**Для выполнения лабораторных работ необходимо ознакомиться с лекциями №3 «Наиболее распространенные угрозы» и №12 «Экранирование, анализ защищенности».**

**Лабораторная работа № 1 выполняется индивидуально каждым студентом.**

**Лабораторные работы 2-4 могут выполняться индивидуально или группой по 3 – 4 человека, в зависимости от числа рабочих мест в лаборатории.**

**ЛАБОРАТОРНАЯ РАБОТА № 1**

Дать развернутый ответ на поставленные вопросы (письменно).

**Контрольные вопросы к лабораторным работам по дисциплине «Основы информационной безопасности»**

**для студентов групп БЭИ 2201 – БЭИ 2203**

Каждый вариант включает подготовку ответов на три вопроса, из перечисленных ниже. Вопросы для варианта задания определяется по формуле: для студентов группы БЭИ 2201 - N, N+R, N+2R, где N – номер студента в списке группы, а R число студентов в группе, для группы БЭИ 2202 - начинается N+10, N+10+R, N+10+2R и БЭИ 2203 – начиная с N+20, N+20+R, N+20+2R.

Перечень контрольных вопросов для лабораторной работы.

1. Назовите основные признаки деления вирусов на классы.
2. Файловые, сетевые …. – продолжите список вирусов.
3. К вирусам какого признака можно отнести макровирусы?
4. Термин «компаньон-вирусы» относятся к каким вирусам?
5. Опишите правила работы загрузочных вирусов.
6. Как макровирусы получают управление?
7. Какие вирусы называют программами типа «червь»?
8. Как действуют вирусы, ориентированные на операционную систему?
9. Опишите стадию жизненного цикла вируса, на которой он наиболее уязвим со стороны антивирусной программы.
10. Перечислите этапы стадии исполнения вируса.
11. На какой стадии вирус может шифровать исполняемый код?
12. Перечислите приёмы модификации кода.
13. Что представляет собой процесс загрузки вируса?
14. Опишите поведение полиморфных вирусов.
15. Опишите поведение стелс-вирусов.
16. Охарактеризуйте невыгружаемые из основной памяти вирусы, приведите пример.
17. Опишите два способа поиска жертвы заражения.
18. Что такое простейший случай заражения вирусом?
19. Как создаётся новый инфицированный файл?
20. Опишите первый способ внедрения вируса в файл.
21. Опишите второй способ внедрения вируса в файл.
22. Опишите третий способ внедрения вируса в файл.
23. Каким вирусам и почему приходится хранить часть своего кода на диске? Назовите место, где должна находится другая часть кода этого вируса.
24. Классификация Касперского, описание.
25. Процесс заражения для макровирусов.
26. Какими могут быть вирусы по деструктивным свойствам?
27. Какими бывают вирусы по отношению к программе-носителю?
28. Чем отличается троянская программа от червей?
29. Какова основная особенность логической бомбы?
30. Назовите классические методы шифрования.
31. На какие два класса можно разделить методы шифрование, в чём их отличие друг от друга?
32. Перечислите параметры алгоритмов симметричного шифрования.
33. Чем объясняются недостатки симметричного шифрования?
34. В чём смысл шифра Цезаря?
35. В чём смысл «магических квадратов»?
36. Объясните понятие «лазейка».
37. Поясните причину появления некоторых достоинств ассиметричного шифрования перед симметричным.
38. В чём состоит смысл метода экспоненциального обмена?
39. Каковы основные элементы PGP?
40. В чём отличие сертификата от ключа?
41. В чём отличие PGP от OpenPGP (дайте развёрнутый ответ)?
42. Каков порядок работы PGP?
43. Что представляет собой S/MIME?
44. В чём отличие S/MIME от PGP?
45. В чём заключаются классические методы распространения файловых вирусов?
46. В чём заключаются классические методы распространения загрузочных вирусов?
47. В чём заключаются классические методы распространения макрокомандных вирусов?
48. Каков основной принцип заражения по электронной почте?
49. Что зачастую приводит к внедрению вредоносных программ на компьютер через активные компоненты? К какому методу распространения вредоносного ПО это относится?
50. Существует ли жертва-посредник при заражении через локальную сеть между жертвой-источником и незаражёнными компьютерами?
51. Назовите другие каналы распространения вредоносных программ, кроме классических способов, электронной почты, сайтов, локальных сетей.
52. Перечислите методы и средства защиты информации.
53. Что такое маска вируса?
54. Каков основной недостаток метода сравнения с эталоном?
55. Какова методика работы эвристического анализа?
56. Антивирусный мониторинг, суть метода.
57. Чем отличается проактивная защита от эвристического анализа?
58. На чём основан метод обнаружения изменений?
59. Что такое программы с автоматическим дозвоном?
60. Против какого типа вирусов направлены встраиваемые в BIOS антивирусы?
61. Какие методы защиты используют программы-фаги?
62. Категории фагов, описание?
63. Методика работы программ-фагов?
64. Какие программы-фаги обеспечивают более надёжную защиту, почему?
65. Что такое CRC-сканеры?
66. Назовите плюсы и минусы программ-ревизоров.
67. На чём основана работа программ-ревизоров?
68. Что такое вирусо опасные ситуации, какие антивирусные программы реагируют на них?
69. Лечение поражённых файлов программами-блокировщиками.
70. Какова основная функция программ-блокировщиков? Каковы их минусы?
71. Чем программы-иммунизаторы отличаются от CRC-сканеров?
72. Сколько типов иммунизаторов можно выделить, чем они отличаются?
73. Перечислите критерии качества антивирусной программы.
74. Назовите основные компоненты антивирусного комплекса, который обеспечит приемлемую защиту от вирусов, не перегружая и затормаживая систему. Обращаем внимание, что вариантов может быть несколько.
75. К каким вирусам относятся вирусы не имеющие сигнатур?
76. Какие вирусы способны перехватить запросы операционной системы на чтение/запись заражённых файлов? С какой целью они это делают?
77. Могут ли макровирусы являться стелс-вирусами?
78. Каким образом вирус может «обмануть» операционную систему так, что она будет считать место его расположения как свободный сектор?
79. Вирусы, построенные для работы на какой платформе, обладают неограниченными потенциальными возможностями?

Лабораторная работа №2

Изучение пакетов антивирусной защиты. Антивирус Dr.Web

Цель работы: Ознакомиться с распространенной программой антивирусной защиты Dr.Web.

2.1. Освоить методы работы с антивирусом.

Задание для выполнения практической части работы

1 Установить программу Dr. Web и активировать месячную лицензию. При

необходимости обновить сигнатурные базы.

2 Ознакомиться с модулями, входящими в состав пакета Dr. Web и

зафиксировать основные настройки каждого из них.

3 Провести проверку на наличие угроз на компьютере и описать

возможности, предоставляемые программой. Обнаружить хотя бы один

вирус, описать его.

2.2.Обязательные иллюстрации к работе

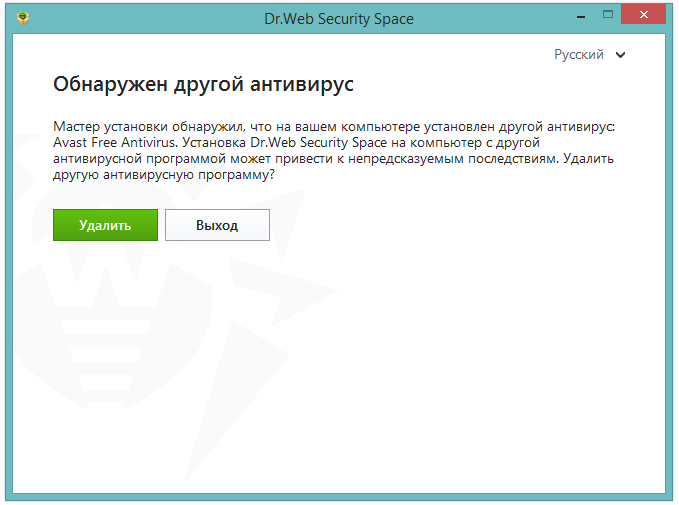
1 Дать скриншоты окон установки антивируса Dr. Web.

