MINISTERU EDUCAȚIEI, CULTURII ȘI CERCETĂRII
UNIVERSITATEA DE STAT „ALECU RUSSO” DIN BĂLȚI
FACULTATEA DE ȘTIINȚE REALE, ECONOMICE ȘI ALE MEDIULUI
CATEDRA DE MATEMATICĂ ȘI INFORMATICĂ

SECURITATEA CALCULATOARELOR. SISTEM ANTIVIRUS

REFERAT LA CURSUL INFORMATICA GENERALĂ

Autor:

Studentul grupei IS11Z

Radion ROMAN

_____

Conducător științific:

Olesea SKUTNIȚKI

magistru, asist. univ.

_____

BĂLȚI, 2021

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Компьютерная безопасность это раздел информационной безопасности характеризующий невозможность возникновения ущерба компьютера, превышающего величину приемлемого ущерба для него от всех выявленных и изученных источников его отказов в определённых условиях работы и на заданном интервале времени.

Меры безопасности, применяемые для защиты вычислительных устройств (компьютеры, смартфоны и другие), а также компьютерных сетей (частных и публичных сетей, включая интернет). Поле деятельности системных администраторов охватывает все процессы и механизмы, с помощью которых цифровое оборудование, информационное поле и услуги защищаются от случайного или несанкционированного доступа, изменения или уничтожения данных, и приобретает всё большее значение в связи с растущей зависимостью от компьютерных систем в развитом сообществе.

Кибербезопастность это процесс использования мер безопасности для обеспечения конфиденциальности, целостности и доступности данных. Системный администратор обеспечивает защиту активов, включая данные локальной сети компьютеров, серверов. Кроме того, под охрану берутся непосредственно здания и, самое главное, персонал. Целью обеспечения кибербезопасности является защита данных (как в процессе передачи и/или обмена так и находящихся на хранении). В целях обеспечения безопасности данных могут быть применены и контрмеры. Некоторые из этих мер включают (но не ограничиваются) контроль доступа, обучение персонала, аудит и отчётность, оценку вероятных рисков, тестирование на проникновение и требование авторизации.

Сейчас в некоторых странах планируется обучение кибербезопасности уже со школьной скамьи. Так, в Великобритании школьникам предлагаются уроки по кибербезопасности, на которых они будут обучаться навыкам, позволяющим обеспечить безопасность британских компаний и организаций от сетевых атак хакеров. Учебная программа разработана Министерством культуры, СМИ и спорта Великобритании. Уроки планируются реализовать как в онлайн-форме так и в форме внеклассных занятий, которые будут проходить четыре раза в неделю и проводиться преподавателями-экспертами. С учащимися будут рассматривать реальные проблемы кибербезопасности и практику их решения. Программа направлена на учеников в возрасте от 14 до 18 лет. Проведение первых пробных занятий запланировано на сентябрь 2017 года.

1. КОМПЬЮТЕРНЫЙ ВИРУС

1.1. Что такое вирус

Вирусы это небольшие программы, которые могут заразить другие здоровые приложения и распространиться.

Каждый раз, когда программа запускается, она запускает тот фрагмент кода, который был введен вирусом. Этот код может выполнять различные команды, включая, в свою очередь, заражение других приложений. Распространяясь таким образом, вирус практически уничтожит операционную систему, в которой он работает. В зависимости от «творческих способностей» программиста вирусы могут делать что угодно. Он может заставить зараженные программы перестать работать, показывая нам ошибки за ошибками и странные вещи, которых обычно не должно происходить.

Фред Коэн, докторант, был первым, кто описал программы, которые можно копировать самостоятельно, назвав их «вирусами».

В 1980-х годах вирусы зависели от людей, чтобы размножаться и заражать другие компьютеры. Обычно программист сохраняет вирус на дискете, а затем раздает дискету другим. Так было до тех пор, пока модемы не стали обычным явлением, и через них могли «путешествовать» вирусы.

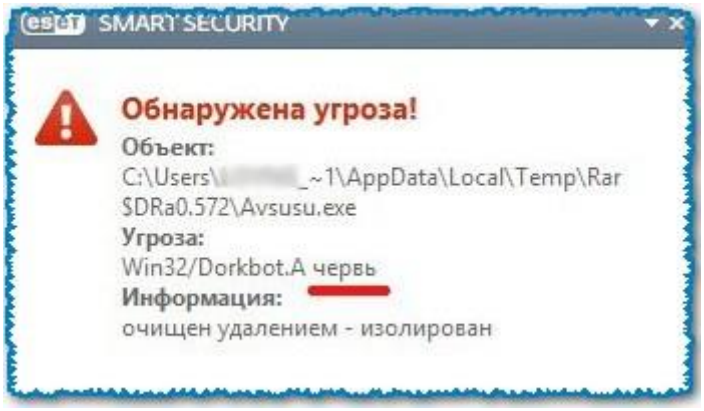
Сегодня проблема стала серьезной. Интернет является крупнейшим источником таких программ, согласно некоторым статистическим данным, более 50% компьютеров в мире в настоящее время заражены хотя бы одним вирусом. Многие компании потеряли большие суммы денег из-за этих небольших вредоносных программ.

