

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Локтионова Оксана Геннадьевна
Должность: проректор по учебной работе
Дата подписания: 06.08.2021 16:27:38
Уникальный программный ключ:
0b817ca911e6668abb13a5d426d39e5f1c11eabbf73e943df4a4851fda56d089

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ

Проректор по учебной работе

О. Г. Локтионова

« 1 » 02

2018 г.



АНТИВИРУСНАЯ ПРОГРАММА: KASPERSKY INTER- NET SECURITY

Методические указания по выполнению лабораторных и
практических занятий
для студентов укрупненной группы специальностей и направ-
лений подготовки 10.00.00, 09.00.00, 38.00.00.

Курск 2018

УДК 004

Составитель: К.А. Тезик

Рецензент

Кандидат технических наук, доцент кафедры «Информационная безопасность» А. Л. Марухленко

Антивирусная программа: Kaspersky Internet Security: методические указания по выполнению лабораторных работ по дисциплине «Защита информационных процессов в компьютерных системах» / Юго-Зап. гос. ун-т; сост.: К. А. Тезик, Курск, 2018. 14 с.: ил. 8, Библиогр.: с. 14.

Содержат краткие теоретические положения о методике настройки и правилах эксплуатации антивирусной программы: Kaspersky Internet Security.

Методические указания соответствуют требованиям программы по направлению подготовки бакалавров: информационная безопасность, программная инженерия, информационные системы и технологии, прикладная информатика, фундаментальная и прикладная лингвистика и специалистов: экономическая безопасность.

Предназначены для студентов укрупненной группы специальностей и направлений подготовки 10.00.00, 09.00.00 ,38.00.00 дневной и заочной формы обучения.

Текст печатается в авторской редакции

Подписано в печать 02.18 . Формат 60x84 1/16.

Усл. печ. 0.81л.. Уч. – изд. 0.73л.. Тираж 100 экз. Заказ. Бесплатно. 245

Юго - Западный государственный университет.

305040, г. Курск, ул. 50 лет Октября, 94.

Практическое занятие

Антивирусная программа: Kaspersky Internet Security

Введение

"Лаборатория Касперского" — российская компания-разработчик антивирусных средств защиты. Первый свой продукт, прототип нынешнего Антивируса Касперского, компания выпустила в 1994 году. Разработка сразу же привлекла к себе внимание рынка средств информационной защиты, опередив на международном тестировании в показателях обнаружения и нейтрализации вирусов другие программные продукты. С тех пор антивирусные продукты "Лаборатории Касперского" постоянно занимают высокие места в рейтингах международных исследований антивирусного программного обеспечения.

Для домашнего использования "Лаборатория Касперского" в настоящее время представляет два пакета, осуществляющие защиту компьютеров: Антивирус Касперского и Kaspersky Internet Security, а также продукт для защиты смартфонов — Kaspersky Mobile Security. Базовым решением обеспечения антивирусной безопасности является Антивирус Касперского. Он обеспечивает безопасность компьютера при работе в Интернете и защиту электронной почты. Используемые им технологии позволяют защищать систему от неизвестных угроз, блокировать доступ к зараженным и опасным веб-сайтам, проверять на вирусы ICQ-сообщения, а также надежно защищать сам антивирус от попыток его отключения вредоносными программами. К дополнительным возможностям Антивируса Касперского относится проверка операционной системы компьютера и программного обеспечения на присутствие уязвимостей и настройка их безопасности, средства для восстановления работоспособности операционной системы и возможность безопасного ввода логинов, паролей и другой конфиденциальной информации при работе в Интернете. Совместно с Антивирусом Касперского для полноценной защиты компьютера компания-производитель рекомендует использовать брандмауэр. Пакет Kaspersky Internet Security обладает более широкими возможностями информационной защиты. Он осуществляет контроль за работой приложений операционной системы и ограничивает их доступ

к системным областям и личным данным пользователя, в том числе к логинам и паролям, включает в себя специальную технологию "безопасной среды" для запуска и открытия в ней подозрительных файлов и сайтов и интеллектуальный метод эффективной фильтрации нежелательных сообщений. В числе других полезных возможностей Kaspersky Internet Security инструмент для анализа работы сети, блокирование рекламы на веб-сайтах и средство, предназначенное для компьютеров, используемых всей семьей, которое позволяет регулировать применение Интернета детьми.