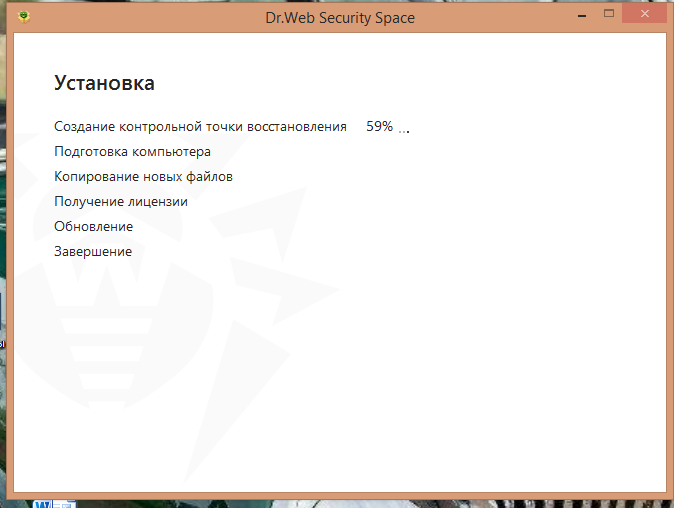
2 Привести скриншоты основных модулей, входящих в состав антивируса

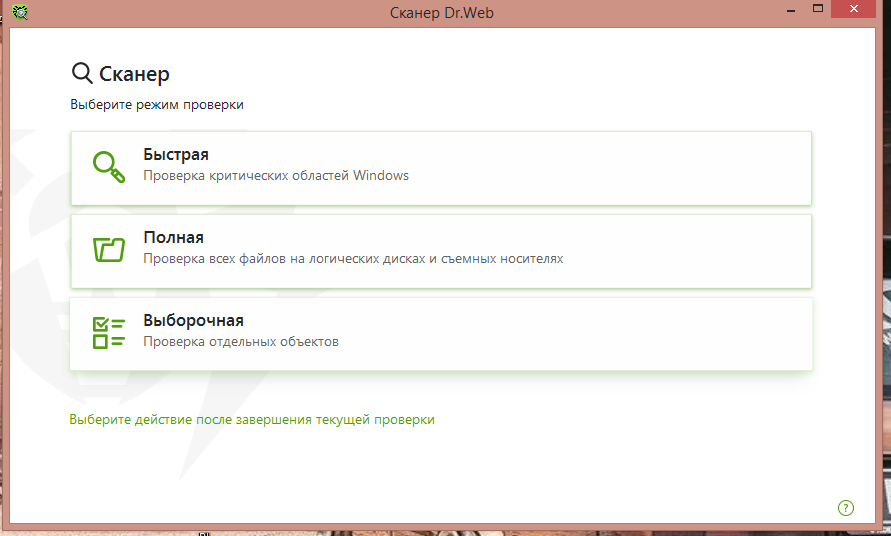
Dr. Web, и основных его настроек.

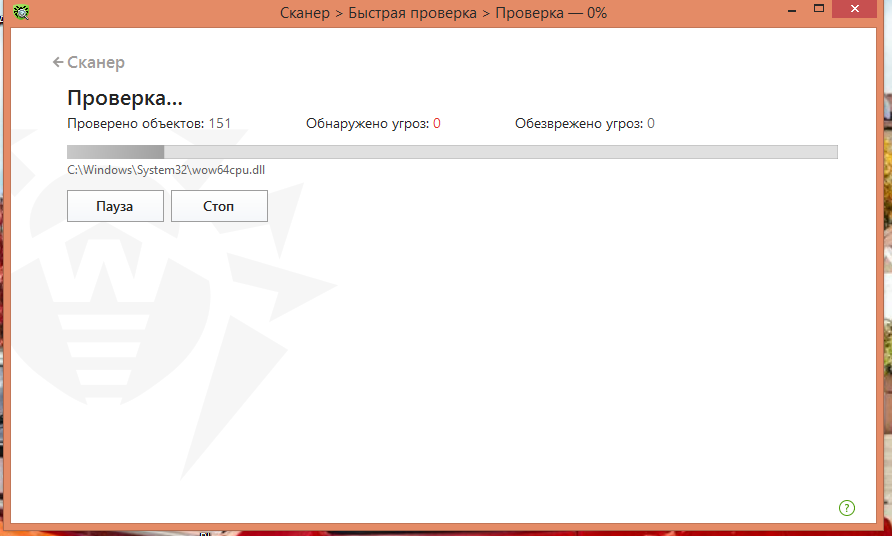
3 Привести скриншот процесса сканирования с обнаружением вируса (или

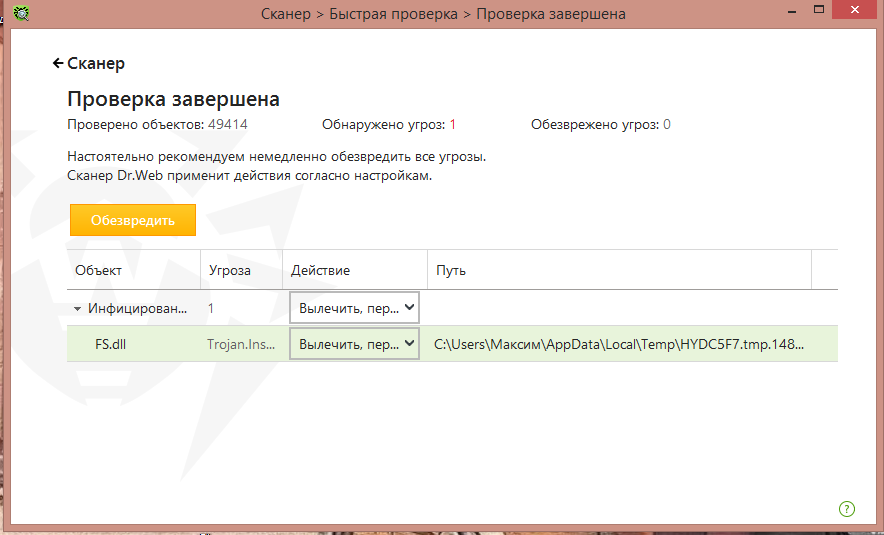
нескольких вирусов).