1.2. Виды вирусов

Вирусы бывают нескольких типов:

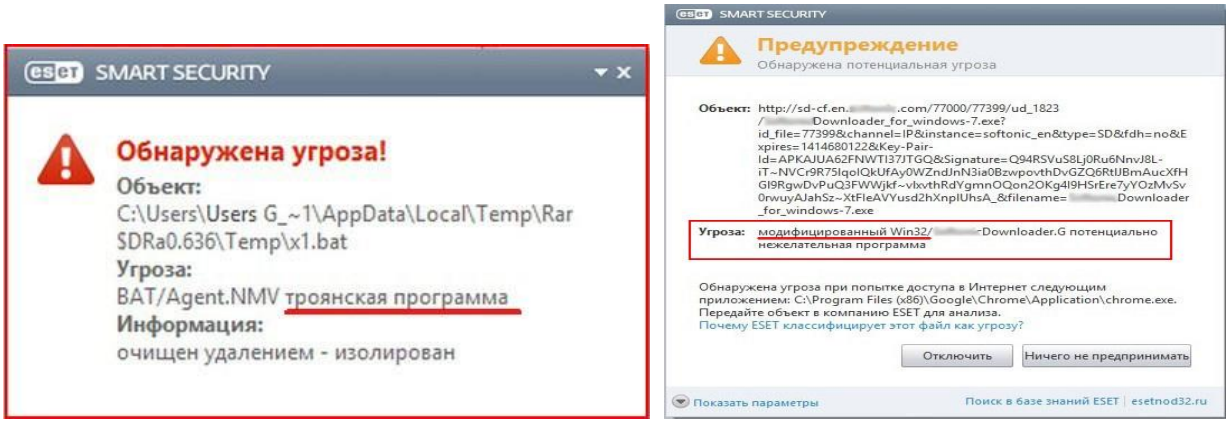
- **Черви** (рис.1) используют дыры в безопасности в сети, сканируют сеть и копируют себя на компьютер, где находят дыру в безопасности. Там он начинают размножаться, снова начав сканировать сеть на предмет новых хостов.

(рис.1)



➢ «**Троянские**» (рис. 2) вирусы представляют собой программы или игры, которые кажутся безопасными, а при запуске приложения вызывают различные повреждения. Троянам не нужно распространяться, другие попадут в ловушку, считая себя безопасными приложениями.

(рис.2)

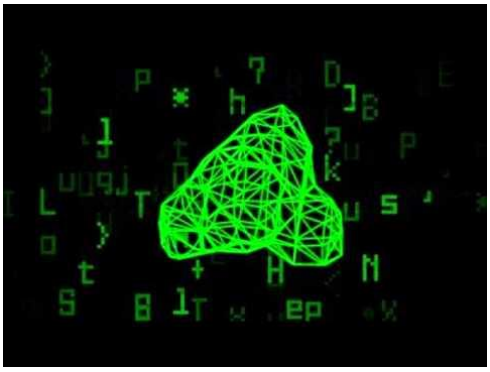


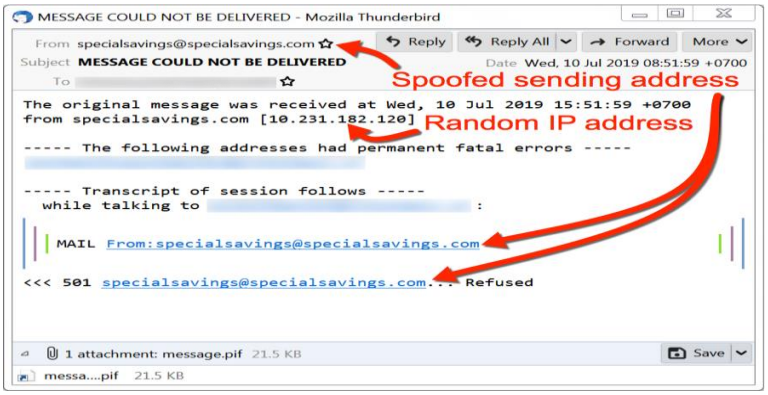
➢ **Рекламное ПО** (рис.3)(программное обеспечение, поддерживаемое рекламой), вирусы могут отображать или загружать различные рекламные объявления и предупреждения во время работы. Некоторые вирусы рекламного ПО также могут быть шпионскими программами и могут отправлять различную информацию с зараженного компьютера.

(рис.3)

➢ **Вирус Mydoom** (рис. 4) всего за месяц заразил около 250 миллионов компьютеров. В марте 1999 года вирус Melissa вынудил Microsoft и другие компании закрыть системы электронной почты до тех пор, пока вирус не будет удален. Программист, написавший вирус, получил 20 месяцев тюрьмы. Аналогичный эффект имел вирус IloveYou в 2000 году. В 2007 году вирус под названием Storm заразил более 50 миллионов компьютеров по всему миру. Это довольно впечатляющая вещь, учитывая, что большинство вирусов невероятно просты.

(рис.4)





➢ **Бутовый вирус** – (рис.5)это специализированная разновидность резидентного файлового вируса, который заражает загрузочный сектор гибкого ил жесткого диска.

Распространяются бутовые вирусы путем заражения бут-сектора дискет, причем как системных, так и несистемных.

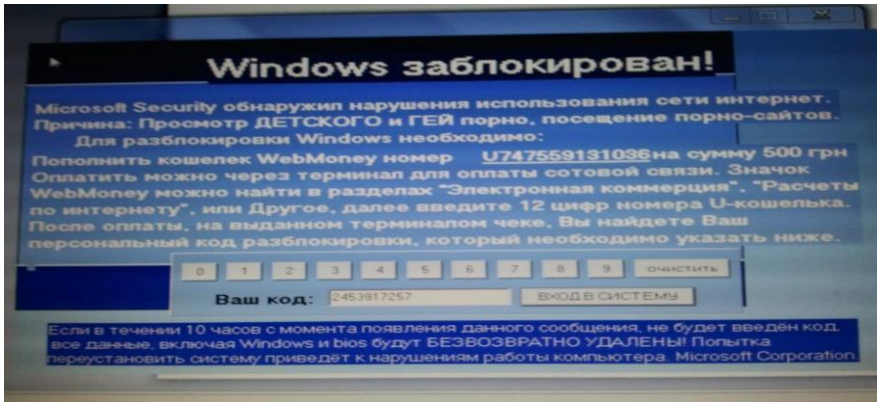
Отличительная особенность – голова вируса располагается в загрузочном секторе, а хвост – в неиспользуемых областях диска.

При загрузке с зараженного диска бутовый вирус получает управление и сначала копирует себя в старшие адреса памяти. Затем он уменьшает размер доступной памяти, чтобы защитить резидентную часть вируса, и адрес прерывания, чтобы перехватить обращения к диску,после этого вирус запускает стандартный системный загрузчик.