Kaspersky Mobile Security — средство защиты для мобильных платформ. С помощью Kaspersky Mobile Security вы можете защитить свой мобильный телефон от проникновения вирусов, хакерских атак, нежелательных звонков и SMS, а также защитить устройство и информацию, хранящуюся на нем, от нежелательного использования. Для осуществления последней функции в Kaspersky Mobile Security встроена система, называемая "Anti-Vop". Она предназначена для случаев потери смартфона или его кражи, и включает следующие средства защиты:

SMS-Block — инструмент блокировки смартфона и хранящихся на нем данных. Для включения блокировки необходимо отправить на его номер SMS с заданным вами заранее паролем. При нахождении телефона разблокировать его можно с помощью введения другого пароля, также ранее заданным вами. SMS-Find — средство для определения местонахождения потерянного или украденного смартфона. Путем отправки SMS с паролем на номер мобильного устройства вы имеете возможность узнать координаты его нахождения в системе картографического сервиса Google Maps — интернет-сервиса, представляющего собой спутниковую карту мира. Средство SMS-Find может использоваться только в смартфонах с поддержкой GPS-навигатора.

SMS-Clean позволяет с помощью отправки SMS удалить всю хранящуюся на смартфоне информацию. Например, в случае невозможности вернуть похищенный телефон.

SIM Watch — инструмент защиты извлечения из смартфона SIM-карты. При попытке извлечь SIM-карту из телефона SIM Watch автоматически блокирует телефон. При установке новой

SIM-карты телефон отправляет вам сообщение, содержащее его новый номер.

Также для защиты данных телефона Kaspersky Mobile Security содержит функцию их шифрования. Для хранения зашифрованных данных используется специальная папка на карте памяти телефона, доступ к которой можно получить только введением задаваемого вами пароля. Даже если карта памяти будет вставлена в другое устройство. Непосредственно для защиты от вирусов Kaspersky Mobile Security содержит антивирусный компонент и сетевой экран. Антивирус обеспечивает постоянную защиту устройства, имеет антивирусный сканер и функцию постоянного обновления вирусных баз. Сетевой экран следит за сетевыми соединениями с целью предупреждения нежелательного проникновения извне. Для защиты от нежелательных звонков и SMS в Kaspersky Mobile Security существует возможность создания "черных" и "белых" списков абонентов. Блокировку SMS можно осуществлять не только по номеру отправителя, но и по ключевым фразам, которые содержатся в сообщении.

Краткие теоретические положения

Пакет Kaspersky Internet Security является решением, предназначенным для комплексной защиты вашего компьютера. В нем имеются как средства для защиты от компьютерных вирусов, троянов и червей, так и средства для защиты от несанкционированного проникновения в сеть, средства защиты от сомнительных сайтов и многое другое.

Скачать дистрибутив KIS 2016 можно на сайте www.kaspersky.ru. Вам будет доступна бесплатная 30-дневная полнофункциональная версия продукта. Перед началом установки вам необходимо ознакомиться с требованиями к оборудованию и программному обеспечению, предоставляемыми разработчиком — Лабораторией Касперского для эффективной работы пакета. Необходимо соблюдать эти требования, т. к. иначе, если вы будете использовать машину с меньшим количеством оперативной памяти или более слабым процессором, после установки антивируса компьютер станет работать существенно медленнее.

Сама по себе установка не вызывает каких-либо трудностей. По заявлениям разработчиков, KIS 2016 при установке автоматически удаляет другие антивирусы. Однако если у вас на компьютере до установки KIS 2016 уже использовался какой-либо антивирусный продукт, лучше все же удалить его вручную, во избежание возможных проблем при установке пакета KIS 2016.

После установки KIS 2016 обязательно должен обновить антивирусные базы через Интернет, так что вам необходимо предоставить программе доступ в глобальную сеть.

Для открытия консоли KIS 2016 нажмите на клавиатуре клавишу или соответствующий значок на рабочем столе. Далее выберите All Programs | Kaspersky Internet Security | Kaspersky Internet Security. Откроется рабочее окно антивируса Kaspersky Internet Security 2016 (рис.1).

