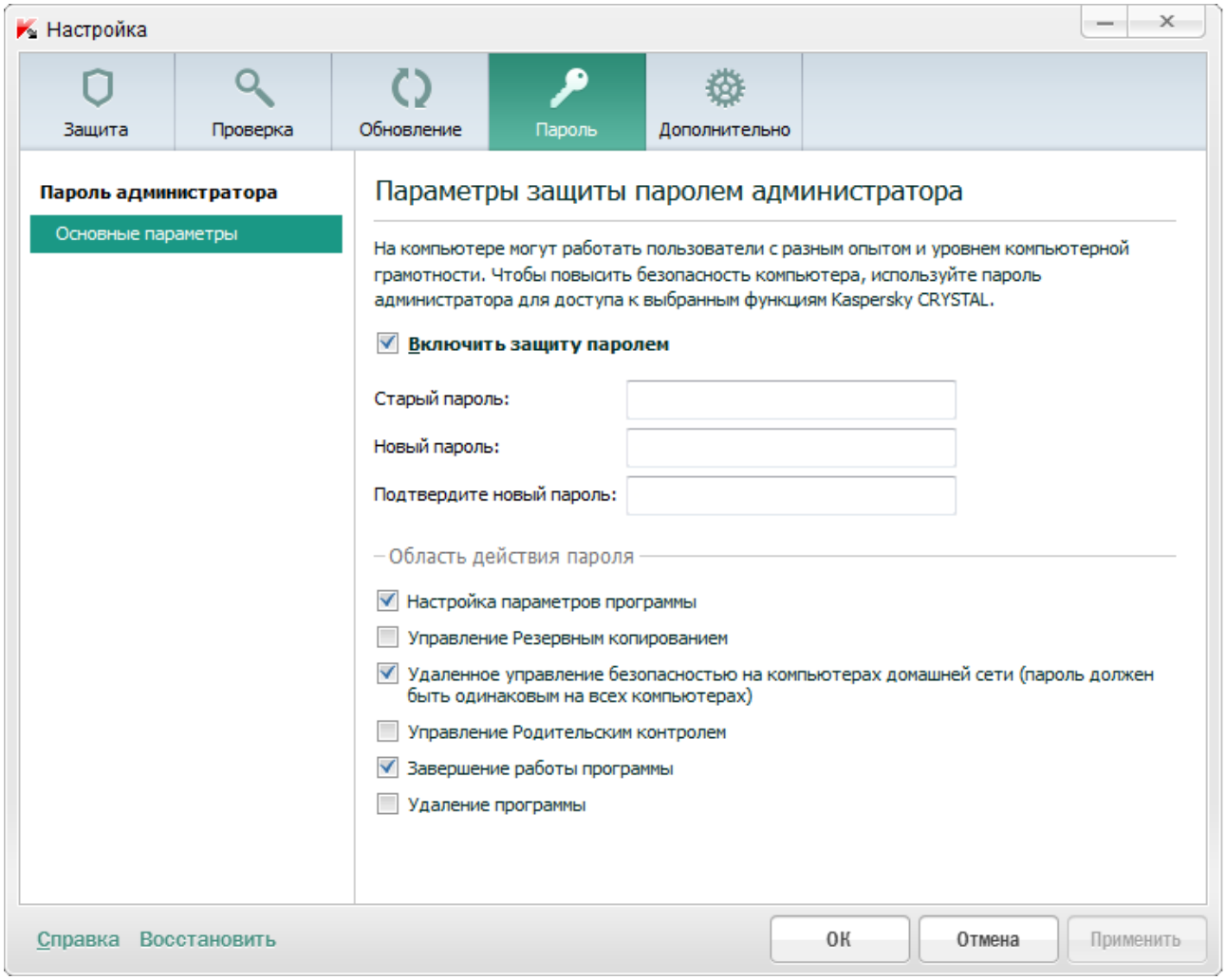

*Рисунок 13. Окно **Настройка**, раздел **Пароль***

4. В правой части окна установите флажок **Включить защиту паролем** и заполните поля **Новый пароль** и **Подтверждение пароля**.

5. Если вы хотите изменить пароль, созданный ранее, введите его в поле **Старый пароль**.

6. В блоке параметров **Область действия пароля** укажите действия с программой, доступ к которым нужно защитить паролем.

7. Нажмите на кнопку **Применить** чтобы сохранить изменения.

Забытый пароль восстановить нельзя. Для восстановления доступа к параметрам Kaspersky CRYSTAL при забытом пароле потребуется обращение в Службу технической поддержки.

Использование Родительского контроля

Родительский контроль позволяет контролировать действия разных пользователей на компьютере и в сети. С помощью Родительского контроля вы можете ограничивать доступ к интернет-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 использовании компьютера и интернета дети сталкиваются с целым рядом угроз:

- потеря времени и / или денег при посещении чатов, игровых ресурсов, интернет-магазинов, аукционов;
- доступ к веб-ресурсам, предназначенным для взрослой аудитории (например, содержащим порнографические, экстремистские материалы, затрагивающим темы оружия, наркотиков, насилия);
- загрузка файлов, зараженных вредоносными программами;
- ущерб для здоровья от чрезмерно длительного нахождения за компьютером;
- контакты с незнакомыми людьми, которые под видом сверстников могут получить личную информацию о ребенке (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.

В этом разделе

НАСТРОЙКА РОДИТЕЛЬСКОГО КОНТРОЛЯ

Если вы не защитили паролем доступ к параметрам Kaspersky CRYSTAL (см. стр. 68), то при первом запуске Родительского контроля Kaspersky CRYSTAL предлагает задать пароль для защиты от несанкционированного изменения параметров контроля. После этого можно 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**.

   Откроется окно **Пользователи компьютера**, в котором отображаются все учетные записи пользователей, созданные на компьютере.

2. Нажмите на кнопку **Выбрать уровень контроля** для нужной учетной записи.

3. В открывшемся окне **Родительский контроль** выполните одно из следующих действий:

   - выберите один из предустановленных уровней контроля (**Сбор статистики**, **Профиль «Ребенок»** или **Профиль «Подросток**);

   - установите ограничения вручную:

     a. Выберите пункт **Выборочные ограничения**.

     b. Нажмите на кнопку **Настройка**.