При чтении любого носителя вирус проверяет его на зараженность и инфицирует загрузочный сектор. Теперь при загрузке с этого носителя произойдет заражение компьютера.

Перечисленные вирусы являются самыми распространёнными вирусами в наше время , но существуют много других различных вирусов.

(рис.5)



2. КОМПЮТЕРНАЯ БЕЗОПАСНОСТЬ

2.1. Защита компьютера

Состояние «безопасности» компьютера - это концептуальный идеал, достигаемый при использовании трех процессов: предотвращение угрозы, обнаружение и ответ. Эти процессы основаны на различных политиках и системных компонентах, которые включают следующее:

- Элементы управления доступом к учетной записи пользователя и криптография могут защищать системные файлы и данные, соответственно.
- Сегодня брандмауэры являются наиболее распространенными системами профилактики с точки зрения сетевой безопасности, поскольку они могут (если правильно настроить) защищать доступ к внутренним сетевым службам и блокировать определенные виды атак посредством фильтрации пакетов. Брандмауэры могут быть как аппаратными, так и программными.
- Системы обнаружения вторжений (IDS) предназначены для обнаружения сетевых атак в процессе разработки и оказания помощи в криминалистике после атаки, в то время как контрольные журналы выполняют аналогичную функцию для отдельных систем. «Ответ» обязательно определяется оцененными требованиями безопасности отдельной системы и может охватывать диапазон от простого обновления защиты до уведомления юридических органов. В некоторых особых случаях лучше всего уничтожить скомпрометированную систему, так как может случиться, что не все уязвимые ресурсы будут обнаружены.

2.2. Соблюдение кибербезопасности

Кибербезопасность в организациях:

У организаций и предприятий существует ряд прописанных правил для сотрудников для использования техники с выходом в сеть. У каждой компании есть свои правила, основными из которых являются:

- запрет на открытие электронной почты с неизвестных и подозрительных адресов
- запрет на открытие и запуск неизвестных файлов
- запрет на скачивание и установку нового софта (в этих целях ставят админ-пароль на все компьютеры)
- запрет на использование съемных цифровых носителей (флешки, диски)
- закрытый доступ к внутренним файлам, использования исключительно корпоративной почты для передачи доступа к ним

- использование сложных паролей с регулярным их изменением
- ограниченный доступ пользователей к подпроектам. Каждый пользователь имеет доступ исключительно к проектам которые нужны ему для работы.
- использование лицензионного софта

Защита личных мобильных устройств:

В настоящее время широкое распространение получило мошенничество с мобильными устройствами. Ниже приведены рекомендации, которые позволят снизить вероятность стать жертвой мошенников:

- никому не сообщайте свои пароли, злоумышленники с лёгкостью могут воспользоваться данной информацией в мошеннических целях
- используйте только официальные приложения, установленные из App Store, Google Play и Microsoft Store
- используйте антивирус для защиты устройств от вредоносного программного обеспечения
- используйте двухфакторную аутентификацию во всех приложениях где это возможно, особенно в приложениях в социальных сетей.
- не переходите по подозрительным ссылкам: мошенники могут заразить ваше устройство вирусом и украсть ваши данные и, возможно, денежные средства с банковских счетов
- заведите вторую Сим-карту для подключения к банковским сервисам и используйте её на телефоне, где нет доступа в интернет и возможности устанавливать стороннее ПО, что позволит сократить риск отправки СМС сообщений в банк без вашего ведома

2.3. Информационная безопасность

Организационная защита объектов информатизации

Организационная защита — это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающей или существенно затрудняющей неправомерное овладение конфиденциальной информацией и проявление внутренних и внешних угроз.

Организационная защита обеспечивает:

- организацию охраны, режима, работу с кадрами, с документами;
- использование технических средств безопасности и информационно-аналитическую деятельность по выявлению внутренних и внешних угроз предпринимательской деятельности

К основным организационным мероприятиям можно отнести:

- организацию режима и охраны. Их цель — исключение возможности тайного проникновения на территорию и в помещения посторонних лиц;
- организацию работы с сотрудниками, которая предусматривает подбор и расстановку персонала, включая ознакомление с сотрудниками, их изучение, обучение правилам работы с конфиденциальной информацией, ознакомление с мерами ответственности за нарушение правил защиты информации и др.;
- организацию работы с документами и документированной информацией, включая организацию разработки и использования документов и носителей конфиденциальной информации, их учёт, исполнение, возврат, хранение и уничтожение;
- организацию использования технических средств сбора, обработки, накопления и хранения конфиденциальной информации;
- организацию работы по анализу внутренних и внешних угроз конфиденциальной информации и выработке мер по обеспечению её защиты;
- организацию работы по проведению систематического контроля за работой персонала с конфиденциальной информацией, порядком учёта, хранения и уничтожения документов и технических носителей.

В каждом конкретном случае организационные мероприятия носят специфическую для данной организации форму и содержание, направленные на обеспечение безопасности информации в конкретных условиях.

Информационная безопасность предприятия

Информационная безопасность предприятия — это состояние защищённости корпоративных данных, при которой обеспечивается их конфиденциальность, целостность, аутентичность и доступность.

Задачи систем информационной безопасности предприятия различны:

- обеспечение защищённого хранения информации на носителях;
- защита данных, передаваемых по каналам связи;
- создание резервных копий, послеаварийное восстановление и т. д.

Обеспечение информационной безопасности предприятия возможно только при системном и комплексном подходе к защите. Полноценная ИБП подразумевает непрерывный контроль всех важных событий и состояний, влияющих на безопасность данных и осуществляется круглогодично.

Информационная безопасность предприятия достигается целым комплексом организационных и технических мер, направленных на защиту корпоративных данных. Организационные меры включают документированные процедуры и правила работы с разными видами информации, IT-сервисами, средствами защиты и т. д. Технические меры заключаются в использовании

аппаратных и программных средств контроля доступа, мониторинга утечек, антивирусной защиты, межсетевого экранирования, защиты от электромагнитных излучений и прочее.