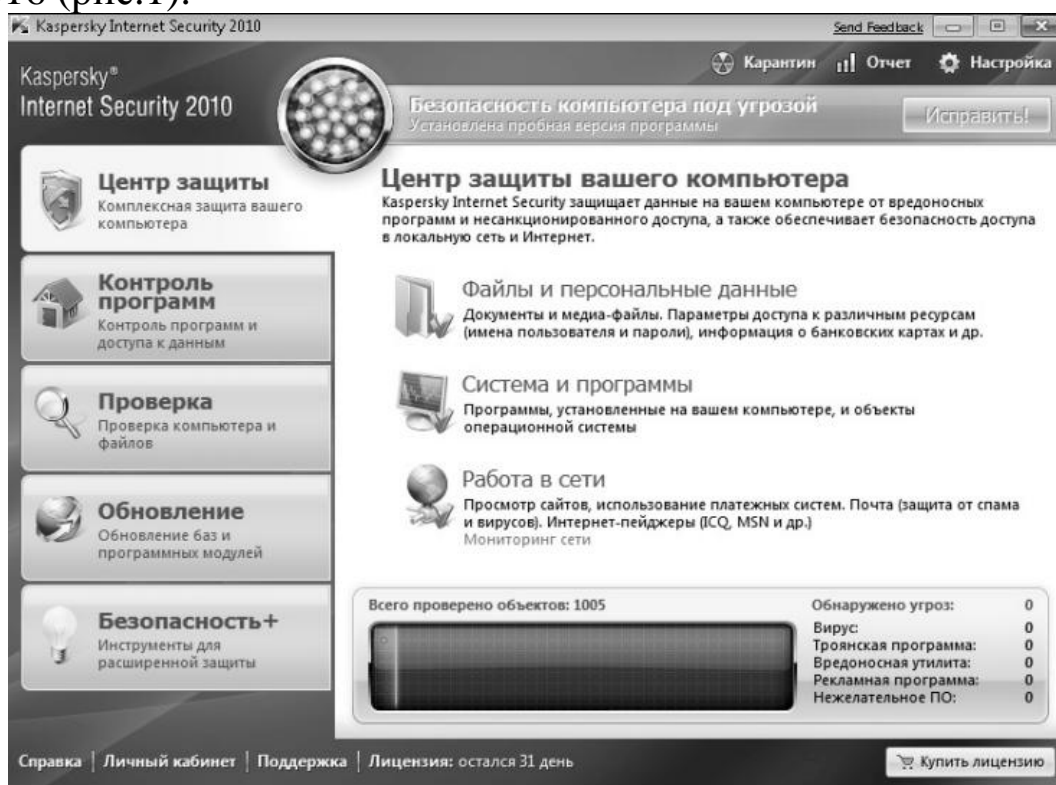


Рис. 1. Центр защиты антивируса KIS 2016

Итак, на рис. 1 перед нами предстает рабочее окно KIS 2016, открытое на вкладке Центр защиты. В верхней части окна находится сигнал светофора, показывающий статус системы на настоящий момент. Статус защиты желтый, т. е. безопасность компьютера под угрозой если используется испытательная версия программы. В

случае если бы не были установлены обновления, сигнал светофора был бы красный. А если бы была установлена коммерческая версия KIS 2016 и последние версии антивирусных баз, то сигнал был бы зеленый. Для того чтобы исправить существующие проблемы, можно воспользоваться кнопкой **Исправить**, в правой верхней части экрана. В нашем случае откроется окно с предложением приобрести лицензию на использование KIS 2016. В случае если используются просроченные антивирусные базы, будет произведено принудительное обновление баз. Также в этом окне вы можете наблюдать за состоянием системы, обнаруженными вредоносными программами, количеством проверенных объектов и т. д. В центральной части окна показан статус защиты различных компонент системы, таких как **Файлы и персональные данные, Система и программы, Работа в сети**. Обратите внимание на то, что около каждого из этих элементов должна стоять зеленая галочка. Это говорит о том, что защита данной компоненты включена.

На второй вкладке **Контроль программ** (рис. 2) производится контроль и предотвращение выполнения программы каких-либо вредоносных действий.