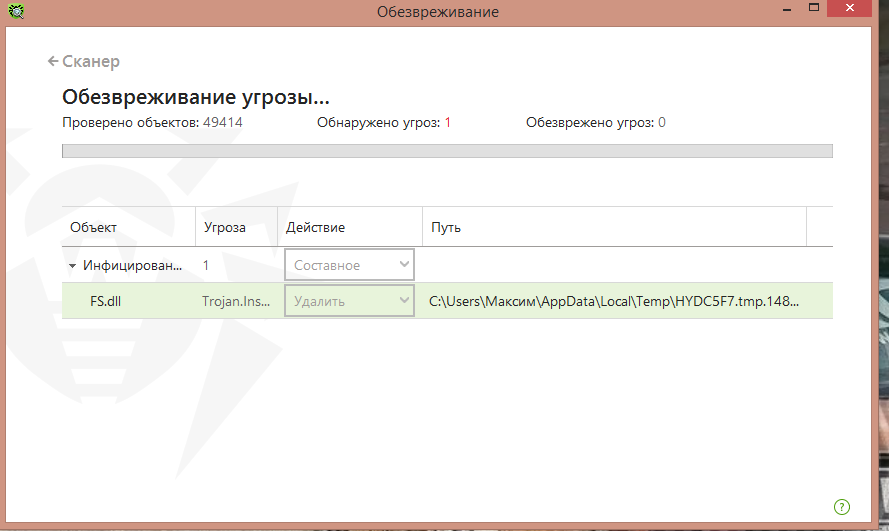


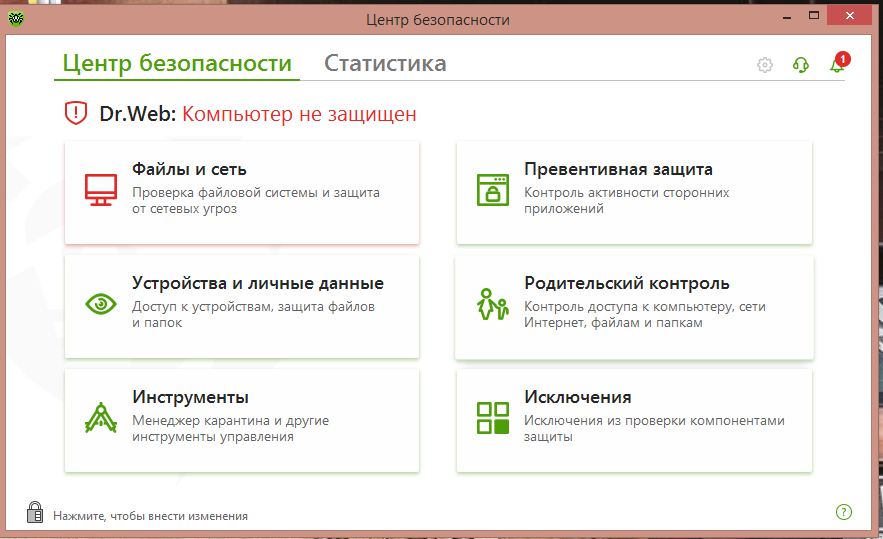


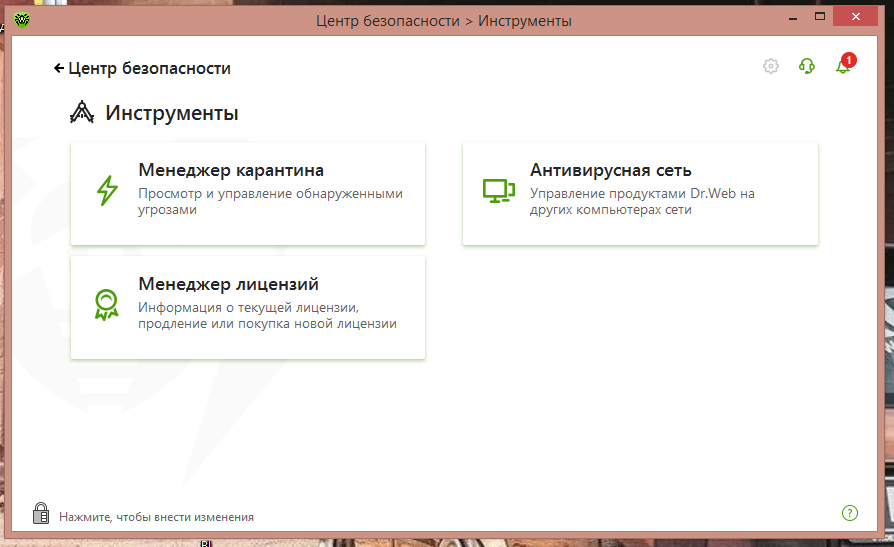


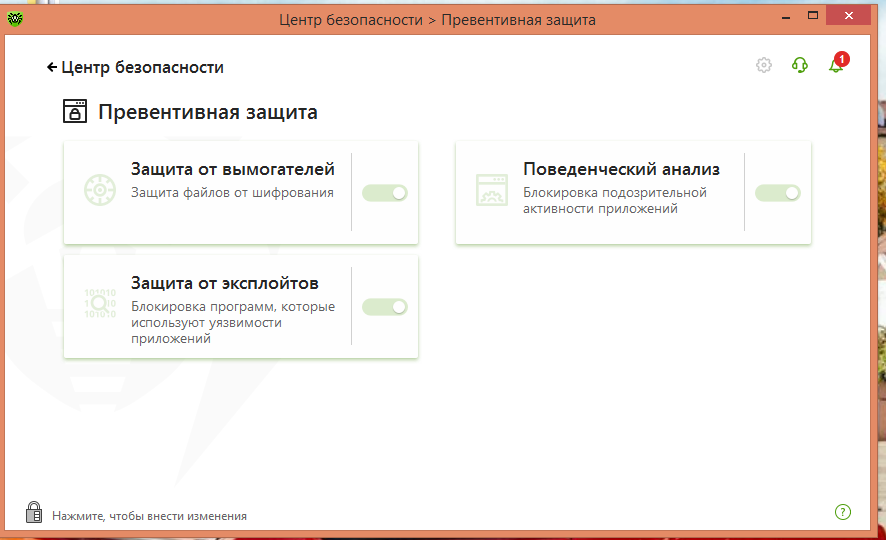












Контрольные вопросы.

1. Вирусы можно разделить на классы по следующим основным признакам:

* среда обитания;
* операционная система (OC);
* особенности алгоритма работы;
* деструктивные возможности.

2. По среде обитания вирусы можно разделить на:

* файловые;
* загрузочные;
* макро;
* сетевые.

3. Макровирусы распространяются под управлением прикладных программ, что делает их независимыми от операционной системы. Подавляющее число макровирусов функционирует под управлением текстового процессора Microsoft Word. В то же время известны макровирусы, работающие под управлением таких приложений, как Microsoft Excel, Lotus Ami Pro, Lotus 1-2-3, Lotus Notes, в операционных системах фирм Microsoft и Apple.

4. Компаньон-вирусы, как и перезаписывающие вирусы, создают свою копию на месте заражаемой программы, но в отличие от перезаписываемых не уничтожают оригинальный файл, а переименовывают или перемещают его. При запуске программы вначале выполняется код вируса, а затем управление передается оригинальной программе.  
Возможно существование и других типов вирусов-компаньонов, использующих иные оригинальные идеи или особенности других операционных систем. Например, PATH-компаньоны, которые размещают свои копии в основном каталоге Windows, используя тот факт, что этот каталог является первым в списке PATH, и файлы для запуска Windows в первую очередь будет искать именно в нем. Данными способом самозапуска пользуются также многие компьютерные черви и [троянские программы](http://www.infobezpeka.com/publications/?id=147).

5. Простейшие загрузочные вирусы, находясь в [памяти](https://ru.wikipedia.org/wiki/%D0%9E%D0%97%D0%A3) заражённого компьютера, обнаруживают в компьютере незаражённый диск и производят следующие действия:

* Выделяют некоторую область диска и делают её недоступной для операционной системы.
* Замещают программу начальной загрузки в загрузочном секторе диска, копируя корректную программу загрузки, а также свой код, в выделенную область диска;
* Организуют передачу управления так, чтобы вначале выполнялся [код](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%B4) вируса и лишь затем — программа начальной загрузки.

6. Макровирусы. Для своего размножения они используют по максимуму все возможности макро-языков и используя все возможности, переносят себя (а точнее программный код) из одного зараженного файла (как правило, это таблица или документ) в другие.

7. Сетевой червь — разновидность [вредоносной программы](https://ru.wikipedia.org/wiki/%D0%92%D1%80%D0%B5%D0%B4%D0%BE%D0%BD%D0%BE%D1%81%D0%BD%D0%B0%D1%8F_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B0), самостоятельно распространяющейся через локальные и глобальные ([Интернет](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82)) компьютерные сети.

9. Как и у любой программы, у компьютерных вирусов можно выделить две основные стадии жизненного цикла — хранение и исполнение.

Стадия хранения соответствует периоду, когда вирус просто хранится на диске совместно с объектом, в который он внедрен. На этой стадии вирус является наиболее уязвимым со стороны антивирусного ПО, так как он не активен и не может контролировать работу ОС с целью самозащиты.

Некоторые вирусы на этой стадии используют механизмы защиты своего кода от обнаружения. Наиболее распространенным способом защиты является шифрование большей части тела вируса. Его использование совместно с механизмами мутации кода (об этом идет речь ниже) делает невозможным выделение сигнатур — устойчивых характеристических фрагментов кода вирусов.

10. Стадия исполнения компьютерных вирусов, как правило, включает пять этапов:

1) загрузка вируса в память;

2) поиск жертвы;

3) заражение найденной жертвы;

4) выполнение деструктивных функций;

5) передача управления программе-носителю вируса.

11.Вирус может шифровать исполняемый код на стадии выполнения действующей функции.

14. Полиморфные вирусы (polymorphic) — это трудно обнаруживаемые вирусы, не имеющие сигнатур, т. е. не содержащие ни одного постоянного участка кода. В большинстве случаев два образца одного и того же полиморфного вируса не будут иметь ни одного совпадения. Полиморфизм встречается в вирусах всех типов — файловых, загрузочных и макровирусах.