        Откроется окно **Родительский контроль**.

     c. В открывшемся окне на закладке **Настройка** выберите тип ограничения в левой части окна и задайте параметры контроля в правой части окна.

     d. Нажмите на кнопку **ОК** чтобы сохранить настроенные параметры контроля.

4. Нажмите на кнопку **ОК** в окне **Родительский контроль**.

ПРОСМОТР ОТЧЕТА О ДЕЙСТВИЯХ ПОЛЬЗОВАТЕЛЯ

Вы можете просматривать отчеты о действиях каждого пользователя, для которого настроен Родительский контроль, отдельно для каждой категории контролируемых событий.

Чтобы просмотреть отчет о действиях контролируемого пользователя, выполните следующие действия:

1. Откройте главное окно программы.

2. В нижней части окна выберите раздел **Родительский контроль**.

3. В открывшемся окне в блоке с учетной записью пользователя нажмите на кнопку  .

   Откроется окно **Родительский контроль**.

4. Выберите закладку **Отчеты**.

5. В левой части окна выберите раздел с названием категории контролируемых действий или содержимого (например, **Использование интернета** или **Личные данные**).

   В правой части окна отобразится отчет о контролируемых действиях и содержимом.

Приостановка и возобновление защиты компьютера

Приостановка защиты означает выключение на некоторое время всех ее компонентов.

Чтобы приостановить защиту компьютера, выполните следующие действия:

1. В контекстном меню значка программы в области уведомлений выберите пункт **Приостановить защиту**.

   Откроется окно **Приостановка защиты** (см. рис. ниже).

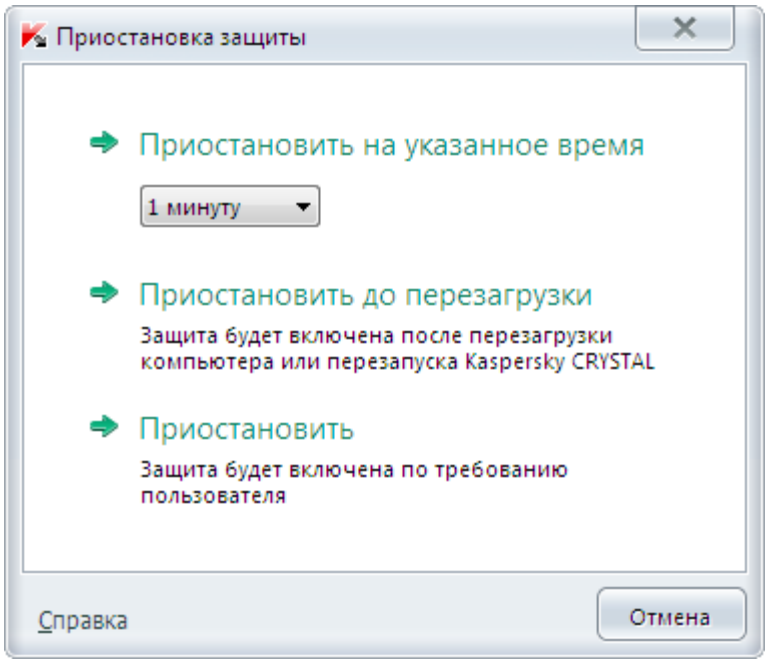

*Рисунок 14. Окно **Приостановка защиты***

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

   - **Приостановить на указанное время** – защита будет включена через интервал, выбранный в раскрывающемся списке ниже.
   - **Приостановить до перезагрузки** – защита будет включена после перезапуска программы или перезагрузки системы (при условии, что включен автоматический запуск программы).
   - **Приостановить** – защита будет включена тогда, когда вы решите возобновить ее.

Чтобы возобновить защиту компьютера,

выберите пункт **Возобновить защиту** в контекстном меню значка программы в области уведомлений.

Просмотр отчета о защите компьютера

Kaspersky CRYSTAL ведет отчеты о работе каждого компонента защиты. С помощью отчета вы можете получить статистическую информацию о защите компьютера (например, узнать, сколько обнаружено и обезврежено вредоносных объектов за определенный период, сколько раз за это время программа обновлялась, сколько обнаружено спам-сообщений и многое другое).

Чтобы просмотреть отчет о защите компьютера, выполните следующие действия:

1. В главном окне программы нажмите на кнопку **Защита компьютера**.

   Откроется окно **Защита компьютера**.

2. По ссылке **Отчеты** в верхней части окна перейдите к окну отчетов о защите компьютера.

   В окне **Отчеты** в виде диаграмм отображаются отчеты о защите компьютера.

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

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

Восстановление стандартных параметров работы программы

Вы в любое время можете восстановить параметры работы Kaspersky CRYSTAL, рекомендуемые «Лабораторией Касперского». Восстановление параметров осуществляется с помощью мастера настройки программы.

В результате работы мастера для всех компонентов защиты будет установлен уровень безопасности *Рекомендуемый*. При восстановлении рекомендуемого уровня безопасности вы можете выборочно сохранять ранее сделанные настройки параметров для компонентов программы.

Чтобы восстановить рекомендуемые параметры работы программы, выполните следующие действия:

1. Откройте главное окно программы.

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

3. В открывшемся окне **Настройка** запустите мастер настройки программы одним из следующих способов:

   - перейдите по ссылке **Восстановить** в левом нижнем углу окна;

- в верхней части окна выберите раздел **Дополнительно**, подраздел **Управление параметрами** и нажмите на кнопку **Восстановить** в блоке **Восстановление параметров по умолчанию** (см. рис. ниже).

