1. Виды компьютерных вирусов. Ознакомление с антивирусными программами.
2. Антивирусные средства защиты. Работа с антивирусной программой.

Первый вопрос: Виды компьютерных вирусов. Ознакомление с антивирусными программами.

Понятие компьютерного вируса.

Массовое применение персональных компьютеров, к сожалению, оказалось связанным с появлением самовоспроизводящихся программ–вирусов, препятствующих нормальной работе компьютера, разрушающих файловую структуру дисков и наносящих ущерб хранимой в компьютере информации. Проникнув в один компьютер, компьютерный вирус способен распространиться на другие компьютеры.

Компьютерный вирус – специально написанная программа деструктивного характера, способная самопроизвольно присоединять к другим программам свои копии и внедрять их в файлы, системные области жестких дисков.

Причины появления и распространения компьютерных вирусов, с одной скрываются в психологии человеческой личности и ее теневых сторонах (тщеславии непризнанных творцов, невозможности конструктивно применить способности), с другой стороны, обусловлены отсутствием аппаратных средств защиты персонального компьютера.

Несмотря на принятые во многих странах законы о борьбе с компьютерными преступлениями и разработку специальных программных средств защиты от вирусов, количество новых программных вирусов постоянно растет. На сегодняшний день известно **более 700 тыс. вирусов!!!**, для которых разработаны антивирусные средства. Это требует от пользователя компьютера знаний о природе вирусов, способах заражения вирусами и защиты от них.

Основными путями проникновения вирусов в компьютер являются **съемные носители (гибкие и лазерные диски), а также компьютерные сети.**

Программа или иной объект, содержащая вирус, называется **зараженной.**

При заражении компьютера вирусом очень важно своевременно его обнаружить. Для этого следует знать об основных **признаках проявления вирусов:**

- прекращение работы или неправильная работа ранее успешно функционирования программ;
- медленная работа компьютера;
- невозможность загрузки операционной системы;
- исчезновение файлов и каталогов или искажение их содержимого;
- изменение даты и времени модификации файлов;
- изменение размеров файлов;

- неожиданное значительное увеличение количества файлов на диске;
- существенное уменьшение размера свободной оперативной памяти;
- вывод на экран непредусмотренных сообщений или изображений;
- подача непредусмотренных звуковых сигналов;
- частые зависания и сбои в работе компьютера.

Следует заметить, что вышеперечисленные явления необязательно вызываются присутствием вируса, а могут быть следствием других причин. Поэтому всегда затруднена правильная диагностика состояния компьютера.

Основные виды вирусов.

В настоящее время известно более 700 тыс. программных вирусов, их можно классифицировать по следующим признакам:

– среде обитания;
– по воздействию;
– по способу заражения ОЗУ;
– по особенностям алгоритма;

В зависимости от среды обитания вирусы можно разделить на сетевые, файловые, загрузочные.

Сетевые вирусы распространяются по локальным и глобальным компьютерным сетям.

Файловые вирусы внедряются главным образом в исполняемые модули, т.е. в файлы, имеющие расширения .**COM** и .**EXE**. Заражая файл, вирус внедряется в его код, чтобы получить управление при запуске этого файла. После запуска вирус помешается в оперативную память и поражает другие исполняемые файлы, к которым обратился пользователь. Кроме своей основной функции – размножения вирус может сделать что–нибудь: спросить, сыграть, показать изображение.

Таким образом, при запуске любого исполнимого файла вирус получает управление (операционная система запускает его сама), устанавливается в память и передает управление вызванному файлу.

Файловые вирусы могут внедряться и в другие типы файлов, но, как правило, записанные в таких файлах, они никогда не получают управление и, следовательно, теряют способность к размножению.

Загрузочные вирусы внедряются в загрузочный сектор диска (Boot–сектор) или в сектор, содержащий программу загрузки системного диска (Master Boot Record).

Загрузочный сектор – это сектор на дискете или жестком диске с которого происходит загрузка операционной системы программами BIOS.

Пусть у нас имеется зараженная дискета и "чистый" компьютер. Нормальная схема начальной загрузки такая: ПЗУ – ПНЗ (программа начальной загрузки в загрузочном секторе) – ОС

Заражая дискету, вирус делает следующее:

– выделяет некоторую область диска и помечает ее как недоступную ОС (сбойные секторы bad);

– копирует в выделенную область диска свой «хвост» и здоровый загрузочный сектор;

– Замещает программу загрузки своей «головой».

В итоге последовательность загрузки изменяется и замедляется, так как появилось новое звено – вирус.

При воздействии вируса схема изменяется **ПЗУ–ВИРУС–ПНЗ–ОС**

Таким же образом поражаются загрузочные секторы винчестеров.

По способу функционирования вирусы делятся на резидентные и нерезидентные.

Резидентный вирус при заражении (инфицировании) компьютера оставляет в оперативной памяти свою резидентную часть, которая потом перехватывает обращение операционной системы к объектам заражения (файлам, загрузочным секторам диска и внедряется в них). Резидентные вирусы находятся в памяти и являются активными до выключения или перезагрузки компьютера. **Нерезидентные вирусы** не заражают память компьютера и являются активными ограниченное время.

По степени воздействия вирусы можно разделить на следующие виды:

– неопасные, не мешающие работе компьютера, но уменьшающие объем оперативной и внешней памяти, действия таких вирусов проявляется в каких–либо графических или звуковых эффектах;

– опасные вирусы, которые могут привести к различным нарушениям в работе компьютера;

– очень опасные, воздействие которых может привести к потере программ, поражению данных, стиранию информации в системных областях диска (Чернобыль 26 апреля «Chih»).

По особенностям алгоритма можно выделить следующие группы вирусов:

– компаньон–вирусы (companion) – это вирусы, не изменяющие файлы, но создающие файлы–компаньоны. Алгоритм работы этих вирусов состоит в том, что они создают для EXE–файлов файлы–спутники, имеющие то же самое имя, но с расширением .COM, (например, для файла ABC.EXE создается файл ABC.COM. Вирус записывается в COM–файл и никак не изменяет EXE–файл. При запуске такого файла ОС первым обнаружит и выполнит COM–файл, т.е. вирус, который затем запустит и EXE–файл. (Пример: I.Worm.Stator.a).

– сетевые вирусы – (черви, worm) распространяются по информационным сетям с одного сервера на другой, как правило, не выполняя деструктивных действий (по причине большого разнообразия и хорошей защищенности различных серверных ОС). Вред сетевых вирусов состоит в дополнительном расходе памяти и каналов связи, кроме того, черви могут служить транспортом для распространения других видов вирусов. Частный случай сетевых вирусов – почтовые черви (mail worm), распространяемые во вложениях к электронным письмам. Весной 2000 года несколько модификаций такого рода вирусов поразили миллионы компьютеров во всём мире. Почтовые черви могут причинить очень опасные повреждения информации, вплоть до полного уничтожения. Кроме того. Почтовые вирусы быстро распространяются, используя для этого адреса пользователей, содержащиеся в адресной книге почтовой программы.

(Пример: **вирус «Анна Курникова»**).

полиморфик–вирусы (polymorphic) – достаточно труднообнаруживаемые вирусы, модифицирующие свой код в зараженных программах таким образом, что два экземпляра одного и того же вируса не совпадают (имеют разные коды). Это вирусы с самомодифицирующимися расшифровщиками. Цель такого шифрования – имея зараженный и оригинальный файлы невозможно определить наличие вируса.

Вирусы–невидимки (стелс–вирусы) – такие вирусы при обращении к файлам используют достаточно оригинальные алгоритмы, позволяющие «обманывать» резидентные антивирусные мониторы предотвращают свое обнаружение тем, что перехватывают обращения операционной системы (и тем самым прикладных программ) к зараженным файлам и областям диска и подставляют вместо своего тела незараженные участки диска. Разумеется, этот эффект наблюдается только на зараженном компьютере – на «чистом» компьютере изменения в файлах и загрузочных областях.

«Троянские» программы (шпионы) маскируясь под полезную программу, разрушают загрузочный сектор и файловую систему дисков. Не способны к самораспространению. **Троянцы,** после своего запуска, скрытно выполняют определенные действия, направленные на снижение защищенности информационной системы: передают по электронной почте или сети пароли, файлы и другую информацию с компьютера

Макровирусы распространяются внутри документов Microsoft Office (файлы с расширениями .DOC, .DOT, .XLS, и др.), позволяющих использовать *макросы – последовательности команд,* автоматически выполняемые при открытии документа. Для защиты от заражения макровирусом достаточно включить предупреждение о наличии макросов в документе и не в коем случае не запускать подозрительные макросы, если только полезность их Вам не очевидна.

Антивирусные программы. Антивирусные средства защиты. (Ознакомление с антивирусными программами).

Для обнаружения, удаления и защиты от компьютерных вирусов разработано несколько видов специальных программ, которые позволяют обнаруживать и уничтожать вирусы. Такие программы называются антивирусными.

Различают следующие виды антивирусных программ:

– программы–детекторы;

– программы–доктора или фаги;

– программы–ревизоры;

– программы–фильтры;

– программы–вакцины или иммунизаторы.

Программы–детекторы осуществляют поиск характерной для конкретного вируса последовательности байтов (сигнатуры вируса) в оперативной памяти и в файлах и при обнаружении выдают соответствующее сообщение. Недостатком таких программ является то, что они могут находить только те вирусы, которые известны разработчикам таких программ.(KidoKiller.exe , на вирус Worms Kido – заражает

библиотеки и перехватывает управление над сетевым трафиком, происходит перегрузка сетевого канала).

Программы–доктора или фаги («от греч. жрать») не только находят зараженные вирусами файлы, но и «лечат» их, т.е. удаляют из файла тело программы вируса, возвращая файлы в исходное состояние. В начале своей работы фаги ищут вирусы в оперативной памяти, уничтожая их, и только затем переходят к «лечению» файлов. Учитывая, что постоянно появляются новые вирусы, программы–детекторы и программы–доктора быстро устаревают, и требуется регулярное обновление их версий. NOD 32, Norton Antivirus, Doctor Web, Awast, Panda, KaV.