Дополнительные действия, которые выполняют полиморфные вирусы на этапе загрузки, состоят в расшифровывании основного тела вируса.

15. Стелс-вирусы (Stealth) способны скрывать свое присутствие в системе и избегать обнаружения антивирусными программами. Эти вирусы могут перехватывать запросы ОС на чтение/запись зараженных файлов, при этом они либо временно лечат эти файлы, либо «подставляют» вместо себя незараженные участки информации, эмулируя «чистоту» зараженных файлов.

17. Поиск жертвы. По способу поиска жертвы вирусы можно разделить два два класса.

К первому классу относятся вирусы, осуществляющие «активный» поиск с использованием функций ОС. Примером являются файловые вирусы, использующие механизм поиска исполняемых файлов в текущем каталоге.

Второй класс составляют вирусы, реализующие «пассивный» механизм поиска, т. е. вирусы, расставляющие «ловушки» дпя программных файлов. Как правило, файловые вирусы устраивают такие ловушки путем перехвата функции Ехес ОС, а макровирусы — с помощью перехвата команд типа Save as из меню File.

Лабораторная работа №3

Изучение пакетов антивирусной защиты. Антивирус Касперского

Цель работы: Ознакомиться с распространенной программой антивирусной защиты Антивирус Касперского. Освоить методы работы с антивирусом, выполнить сравнительный анализ с антивирусным ПО Dr.Web.

Пакет антивирусной защиты Антивирус Касперского

Антивирус Касперского (англ. Kaspersky Antivirus, KAV) — антивирусное программное обеспечение, разрабатываемое Лабораторией Касперского. Предоставляет пользователю защиту от вирусов, троянских программ, шпионских программ, руткитов, adware, а также неизвестных

Антивирус Касперского предлагает следующие функции базовой защиты:

* Защита от вирусов, троянских программ и червей
* Защита от шпионских и рекламных программ
* Проверка файлов в автоматическом режиме и по требованию
* Проверка почтовых сообщений (для любых почтовых клиентов)
* Проверка интернет-трафика (для любых интернет-браузеров)
* Защита интернет-пейджеров (ICQ, MSN)
* Проактивная защита от новых вредоносных программ
* Проверка Java- и Visual Basic-скриптов
* Защита от скрытых и поврежденных ссылок
* Постоянная проверка файлов в автономном режиме
* Постоянная защита от фишинговых сайтов

Порядок выполнения лабораторной работы

1 Установить программу Антивирус Касперского. Обновить сигнатурные

2 Ознакомиться с модулями, входящими в состав пакета Антивирус

Касперского и зафиксировать основные настройки каждого

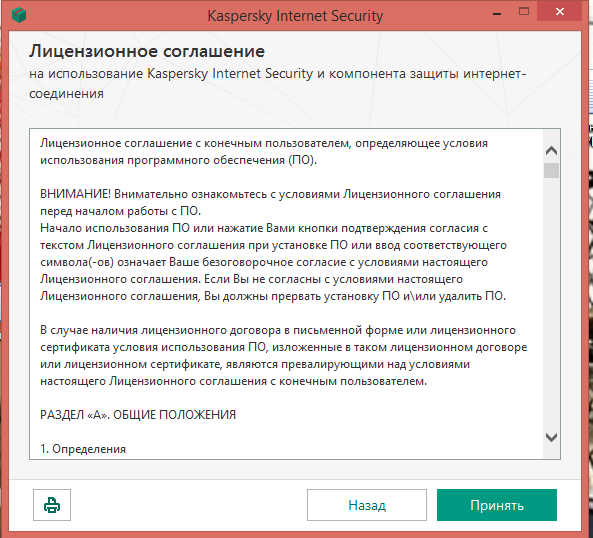
3 Провести проверку на наличие угроз на компьютере и описать

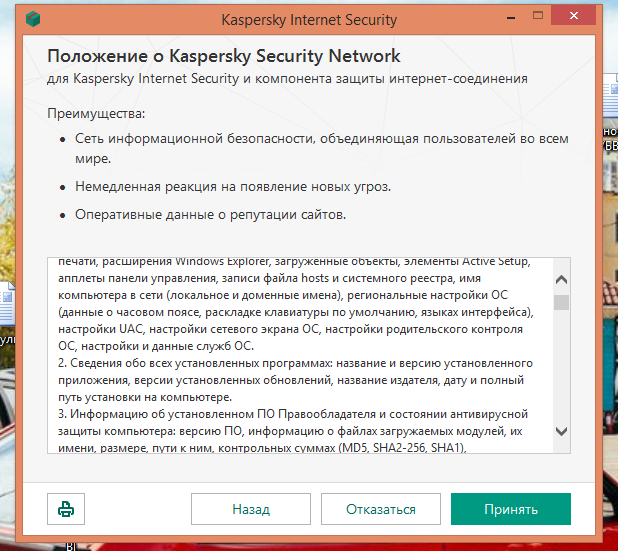
возможности, предоставляемые программой. Обнаружить хотя бы один

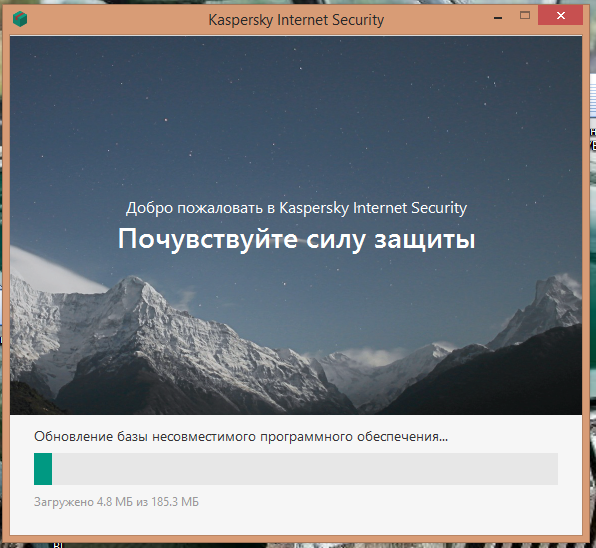
вирус, описать его.

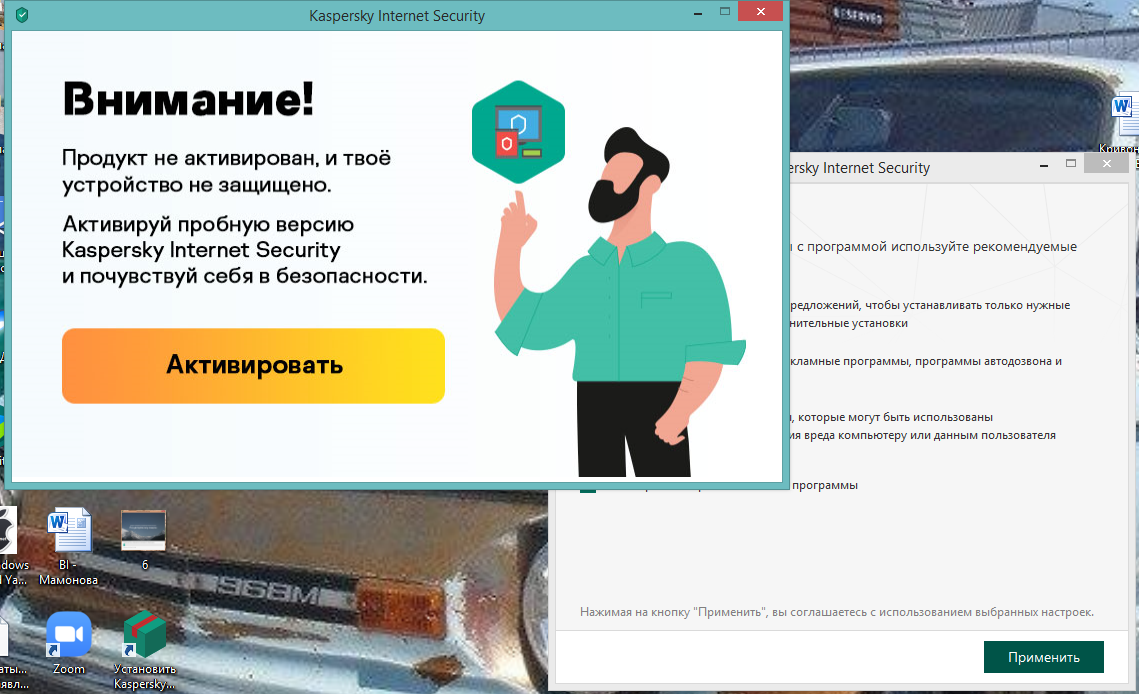
4 Выполнить сравнение антивирусных программ Антивирус Касперского и Dr. Web.