Обеспечение информационной безопасности — это непрерывный процесс, включающий в себя, пять ключевых этапов:

1. оценка стоимости;
2. разработка политики безопасности;
3. реализация политики;
4. квалифицированная подготовка специалистов;
5. аудит.

С оценки имущества начинается процесс обеспечения информационной безопасности, определения информационных активов организации, факторов, угрожающих этой информации, и её уязвимости, значимости общего риска для организации. В зависимости от имущества и будет составляться программа защиты этих активов. После того, как риск будет выявлен и будет составлена его количественная оценка, можно будет выбрать рентабельную контрмеру для уменьшения этого риска.

Цели оценки информационной безопасности:

- определить ценность информационных активов;
- определить угрозы для конфиденциальности, целостности, доступности и/или идентифицируемости этих активов;
- определить существующие уязвимые места в практической деятельности организации;
- установить риски организации в отношении информационных активов;
- предложить изменения в существующей практике работы, которые позволят сократить величину рисков до допустимого уровня;
- обеспечить базу для создания проекта обеспечения безопасности.

Пять основных видов оценки:

- Оценка уязвимых мест на системном уровне. Компьютерные системы исследованы на известные уязвимости и простейшие политики соответствия техническим требованиям.
- Оценка на сетевом уровне. Произведена оценка существующей компьютерной сети и информационной инфраструктуры, выявлены зоны риска.
- Общая оценка риска в рамках организации. Произведен анализ всей организации с целью выявления угроз для её информационных активов.
- Аудит. Исследована существующая политика и соответствие организации этой политике.
- Испытание на возможность проникновения. Исследована способность организации реагировать на смоделированное проникновение.

При проведении оценки должны быть исследованы такие документы, как:

- политика безопасности;
- информационная политика;
- политика и процедуры резервного копирования;
- справочное руководство работника или инструкции;
- процедуры найма-увольнения работников;
- методология разработки программного обеспечения;
- методология смены программного обеспечения;
- телекоммуникационные политики;
- диаграммы сети.

Получив вышеуказанные политики и процедуры, каждая из них исследуется на предмет значимости, правомерности, завершенности и актуальности, так как политики и процедуры должны соответствовать цели, определённой в документе.

После оценки необходимо заняться разработкой политик и процедур, которые определяют предполагаемое состояние безопасности и перечень необходимых работ. Нет политики — нет плана, на основании которого организация разработает и выполнит эффективную программу ИБП.

Необходимо разработать следующие политики и процедуры:

- Информационная политика. Выявляет секретную информацию и способы её обработки, хранения, передачи и уничтожения.
- Политика безопасности. Определяет технические средства управления для различных компьютерных систем.
- Политика использования. Обеспечивает политику компании по использованию компьютерных систем.
- Политика резервного копирования. Определяет требования к резервным копиям компьютерных систем.
- Процедуры управления учётными записями. Определяют действия, выполняемые при добавлении или удалении пользователей.
- План на случай чрезвычайных обстоятельств. Обеспечивает действия по восстановлению оборудования компании после стихийных бедствий или инцидентов, произошедших по вине человека.

Реализация политики безопасности заключается в реализации технических средств и средств непосредственного контроля, а также в подборе штата безопасности. Могут потребоваться изменения в конфигурации систем, находящихся вне компетенции отдела безопасности, поэтому в проведении программы безопасности должны участвовать системные и сетевые администраторы.

При применении любых новых систем безопасности нужно располагать квалифицированным персоналом. Организация не может обеспечить защиту секретной информации, не привлекая своих сотрудников. Грамотная профессиональная переподготовка — это механизм обеспечения сотрудников необходимой информацией.

3. СИСТЕМА АНТИВИРУСОВ И ИХ КЛАССИФИКАЦИЯ

3.1. Антивирусная программа

Антивирусная программа (антивирус, средство антивирусное защиты , средство обнаружения вредоносных программ]) - специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ и восстановления зараженных (модифицированных) такими программами файлов и профилактики - предотвращение заражения (модификации) файлов или операционной системы вредоносным кодом.

3.2. История антивирусных программ

Первые антивирусы появились в конце 1980-х годов, однозначно установить время их появления затруднительно. Пионер были AntiVir и Dr. Solomon's Anti-Virus Toolkit, созданные в 1988 году, а также Symantec antivirus for Macintosh, Запущенные годом позже.

3.3. Методы зашиты от вирусов

Для защиты от вирусов употребляют три группы методов :

1. Методы, основанные на анализе содержимого файлов (как файлов данных, так и файлов с кодами команд). К этой группе относятся сканирование сигнатур вирусов, а также проверка целостности и сканирование подозрительных команд.
2. Методы, основанные на отслеживание поведения программ при их выполнении. Эти методы заключаются в протоколированием всех событий, угрожающих безопасности системы и происходящих либо при реальном выполнении проверяемого кода, либо при его программной эмуляции.
3. Методы регламентации порядка работы с файлами и программами. Эти методы относятся к административным мерам обеспечения безопасности.

1. Метод сканирования сигнатур

Основан на поиске в файлах уникальнойпоследовательности байтов сигнатуры, характерной для определенного вируса.

Для каждого вновь обнаруженных вируса специалистами антивирусное лаборатории выполняется анализ кода, на основании которого определяется его сигнатура. Полученный

кодовый фрагмент помещают в специальную базу данных вирусных сигнатур, с которой работает антивирусная программа.

Достоинством данного метода является низкая доля ложных срабатываний, а главным недостатком принципиальная невозможность обнаружения в системе нового вируса, для которого отсутствует сигнатура в базе данных антивирусное программы, поэтому требуется своевременная актуализация базы данных сигнатур

2. **Метод контроля целостности**

Основывается на том, что любое неожиданное и беспричинное изменение данных на диске является подозрительным событием, требующим особого внимания антивирусное системы. Вирус обязательно оставляет свидетельства своего пребывания (изменение данных существующих (особенно системных или исполняемых) файлов, появление новых исполняемых файлов и т. Д.).