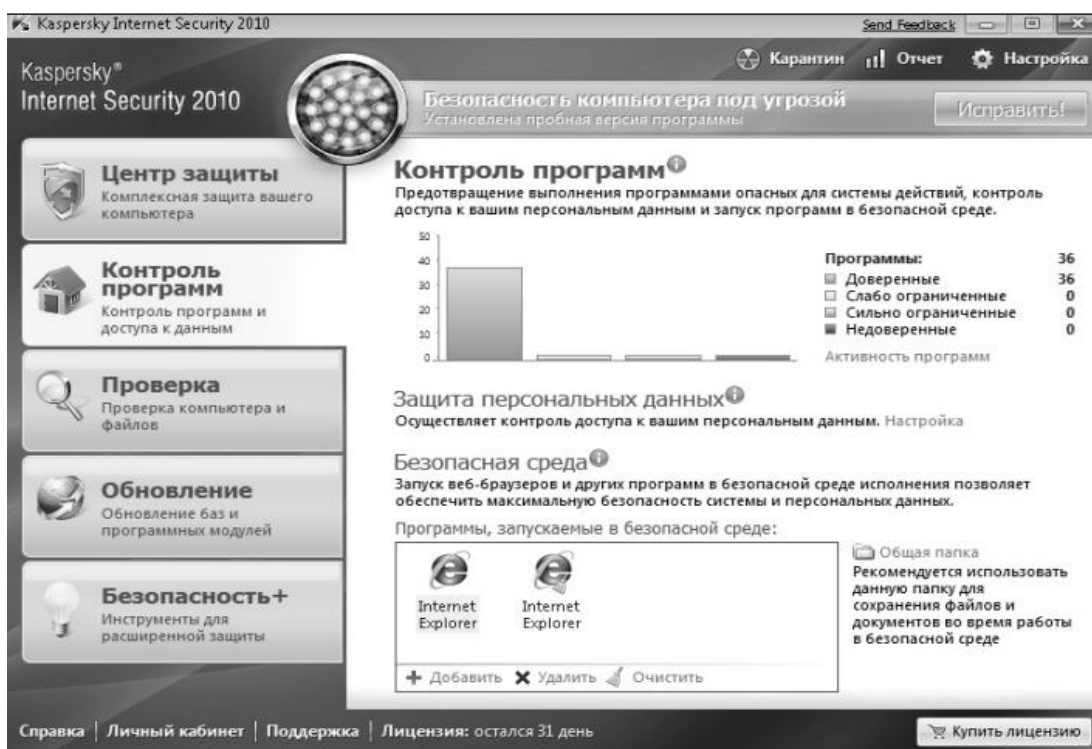


Рис. 2. Вкладка контроля программ и доступа к данным

На вкладке контроля программ графически представлена активность различных приложений на вашем компьютере. Также в этой вкладке можно настроить защиту персональных данных.

Еще одним новым средством защиты в KIS 2016 является безопасная среда. В нее можно помещать различные приложения, например веб-браузер или же клиент электронной почты. Работа в безопасной среде позволяет оградить работающее приложение от основной среды, и в случае проникновения вредоносного кода в данное приложение, например при заражении веб-браузера, злоумышленник не сможет проникнуть в другие приложения и использовать их ресурсы.

Во вкладке **Проверка** вы можете произвести полную проверку системы или же произвести выборочное сканирование отдельных дисков компьютера (рис. 3). Также здесь можно открыть окно поиска уязвимостей.