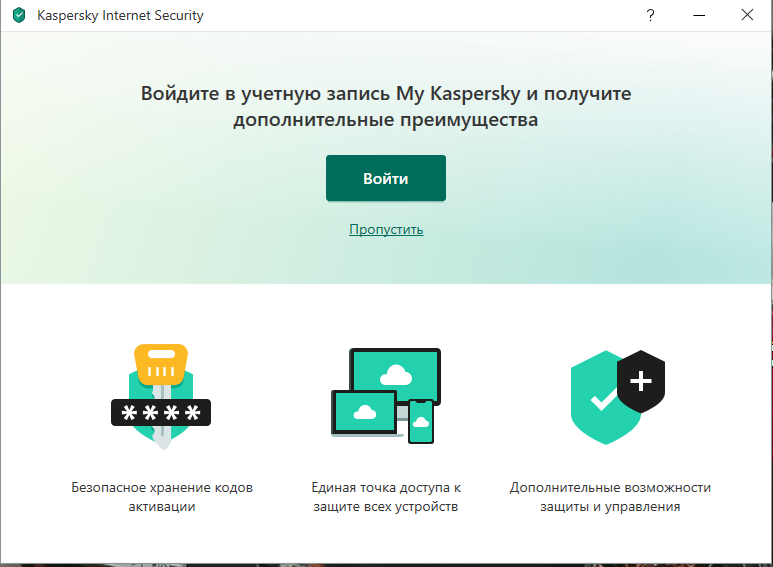


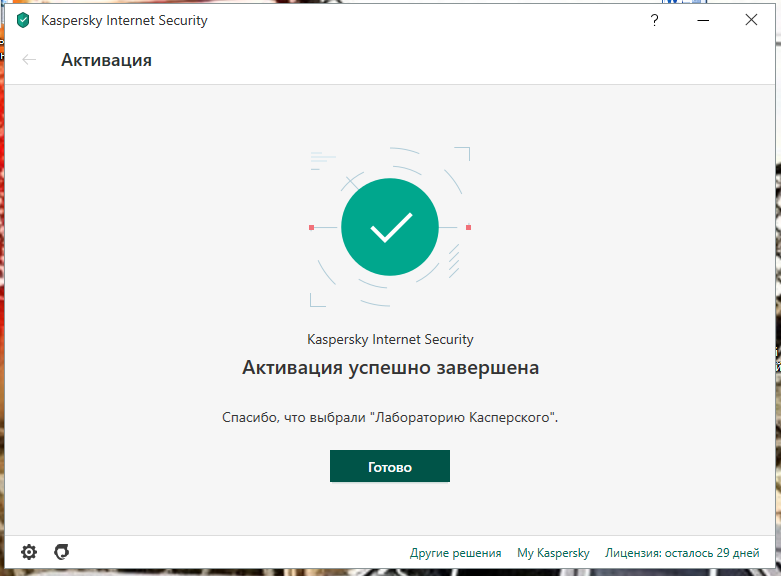


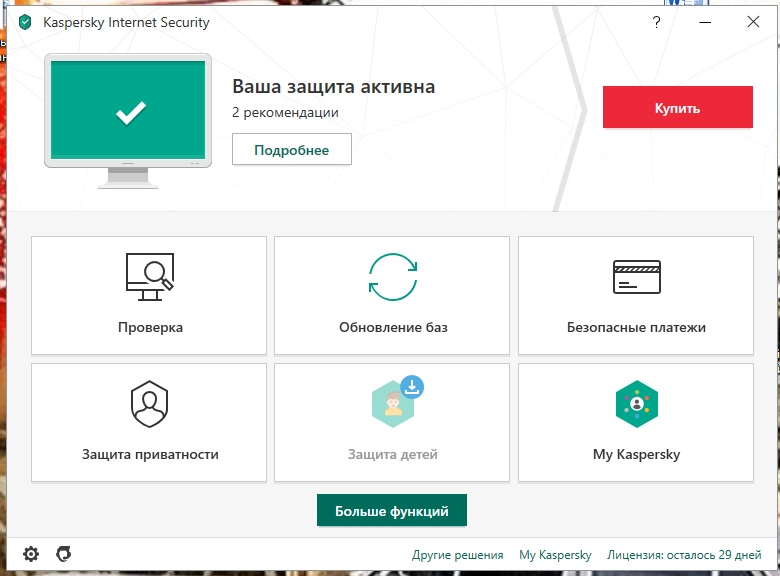












Контрольные вопросы.

1. Файловые вирусы распространяются вместе с файлами программ в результате обмена дискетами и программами, загрузки программ из сетевых каталогов, сWeb- или ftp-серверов. Загрузочные вирусы попадают на компьютер, когда пользователь забывает зараженную дискету в дисководе, а затем перезагружает ОС. Загрузочный вирус также может быть занесен на компьютер вирусами других типов. Макрокомандные вирусы распространяются в результате обмена зараженными файлами офисных документов, такими как файлы Microsoft Word, Excel, Access.

Если зараженный компьютер подключен к локальной сети, вирус легко может оказаться на дисках файл-сервера, а оттуда через каталоги, доступные для записи, попасть на все остальные компьютеры сети. Так начинается вирусная эпидемия. Системному администратору следует помнить, что вирус имеет в сети такие же права, что и пользователь, на компьютер которого этот вирус пробрался. Поэтому он может попасть во все сетевые каталоги, доступные пользователю. Если же вирус завелся на рабочей станции администратора сети, последствия могут быть очень тяжелыми.

4. Вирус электронной почты состоит из вредоносного кода, который распространяется в сообщениях электронной почты, и его можно активировать, когда пользователь щелкает ссылку в сообщении электронной почты, открывает вложение электронной почты или каким-либо другим образом взаимодействует с зараженным сообщением электронной почты.

5.Методы защиты информации

* препятствие– метод физического преграждения пути злоумышленнику к защищаемой информации
* управление доступом– метод определения и распределения ресурсов системы санкционированным пользователям
* шифрование- метод защиты информации в коммуникационных каналах путем ее криптографического закрытия. Этот метод защиты широко применяется как для обработки, так и для хранения информации. При передаче информации по коммуникационным каналам большой протяженности этот метод является единственно надежным.
* регламентация– метод защиты информации, создающий специальные условия автоматизированной обработки, хранения и передачи защищаемой информации, при которых возможности несанкционированного доступа к ней сводились бы к минимуму.
* принуждение- такой метод защиты информации, при котором пользователи и персонал системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.
* побуждение- метод защиты информации, который стимулирует пользователя и персонал системы не нарушать установленных норм (высокая зарплата)

Средства

1. технические реализуются в виде электрических, электромеханических и электронных устройств. Вся совокупность технических средств делится на аппаратные и физические.

Под аппаратными принято понимать встроенные электронные устройства. Из наиболее известных аппаратных средств можно назвать схемы контроля информации по четности, схемы защиты полей памяти по ключу и т. д.

Физические средства реализуются в виде автономных устройств и систем. Например, замки на дверях помещений с аппаратурой, решетки на окнах, охранная сигнализация, камеры видеонаблюдения.

Физические средства защиты:

* обеспечивают безопасность помещений, где размещены серверы сети;
* ограничение посторонним лицам физического доступа к серверам, концентраторам, коммутаторам, сетевым кабелям и другому оборудованию;
* обеспечивают защиту от сбоев электросети.

1. программные средства представляют собой программное обеспечение, специально предназначенное для выполнения функций защиты информации.