Программы–ревизоры относятся к самым надежным средствам защиты от вирусов. Ревизоры запоминают исходное состояние программ, каталогов и системных областей диска тогда, когда компьютер не заражен вирусом, а затем периодически или по желанию пользователя сравнивают текущее состояние с исходным. Обнаруженные изменения выводятся на экран монитора. Как правило, сравнение состояний производят сразу после загрузки операционной системы. При сравнении проверяются длина файла, код циклического контроля (контрольная сумма файла), дата и время модификации, другие параметры.

Программы–ревизоры имеют достаточно развитые алгоритмы, обнаруживают стелс–вирусы и могут даже отличить изменения версии проверяемой программы от изменений, внесенных вирусом. К числу программ–ревизоров относится широко распространенная в России программа ADinf фирмы "Диалог–Наука". Awast

Программы–фильтры или "сторожа" представляют собой небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вирусов. Такими действиями могут являться:

– попытки коррекции файлов с расширениями COM и EXE;
– изменение атрибутов файлов;
– запись в загрузочные сектора диска;
–загрузка резидентной программы.

При попытке какой–либо программы произвести указанные действия «сторож» посылает пользователю сообщение и предлагает запретить или разрешить соответствующее действие. Программы–фильтры весьма полезны, так как способны обнаружить вирус на самой ранней стадии его существования до размножения. Однако они не "лечат" файлы и диски. Для уничтожения вирусов требуется применить другие программы, например фаги. К недостаткам программ–сторожей можно отнести их "назойливость" (например, они постоянно выдают предупреждение о любой попытке копирования исполняемого файла), а также возможные конфликты с другим программным обеспечением.

Вакцины или иммунизаторы – это резидентные программы, предотвращающие заражение файлов. Вакцины применяют, если отсутствуют программы–доктора, «лечащие» этот вирус. Вакцинация возможна только от известных вирусов. Вакцина модифицирует программу или диск таким образом, чтобы это не отражалось на их работе вирус будет воспринимать их зараженными и поэтому не внедрится. Panda Reaserch USB Vaccine 1.0

Современные антивирусные пакеты включают несколько программ с различными функциями.

Сегодня одним из наиболее популярных антивирусных пакетов является Dr.Web, антивирус Касперского (Kaspersky Anti–Virus – KAV).

Для проверки функционирования антивируса существует тест, созданный Европейским институтом антивирусных исследований – файл EICAR.com (всего 68 байт). Антивирус выдает сообщение: «Test (Not a Virus)», в графе действие – «неизлечим».

Подробнее:

Антивирус Касперского специально разработан для защиты персонального компьютера. Простые интерфейсы, централизованное управление, автоматическая работа позволяют продукту функционировать в фактически фоновом режиме до тех пор, пока компьютеру и данным не грозит опасность. В случае попытки проникновения вируса продукт автоматически определит источник угрозы и эффективно нейтрализует ее при минимальном участии пользователя.

Антивирус Касперского имеет специальные средства защиты – он проверяет входящую и исходящую почту, контролирует базы почтовых сообщений, обеспечивает безопасность подключений к Интернету и любых устанавливаемых программ.

Антивирус Касперского является последним технологическим достижением Лаборатории Касперского в области защиты домашнего компьютера от вирусных угроз. Возможности: 100%-ная защита от макровирусов. Защита даже от неизвестных вирусов. Надежный контроль целостности данных. Комплексная проверка почтовой корреспонденции. Защита мест хранения данных. Проверка памяти запущенных программ.

NOD 32 Antivirus System обеспечивает хорошо сбалансированную безупречную защиту персональных компьютеров и корпоративных систем, работающих на платформах MS Windows 95/98/ ME/NT/2000/2003/XP и т.д., UNIX/Linux и т.д., Novell, MS DOS, а также для почтовых серверов MS Exchange Server, Lotus Doino и др. Вирусы, черви, троянские программы и другой вредоносный код находятся на безопасном расстоянии от данных. Передовые методы обнаружения, используемые в программном обеспечении, защищают даже от будущих потенциальных опасностей и от большинства новых червей и вирусов.

Главным преимуществом NOD 32 является его быстрая работа, низкое потребление системных ресурсов, способность ловить почти 100 % вирусов.

Широко применяется программа-доктор *Dr. Web*. Она входит в состав антивирусного пакета DSAV, который распространяет фирма «Диалог-Наука». Программа-ревизор ADINF проверяет диски, программа Dr.Web анализирует новые и измененные файлы и выдает на экран сообщения и запросы.

После запуска Dr.Web открывается оболочка с меню, расположенным в верхней строке экрана. Для проверки следует выбрать пункты меню Тест -> Тестирование и указать путь для выполнения теста. После ввода откроется окно тестирования. С помощью пункта Настройка нужно задать общие установки тестирования, уровень эвристики, высоту экрана, цветовую схему и т. д., а также действия при обнаружении зараженных файлов. После проверки выдается окно отчета о выполнении тестирования. Если обнаружен вирус, Dr.Web выведет отчет красным цветом.

Основные правила лечения файлов и системных областей дисков:
–запрещается выполнять непродуманные действия, которые могут привести к заражению ПК;
–если вирус еще не активизирован, то следует немедленно выключить компьютер;
–при заражении ПК вирусом компьютер следует перезагрузить и начать его лечение с дискет;
–все операции по обнаружению вируса и лечению ПК должны выполняться с эталонной, защищенной от записи дискеты с ОС;
–при лечении поиск вирусов следует проводить во всех файлах (например, задавая в программе Dr.Web параметр /al).

Профилактика заражения компьютера вирусами.

Для того чтобы не подвергнуть компьютер заражению вирусами и обеспечить надежное хранение информации на дисках, необходимо соблюдать следующие правила:
– оснастите свой компьютер современным антивирусным ПО и **постоянно обновляйте их базы;**
– используйте антивирусные программы для входного контроля **всех исполняемых файлов, получаемых из интернета**;
– перед считыванием с дискет, флэшек информации, записанной на других компьютерах**, всегда проверяйте съемные носители на наличие вирусов**, запуская антивирусные программы своего компьютера;
– при переносе на свой компьютер файлов в архивированном виде **проверяйте их перед распаковкой**;
– периодически проверяйте на наличие вирусов жесткие диски компьютера, запуская антивирусные программы для тестирования файлов, памяти и системных областей дисков, предварительно загрузив операционную систему с загрузочного диска;
– обязательно делайте архивные копии ценной для вас информации;
– не оставляйте съемные носители (флэшки, дискеты, мобил-рэк) при включении или перезагрузке операционной системы, чтобы исключить заражение компьютера загрузочными вирусами.

Второй вопрос: <u>Антивирусные средства защиты. Работа с антивирусной программой.</u>

Самые распространенные антивирусные средства защиты (антивирусные программы) рассмотрены в вопросе 1.

Более подробно рассмотрим работу с Антивирусом Касперского.

Лаборатория Касперского является одним из самых популярных и надежных представителей рынка антивирусных программ в мире. Несмотря на то, что главный офис ее находится в России, продукция Касперского пользуется огромным спросом во всех частях света, предоставляя свои услуги более чем в 200 странах. За годы своего существования, эта компания добилась значительных достижений в деле защиты и сохранения электронной информации.

Ежедневно появляющиеся угрозы безопасности для ПК и других устройств, заставляют специалистов Лаборатории Касперского искать все новые пути их устранения. Однако, данной продукции свойственен и стандартный для наиболее популярных антивирусных программ набор функций, позволяющий оградить пользователей от самых распространенных и опасных типов угроз, связанных с эксплуатацией ПК.

Такими функциями являются:

- личный брандмауэр с системой IDS/IPS;
- выявление вредоносного кода;
- самообновление баз;
- полноценная защита от вирусов;
- проведение анализа по сигнатурным базам;
- стандартная защита от всех видов интернет-атак;
- исследование файлов;
- интернет-трафик и почта, в режиме постоянного мониторинга;
- недопущение утечек личной информации;
- родительский контроль;
- протекция от фишинга и спама.

Плюсы и минусы антивируса Касперского

Конечно, как и любая продукция, антивирусная программа Касперского обладает, как положительными, так и отрицательными сторонами, которые определяют сами пользователи, доверившие защиту своих персональных компьютеров лаборатории Касперского.

Преимущества антивируса Касперского:

- Обеспечение качественной и надежной защиты ПК, независимо от типа угроз.

- Удобство в использовании и приятный дизайн.
- Регулярные обновления.

Недостатки антивируса Касперского:

- Влияет на скорость обработки информации, замедляя работу системы.
- Навязчивость некоторых функций.
- Совершает ошибки при распознавании вирусов, путая их с нормальными файлами.
-

Несмотря на различность мнений, относительно эффективности использования антивируса Касперского, его с уверенностью можно назвать одним из лучших антивирусов современности. Это утверждение, безусловно, подтверждает наличие большого количества наград, полученных лабораторией Касперского от различных международных организаций за достижения в области защиты ПК и других электронных устройств.

Пользуясь данным антивирусом, можно быть спокойным при совершении каких-либо электронных сделок, включая покупку товаров, перевод средств, оплату услуг и др. Безопасность таких действий гарантируется, как при использовании электронной клавиатуры, так и сенсорного монитора.

Однако, подводя итог, необходимо отметить дороговизну антивируса Касперского. Цена любой его версии превышает среднерыночную цену антивирусных программ. Но, учитывая все вышеперечисленные достоинства, можно сделать вывод о том, что такая переплата не заставит пользователей пожалеть о сделанном выборе.