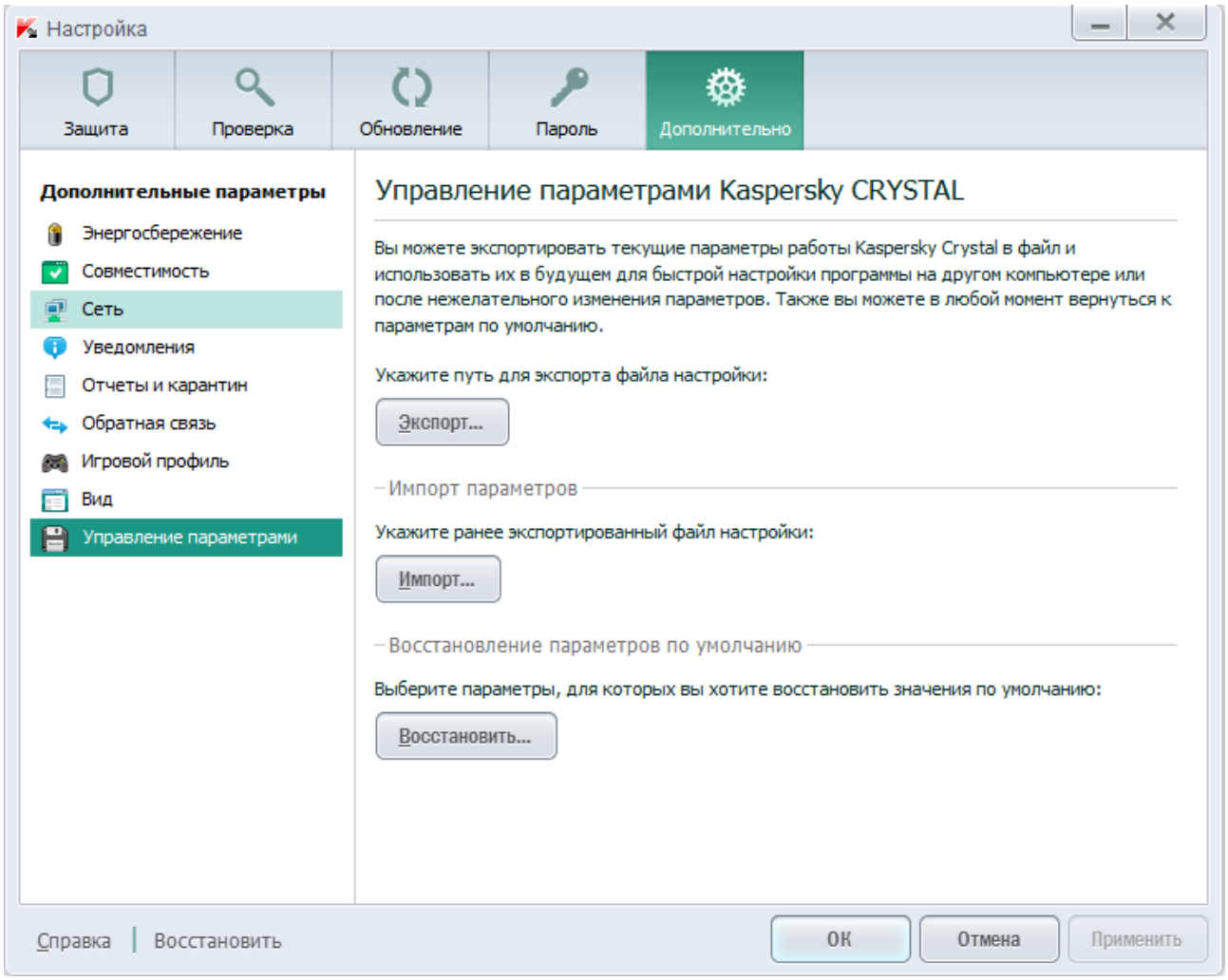

*Рисунок 15. Окно **Настройка**, подраздел **Управление параметрами***

Рассмотрим подробнее шаги мастера.

Шаг 1. Начало работы мастера

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

Шаг 2. Восстановление параметров

В этом окне мастера представлены компоненты защиты Kaspersky CRYSTAL, параметры которых были изменены пользователем или накоплены Kaspersky CRYSTAL в результате обучения компонентов защиты Сетевой экран и Анти-Спам. Если для какого-либо компонента были сформированы уникальные параметры, они также будут представлены в окне (см. рис. ниже).

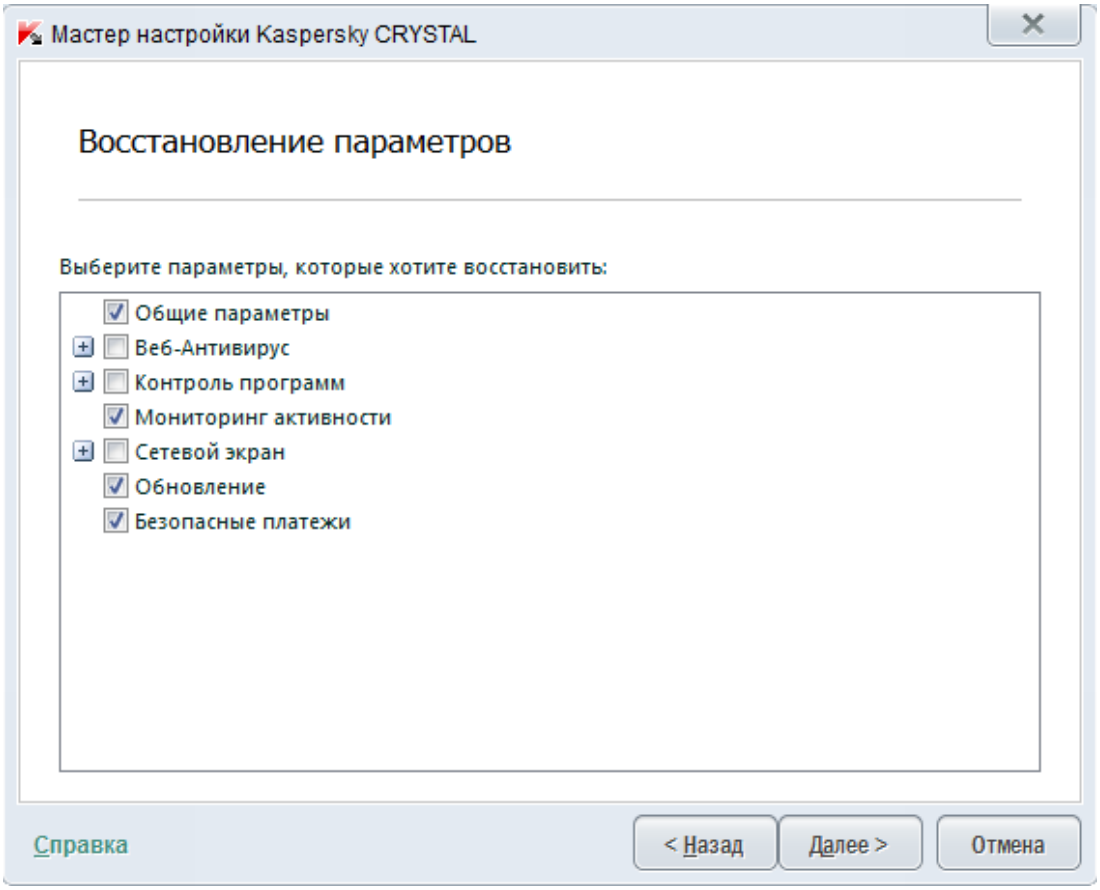

*Рисунок 16. Окно **Восстановление параметров***

В число уникальных параметров входят списки разрешенных и запрещенных фраз и адресов, используемых Анти-Спамом, списки доверенных интернет-адресов и телефонных номеров интернет-провайдеров, правила исключений защиты для компонентов программы, правила фильтрации пакетов и программ Сетевого экрана.