Факт изменения данных - нарушение целостности - легко устанавливается путем сравнения контрольной суммы , заранее подсчитанной для исходного состояния тестируемого кода, и контрольной суммы текущего состояния тестируемого кода. и контрольной суммы (дайджеста) текущего состояния тестируемого кода. Если они НЕ совпадают, значит, целостность нарушена и имеются все основания провести для этого кода дополнительную проверку, например, путем сканирования вирусных сигнатур.

Указанный метод работает быстрее метода сканирования сигнатур, поскольку подсчет контрольных сумм требует меньше вычислений, чем операции побайтового сравнения кодовых фрагментов, кроме того он позволяет Обнаружив следы деятельности любых, в том числе неизвестных, вирусов, для которых в базе данных еще нет сигнатур.

3. **Метод сканирования подозрительных команд**

Основан на выявление в сканируемого файле некоторых числа подозрительных команд и (или) признаков подозрительных кодовых последовательностей (например, команда форматирования жесткого диска или функция внедрения в выполняющийся процесс или исполняемый код). После этого делается предположение о вредоносной сущности файла и предпринимаются дополнительные действия по его проверке.

Этот метод обладает хорошим быстродействием, но довольно часто Он не способен выявлять новые вирусы.

4. **Метод отслеживания поведения программ**

Принципиально отличается от методов сканирования содержимого файлов, упомянутых ранее. Этот метод основан на анализе поведения запущенных программ, Сравнимые с поимкой преступника «за руку» на месте преступления.

Антивирусный средства данного типа часто требуют активного участия пользователя, призвание воспринимать решения в ответ на многочисленные предупреждения системы, значительная часть которых может оказаться в последствии ложными тревогу. Частота ложных срабатываний (подозрение на вирус для безвредного файла или пропуск вредоносного файла) при превышение определенного порога делает этот метод неэффективным, а пользователь может перестать реагировать на предупреждения или выбрать оптимистическую стратегию (разрешать все действия всем запускаемым программам или отключить данную функцию антивирусного средства).

При использовании антивирусных систем, анализирующий поведение программ, всегда существует риск выполнения команд вирусного кода, способных нанести ущерб защищаемому компьютеру или сети. Для устранения подобного недостатка позднее был разработан метод эмуляции (имитации), позволяющий запускать тестируемую программу в искусственно созданной (виртуальной) среде, которую часто называют песочнице без опасности повреждения информационного окружения.

Использование методов анализа поведения программ показало их высокую эффективность при обнаружении как известных, так и неизвестных вредоносных программ .

3.4. **Специальные антивирусы**

В ноябре 2014 года международная правозащитная организация Amnesty International выпустила антивирусную программу Detect, предназначенную для выявления вредоносного ПО, распространяемом государственными учреждениями для слежка за гражданский активистами и политическими оппонентами. Антивирус, по заявлению создателей, выполняет более глубокое сканирование Жёсткий диск, нежели обычные антивирусы

3.5. **Эффективность антивирусов**

Аналитическая компания Imperva в рамках проекта Hacker Intelligence Initiative опубликовал интересное исследование , которое показывает малую эффективность большинства антивирусов в реальных условиях.

По итогам различных синтетических тестов антивирусы показывают среднюю эффективность в районе 97%, но эти тесты проводятся на базах из сотен тысяч образцов, абсолютное большинство которых (может быть, около 97%) уже не используются для проведения атак.

Вопрос в том, насколько эффективными являются антивирусы против самых актуальных угроз. Чтобы ответить на этот вопрос, компания Imperva и студенты Тель-авивского университета раздобылы на российских подпольных форумах 82 образца самого свежего

вредоносного ПО - и проверили его по базе VirusTotal, то есть против 42 антивирусных движков.

Результат оказался плачевным.

1. Эффективность антивирусов против только что скомпилированных зловредов оказалась менее 5%. Это вполне логичны результат, поскольку создатели вирусов обязательно тестируют их по базе VirusTotal.
2. Вот появления вируса в начала его распознавания антивирусами проходит в четырёх недель. Такой показатель достигается «элитнымы» антивирусами, а в остальных антивирусов срок может доходит до 9-12 месяцев. Например, в начале исследования 9 февраля 2012 года был проверен свежей образец фальшивого инсталлятор Google Chrome. После окончания исследования 17 ноября 2012 года его определяли только 23 из 42 антивирусов.
3. В антивирусов с Самым высоким процентом определения зловредов присутствует также высокий процент ложных срабатываний.
4. Хотя исследование сложно назвать объективным, ибо выборка зловредов была слишком маленькой, но можно предположить, что антивирусы совершенно непригодны против свежих киберугроз.

3.6. **Классификация антивирусных программ**

Антивирусный программы подразделяются по исполнению на:

- программные;
- программно-аппаратные.

По признаку размещения в оперативной памяти выделяют:

- **резидентные** (начинают свою работу при запуске операционной системы, постоянно находятся в памяти компьютера и осуществляют автоматическую проверку файлов);
- **нерезидентные** (запускаются по требованию пользователя или в согласовании с заданным для них расписанием).