«Работа с Антивирусом Касперского 2011»

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

Рисунок 26 – Сообщение об отключении защиты

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

- Критические – информируют о событиях, имеющих первостепенную важность с точки зрения безопасности компьютера: например, об обнаружении вредоносного объекта или опасной активности в системе. Окна уведомлений и всплывающие сообщения такого типа имеют красный цвет.
- Важные – информируют о событиях, потенциально важных с точки зрения безопасности компьютера: например, об обнаружении возможно заражённого объекта или подозрительной активности в системе. Окна уведомлений и всплывающие сообщения такого типа имеют жёлтый цвет.
- Информационные – информируют о событиях, не имеющих первостепенной важности с точки зрения безопасности. Окна уведомлений и всплывающие сообщения такого типа имеют зелёный цвет.

Окно настройки параметров программы

Окно настройки параметров Kaspersky Internet Security предназначено для настройки параметров работы программы в целом, отдельных компонентов защиты, задач проверки и обновления, а также для выполнения других задач расширенной настройки.

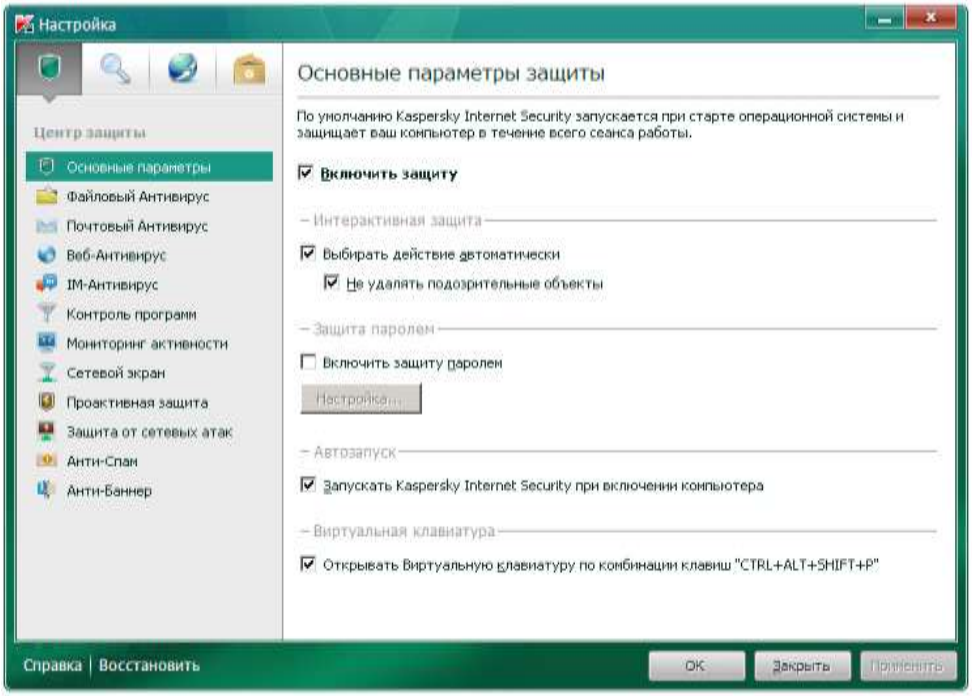


Рисунок 27 – Окно настройки параметров Kaspersky Internet Security

Окно настройки состоит из двух частей:

- В левой части окна можно выбрать компонент программы, задачу или другую составляющую, которую нужно настроить;
- В правой части окна содержатся элементы управления, с помощью которых можно настроить работу составляющей, выбранной в левой части окна.

Компоненты, задачи и другие составляющие в левой части окна объединены в следующие разделы:

– Центр защиты;

– Проверка компьютера;

– Обновление;

– Дополнительные параметры.

Чтобы открыть окно настройки, выполните одно из следующих действий:

- Перейдите по ссылке Настройка в верхней части главного окна программы;
- Выберите пункт Настройка в контекстном меню;
- Нажмите на кнопку Настройка в интерфейсе Kaspersky Gadget (только для операционных систем Microsoft Windows Vista и Microsoft Windows 7). Для кнопки должна быть назначена функция открывания окна настройки.

Kaspersky Gadget

При использовании Kaspersky Internet Security на компьютере под управлением операционной системы Microsoft Windows Vista или Microsoft Windows 7 будет доступен Kaspersky Gadget (далее также *гаджет*).

Kaspersky Gadget предназначен для быстрого доступа к основным функциям программы: индикации состояния защиты компьютера, проверке объектов на вирусы, просмотру отчётов о работе программы и т. д.

После установки Kaspersky Internet Security на компьютер под управлением операционной системы Microsoft Windows 7 гаджет появляется на рабочем столе автоматически. После установки программы на компьютер под управлением операционной системы Microsoft Windows Vista гаджет нужно добавить на боковую панель Microsoft Windows вручную.

Рисунок 28 – Kaspersky Gadget

Структура и настройки

Представлено изучение **Окна настроек** и на его примере - структуры **Антивируса Касперского 2011.**

Как и любой антивирус для рабочей станции, персональный **Антивирус Касперского** 2011 обеспечивает:

- Проверку в режиме реального времени, то есть «на лету» или постоянную защиту. В терминах **Антивируса Касперского 2011** это называется одним словом – **«Защита»,** которая в свою очередь делится на защиту файловой системы, почты, проверку просматриваемых веб-страниц и проактивную защиту. Эти элементы называются «компонентами защиты», настраивать и управлять ими можно по отдельности.
- **Проактивная защита** позволяет обнаружить новую вредоносную программу ещё до того, как она успеет нанести вред. Компонент основан на контроле и анализе поведения всех программ, установленных на компьютере. На основании выполняемых действий Kaspersky Internet Security 2011 принимает решение о том, является программа потенциально опасной или нет. Таким образом, компьютер защищён не только от уже известных вирусов, но и от новых, ещё не исследованных.

Помимо проактивной защиты антивирус Касперского использует эвристический анализатор для обнаружения вредоносных программ.

Эвристический анализатор – технология обнаружения угроз, неопределяемых с помощью баз Антивируса. Позволяет находить объекты, которые подозреваются на заражение неизвестным вирусом или новой модификацией известного. С помощью эвристического анализатора обнаруживаются до 92% новых угроз. Этот механизм достаточно эффективен и очень редко приводит к ложным срабатываниям. Файлы, обнаруженные с помощью эвристического анализатора, признаются подозрительными.

Эвристический анализатор является частью **проактивной защиты** и позволяет обнаруживать вредоносные программы в исполняемых файлах, секторах и памяти. Отличительной особенностью эвристического анализатора является гибкая архитектура и комбинация различных методов, позволяющих добиться достаточного уровня обнаружения новых вредоносных программ с минимальным количеством ложных срабатываний.

Проактивная защита – понятие более ёмкое. **Лаборатория Касперского** разработала развитую проактивную защиту, анализирующую весь цикл вторжения вредоносных программ в систему. В отличие от **Эвристичекого Анализатора Проактивная защита** детектирует вирус по поведению в системе, а не на основе сигнатур.

Настройка общих параметров для задач проверки, в терминах **Антивируса Касперского 2011** – задачи типа **«Проверка»**

Средства обновления антивирусных баз объединяется термином **«Обновление»;**

Настройка общих параметров работы Антивируса Касперского 2011 – «Настройка», «Основные параметры».

В задании необходимо перейти к окну **Настройка** и с помощью расположенного в нём дерева настроек изучить структуру антивируса.

1. Откройте главное окно интерфейса антивируса.

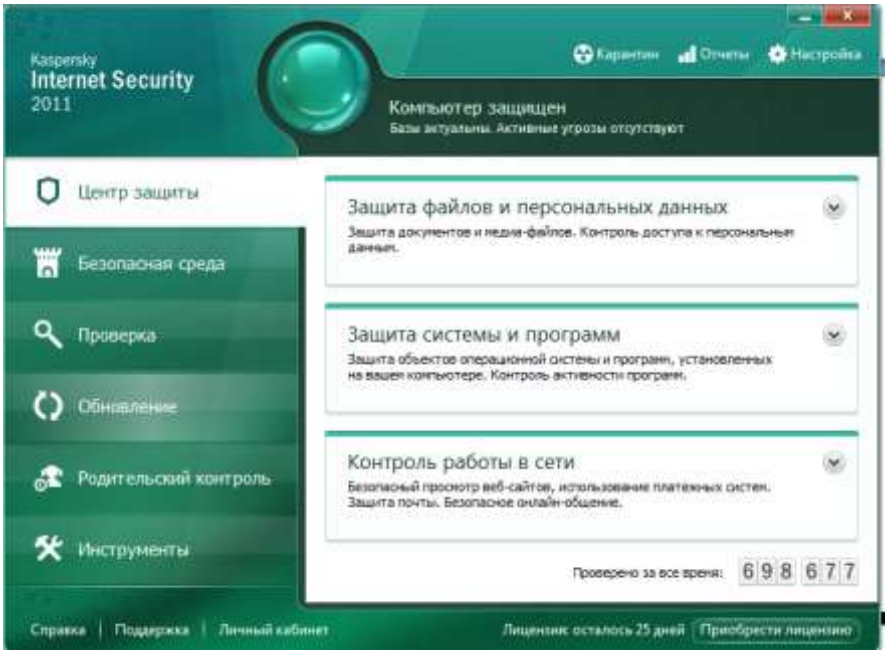


Рисунок 29 – Главное окно интерфейса антивируса

2. Перейдите к окну настроек, нажав ссылку

3. Открывшееся окно **Настройка** разделено вертикально на две части. Слева – дерево настроек, в котором можно выбирать нужный компонент или группу параметров. В правой части выводятся все настройки, относящиеся к выбранному в левой части (в дереве) пункту.

Как видно из структуры дерева, все настройки **Антивируса Касперского** делятся на 4 большие группы в соответствии с описанными в начале задания функциями: **Центр защиты, Проверка компьютера, Обновление** и **Дополнительные параметры** (прочитайте об этих группах в **Справке).**

Ознакомьтесь с окном **Настройка,** поочередно переходя по соответствующим пунктам дерева в левой части окна.