Уникальные параметры формируются в процессе работы с Kaspersky CRYSTAL с учетом индивидуальных задач и требований безопасности. «Лаборатория Касперского» рекомендует сохранять уникальные параметры при восстановлении первоначальных параметров программы.

Установите флажки для тех параметров, которые нужно сохранить и нажмите на кнопку **Далее**.

Шаг 3. 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.

По завершении анализа мастер автоматически переходит к следующему шагу.

Шаг 4. Завершение восстановления

Для завершения работы мастера нажмите на кнопку **Завершить**.

Импорт параметров программы в Kaspersky CRYSTAL, установленный на другом компьютере

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.

Перенос параметров Kaspersky CRYSTAL с одного компьютера на другой производится в три этапа:

1. Экспорт параметров программы в файл настройки.
2. Перенос файла настройки на другой компьютер (например, по электронной почте или на съемном носителе).
3. Применение параметров из файла настройки к программе, установленной на другом компьютере.

Чтобы сохранить параметры программы Kaspersky CRYSTAL в файле настройки, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В верхней части окна **Настройка** выберите в разделе **Дополнительно** подраздел **Управление параметрами**.
4. В подразделе **Управление параметрами** нажмите на кнопку **Экспорт**.
5. В открывшемся окне введите название файла настройки и укажите место его сохранения.
6. Нажмите на кнопку **ОК**.

Чтобы применить параметры из файла настройки к программе, установленной на другом компьютере, выполните следующие действия:

1. Откройте главное окно программы.
2. В верхней части окна перейдите по ссылке **Настройка**.
3. В верхней части окна **Настройка** выберите в разделе **Дополнительно** подраздел **Управление параметрами**.
4. В подразделе **Управление параметрами** нажмите на кнопку **Импорт**.
5. В открывшемся окне выберите файл, из которого вы хотите импортировать параметры Kaspersky CRYSTAL.
6. Нажмите на кнопку **ОК**.

СОЗДАНИЕ И ИСПОЛЬЗОВАНИЕ ДИСКА АВАРИЙНОГО ВОССТАНОВЛЕНИЯ

Диск аварийного восстановления представляет собой программу Kaspersky Rescue Disk, записанную на съемный носитель (компакт-диск или USB-устройство).

Вы сможете использовать Kaspersky Rescue Disk для проверки и лечения зараженного компьютера, который нельзя вылечить другим способом (например, с помощью антивирусных программ).

В ЭТОМ РАЗДЕЛЕ

СОЗДАНИЕ ДИСКА АВАРИЙНОГО ВОССТАНОВЛЕНИЯ

Создание диска аварийного восстановления заключается в формировании образа диска (файла формата ISO) с актуальной версией программы Kaspersky Rescue Disk и его записи на съемный носитель.

Исходный образ диска можно загрузить с сервера «Лаборатории Касперского» или скопировать с локального источника.

Диск аварийного восстановления создается с помощью мастера создания и записи Kaspersky Rescue Disk. 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\AVP13\Data\Rdisk\;
- в операционных системах Microsoft Windows Vista, Microsoft Windows 7 и Microsoft Windows 8 – в папке ProgramData\Kaspersky Lab\AVP13\Data\Rdisk\.

Чтобы создать диск аварийного восстановления, выполните следующие действия:

1. Откройте главное окно программы.
2. В нижней части окна выберите раздел **Дополнительные инструменты**.
3. В открывшемся окне **Kaspersky Rescue Disk** нажмите на кнопку **Создать**.

   Откроется окно **Мастер создания диска аварийного восстановления**.

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**.

Рассмотрим подробнее шаги мастера.

Шаг 1. Начало работы мастера. Поиск существующего образа диска

В первом окне мастера представлена информация о программе Kaspersky Rescue Disk.

Если мастер обнаружит ранее созданный файл образа диска в предназначенной для этого папке (см. выше), то в первом окне мастера отобразится флажок **Использовать существующий образ**. Чтобы использовать найденный файл в качестве исходного образа диска и сразу перейти к шагу **Обновление файла образа** (см. ниже), установите этот флажок. Если вы не хотите использовать найденный образ диска, снимите этот флажок. Мастер перейдет к окну **Выбор источника образа диска**.

Шаг 2. Выбор источника образа диска

Если в первом окне мастера вы установили флажок **Использовать существующий образ**, то этот шаг пропускается.

На этом шаге вам следует выбрать источник образа диска из предложенных вариантов:

- Если у вас уже есть записанный диск аварийного восстановления или его образ (файл формата ISO), сохраненный на вашем компьютере или на ресурсе локальной сети, выберите вариант **Копировать образ с локального или сетевого диска**.

- Если у вас нет файла образа диска аварийного восстановления, и вы хотите загрузить его с сервера «Лаборатории Касперского» (размер файла составляет примерно 175 МБ), выберите вариант **Загрузить образ с сервера «Лаборатории Касперского»**.

Шаг 3. Копирование (загрузка) образа диска

Если в первом окне мастера вы установили флажок **Использовать существующий образ**, то этот шаг пропускается.

Если на предыдущем шаге вы выбрали вариант **Копировать образ с локального или сетевого диска**, нажмите на кнопку **Обзор**. Указав путь к файлу, нажмите на кнопку **Далее**. В окне мастера будет отображен процесс копирования образа диска.

Если на предыдущем шаге 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 4. Обновление файла образа диска

Процедура обновления файла образа диска включает в себя следующие действия:

- обновление баз программы;

- обновление конфигурационных файлов.