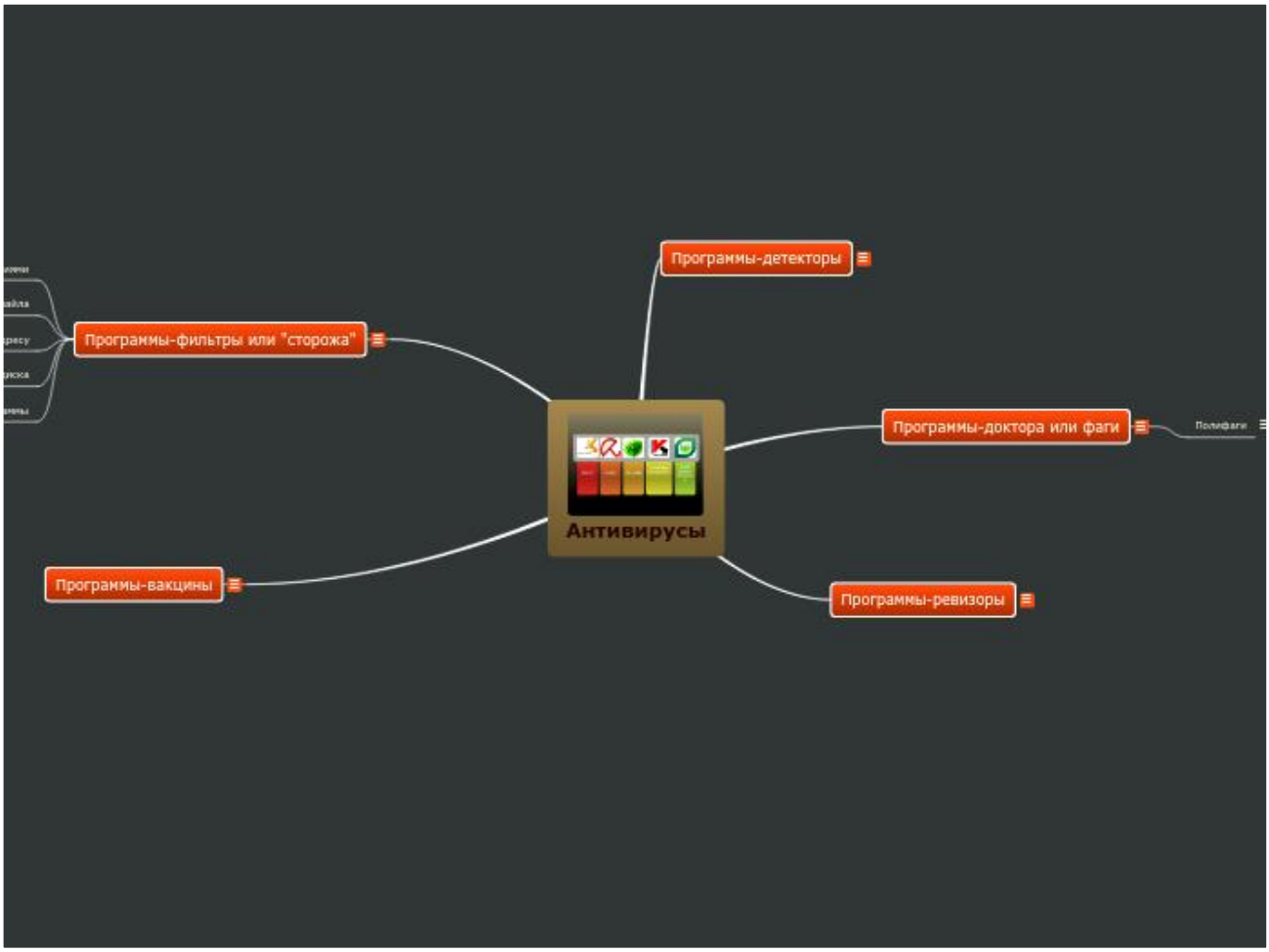
По виду защиты от вирусов различают:

- Программы-детекторы, или сканеры, находят вирусы в оперативной памяти, на внутренних и внешних носителях, выводя сообщение при обнаружении вируса.
- Программы-доктора находят зараженные файлы и «лечат» их. Среди этого вида программ существуют полифаги, которые способны удалять разнообразные виды вирусов, самые известные из антивирусов-полифагов Norton AntiVirus, Doctor Web, Kaspersky Antivirus.
- Программы-вакцины (иммунизаторы) выполняют иммунизацию системы (файлов, каталогов) блокируя действие вирусов.
- Программы-ревизоры являются наиболее надежными в плане защиты от вирусов. Ревизоры запоминают исходное состояние программ, каталогов, системных областей диска до момента инфицирования компьютера (как правило, на основе подсчета контрольных сумм), затем сравнивают текущее состояние с первоначальным, выводя найденные изменения на дисплей.
- Программы-мониторы начинают свою работу при запуске операционной системы, постоянно находятся в памяти компьютера и осуществляют автоматическую проверку файлов по принципу «здесь и сейчас».
- Программы-фильтры (сторожа) обнаруживают вирус на ранней стадии, пока он не начал размножаться. Программы-сторожа — небольшие резидентные программы, целью которых является обнаружение действий, характерных для вирусов.

3.7. **Основные виды антивирусных программ**

- **Программы-детекторы** обеспечивают поиск и обнаружение вирусов в оперативной памяти и на внешних носителях, и при обнаружении выдают соответствующее сообщение. Различают детекторы *универсальные* и *специализированные*.
- **Программы-доктора (фаги)** 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. Среди фагов выделяют полифаги, т.е. программы-доктора, предназначенные для поиска и уничтожения большого количества вирусов. Учитывая, что постоянно появляются новые вирусы, программы-детекторы и программы-доктора быстро устаревают, и требуется регулярное обновление их версий.
- **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.

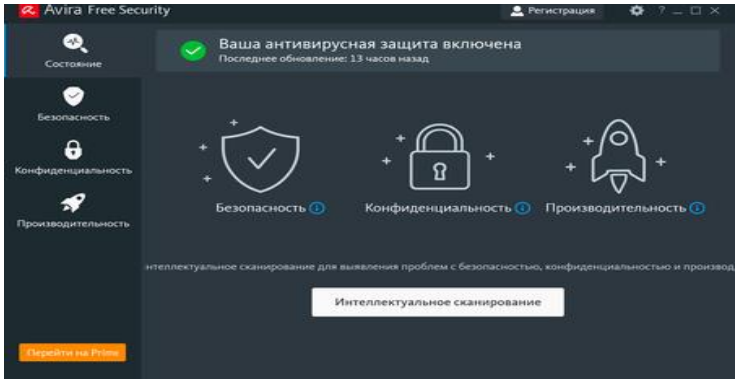
- **Программы-фильтры (сторожа)** представляют собой небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вирусов.
- **Программы-вакцины (иммунизаторы)** - это резидентные программы, предотвращающие заражение файлов. Вакцины применяют, 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, а вирус будет воспринимать их зараженными и поэтому не внедрится. Существенным недостатком таких программ является их ограниченные возможности по предотвращению заражения от большого числа разнообразных вирусов.