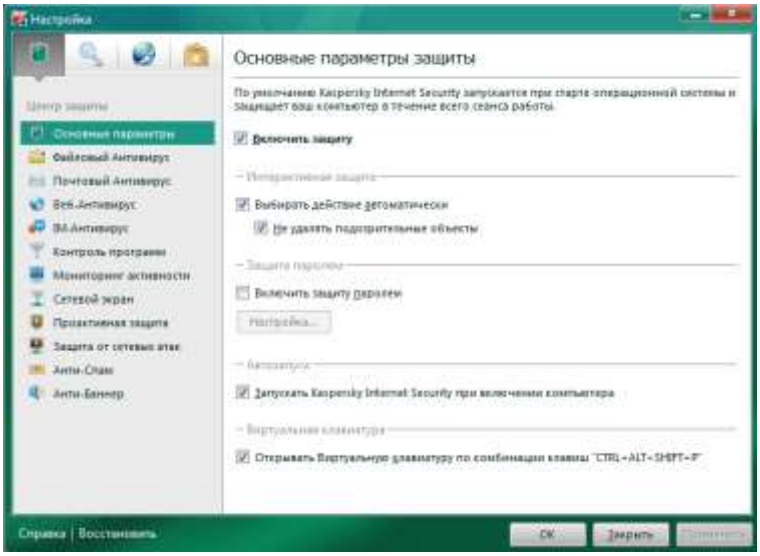


Рисунок 30 – Окно настройки

4. Перейдите к группе **Проверка компьютера.** Это – настройки проверки по требованию, то есть по требованию пользователя. Она используется в случае, если необходимо проверить некий объект или группу объектов.

Для запуска проверки по требованию нужно определить две вещи: что проверять и с какими настройками это делать.

Антивирус Касперского позволяет выбрать объекты, которые нужно проверить, двумя путями:

Антивирус встраивается в контекстное меню каждого файла, размещённого на жёстком диске **(Проверить на вирусы).** В этом случае производится проверка только выделенного объекта или объектов. При этом используются общие настройки, то есть те, которые выводятся при нажатии пункта **Поиск вирусов**.

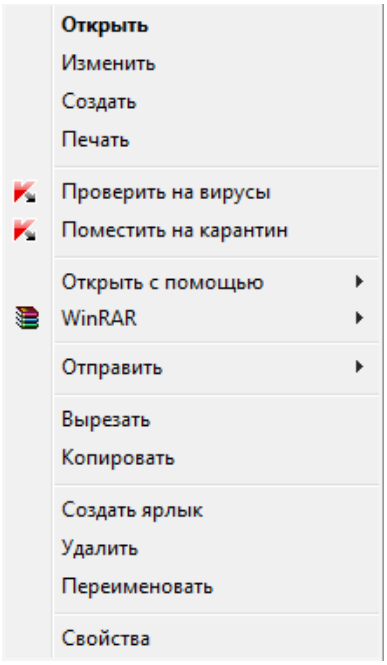


Рисунок 31 – Проверка на вирус, вызываемая из контекстного меню

Можно заранее определить папку или группу папок, или объектов и сформировать отдельную задачу. Тогда для неё можно задать свои собственные настройки и в дальнейшем запускать эту задачу одним нажатием кнопки. По умолчанию **Антивирус Касперского** создает четыре такие системные задачи с заранее определённым набором проверяемых объектов: **Полная проверка, Проверка важных областей, Проверка объектов** и **Поиск уязвимостей.**

Таким образом, настройки группы **Проверка** соответствуют настройкам задачи, запускаемой из контекстного меню различных объектов. При этом она содержит четыре подгруппы, соответствующие другим задачам проверки по требованию с заданным набором проверяемых объектов: **Полная проверка, Проверка важных областей, Проверка объектов** и **Поиск уязвимостей.** По мере формирования пользовательских задач проверки по требованию, они будут аналогично добавляться в дерево настроек в группу **Проверка.**

Ознакомьтесь с доступными для настройки параметрами системных задач проверки по требованию, поочередно выделяя пункты **Полная проверка, Проверка важных областей Проверка объектов** и **Поиск уязвимостей**.

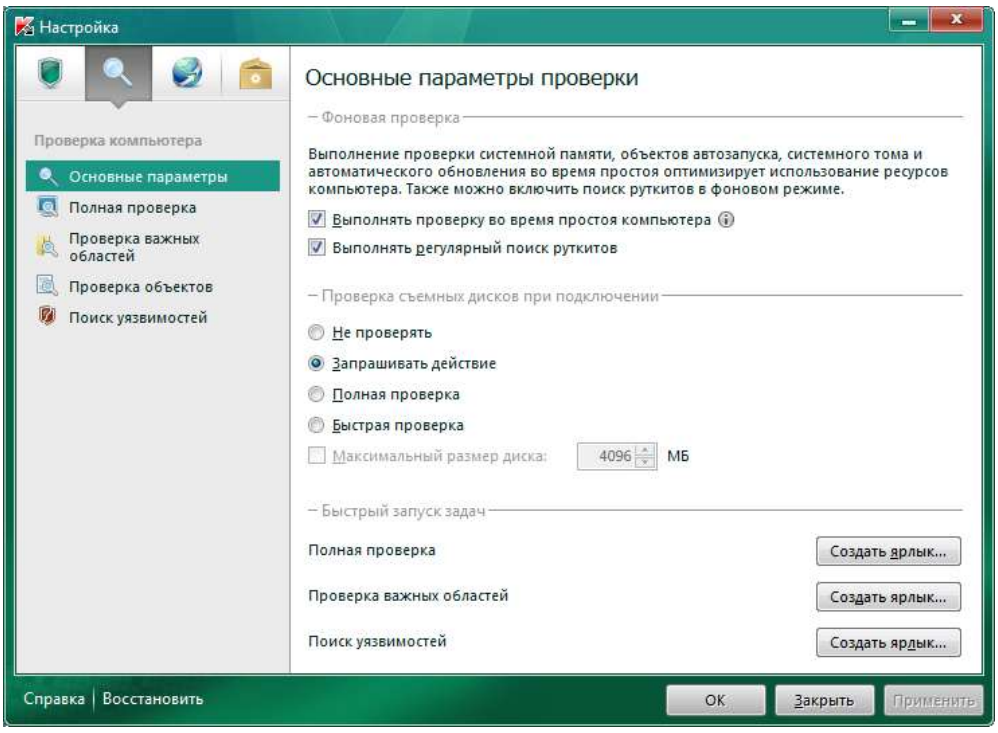


Рисунок 32 – Группа Проверка

5. Перейдите к группе настроек **Обновление**.

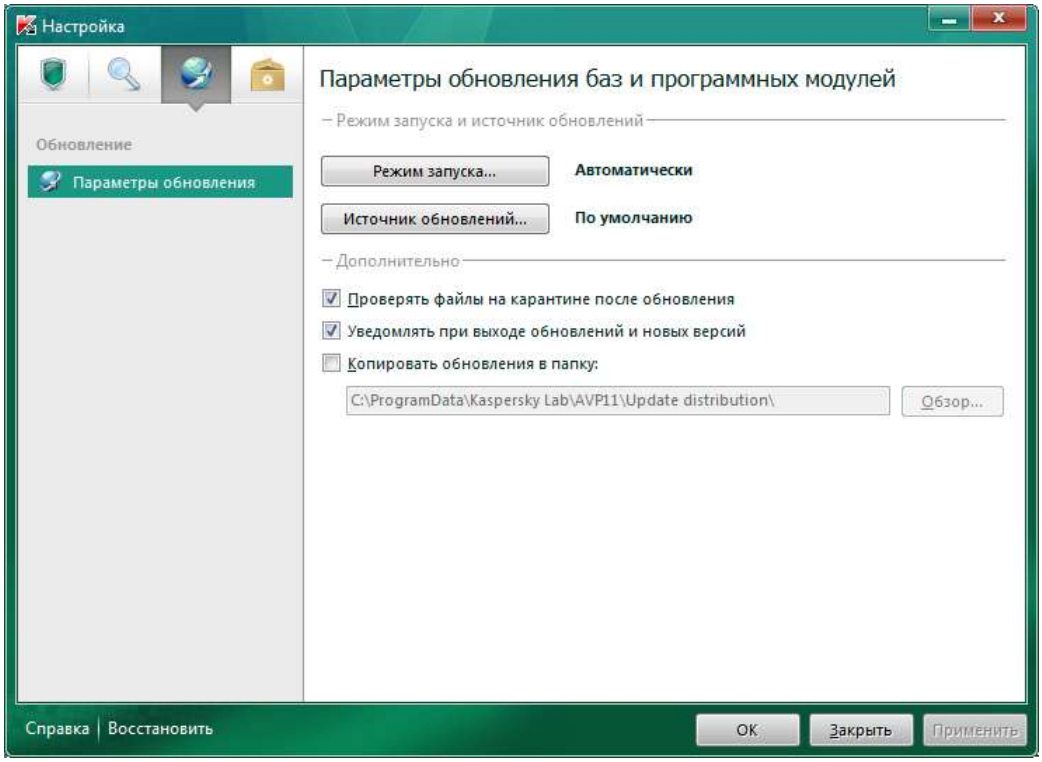


Рисунок 33 – Обновление

6. Нажмите **Отмена** и вернитесь в главное окно **Антивируса Касперского.**
7. **Закройте интерфейс** Антивируса Касперского.

Постоянная защита

Работу с постоянной защитой можно разделить на три части:

- **Настройка** – выполняется в одноимённом окне и была рассмотрена в предыдущем задании.
- **Управление** – каждый компонент постоянной защиты можно при необходимости приостановить, а потом запустить. Эти действия выполняются в главном окне интерфейса (элементы управления дополнительно продублированы в окне статистики).
- **Обслуживание,** то есть работу со статистикой. Выполняется в окне статистики.