Конфигурационные файлы определяют возможность загрузки компьютера со съемного носителя (например, CD / DVD-диска или USB-устройства с Kaspersky Rescue Disk), полученного в результате работы мастера.

При обновлении баз программы используются базы, полученные при последнем обновлении Kaspersky CRYSTAL. Если базы устарели, рекомендуется выполнить задачу обновления и запустить мастер создания и записи Kaspersky Rescue Disk заново.

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

Шаг 5. Запись образа диска на носитель

На этом шаге мастер проинформирует вас об успешном создании образа диска и предложит записать образ диска на носитель.

Укажите носитель для записи Kaspersky Rescue Disk:

- Для записи на CD / DVD-диск выберите вариант **Записать на CD/DVD диск** и укажите диск, на который вы хотите записать образ диска.
- Для записи на USB-устройство выберите вариант **Записать на USB-устройство** и укажите устройство, на которое вы хотите записать образ диска.

> «Лаборатория Касперского» не рекомендует записывать образ диска на устройства, не предназначенные исключительно для хранения данных, например, смартфоны, мобильные телефоны, КПК, MP3-плееры. В дальнейшем такие устройства, использованные для записи образа диска, могут работать неправильно.

- Для записи на жесткий диск на вашем компьютере или на другом компьютере, к которому вы имеете доступ по сети, выберите вариант **Сохранить образ в файл на локальном или сетевом диске** и укажите папку, в которую вы хотите записать образ диска, и имя файла формата ISO.

Шаг 6. Завершение работы мастера

Для завершения работы мастера нажмите на кнопку **Завершить**. Созданный диск аварийного восстановления вы можете использовать для загрузки компьютера (см. стр. 79), если в результате действий вирусов или вредоносных программ невозможно выполнить загрузку компьютера и запуск Kaspersky CRYSTAL в обычном режиме.

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 или USB-устройство с записанной на него программой Kaspersky Rescue Disk (см. раздел «Создание диска аварийного восстановления» на стр. 77).

> Загрузка компьютера со съемного носителя не всегда возможна. В частности, она не поддерживается некоторыми устаревшими моделями компьютеров. Прежде чем выключить компьютер для последующей загрузки со съемного носителя, уточните возможность такой загрузки.

Чтобы загрузить компьютер с помощью диска аварийного восстановления, выполните следующие действия:

1. В параметрах BIOS включите загрузку с CD / DVD-диска или USB-устройства (подробную информацию можно получить из документации к материнской плате вашего компьютера).
2. Поместите в дисковод зараженного компьютера CD / DVD-диск или подключите USB-устройство с предварительно записанной программой Kaspersky Rescue Disk.
3. Перезагрузите компьютер.

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

ОБРАЩЕНИЕ В СЛУЖБУ ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ

Этот раздел содержит информацию о способах получения технической поддержки и о том, какие условия требуются для получения помощи от Службы технической поддержки.

В ЭТОМ РАЗДЕЛЕ

Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации к программе или в одном из источников информации о программе (см. раздел «Источники информации о программе» на стр. 9), рекомендуем обратиться в Службу технической поддержки «Лаборатории Касперского». Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании программы.

Прежде чем обратиться в Службу технической поддержки, ознакомьтесь с правилами предоставления технической поддержки (http://support.kaspersky.ru/support/rules).

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- Позвонить по телефону. Этот способ позволяет проконсультироваться по телефону со специалистами русскоязычной или интернациональной Службы технической поддержки.
- Отправить запрос из Личного кабинета на веб-сайте Службы технической поддержки. Этот способ позволяет вам связаться со специалистами Службы технической поддержки через форму запроса.

Техническая поддержка предоставляется только пользователям, которые приобрели коммерческую лицензию на использование программы. Техническая поддержка для владельцев пробных лицензий не осуществляется.

Техническая поддержка по телефону

Если возникла неотложная проблема, вы можете позвонить специалистам русскоязычной или международной технической поддержки (http://support.kaspersky.ru/support/international).

Перед обращением в Службу технической поддержки, пожалуйста, ознакомьтесь с правилами предоставления поддержки (http://support.kaspersky.ru/support/details). Это позволит нашим специалистам быстрее помочь вам.

Получение технической поддержки через Личный кабинет

Личный кабинет – это ваш персональный раздел (https://my.kaspersky.ru) на сайте Службы технической поддержки.

Для доступа к Личному кабинету вам требуется зарегистрироваться на странице регистрации (https://my.kaspersky.com/ru/registration). Вам нужно указать адрес электронной почты и пароль для доступа в Личный кабинет.

В Личном кабинете вы можете выполнять следующие действия:

- отправлять запросы в Службу технической поддержки и Вирусную лабораторию;
- обмениваться сообщениями со Службой технической поддержки без использования электронной почты;
- отслеживать состояние ваших запросов в реальном времени;
- просматривать полную историю ваших запросов в Службу технической поддержки;
- получать копию файла ключа в случае, если файл ключа был утерян или удален.

Электронный запрос в Службу технической поддержки

Вы можете отправить электронный запрос в Службу технической поддержки на русском, английском, немецком, французском или испанском языках.

В полях формы электронного запроса вам нужно указать следующие сведения:

- тип запроса;
- название и номер версии программы;
- текст запроса;
- номер клиента и пароль;
- электронный адрес.

Специалист Службы технической поддержки направляет ответ на ваш вопрос в ваш Личный кабинет и по адресу электронной почты, который вы указали в электронном запросе.

Электронный запрос в Вирусную лабораторию

Некоторые запросы требуется направлять не в Службу технической поддержки, а в Вирусную лабораторию.

Вы можете направлять в Вирусную лабораторию запросы следующих типов:

- *Неизвестная вредоносная программа* – вы подозреваете, что файл содержит вирус, но Kaspersky CRYSTAL не обнаруживает его в качестве зараженного.

  Специалисты Вирусной лаборатории анализируют присылаемый вредоносный код и при обнаружении неизвестного ранее вируса добавляют его описание в базу данных, доступную при обновлении антивирусных программ.

- *Ложное срабатывание антивируса* – Kaspersky CRYSTAL определяет файл как содержащий вирус, но вы уверены, что файл не является вирусом.