Стандартные защищенные программные средства:

* Средства защиты, использующие парольную идентификацию и ограничивающие доступ пользователей согласно назначенным правам - управление доступом и разграничение полномочий (идентификация+ аутентификация +авторизация)

Идентификация позволяет субъекту (пользователю, процессу, действующему от имени определенного пользователя, или иному аппаратно-программному компоненту) назвать себя (сообщить свое имя). Посредством аутентификации вторая сторона убеждается, что субъект действительно тот, за кого он себя выдает. В качестве синонима слова "аутентификация" иногда используют словосочетание "проверка подлинности".

* Регистрация и анализ событий, происходящих в системе - обеспечивает получение и анализ информации о состоянии ресурсов системы с помощью специальных средств контроля, а также регистрацию действий, признанных потенциально опасными для безопасности системы. Анализ собранной информации позволяет выявить средства и априорную информацию, использованные нарушителем при воздействии на систему и определить, как далеко зашло нарушение, подсказать метод его расследования и способы исправления ситуации;
* Контроль целостности ресурсов системы предназначен для своевременного обнаружения их модификации. Это позволяет обеспечить правильность функционирования системы и целостность обрабатываемой информации.
* Криптографическое закрытие информации
* Защита от внешних вторжений - брандмауэры
* Защита от компьютерных вирусов – антивирусные пакеты, антиспамовые фильтры
* Средства резервного копирования и восстановления данных

1. аппаратно-программные средства защиты основаны на использовании различных электронных устройств и специальных программ, входящих в состав системы защиты информации и выполняющих такие (самостоятельно или в комплексе с другими средствами) функции защиты, как: идентификация и аутентификация пользователей, разграничение доступа к ресурсам, регистрация событий, криптографическое закрытие информации, обеспечение отказоустойчивости компонент и системы в целом и т.д.
2. Организационные средства защиты представляют собой организационно-технические и организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации специального ПО и аппаратных устройств для обеспечения защиты информации. Организационные мероприятия охватывают все структурные элементы на всех этапах жизненного цикла защищаемой системы (создание охраняемого периметра, строительство помещений, проектирование системы в целом, монтаж и наладка оборудования, испытания и эксплуатация), а также кадровую политику и подбор персонала.
3. морально-этические средства защиты реализуются в виде норм, которые сложились традиционно или складываются по мере распространения ВТ и средств связи в данной стране или обществе. Эти нормы, как правило, не являются обязательными, как законодательные меры, однако несоблюдение их ведет к потере авторитета и престижа организации.
4. законодательные – средства защиты определяются законодательными актами страны. В них регламентируются правила использования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил.

11. В процессе эвристического анализа производится проверка эмулируемой программы анализатором кода. К примеру, программа инфицирована полиморфным вирусом, состоящим из зашифрованного тела и расшифровщика. Эмулятор кода считывает инструкции в буфер антивируса, разбирает их на инструкции и производит их исполнение по одной инструкции, после этого анализатор кода подсчитывает контрольную сумму и сверяет её с той, которая хранится в базе. Эмуляция будет продолжаться до тех пор, пока необходимая для подсчета контрольной суммы часть вируса не будет расшифрована. Если сигнатура совпала — программа определена.

12. **Антивирусный мониторинг**. Суть данного метода состоит в том, что в памяти компьютера постоянно находится антивирусная программа, осуществляющая мониторинг всех подозрительных действий, выполняемых другими программами. Антивирусный мониторинг позволяет проверять все запускаемые программы, создаваемые, открываемые и сохраняемые документы, файлы программ и документов, полученные через Интернет или скопированные на жесткий диск с дискеты либо компакт-диска. Антивирусный монитор сообщит пользователю, если какая-либо программа попытается выполнить потенциально опасное действие. Пример такой программы – сторож Spider Guard, который входит в комплект сканера Dr. Web и выполняет функции антивирусного монитора.

13. Проактивные технологии — совокупность технологий и методов, используемых в [антивирусном программном обеспечении](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D1%82%D0%B8%D0%B2%D0%B8%D1%80%D1%83%D1%81%D0%BD%D0%B0%D1%8F_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B0), основной целью которых, в отличие от [реактивных (сигнатурных) технологий](https://ru.wikipedia.org/wiki/%D0%9E%D0%B1%D0%BD%D0%B0%D1%80%D1%83%D0%B6%D0%B5%D0%BD%D0%B8%D0%B5,_%D0%BE%D1%81%D0%BD%D0%BE%D0%B2%D0%B0%D0%BD%D0%BD%D0%BE%D0%B5_%D0%BD%D0%B0_%D1%81%D0%B8%D0%B3%D0%BD%D0%B0%D1%82%D1%83%D1%80%D0%B0%D1%85), является предотвращение заражения системы пользователя, а не поиск уже известного [вредоносного программного обеспечения](https://ru.wikipedia.org/wiki/%D0%92%D1%80%D0%B5%D0%B4%D0%BE%D0%BD%D0%BE%D1%81%D0%BD%D0%B0%D1%8F_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B0) в системе. При этом проактивная защита старается блокировать потенциально опасную активность программы только в том случае, если эта активность представляет реальную угрозу. Серьезный недостаток проактивной защиты — блокирование легитимных программ (ложные срабатывания).

14. Обнаружение изменений — метод обнаружения вирусов и вредоносных программ различного типа, основанный на обнаружении изменений, вызываемых вирусами и вредоносными программами в файлах.

Пояснение

Данный метод используется программами с названием *ревизоры диска*или системы контроля целостности.

Ревизоры диска периодически сканируют содержимое дисков компьютера, записывая в свою базу данных контрольные суммы файлов и критически важных внутренних областей файловых систем. При сканировании новые значения контрольных сумм сравниваются со старыми значениями.

Если при сравнении обнаруживаются изменения, ревизор диска отображает на экране предупреждающее сообщение.

С помощью ревизора диска можно обнаружить любые изменения, сделанные в файлах компьютерными вирусами и другими вредоносными программами, а также пользователями.

Этот факт позволяет использовать ревизоры диска не только для защиты от вредоносных программ, но и для контроля целостности важных файлов и документов.

15.Автодозвон - это функция, позволяющая самостоятельно набирать номер телефона определенное количество раз без вашего участия.

21. Принцип работы CRC-сканеров основан на подсчете CRC-сумм (контрольных сумм) для присутствующих на диске файлов/системных секторов. Эти CRC-суммы затем сохраняются в базе данных антивируса, как, впрочем, и некоторая другая информация: длины файлов, даты их последней модификации и т.д. При последующем запуске CRC-сканеры сверяют данные, содержащиеся в базе данных, с реально подсчитанными значениями. Если информация о файле, записанная в базе данных, не совпадает с реальными значениями, то CRC-сканеры сигнализируют о том, что файл был изменен или заражен вирусом.

CRC-сканеры, использующие анти-стелс алгоритмы, являются довольно сильным оружием против вирусов: практически 100% вирусов оказываются обнаруженными почти сразу после их появления на компьютере. Однако у этого типа антивирусов есть врожденный недостаток, который заметно снижает их эффективность. Этот недостаток состоит в том, что CRC-сканеры не способны поймать вирус в момент его появления в системе, а делают это лишь через некоторое время, уже после того, как вирус разошелся по компьютеру. CRC-сканеры не могут определить вирус в новых файлах (в электронной почте, на дискетах, в файлах, восстанавливаемых из backup или при распаковке файлов из архива), поскольку в их базах данных отсутствует информация об этих файлах. Более того, периодически появляются вирусы, которые используют эту «слабость» CRC-сканеров, заражают только вновь создаваемые файлы и остаются, таким образом, невидимыми для них.

29. Качество антивирусной программы можно оценить по нескольким критериям:

- надежность и удобство работы — отсутствие «зависаний» антивируса и прочих технических проблем, требующих от пользователя специальной подготовки;

- качество обнаружения вирусов всех распространенных типов, сканирование внутри файлов-документов/таблиц (MS Word, Excel, Office), упакованных и архивированных файлов; возможность лечения зараженных объектов;

- существование версий антивируса под все популярные платформы (DOS, Windows NT, Novell NetWare, OS/2, Alpha, Linux и т. д.); наличие режимов сканирования «по запросу» и «на лету», существование серверных версий с возможностью администрирования сети;

- скорость работы и другие полезные особенности. Надежность работы антивируса является наиболее важным критерием, поскольку даже «абсолютный» антивирус может оказаться бесполезным, если он не в состоянии довести процесс сканирования до конца, т. е. «повиснет» и не проверит часть дисков и файлов и, в результате, вирус останется незамеченным в системе.