В этом задании нужно изучить последние две задачи: управление компонентами постоянной защиты и работу с отчётами.

1. Откройте главное окно интерфейса **Антивируса Касперского 2011**.

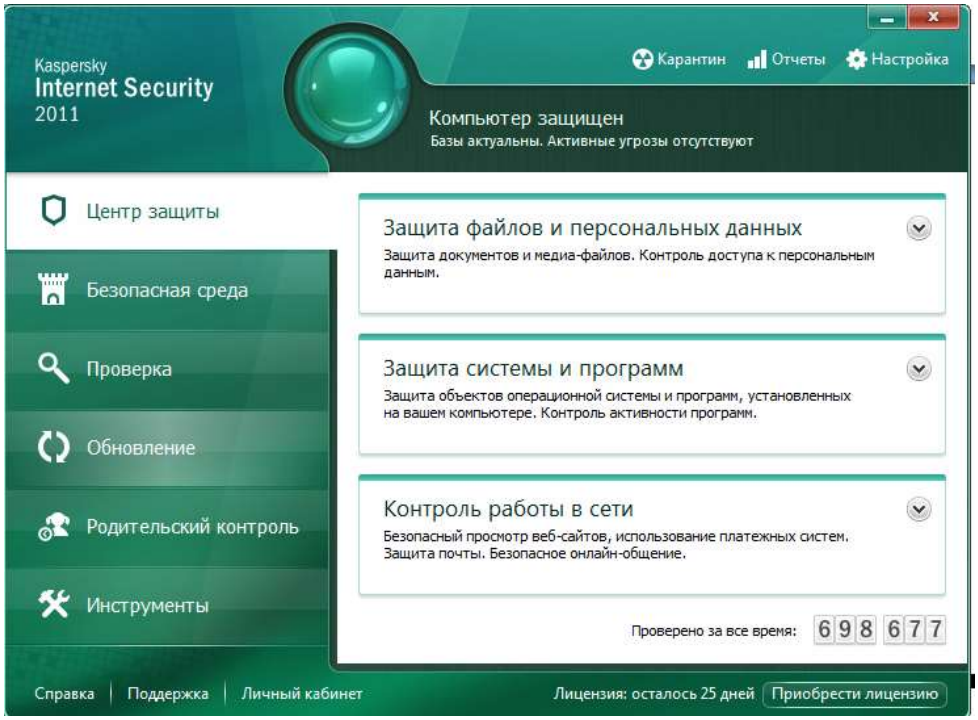


Рисунок 34 – Главное окно интерфейса

2. Перейдите к разделу **Центр защиты,** выделив одноимённый пункт.
3. При вызове интерфейса **Антивируса Касперского** через системное меню. **Пуск** или щелчком по иконке, по умолчанию выбран пункт **Центр защиты.**

4. В общем случае приостанавливать или останавливать работу защиты не рекомендуется. Однако иногда это может потребоваться – например, при перемещении с диска на диск большого файла, и заведомо известно, что он безопасен. Поэтому при выборе строки **Приостановка защиты** из контекстного меню появляется окно с предложением выбрать, когда нужно вернуть защиту в строй: через некий промежуток времени, после перезапуска антивируса или это должен сделать сам пользователь вручную.

Ознакомьтесь со всеми предлагаемыми сценариями включения защиты и нажмите соответствующий.

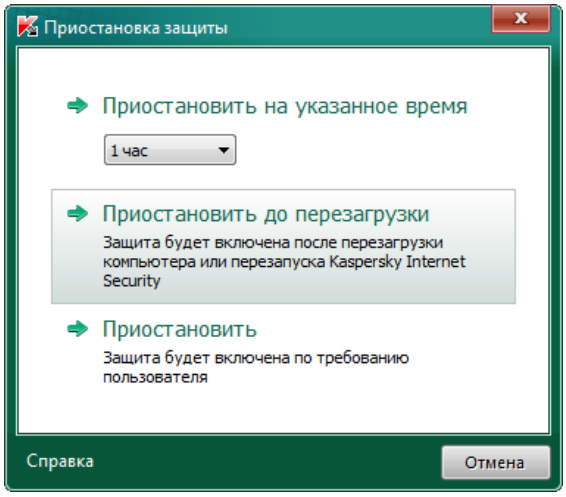


Рисунок 35 – Окно приостановки защиты

5. Вернувшись к главному окну, проследите за произошедшими изменениями. Обратите внимание, что в главном окне на вкладке Центр защиты возле значков.

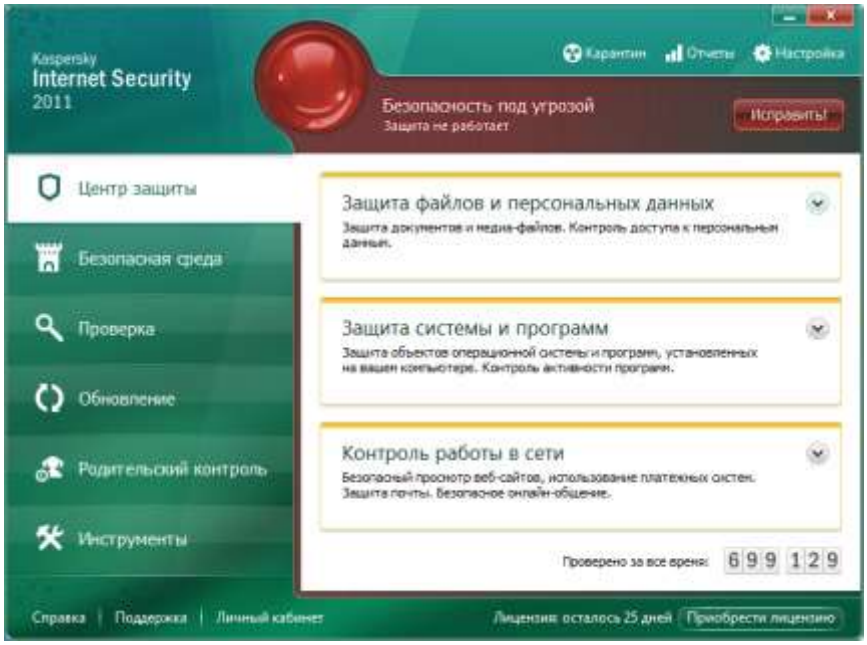


Рисунок 36 – Отключение защиты файлов и персональных данных

6. Перейдите к подразделу **Файловый Антивирус.**
7. Изучите представленную в окне информацию. Обратите внимание на правую часть окна Настройки защиты файловой системы компьютера, в ней находятся основные настройки Файлового антивируса. В данном случае видно, что **Файловый Антивирус** приостановлен, об этом свидетельствует невозможность выбора компонентов настройки.

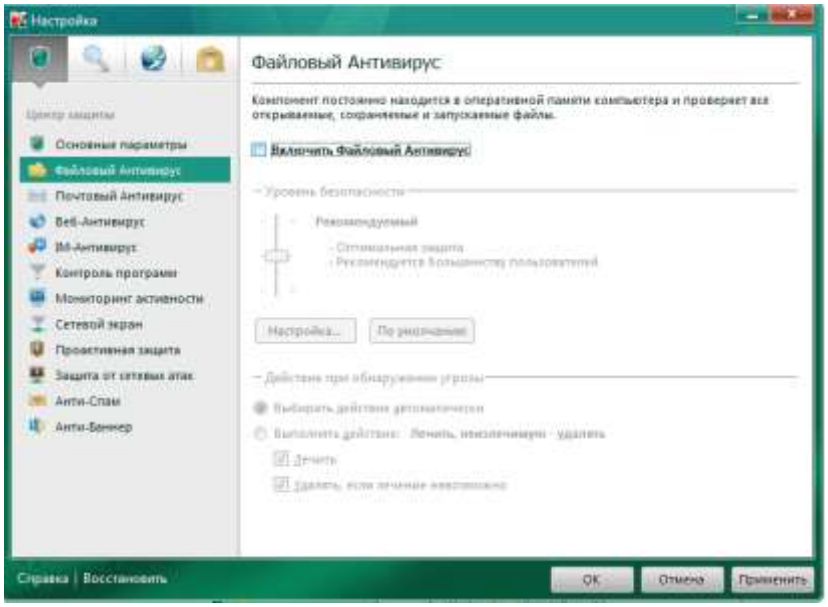


Рисунок 37 – Отключение Файлового Антивирусника

8. Запустите **Файловый Антивирус,** откройте Настройки вкладка Файловый Антивирус и поставьте галочку Включить Файловый Антивирусник.
9. Теперь повторите эти же действия, начиная с пункта 7, только применительно ко всем трём оставшимся компонентам защиты: почтовому антивирусу, веб-антивирусу, IM антивирусу и проактивной защите.

В результате выполнения этого задания все компоненты постоянной защиты должны быть включены.