3.8. Топ восемь антивирусных программ

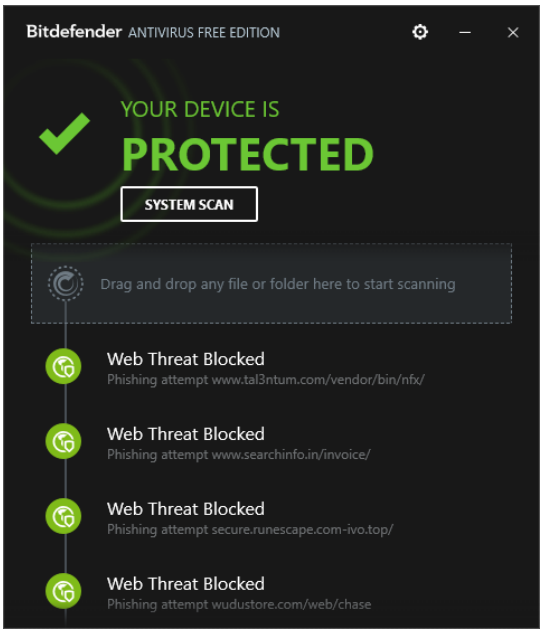
I. Avira Free Security Suite

Очень простой, поэтому и популярный антивирус, эффективно защищающий от вредоносов. Одной из особенностей является поддержка технологии облачного сканирования, что позволяет защитить ПК от самых новых угроз. Также можно расширить функционал, загрузив разные модули.



II. Bitdefender Antivirus Free Edition

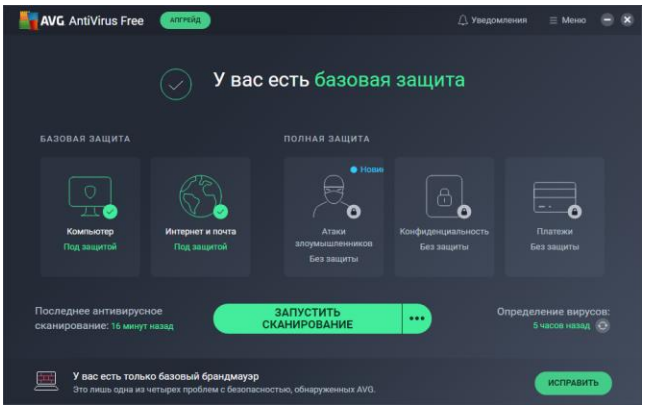
Победитель многих международных рейтингов лучших антивирусов. Эффективная защита от вирусов, быстрое распознавание и блокирование фишинговых атак, простой интерфейс.



III. AVG Antivirus Free

Более 5 миллионов пользователей по всему миру выбрали этот антивирус для защиты своего ПК. Присутствует эта программа и в нашем рейтинге антивирусов. Среди основных преимуществ AVG Antivirus Free – простой и понятный интерфейс, автоматическое сканирование программ и файлов при их первом запуске, возможность настроить сканер по расписанию.

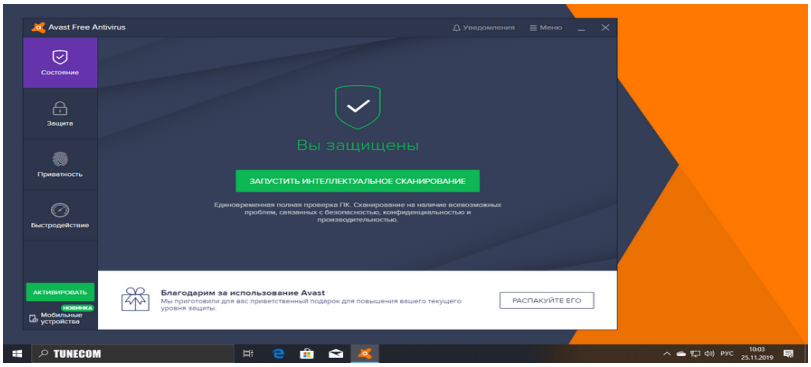
В целом, этот антивирус характеризуется отличными показателями защиты компьютера и скромным потреблением системных ресурсов.(рис.7)



(рис. 7)

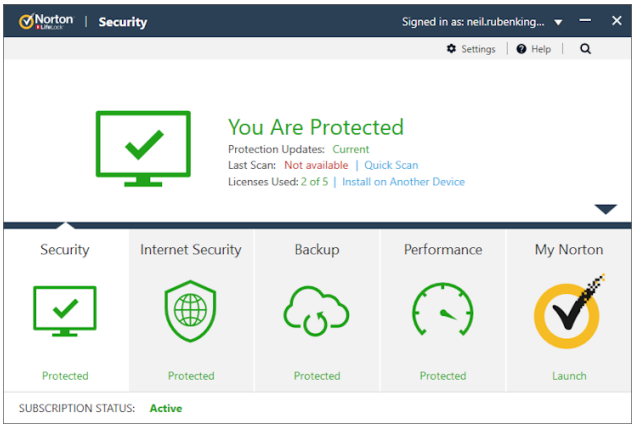
IV. Avast Free Antivirus

Бесплатный универсальный софт, который проводит диагностику вирусов, блокирует вредоносные и шпионские программы. При чем еще до того, как они заразят компьютер. Еще преимуществами этого антивируса являются удобный дизайн и менеджер паролей, а также «игровой режим». Он означает, что при запуске игр на компьютере Avast максимально освободит все системные ресурсы и предоставит их игре.