Качество обнаружения вирусов стоит на следующем месте по вполне естественной причине. Главная обязанность антивирусных программ — обнаруживать 100% вирусов и лечить их. При этом антивирусная программа не должна иметь высокий уровень ложных срабатываний.

Следующий по важности критерий — многоплатформенность антивируса, поскольку только программа, рассчитанная на конкретную ОС, может полностью использовать функции этой системы. Моментальная и принудительная проверка приходящих на компьютер файлов и вставляемых дискет — это практически 100%-я гарантия от заражения вирусом. Если в серверном варианте антивируса присутствует возможность антивирусного администрирования сети, то его ценность еще более возрастает.

Скорость работы также является важным критерием качества антивирусной программы. В разных антивирусах используются различные алгоритмы поиска вирусов, один алгоритм может оказаться более быстрым и качественным, другой — медленным и менее качественным.

31. Полиморфик-вирусы

Лабораторная работа №4

Изучение межсетевых экранов. Zone Alarm.

Цель работы: Ознакомиться с принципами работы межсетевых экранов.

Освоить методы работы с распространенной программой межсетевого

экранирования Zone Alarm.

Порядок выполнения лабораторной работы

1 Установить программу Zone Alarm. Проверить и при необходимости

обновить.

2 Ознакомиться и зафиксировать основные настройки различных

пунктов меню.

3 Настроить должным образом программу Zone Alarm.

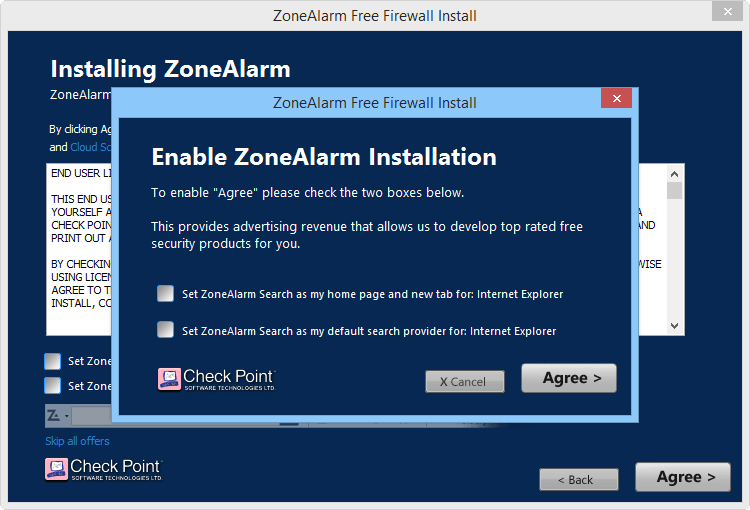
4 Обнаружить хотя бы одну попытку доступа на компьютер,

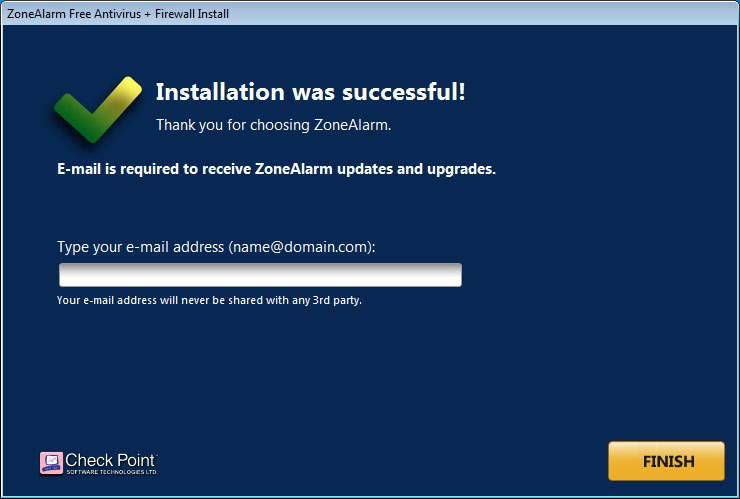
зафиксировать реакцию фаервола Zone Alarm.

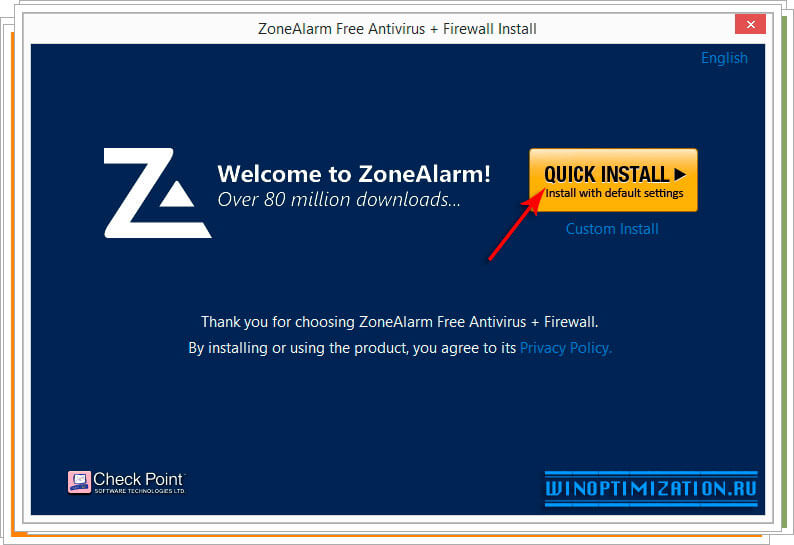
5 Провести попытку войти на доступный сетевой ресурс и на другие

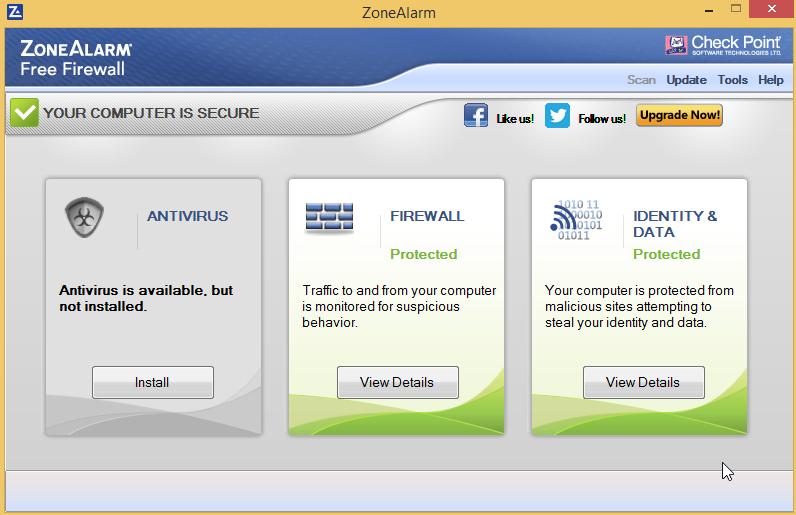
компьютеры локальной сети, зафиксировать реакцию фаервола Zone

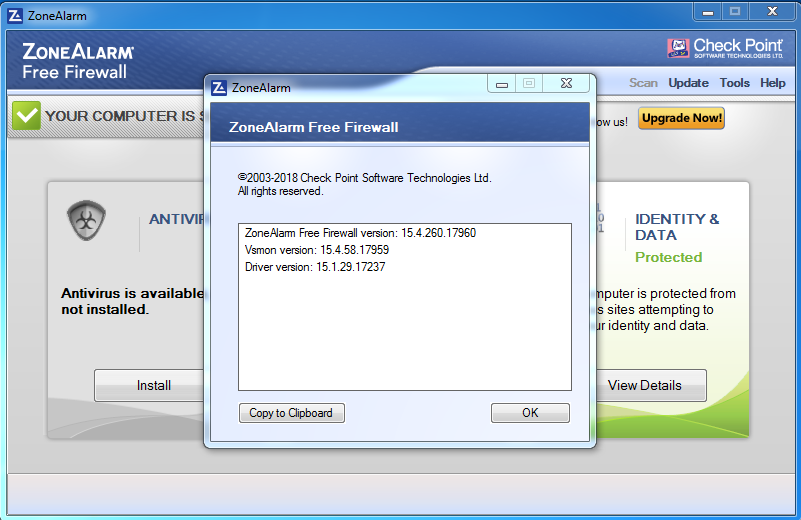
Alarm.