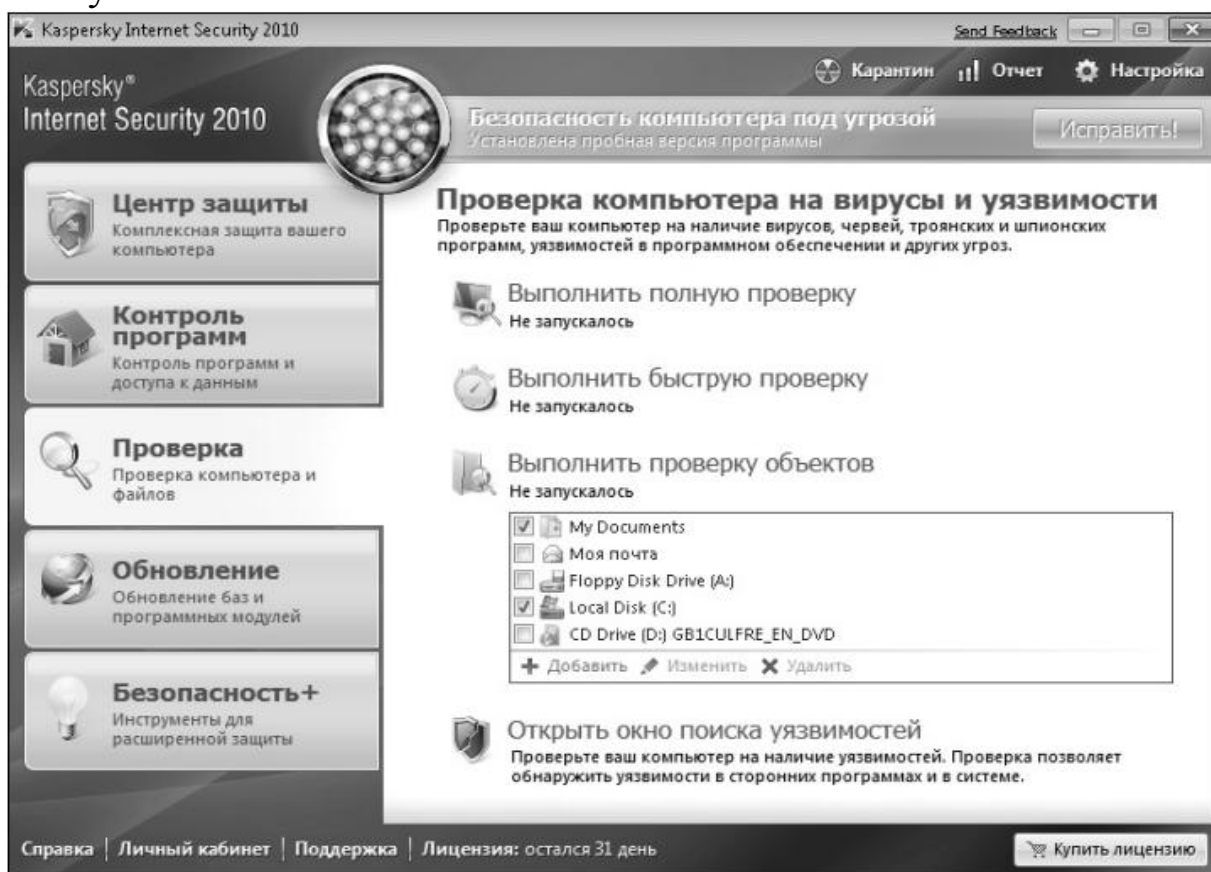


Рис. 3. Вкладка проверки компьютера и файлов

На вкладке **Обновление** показан статус всех баз, используемых KIS 2016.