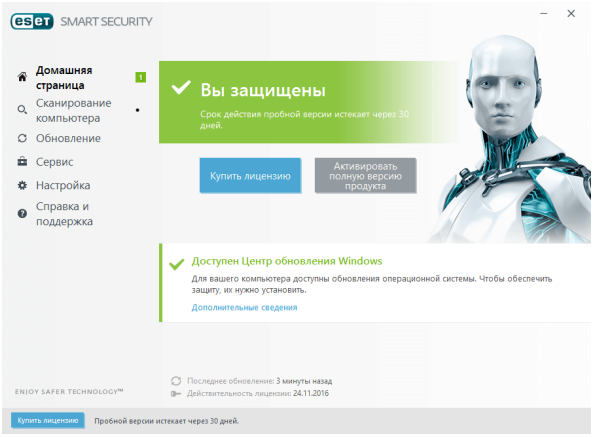
V. Norton SECURITY DELUX ($49.99)

Предотвращает заражение компьютера большинством известных вредоносных программ и захищает его от взломов. Это обеспечивается благодаря тому, что программа осуществляет мониторинг за всеми процессами на компьютере на предмет подозрительной активности в режиме реального времени. Также к основным характеристикам Norton Security Deluxe относятся:



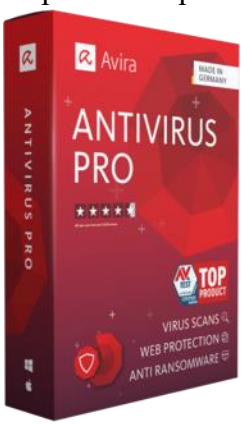
VI. ESET Smart Security ($59.99)

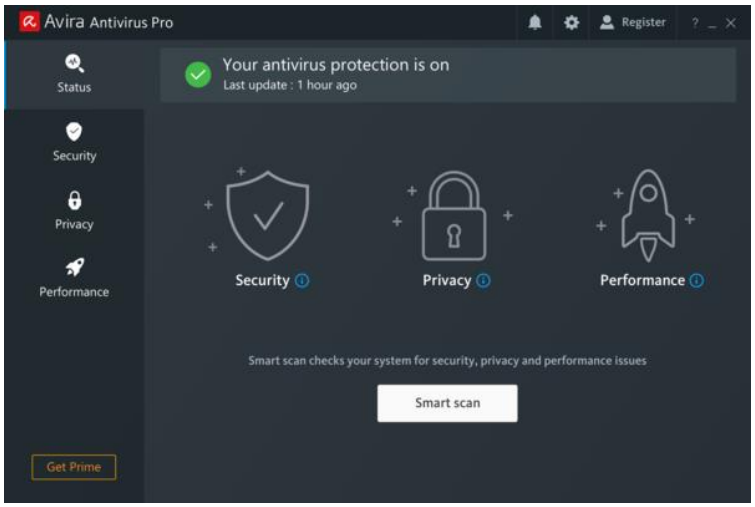
Основными особенностями этого антивируса являются: многоуровневая защита от вирусов и нежелательного ПО, контроль и сканирование подсоединенных устройств, родительский контроль, возможность найти и вернуть утерянный ноутбук и т.д. Из недостатков ESET Smart Security можно отметить значительное потребление ресурсов.



VII. Avira Antivirus Pro ($23.95)

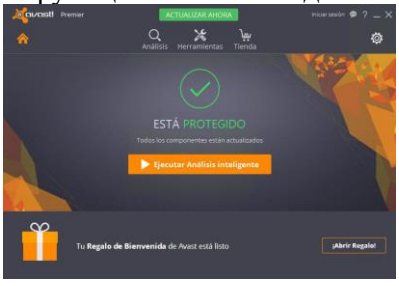
Все программы из нашего рейтинга обладают примерно одинаковыми функциями. Платная версия уже упоминающегося антивируса Avira – не исключение. Программа достаточно популярна благодаря отличным показателям в защите устройств от вредоносного ПО. Среди самых интересных характеристик антивируво.

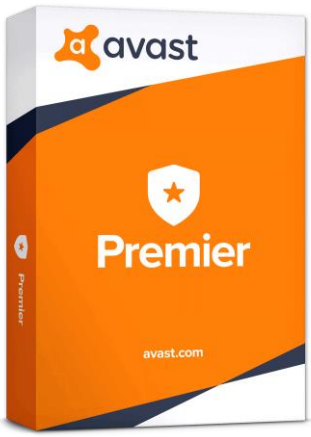




VIII. Avast Premier ($55.99)

Если Avast Free постоянно занимает лидирующие позиции в рейтинге бесплатных антивирусов, то можете представить, каким функционалом обладает платная версия продукта.





ВЫВОДЫ

Начнём с того что наш компьютер находится под угрозой с момента подключения к интернету и чтобы защитить свой компьютер мы естественно сразу же устанавливаем себе антивирус, ограждаем себя от незащищенных сайтов, и на все сто процентов полагаемся на антивирус.

Но ни одна антивирусная программа не сможет обеспечить стопроцентный уровень защиты компьютера.

Необходимо адекватно оценивать возможности вредоносных программ. Например, очень неразумно будет отформатировать жесткий диск только из за того, что на нём было обнаружено подозрение на какой-то вирус. Это приведет к неоправданной потере информации и сильной потери времени и сил, что, по нанесенному ущербу, будет больше, чем смог бы сделать сам вирус.

Не стоит пытаться защитить компьютер несколькими антивирусными программами одновременно. Это может привести к неэкономному использованию аппаратных возможностей компьютера, а следовательно, и к невозможности выполнения некоторых важных задач.

Еще раз стоит отметить, что универсальной антивирусной программы не существует. Ни одна из них не может гарантировать нам стопроцентную защиты от вирусов, и во многом выбор антивирусной программы зависит от выбора пользователя.

БИОГРАФИЯ

1.