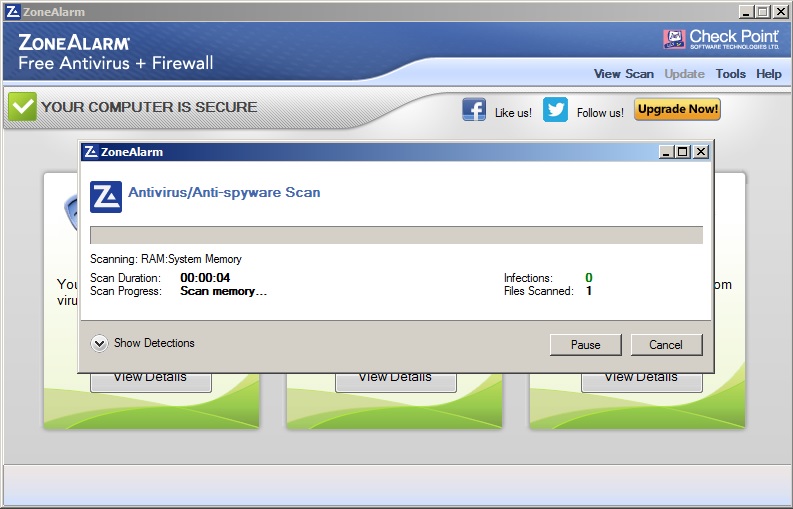


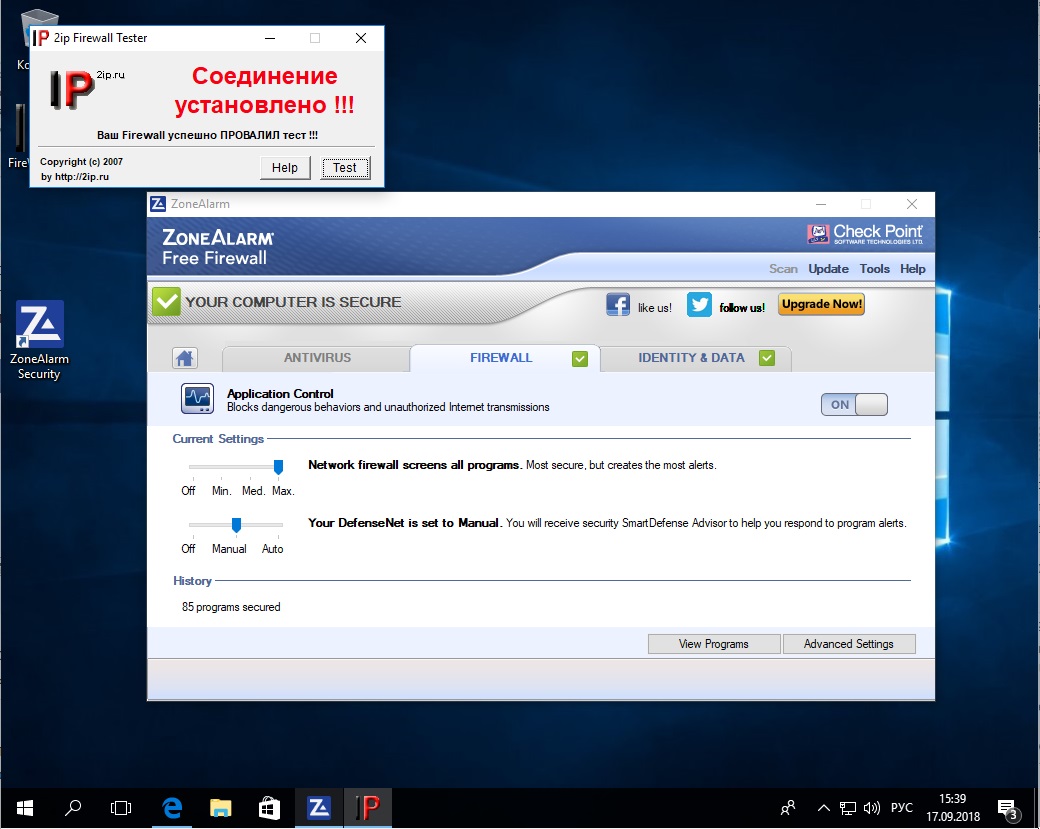












Контрольные вопросы.

1. До сих пор не существует единой и общепризнанной классификации межсетевых экранов. Однако в большинстве случаев поддерживаемый уровень сетевой модели [OSI](https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D0%B0%D1%8F_%D0%BC%D0%BE%D0%B4%D0%B5%D0%BB%D1%8C_OSI) является основной характеристикой при их классификации. Учитывая данную модель, различают следующие типы межсетевых экранов

1. Управляемые коммутаторы.
2. Пакетные фильтры.
3. Шлюзы сеансового уровня.
4. Посредники прикладного уровня.
5. Инспекторы состояния.
6. Наиболее распространённое место для установки межсетевых экранов — граница периметра [локальной сети](https://ru.wikipedia.org/wiki/%D0%9B%D0%BE%D0%BA%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D0%B2%D1%8B%D1%87%D0%B8%D1%81%D0%BB%D0%B8%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C) для защиты внутренних хостов от атак извне. Однако атаки могут начинаться и с внутренних узлов — в этом случае, если атакуемый хост расположен в той же сети, трафик не пересечёт границу сетевого периметра, и межсетевой экран не будет задействован. Поэтому в настоящее время межсетевые экраны размещают не только на границе, но и между различными сегментами сети, что обеспечивает дополнительный уровень безопасности

3. В некоторых случаях может понадобиться настройка блокировки портов компьютера, причем требуется не просто закрыть доступ к порту (что несложно), а разрешить доступ к порту только для ограниченного списка IP адресов (для остальных - запретить).  
В случае корпоративного прокси-сервера или шлюза всё довольно просто, поскольку корпоративное программное обеспечение, как правило, обладает достаточным функционалом. Однако в случае, если используется обычная точка доступа, можно или отключить доступ к определенному порту компьютера, или включить его.

7. При стандартном сценарии атаки, узел A отправляет эхо-запрос ICMP (пинг) на узел B, вызывая автоматический ответ. Время, необходимое для получения ответа, используется как мера виртуального расстояния между двумя узлами.

В широковещательной IP-сети запрос проверки связи отправляется на каждый узел, запрашивая ответ от каждого из получателей. Злоумышленники используют эту функцию для усиления трафика атаки.

8. Контролируют прохождение трафика на основе информации, содержащейся в заголовке [пакетов](https://ru.wikipedia.org/wiki/%D0%9F%D0%B0%D0%BA%D0%B5%D1%82_(%D1%81%D0%B5%D1%82%D0%B5%D0%B2%D1%8B%D0%B5_%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D0%B8)).

9. Пакетные фильтры функционируют на [сетевом уровне](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB%D1%8B_%D1%81%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B3%D0%BE_%D1%83%D1%80%D0%BE%D0%B2%D0%BD%D1%8F).

10. NAT— это механизм в [сетях](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C) [TCP/IP](https://ru.wikipedia.org/wiki/%D0%A1%D1%82%D0%B5%D0%BA_%D0%BF%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB%D0%BE%D0%B2_TCP/IP), позволяющий изменять [IP-адрес](https://ru.wikipedia.org/wiki/IP-%D0%B0%D0%B4%D1%80%D0%B5%D1%81) в заголовке [пакета](https://ru.wikipedia.org/wiki/%D0%9F%D0%B0%D0%BA%D0%B5%D1%82_(%D1%81%D0%B5%D1%82%D0%B5%D0%B2%D1%8B%D0%B5_%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D0%B8)), проходящего через [устройство маршрутизации](https://ru.wikipedia.org/wiki/%D0%9C%D0%B0%D1%80%D1%88%D1%80%D1%83%D1%82%D0%B8%D0%B7%D0%B0%D1%82%D0%BE%D1%80) трафика.