- *Запрос на описание вредоносной программы* – вы хотите получить описание вируса, обнаруженного Kaspersky CRYSTAL, на основе названия этого вируса.

Вы также можете направлять запросы в Вирусную лабораторию со страницы с формой запроса (http://support.kaspersky.ru/virlab/helpdesk.html), не регистрируясь в Личном кабинете. При этом вам не требуется указывать код активации программы.

Создание отчета о состоянии системы и использование скрипта AVZ

После того как вы проинформируете специалистов Службы технической поддержки о возникшей проблеме, они могут попросить вас сформировать отчет с информацией об операционной системе и отправить его в Службу технической поддержки. Также специалисты Службы технической поддержки могут попросить вас создать файл с технической информацией о работе системы. Этот файл позволяет отследить процесс пошагового выполнения команд программы и обнаружить, на каком этапе работы программы возникает ошибка.

В результате анализа присланных вами данных специалисты Службы технической поддержки могут создать и отправить вам скрипт AVZ. Выполнение скриптов AVZ позволяет проводить анализ запущенных процессов на наличие вредоносного кода, проверять систему на наличие вредоносного кода, лечить / удалять зараженные файлы и создавать отчеты о результатах проверки системы.

В этом разделе

Создание отчета о состоянии системы

Чтобы создать отчет о состоянии системы, выполните следующие действия:

1. Откройте главное окно программы.
2. По ссылке **Поддержка** в нижней части главного окна откройте окно **Поддержка**.

   Нажмите на кнопку **Мониторинг проблем**.
3. В открывшемся окне **Мониторинг проблем** нажмите на кнопку **Создать отчет о системе**.

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. По ссылке **Поддержка** в нижней части главного окна откройте окно **Поддержка**.

   Нажмите на кнопку **Мониторинг проблем**.

3. В открывшемся окне **Мониторинг проблем** нажмите на кнопку **Просмотреть отчет**.

4. Откройте архив sysinfo.zip, содержащий файлы отчета.

Сбор технической информации о работе программы

Для сбора технической информации о работе программы и операционной системы вы можете использовать запись событий. Отчет о записанных событиях позволит специалистам Службы технической поддержки произвести анализ проблемы, возникшей при работе программы.

Чтобы собрать и записать информацию о проблеме в работе программы, выполните следующие действия:

1. Откройте главное окно программы.

2. По ссылке **Поддержка** в нижней части главного окна откройте окно **Поддержка**.

3. В окне **Поддержка** нажмите на кнопку **Мониторинг проблем**.

4. В разделе **Мониторинг проблем** в раскрывающемся списке **Записывать события** выберите уровень важности событий.

   Вы можете выбрать следующие уровни важности сохраняемых в отчете событий:

   - Важные. Kaspersky CRYSTAL сохраняет в отчете сведения событиях, потенциально важных для обеспечения безопасности компьютера (например, об обнаружении возможно зараженного объекта или подозрительной активности в системе).

   - Рекомендуемые. Kaspersky CRYSTAL сохраняет в отчете сведения о важных событиях, а также о событиях, не имеющих первостепенной важности для обеспечения безопасности компьютера.

   - Все. Kaspersky CRYSTAL составляет подробный отчет обо всех событиях, которые могут быть использованы для диагностики работы программы.

5. Чтобы начать запись событий, нажмите на кнопку **Включить запись**.

6. Закройте окно **Поддержка**, затем воспроизведите ситуацию, при которой возникает проблема в работе программы.

7. После воспроизведения ситуации вернитесь к разделу **Мониторинг проблем** в окне **Поддержка** и нажмите на кнопку **Выключить запись**.

   Kaspersky CRYSTAL остановит запись технической информации о работе программы и всей операционной системы.

После сбора служебной информации о работе программы вы можете отправить собранную информацию в Службу технической поддержки «Лаборатории Касперского».

Отправка файлов данных

После сбора технической информации о работе программы и создании 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 технической поддержки, выполните следующие действия:

1. Откройте главное окно программы.
2. По ссылке **Поддержка** в нижней части окна откройте окно **Поддержка**.
3. В открывшемся окне нажмите на кнопку **Мониторинг проблем**.

   Откроется окно **Мониторинг проблем**.
4. В открывшемся окне нажмите на кнопку **Отправить служебную информацию в Службу технической поддержки**.

   Откроется окно **Отправка отчета**.
5. Установите флажки рядом с теми данными, которые вы хотите отправить в Службу технической поддержки, и нажмите на кнопку **Отправить**.

   Откроется окно **Введите номер запроса**.
6. Укажите номер, присвоенный вашему запросу при обращении в Службу технической поддержки через Личный кабинет, и нажмите на кнопку **ОК**.

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 диске, выполните следующие действия:

1. Откройте главное окно программы.
2. По ссылке **Поддержка** в нижней части окна откройте окно **Поддержка**.
3. В открывшемся окне нажмите на кнопку **Мониторинг проблем**.
4. Откроется окно **Мониторинг проблем**.
5. В открывшемся окне нажмите на кнопку кнопку **Отправить служебную информацию в Службу технической поддержки**.

   Откроется окно **Отправка отчета**.
6. Установите флажки рядом с теми данными, которые вы хотите отправить в Службу технической поддержки, и нажмите на кнопку **Отправить**.

   Откроется окно **Введите номер запроса**.
7. Нажмите на кнопку **Отмена** и в открывшемся окне подтвердите сохранение файлов на диске, нажав на кнопку **Да**.

   Откроется окно сохранения архива.
8. Задайте имя архива и подтвердите сохранение.

Созданный архив вы можете отправить в Службу технической поддержки через Личный кабинет.

Выполнение скрипта AVZ

Не рекомендуется вносить изменения в текст скрипта, присланного вам специалистами «Лаборатории Касперского». В случае возникновения проблем в ходе выполнения скрипта обращайтесь в Службу технической поддержки (см. раздел «Способы получения технической поддержки» на стр. 80).

Чтобы выполнить скрипт AVZ, выполните следующие действия:

1. Откройте главное окно программы.
2. По ссылке **Поддержка** в нижней части окна откройте окно **Поддержка**.
3. В открывшемся окне нажмите на кнопку **Мониторинг проблем**.

   Откроется окно **Мониторинг проблем**.
4. В открывшемся окне нажмите на кнопку нажмите на кнопку **Выполнить скрипт**.