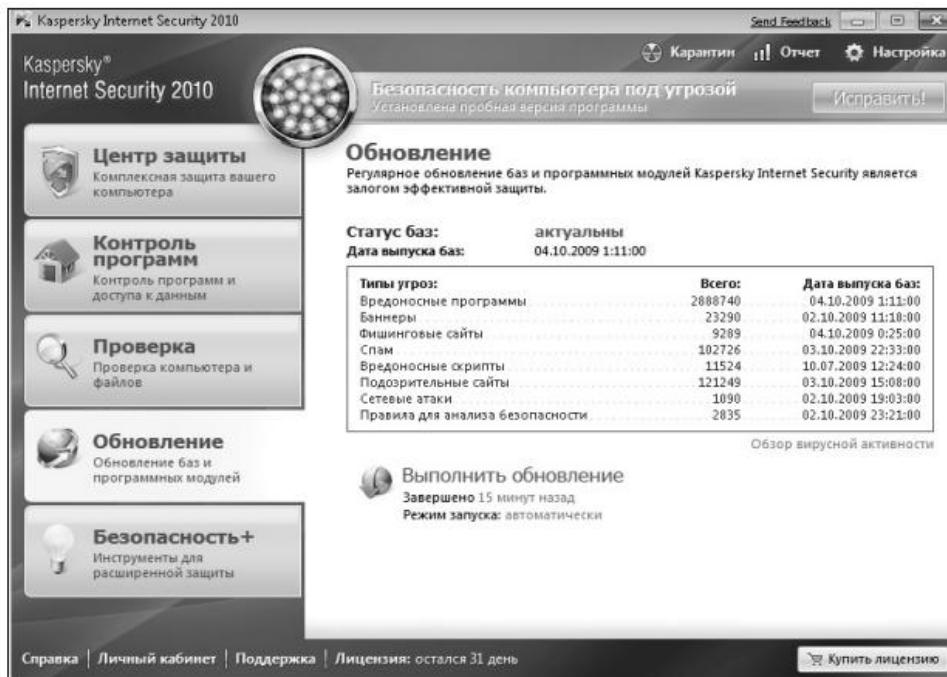


Рис. 4. Вкладка управления обновлениями программы

Здесь мы можем видеть количество сигнатур для различных угроз, а также даты выпуска этих баз. При необходимости можно выполнить принудительное обновление, щелкнув ссылку **Выполнить обновление**. На вкладке **Безопасность+** находятся дополнительные инструменты и сервисы для обеспечения безопасности вашего компьютера и оптимизации выполнения различных задач (рис. 5).



Рис. 5. Вкладка инструментов расширенной защиты

Например, с помощью виртуальной клавиатуры вы можете защититься от клавиатурных перехватчиков. С помощью ссылки **Родительский контроль** ограничить доступ пользователей к определенным веб-ресурсам. Также здесь имеются различные средства для восстановления системы. Вернемся к уже упоминавшемуся средству по поиску уязвимостей. Для того чтобы воспользоваться этим средством, необходимо открыть вкладку **Проверка основного окна Kaspersky Internet Security 2016** и затем выбрать ссылку **Открыть окно поиска уязвимостей**. Откроется окно **Поиск уязвимостей** (рис. 6).

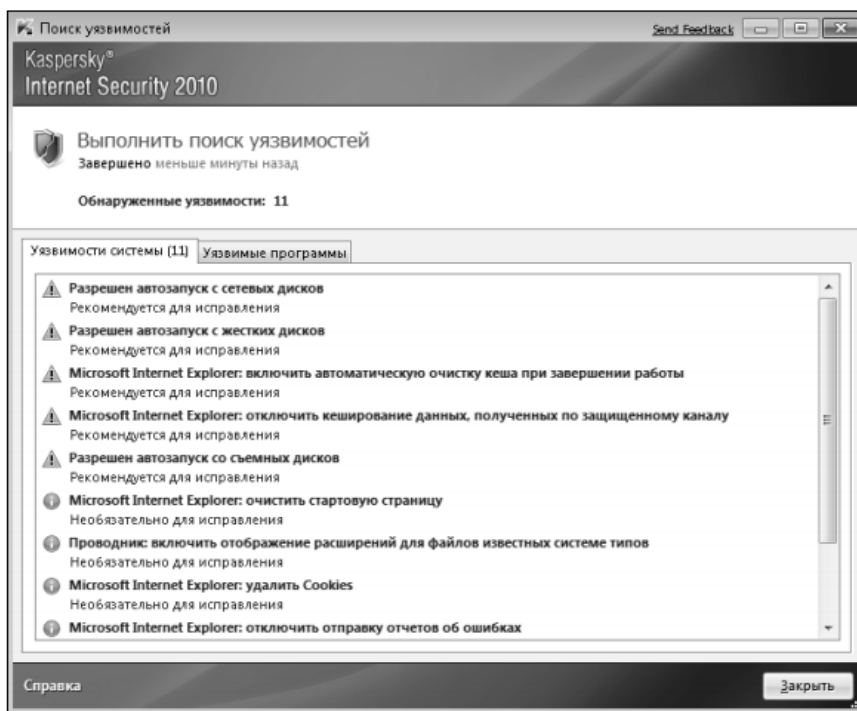


Рис. 6. Окно поиска уязвимостей

Здесь вы можете проверить ваш компьютер на наличие уязвимостей. Программа KIS 2016 содержит сведения об известных уязвимостях в операционной системе и установленных приложениях. Еще одним интересным средством является **Мастер восстановления системы** (рис. 7). С помощью данного средства вы сможете восстановить систему после воздействия вредоносного кода, а также устранить последствия некорректной настройки отдельных компонентов системы. Общие настройки KIS 2016, в которых содержатся параметры всех ранее описанных компонент, и многое другое открываются щелчком на ссылке **Настройка** в главном

окне Kaspersky Internet Security 2016 (рис. 8). Здесь вы можете найти настройки любого элемента KIS 2016 и произвести соответствующие изменения.