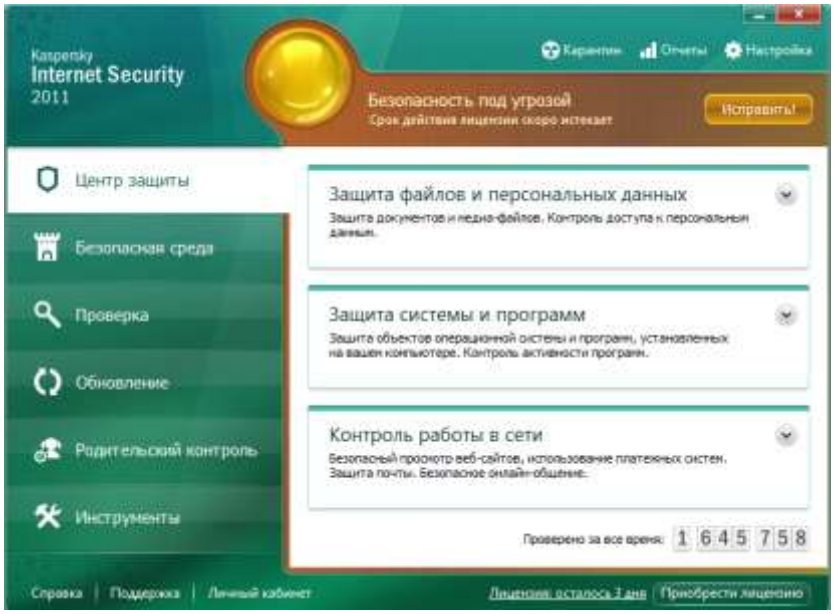


Рисунок 38 – Главное окно интерфейса: все компоненты включены

Задание 1.4 Настройка обновления

В этом задании нужно ознакомиться с настройками по умолчанию для задачи получения обновлений и при необходимости внести в них изменения (в соответствии с использующимися на компьютере пользователя настройками сети).

Каждый день в мире появляются новые вирусы, троянские и другие вредоносные программы, поэтому крайне важно быть уверенным в том, что информация на компьютере находится под надёжной защитой. Информация об угрозах и способах их нейтрализации находится в антивирусных базах Антивируса Касперского/Kaspersky Internet Security версии 2011, поэтому очень важно регулярно проводить обновление антивирусных баз.

В процессе обновления антивирусных баз, загружаются и устанавливаются на компьютер следующие объекты:

Базы Антивируса Касперского/Kaspersky Internet Security версии 2011. Защита информации обеспечивается на основании баз данных, содержащих описания сигнатур угроз и сетевых атак, а также методы борьбы с ними. Компоненты защиты используют их при поиске и обезвреживании опасных объектов на компьютере. Базы регулярно

пополняются записями о новых угрозах и способах борьбы с ними. Также в процессе обновления Баз Антивируса Касперского/Kaspersky Internet Security версии 2011 обновляются сетевые драйверы, обеспечивающие функциональность для перехвата сетевого трафика компонентами защиты.

Программные модули. Пакеты обновлений программных модулей устраняют уязвимости Антивируса Касперского/Kaspersky Internet Security версии 2011, добавляют новые функции или улучшают существующие.

Источником обновлений антивирусных баз и программных модулей Антивируса Касперского/Kaspersky Internet Security версии 2011 являются специальные серверы обновлений Лаборатории Касперского.

Для успешной загрузки обновлений с серверов необходимо, чтобы компьютер, на котором установлен продукт Лаборатории Касперского версии 2011, был подключен к сети Интернет. По умолчанию параметры подключения к сети Интернет определяются автоматически. Если параметры прокси-сервера не определяются автоматически, необходимо настроить параметры подключения к нему. Информацию о том, как настроить параметры прокси-сервера можно найти в статьях Базы знаний Лаборатории Касперского.

В процессе обновления программные модули и антивирусные базы на компьютере сравниваются с расположенными в источнике обновлений. Если на компьютере установлена последняя версия антивирусных баз и программных модулей, на экран будет выведено информационное сообщение об актуальности антивирусных баз.

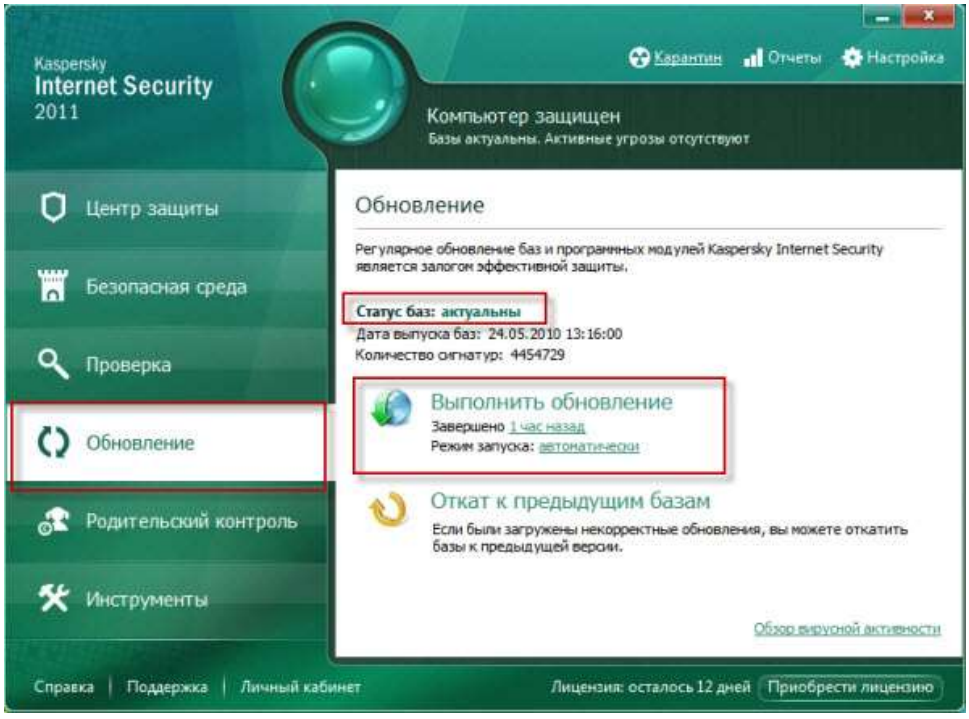


Рисунок 39 – Сообщение об актуальности антивирусных баз

Если антивирусные базы и программные модули отличаются, на компьютер будет установлена недостающая часть обновлений.

Полное копирование антивирусных баз и программных модулей с серверов обновлений Лаборатории Касперского не производится, что позволяет существенно увеличить скорость обновления и снизить объём трафика.

Перед обновлением антивирусных баз и программных модулей продукт Лаборатории Касперского версии 2011 создает их резервную копию на тот случай, если по каким-либо причинам необходимо вернуться к использованию предыдущих версии баз. Данная возможность необходима, например, если обновлены базы, но в процессе работы они были повреждены.

Поддержка защиты в актуальном состоянии – залог безопасности компьютера. Поэтому крайне важно регулярно обновлять базы и программные модули программы.

По умолчанию Kaspersky Internet Security 2011 загружает обновления автоматически, но можно выбрать режим Вручную или По расписанию.

Автоматически – Kaspersky Internet Security проверяет наличие пакета обновлений в источнике обновлений с заданной периодичностью. Частота проверки может увеличиваться во время вирусных эпидемий и сокращаться при их отсутствии. Обнаружив свежие обновления, программа загружает их и устанавливает на компьютер.

При выборе параметра «Автоматически» компонент обновления производит попытку обновления сигнатур угроз (антивирусных баз) согласно информации в файле updcfg.xml, в котором прописан рекомендуемый период обновления, составляющий по умолчанию 2 часа. Если компонент обновления сигнатур угроз (антивирусных баз) не может скачать обновления, то он пытается скачать сигнатуры угроз через 2 часа с момента последней попытки.

Возможность изменения параметра частоты обновления позволяет специалистам Лаборатории Касперского регулировать частоту обновлений в случае вирусных эпидемий и других опасных ситуаций. Программа своевременно будет получать самые последние обновления сигнатур угроз (антивирусных баз), сетевых атак и программных модулей, что исключит возможность проникновения опасных программ на ваш компьютер.

По расписанию – обновление будет запускаться автоматически по сформированному расписанию (в зависимости от параметров расписания интервал может изменяться).

Вручную – в этом случае возможно самостоятельно запускать обновление Kaspersky Internet Security.

Если выбран режим По расписанию, то в этом случае можно настроить автоматический запуск пропущенной задачи обновления. Для этого поставьте флажок для опции Запускать пропущенные задачи.

Для того чтобы изменить режим запуска задачи обновления, выполните следующие действия:

- откройте главное окно программы;
- в левой части главного окна программы выберите раздел Обновление;
- в правом верхнем углу окна нажмите ссылку Настройка;
- в правой части окна Настройка в блоке Режим запуска нажмите кнопку Настройка;
- в окне Обновление: настройка на закладке Режим запуска в блоке Расписание выберите режим: автоматически, вручную, по расписанию.

Если выбран режим По расписанию, сформируйте расписание:

- нажмите кнопку ОК два раза;
- закройте главное окно программы.

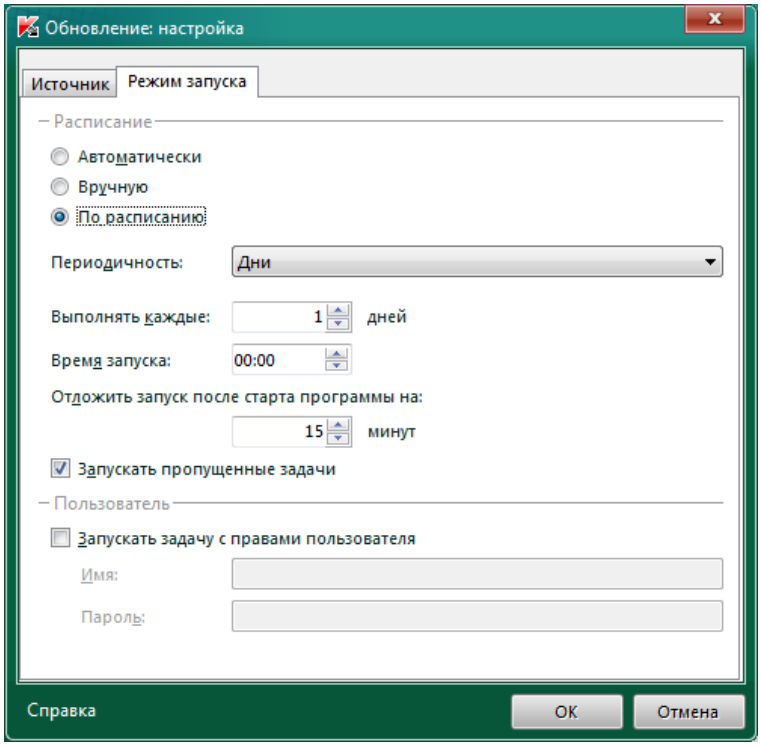


Рисунок 40 – Вкладка Режим запуска

Изменение режима запуска задачи обновления в Kaspersky Internet Security 2011.