   Откроется окно **Выполнение скрипта AVZ**.
5. Скопируйте текст скрипта, полученного от специалистов Службы технической поддержки, вставьте его в поле ввода в открывшемся окне и нажмите на кнопку **Далее**.

   Запустится выполнение скрипта.

В случае успешного выполнения скрипта работа мастера завершится автоматически. Если во время выполнения скрипта возникнет сбой, мастер выведет на экран соответствующее сообщение.

ГЛОССАРИЙ

К

Kaspersky Security Network (KSN)

Инфраструктура онлайн-служб и сервисов, предоставляющая доступ к оперативной базе знаний «Лаборатории Касперского» о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции программ «Лаборатории Касперского» на неизвестные угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

А

Активация программы

Перевод программы в полнофункциональный режим. Активация выполняется пользователем во время или после установки программы. Для активации программы пользователю необходим код активации.

Б

База вредоносных веб-адресов

Список адресов веб-ресурсов, содержимое которых может быть расценено как 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, которые содержат информацию об угрозах компьютерной безопасности, известных «Лаборатории Касперского» на момент выпуска баз. Записи в базах позволяют обнаруживать в проверяемых объектах вредоносный код. Базы формируются специалистами «Лаборатории Касперского» и обновляются каждый час.

Безопасные платежи

Модуль программы, предназначенный для защиты конфиденциальных данных, которые пользователь вводит на веб-сайтах банков и платежных систем, а также для предотвращения кражи денег при проведении платежей онлайн.

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 модифицированный участок кода известной программы, представляющей угрозу, или объект, напоминающий такую программу по своему поведению.

Возможный спам

Сообщение, которое нельзя однозначно классифицировать как спам, но которое обладает некоторыми признаками спама (например, некоторые виды рассылок и рекламных сообщений).

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

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 жестком 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, участок кода которого полностью совпадает с участком кода известной программы, предоставляющей угрозу. Специалисты «Лаборатории Касперского» не рекомендуют вам работать с такими объектами.

Защищенный браузер

Браузер, запущенный в режиме Безопасных платежей. Запуск защищенного браузера производится при обращении к сайту интернет-банкинга, что позволяет программе обеспечить защиту пользовательских данных от кражи. При этом в обычном браузере, использованном для обращения к веб-сайту, отображается сообщение о запуске защищенного браузера.

К

Карантин

Специальное хранилище, в которое программа помещает резервные копии файлов, измененных или удаленных во время лечения. Копии файлов хранятся в специальном формате и не представляют опасности для компьютера.

Клавиатурный 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.

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.

Л

Лечение объектов

Способ обработки зараженных объектов, в результате применения которого происходит полное или частичное восстановление данных. Не все зараженные объекты можно вылечить.

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 из-за 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 файла общими символами. Основными символами, используемыми в масках файлов, являются * и ? (где * - любое число любых символов, а ? – любой один символ).

Мастер-пароль

Единый пароль, который используется для защиты базы Менеджера паролей и обеспечивает доступ к данным.

Н

Неизвестный вирус

Новый вирус, информации о котором нет в базах. Как правило, неизвестные вирусы обнаруживаются программой в объектах при помощи эвристического анализатора. 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

Функция программы «Лаборатории Касперского», позволяющая поддерживать защиту компьютера в актуальном состоянии. Во время обновления программа копирует обновления баз и модулей программы с серверов обновлений «Лаборатории Касперского» на компьютер и автоматически устанавливает и применяет их.

Объекты автозапуска

Набор программ, необходимых для запуска и правильной работы операционной системы и программного обеспечения вашего компьютера. Каждый раз при старте операционная система запускает эти объекты.

Существуют вирусы, способные поражать именно объекты автозапуска, что может привести, например, к блокированию запуска операционной системы.

Онлайн-хранилище

Способ хранения информации на удаленных, часто географически распределенных серверах. Использование Онлайн-хранилища упрощает синхронизацию данных на разных компьютерах и мобильных устройствах. Для работы с Онлайн-хранилищем нужен доступ к интернету.

П

Пакет обновлений

Пакет файлов для обновления модулей программы. Программа «Лаборатории Касперского» копирует пакеты обновлений с серверов обновлений «Лаборатории Касперского», затем автоматически устанавливает и применяет их.

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 карантина.

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, зараженные или возможно зараженные объекты обрабатываются в соответствии с параметрами задачи (лечатся, удаляются).

Проверка трафика

Проверка в режиме реального времени с использованием информации текущей (последней) версии баз объектов, передаваемых по всем протоколам (например, HTTP, FTP и прочим).

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 изменен прокси-сервером в определенных 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, FTP и NNTP.

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

Руткит

Программа или набор программ для скрытия следов присутствия злоумышленника или вредоносной программы в системе.

В системах Windows под руткитом принято подразумевать программу, которая внедряется в систему и перехватывает системные функции (Windows API). Перехват и модификация низкоуровневых API-функций, в первую очередь, позволяет такой программе достаточно качественно маскировать свое присутствие в системе. Кроме того, как правило, руткит может маскировать присутствие в системе любых описанных в его конфигурации процессов, каталогов и файлов на диске, ключей в реестре. Многие руткиты устанавливают в систему свои драйверы и службы (они также являются «невидимыми»).

С

Серверы обновлений «Лаборатории Касперского»

HTTP-серверы «Лаборатории Касперского», с которых программа «Лаборатории Касперского» получает обновления баз и модулей программы.

Скрипт

Небольшая компьютерная программа или независимая часть программы (функция), как правило, написанная для выполнения конкретной задачи. Наиболее часто применяется при использовании программ, встраиваемых в гипертекст. Скрипты запускаются, например, когда вы открываете некоторые веб-сайты.

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.

Срок действия лицензии

Период времени, в течение которого вы можете пользоваться функциями программы и дополнительными услугами.

Срочное обновление

Критическое обновление модулей программы «Лаборатории Касперского».

Степень угрозы

Показатель вероятности, с которой компьютерная программа может представлять угрозу для операционной системы. Степень угрозы вычисляется с помощью эвристического анализа на основании критериев двух типов:

- статических (например, информация об исполняемом файле программы: размер файла, дата создания и тому подобное);

- динамических, которые применяются во время моделирования работы программы в виртуальном окружении (анализ вызовов программой системных функций).