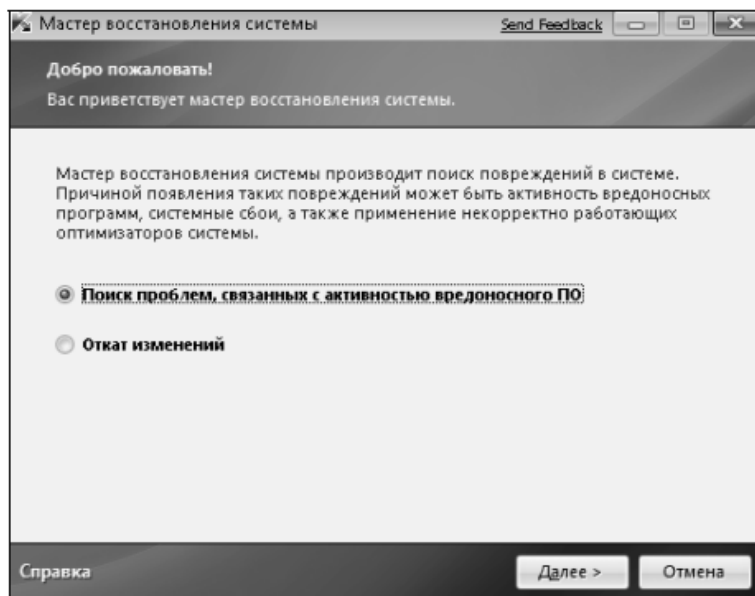


Рис. 7. Мастер восстановления системы

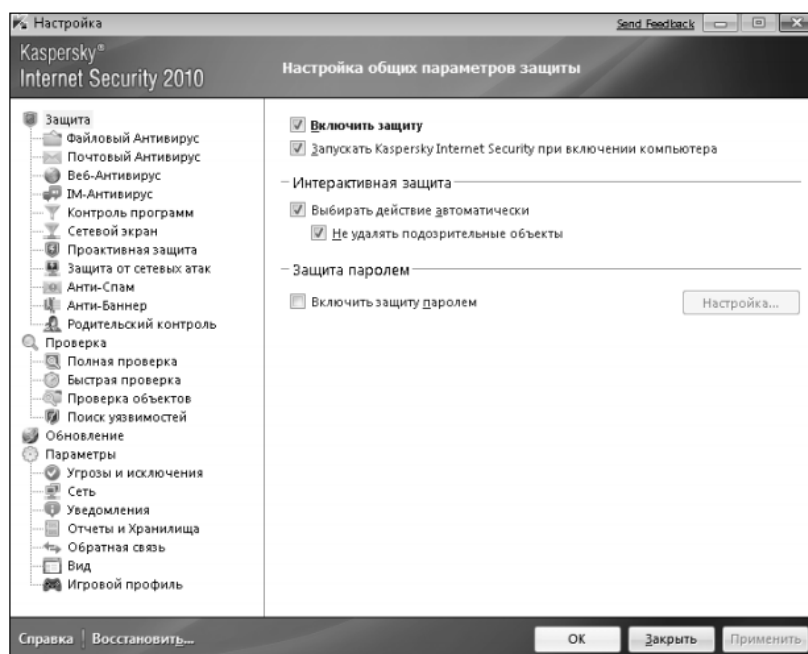


Рис. 8. Окно настройки параметров защиты

Практическое задание

Цель работы: изучить интерфейс, методику эксплуатации и настройки программы **Kaspersky Internet Security**.