Для того чтобы обновить базы Kaspersky Internet Security 2011, выполните следующие шаги:

Шаг 1. Откройте главное окно программы;

Шаг 2. В главном окне программы перейдите на закладку Обновление;

Шаг 3. Нажмите кнопку Выполнить обновление;

Рисунок 41 – Вкладка Обновление

Шаг 4. Дождитесь окончания обновления

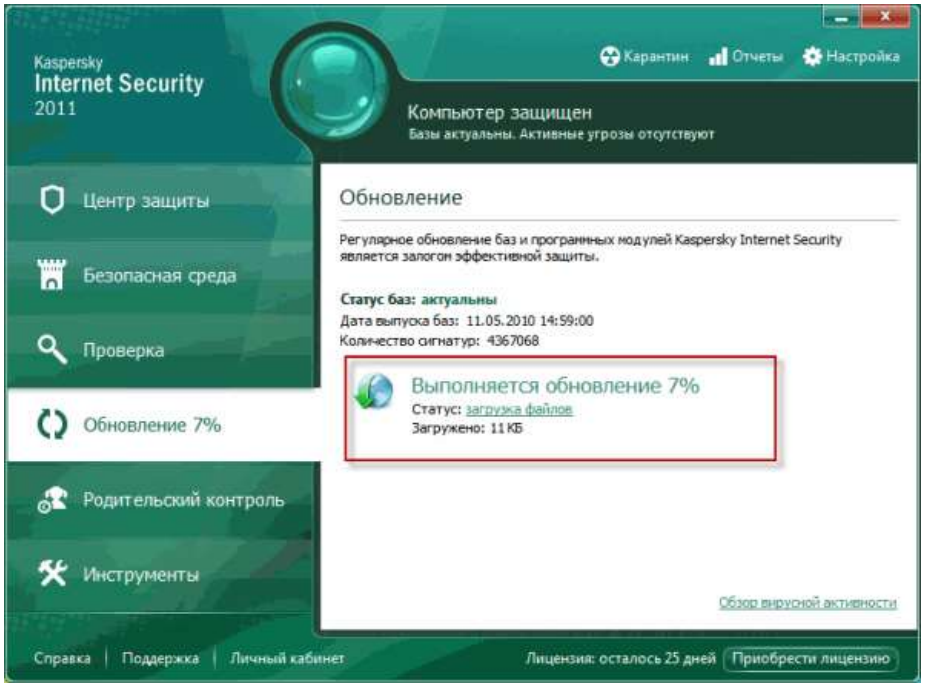


Рисунок 42 – Выполняется обновление

В Антивирусе Касперского/Kaspersky Internet Security версии 2011 для обновления компьютеров по локальной сети или отдельно стоящих компьютеров реализован процесс ретрансляции антивирусных баз и программных модулей в локальный источник (папку на диске, сетевой ресурс). Для организации обновления

антивирусных баз из локальной папки необходим как минимум один компьютер, имеющий доступ к сети Интернет. Подробную информацию о том, как произвести обновление антивирусных баз из локальной папки можно найти в статьях Базы знаний Лаборатории Касперского.

Для обновления Kaspersky Internet Security 2011 из локальной папки необходимы два компьютера с установленным продуктом одинаковой версии, например 11.0.0.232. С одного компьютера будет осуществляться выход в интернет и скачивание антивирусных баз с серверов обновления Лаборатории Касперского, а второй компьютер будет обновлять антивирусные базы из локальной папки первого.

В Kaspersky Internet Security 2011 для обновления компьютеров по локальной сети или отдельно стоящих компьютеров был реализован процесс ретрансляции антивирусных баз и программных модулей в локальный источник (папку на диске, сетевой ресурс). Для организации обновления антивирусных баз из локальной папки необходим как минимум один компьютер, имеющий доступ к сети Интернет.

Если в локальной сети установлено несколько копий Kaspersky Internet Security 2011, то обновление для каждой копии можно настроить из локальной папки с помощью ретрансляции (приема и передачи) баз в эту папку. Для этого необходимо выполнить следующее:

- один компьютер необходимо настроить на обновление из Интернета с серверов Лаборатории Касперского,
- на этом компьютере создать папку для файлов обновления и открыть доступ по сети к этой папке или к папке по умолчанию:

- для Windows XP папка по умолчанию \Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP11\Update distribution,
- для Windows Vista/7 папка по умолчанию \ProgramData\Kaspersky Lab\AVP11\Update distribution.

По умолчанию эта папка является скрытой и недоступна для просмотра. Если хотите использовать эту папку для ретрансляции сигнатур угроз, то необходимо включить опцию Показывать скрытые файлы и папки. Подробную информацию о том, как включить данную опцию можно узнать в статье KB3580.

На следующем этапе необходимо настроить процесс копирования баз в локальный источник:

1. откройте главное окно программы,
2. в левой части окна Kaspersky Internet Security выберите раздел Обновление,
3. в правом верхнем углу окна Kaspersky Internet Security нажмите ссылку Настройка,
4. в правой части окна в блоке Дополнительно поставьте галку для опции Копировать обновления в папку,

5. нажмите кнопку Обзор, если необходимо указать папку для баз отличную от папки по умолчанию,
6. нажмите кнопку ОК два раза,
7. запустите обновление антивирусных баз.

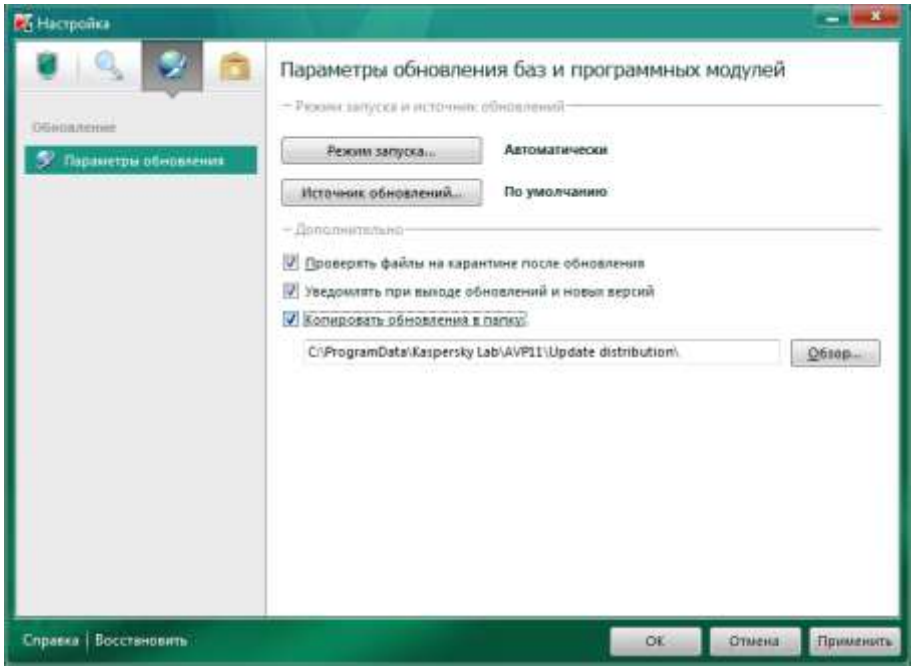
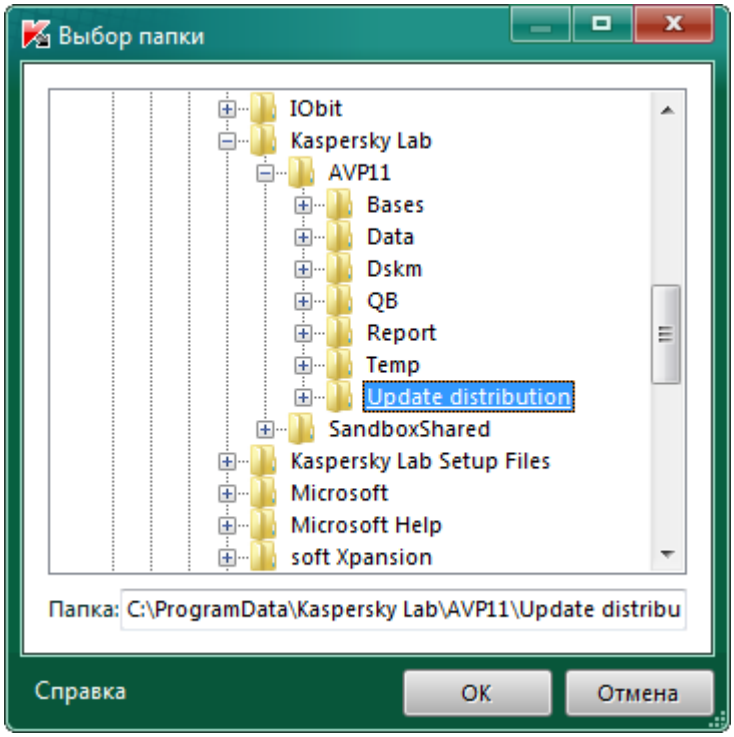


Рисунок 43 – Вкладка Параметры обновления

Для организации обновления компьютеров в локальной сети или отдельно стоящих компьютеров необходимо открыть доступ по сети к папке с обновлением или скопировать папку с обновлением на компьютеры, антивирусные базы на которых необходимо обновить. Компьютер с установленным Kaspersky Internet Security 2011, антивирусные базы которого требуется обновить из локальной папки, необходимо настроить следующим образом:

1. откройте главное окно программы,
2. в левой части окна Kaspersky Internet Security выберите раздел Обновление,
3. в правом верхнем углу окна нажмите ссылку Настройка,
4. в правой части окна в блоке Режим запуска и источник обновлений нажмите кнопку Источник обновлений,
5. в окне Обновление: настройка на закладке Источник нажмите кнопку Добавить,
6. выберите папку, в которую были ретранслированы базы и модули программы ранее
7. нажмите кнопку ОК,
8. на закладке Источник снимите галку для опции Серверы обновлений «Лаборатории Касперского»,
9. нажмите кнопку ОК,
10. запустите обновление антивирусных баз.