Степень угрозы позволяет выявить поведение, типичное для вредоносных программ. Чем ниже степень угрозы, тем больше действий в системе разрешено программе.

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 (базы программы 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 которому был присвоен статус *не заражен*. 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 базы программы, 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.

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 карантине (если данная функциональность не отключена).

Упакованный файл

Файл архива, который содержит в себе программу-распаковщик и инструкции операционной системе для ее выполнения.

Уровень безопасности

Под уровнем безопасности понимается предустановленный набор параметров работы компонента программы.

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.

Ф

Фишинг

Вид интернет-мошенничества, заключающийся в рассылке электронных сообщений с целью кражи конфиденциальной информации, как правило, финансового характера.

Х

Хранилище резервных копий

Дисковое пространство или носитель информации, выделенные для создания резервных копий файлов при выполнении задач резервного копирования.

Ц

Центр защиты

Модуль программы, который обеспечивает комплексную защиту компьютера от различных угроз. Центр защиты обеспечивает антивирусную защиту компьютера, а также защиту от спама и сетевых атак. В состав модуля входят компоненты Обновление, Мониторинг активности программ и Карантин.

Цифровая подпись

Зашифрованный блок данных, который входит в состав документа или программы. Цифровая подпись используется для идентификации автора документа или программы. Для создания цифровой подписи автор документа или программы должен иметь цифровой сертификат, который подтверждает личность автора.

Цифровая подпись позволяет проверить источник и целостность данных, и защититься от подделки.

Э

Эвристический анализатор

Технология обнаружения угроз, информация о которых еще не занесена в базы «Лаборатории Касперского». Эвристический анализатор позволяет обнаруживать объекты, поведение которых в системе может представлять угрозу безопасности. Объекты, обнаруженные с помощью эвристического анализатора, признаются возможно зараженными. Например, возможно зараженным может быть признан объект, который содержит последовательности команд, свойственные вредоносным объектам (открытие файла, запись в файл).

ЗАО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

«Лаборатория Касперского» – известный в мире производитель систем защиты компьютеров от угроз: вирусов и других вредоносных программ, нежелательной почты (спама), сетевых и хакерских атак.

В 2008 году «Лаборатория Касперского» вошла в четверку ведущих мировых лидеров рынка программных решений для обеспечения информационной безопасности для конечных пользователей (рейтинг «IDC Worldwide Endpoint Security Revenue by Vendor»). По результатам исследования КОМКОН TGI-Russia 2009, «Лаборатория Касперского» – самый предпочитаемый производитель систем защиты для домашних пользователей в России.

«Лаборатория Касперского» основана в России в 1997 году. Сегодня «Лаборатория Касперского» – это международная группа компаний с центральным офисом в Москве и пятью региональными дивизионами, управляющими деятельностью компании в России, Западной и Восточной Европе, на Ближнем Востоке, в Африке, в Северной и Южной Америке, в Японии, Китае и других странах Азиатско-Тихоокеанского региона. В компании работает более 2000 квалифицированных специалистов.

Продукты. Продукты «Лаборатории Касперского» защищают как домашние компьютеры, так и компьютерные сети организаций.

Линейка персональных продуктов включает антивирусные приложения для настольных компьютеров и ноутбуков, для карманных компьютеров, смартфонов и других мобильных устройств.

Компания предлагает программы и сервисы для защиты рабочих станций, файловых и веб-серверов, почтовых шлюзов, сетевых экранов. Использование этих решений в сочетании с централизованными средствами управления позволяет построить и эксплуатировать эффективную автоматизированную защиту организации от компьютерных угроз. Продукты «Лаборатории Касперского» сертифицированы крупными тестовыми лабораториями, совместимы с программным обеспечением многих поставщиков программного обеспечения и оптимизированы для работы на многих аппаратных платформах.

Вирусные аналитики «Лаборатории Касперского» работают круглосуточно. Каждый день они находят сотни новых компьютерных угроз, создают средства их обнаружения и лечения и включают их в базы, используемые программами «Лаборатории Касперского». *Антивирусная база «Лаборатории Касперского» обновляется ежечасно*, *база Анти-Спама – каждые 5 минут*.

Технологии. Многие технологии, без которых трудно представить себе современный антивирус, впервые разработаны именно «Лабораторией Касперского». Не случайно программное ядро Антивируса Касперского используют в своих продуктах многие другие разработчики программ: среди них SafeNet (USA), Alt-N Technologies (USA), Blue Coat Systems (USA), Check Point Software Technologies (Israel), Clearswift (UK), CommuniGate Systems (USA), Critical Path (Ireland), D-Link (Taiwan), M86 Security (USA), GFI (Malta), IBM (USA), Juniper Networks (USA), LANDesk (USA), Microsoft (USA), NETASQ (France), NETGEAR (USA), Parallels (Russia), SonicWALL (USA), WatchGuard Technologies (USA), ZyXEL Communications (Taiwan). Многие из инновационных технологий компании подтверждены патентами.

Достижения. За годы борьбы с компьютерными угрозами «Лаборатория Касперского» завоевала сотни наград. Например, в 2010 году Антивирус Касперского получил несколько высших наград Advanced+ в тестах, проведенных авторитетной австрийской антивирусной лабораторией AV-Comparatives. Но главная награда «Лаборатории Касперского» – это приверженность пользователей по всему миру. Продукты и технологии компании защищают более 300 миллионов пользователей. Количество организаций, являющихся ее клиентами, превышает 200 тысяч.

Веб-сайт «Лаборатории Касперского»:	http://www.kaspersky.ru
Вирусная энциклопедия:	http://www.securelist.com/ru/
Антивирусная лаборатория:	newvirus@kaspersky.com (только для отправки возможно зараженных файлов 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

Информация о стороннем коде содержится в файле legal_notices.txt, расположенном в папке установки программы.

УВЕДОМЛЕНИЯ О ТОВАРНЫХ ЗНАКАХ

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Google Chrome – товарный знак Google, Inc.

Intel, Pentium и Atom – товарные знаки Intel Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

Microsoft, Windows, Windows Vista и Internet Explorer – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

Mozilla и Firefox – товарные знаки Mozilla Foundation.

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

М

О

П

Р

С

У

Х

Ш