Порядок выполнения работы:

- 1) Проверьте статус защиты компонент системы: **Файлы и персональные данные, Система и программы, Работа в сети**.
- 2) Обновите антивирусные базы Kaspersky Internet Security.
- 3) Проверьте активность приложений на вашем компьютере. Проанализируйте, являются ли все приложения доверенными.
- 4) Настройте защиту персональных данных.
- 5) Установите Web-браузер в безопасную среду.
- 6) Проведите сканирование диска D.
- 7) Воспользуйтесь виртуальной клавиатурой для набора абзаца текста.
- 8) С помощью ссылки **Родительский контроль** ограничьте доступ пользователя к Web-сайту знакомств.
- 9) Проверьте операционную систему и установленные приложения на наличие уязвимостей.
- 10) Оптимизируйте настройку системы с помощью **Мастера восстановления системы**.
- 11) Настройте межсетевой экран.
- 12) Настройте анти-спам.
- 13) Настройте анти-баннер.
- 14) Настройте защиту от сетевых атак.
- 15) Выполните резервное копирование информации.

Список контрольных вопросов

- 1) Дайте классификацию компьютерных вирусов.
- 2) В чем основное отличие вирусов-сценариев от файловых вирусов?
- 3) Существование каких вирусов зависит от конкретной программы?
- 4) В чем основное отличие троянской программы от вируса. Приведите пример троянской программы.
- 5) Дайте классификацию компьютерных червей. Приведите примеры компьютерных червей.
- 6) Перечислите методы обнаружения вирусов.
- 7) Какой метод выявления вирусов позволяет обнаруживать только известные вирусы?
- 8) В чем сущность метода обнаружения вирусов, основанного на сигнатурах?
- 9) В чем сущность метода выявления вирусов – обнаружение программ подозрительного поведения?
- 10) В чем сущность метода обнаружения вирусов при помощи “белого списка”?
- 11) В чем сущность обнаружения вирусов при помощи эмуляции работы программы?
- 12) В чем сущность метода выявления вируса - эвристический анализ?
- 13) Почему не рекомендуется на одной ЭВМ использовать одновременно несколько антивирусов?
- 14) Какая антивирусная программа не конфликтует с другими антивирусами?
- 15) Приведите примеры бесплатных антивирусов.
- 16) Дайте общую характеристику возможностей программы Kaspersky Internet Security.

Список литературы

1. Нестеров С.А. Основы информационной безопасности [Электронный ресурс] : учебное пособие / С.А. Нестеров - СПб : Издательство Политехнического университета, 2014. - 322 с. // Режим доступа -<http://biblioclub.ru/index.php?page=book&id=363040>
2. Грибунин В. Г. Комплексная система защиты информации на предприятии [Текст] : учебное пособие / В. Г. Грибунин, В. В. Чудовский. – М.: Академия, 2009. - 416 с.
3. Садердинов А. А. Информационная безопасность предприятия[Текст]: учебное пособие/ А. А. Садердинов, В. А. Трайнев, А. А. Федулов. 2-е изд. – М.: Дашков и К., 2004. - 336 с.
4. Игнатъев В. А. Защита информации в корпоративных информационно-вычислительных сетях [Текст]: монография.- Старый Оскол: ТНТ, 2005. – 552 с.
5. Безбогов А. А., Яковлев А. В., Шамкин В. Н. Методы и средства защиты компьютерной информации [электронный ресурс]: Учебное пособие. – Тамбов: Издательство ТГТУ, 2006.- 196 с. /Электронная библиотека «Единое окно доступа к образовательным ресурсам» - <http://window.edu.ru>
6. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства / Шаньгин В. Ф. – М. : ДМК Пресс, 2010.-544 с.
7. Жадаев А. Г. Антивирусная защита ПК: от “чайника” к пользователю.
8. Технологии защиты информации в компьютерных сетях. Межсетевые экраны и интернет-маршрутизаторы [Текст] : учебное пособие / Е. А. Богданова [и др.]. - М. : Национальный Открытый Университет "ИНТУИТ", 2013. - 743 с.
9. Заика А. Компьютерная безопасность [Электронный ресурс] / А. Заика. - М. : РИПОЛ классик, 2013. - 160 с. // Режим доступа –
<http://biblioclub.ru/index.php?page=book&id=227317>