Как обновить базы Kaspersky Internet Security 2011, если компьютер, на котором он установлен, не имеет выхода в интернет?

Внимание! *Описанный ниже способ обновления является вспомогательным, не основным – используйте его только в случае, если компьютер, на котором установлен Kaspersky Internet Security 2011, не имеет выхода в интернет. Данный способ получения баз не может обеспечить моментальной доставки выпущенных обновлений и, как следствие, поддержания программы в актуальном состоянии.*

Для обновления всех необходимых баз и модулей программы Kaspersky Internet Security можно использовать специальную утилиту обновления, которая будет запускаться вручную с любого другого компьютера или с flash-носителя («флешки»), который подключен к компьютеру, имеющему выход в интернет.

При первом запуске утилиты все базы и модули, необходимые Kaspersky Internet Security и выпущенные к настоящему времени, скачиваются в специальную папку, расположенную в той же папке, что и утилита обновления (именно поэтому первый запуск утилиты очень продолжителен). При каждом последующем запуске в эту папку будут докачиваться только недостающие базы и модули, т.е. только то, что было выпущено позднее предыдущего запуска утилиты обновления.

По состоянию на май 2010 года объём баз Kaspersky Internet Security занимает на носителе около 395MB. Используйте эту информацию при выборе flash-носителя для сохранения обновлений. С течением времени объём баз будет увеличиваться.

Краткое описание работы с утилитой обновления.

Сохраните папку с утилитой на flash-носитель, подключите его к компьютеру, имеющему выход в интернет, и запустите утилиту (файл Updater.bat).

После окончания работы утилиты подключите flash-носитель к компьютеру с установленным Kaspersky Internet Security 2011 и настройте эту программу на обновление из папки с базами на flash-носителе (папка Updates).

В дальнейшем регулярно подключайте эту же «флешку» к любому компьютеру, подключенному к интернету, докачивайте новые базы (т.е. запускайте файл Updater.bat) и обновляйте с flash-носителя установленный Kaspersky Internet Security 2011,…….(используя новые версии данного программного продукта).

Однако развитие вирусов не стоит на месте, новые версии вредоносного кода и рассылка спама, растущие год от года, требует от разработчиков свежих идей и новых решений.

Облачная защита данных

Ведущие антивирусные компании ежегодно улучшают свои рецепты безопасности, причем тенденция указывает на широкое использование «облачных» технологий. В связке с клиентской частью они делают реакцию на угрозы моментальной, предоставляя антивирусу больше информации и одновременно снижая нагрузку на ПК.

Рисунок 45 - Облачный антивирус "Касперского"

Что нужно рядовому пользователю антивируса? Он должен моментально реагировать на новые вредоносные программы, эффективно блокировать атаки из Сети, экономить рабочее время, самостоятельно фильтруя спам, и, конечно же, не допускать попадания персональной информации в руки злоумышленникам. Важно, чтобы при всем этом компьютер еще и не тормозил. Ежедневно в мире появляется около 35 000 новых вредоносных программ, и, чтобы эффективно им противостоять, нужна постоянная модернизация антивирусного ПО. Прошел такую модернизацию и Kaspersky Internet Security (KIS). В версии 2012 разработчики добавили немало нововведений. И все же ее можно назвать эволюционной: шлифовка уже имеющихся механизмов позволила приблизить данный пакет к идеалу защиты ПК.

«Облачная» система безопасности

Говоря об эволюции, мы подразумеваем поднятие уже имеющихся в KIS функций на более высокий уровень реализации. Наиболее сильно это затронуло появившуюся в версии 2010 «облачную» технологию Kaspersky Security Network (KSN). Механизм ее работы заключается в том, что множество компьютеров, входящих в KSN, сообщают «облаку» об источниках заражения и обнаруженной подозрительной активности. После обработки данные об угрозах становятся доступны другим ПК, имеющим соединение с «облаком». Однако одной лишь «облачной» защиты для обеспечения безопасности недостаточно. В KIS 2012 существенно улучшены механизмы мониторинга по сигнатурам и слежения за подозрительными приложениями. В совокупности это обеспечивает своего рода гибридную защиту, моментально реагирующую на любые угрозы.

Возвращаясь к технологии KSN, стоит подчеркнуть, что она задействована во многих защитных механизмах KIS 2012. Это и слежение за подозрительными программами, и антиспам, и безопасный веб-серфинг. Несмотря на то, что данный сервис задумывался как полностью автоматизированный, имеется возможность использовать его в ручном режиме. С помощью специального пункта в контекстном меню Проводника Windows вы можете оценить репутацию любого исполняемого файла.

Автоматическая защита

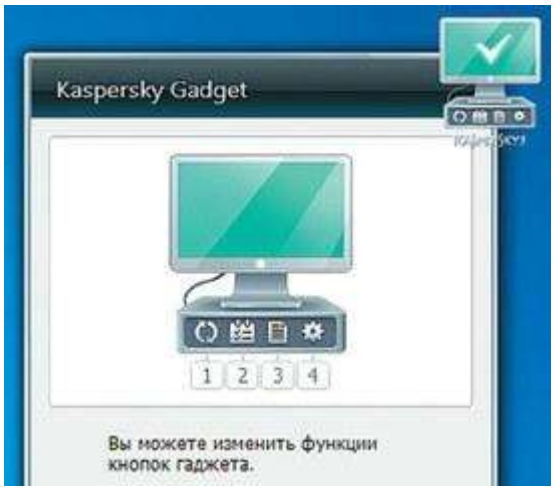


Рисунок 46 - Новый виджет информирует пользователя о состоянии защиты

Для подозрительных программ или веб-страниц применяется технология эмуляции виртуального пространства, в котором и осуществляется их запуск. Так пользователь может предварительно оценить действия программы, не предоставляя ей доступ к системе и личным данным. В KIS 2012 защищенный режим активируется автоматически, когда вы заходите наподозрительный веб-сайт.

Кстати, есть возможность и запускать в защитной среде лишь интернет браузер — причем не только тот, который задан по умолчанию, но и любой другой по выбору пользователя.

Даже если программа прошла проверку «песочницей», KIS 2012 продолжает следить за ее действиями — за это отвечает специальный модуль System Watcher. Онзапоминает все изменения, сделанные приложением в системе (причем за несколько сессий), и, если приложение все же попытается каким-то образом атаковать систему, Kaspersky Internet Security 2012 не только заблокирует его, но и сможет отменить все предыдущие действия. Кстати, помимо System Watcher за программой следит и технология контроля над приложениями. Получая информацию из облачной системы безопасности KSN, она оценивает репутацию программы и автоматически принимает решение, насколько ей можно доверять.

Антиспам обучать не нужно

В новой версии KIS в борьбе со спамом активно используется опять же «облачная» система. В ней накапливается информация не только о вредоносных и чистых файлах, потенциально опасных веб-сайтах, но и автоматически формируется список для эффективной фильтрации спама. Это означает, что вам не нужно делать лишних движений, чтобы указывать фильтру письма со спамом, — KIS 2012 способен заблокировать большинство непрошеных сообщений сразу после начала работы.

Как выглядит новый KIS

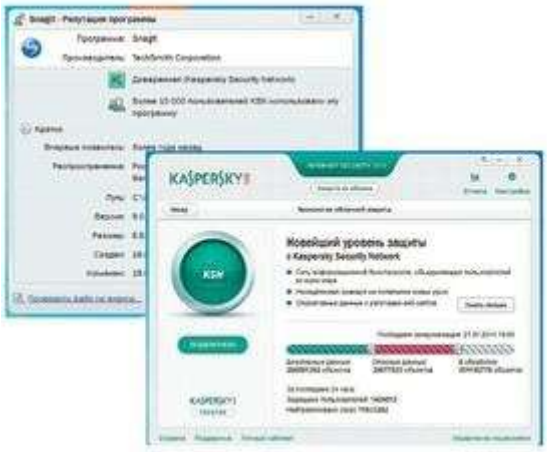


Рисунок 47 – Внешний вид Kaspersky.

Новый интерфейс стал трехмерным и анимированным. Так, при загрузке ПК теперь выводится окно «Добро пожаловать в Kaspersky Internet Security 2012». При клике по кнопке «закрыть» это окно эффектно оборачивается, и перед пользователем уже оказывается главный экран управления защитой. Анимированная полоса в главном окне содержит иконки, отражающие основные операции. Такая эргономичность делает удобной работу с антивирусом даже на устройствах с сенсорными экранами.

Одно из нововведений — кнопка «Защита из облака», расположенная вверху главного окна. Она открывает индикатор работы Kaspersky Security Network. В нем

отображается, сколько в базе помечено объектов — безопасных, опасных и находящихся в обработке.

Эффективнее и быстрее

По данным независимой компании AV-Test, антивирус Kaspersky Internet Security 2012 обнаруживает 99,4% угроз. Этот показатель заметно выше среднего по индустрии (98,5%). В тесте на обнаружение угроз, активно распространяющихся в Сети, программой были обнаружены 100% семплов. 100-процентный результат был продемонстрирован и в тесте на лечение системы, зараженной вирусами (при среднем показателе в 85,7%). Независимые эксперты отметили и значительное увеличение производительности программы по сравнению с предыдущей версией. Так, скорость сканирования системы увеличилась на 90%.