Основы информационной безопасности критически важных объектов

Учебная дисциплина ОИБ КВО

Тема 6

Защита информации от воздействий вредоносных программ (ЗотВП)

Толстой Александр Иванович

к.т.н., доцент

Кафедра «Информационная безопасность банковских систем»

Институт интеллектуальных кибернетических систем

Факультет «Кибернетика и информационная безопасность»

НИЯУ МИФИ

Москва, 2017

Содержание

1.Введение

2.Основные понятия и виды вредоносных программ (ВП)

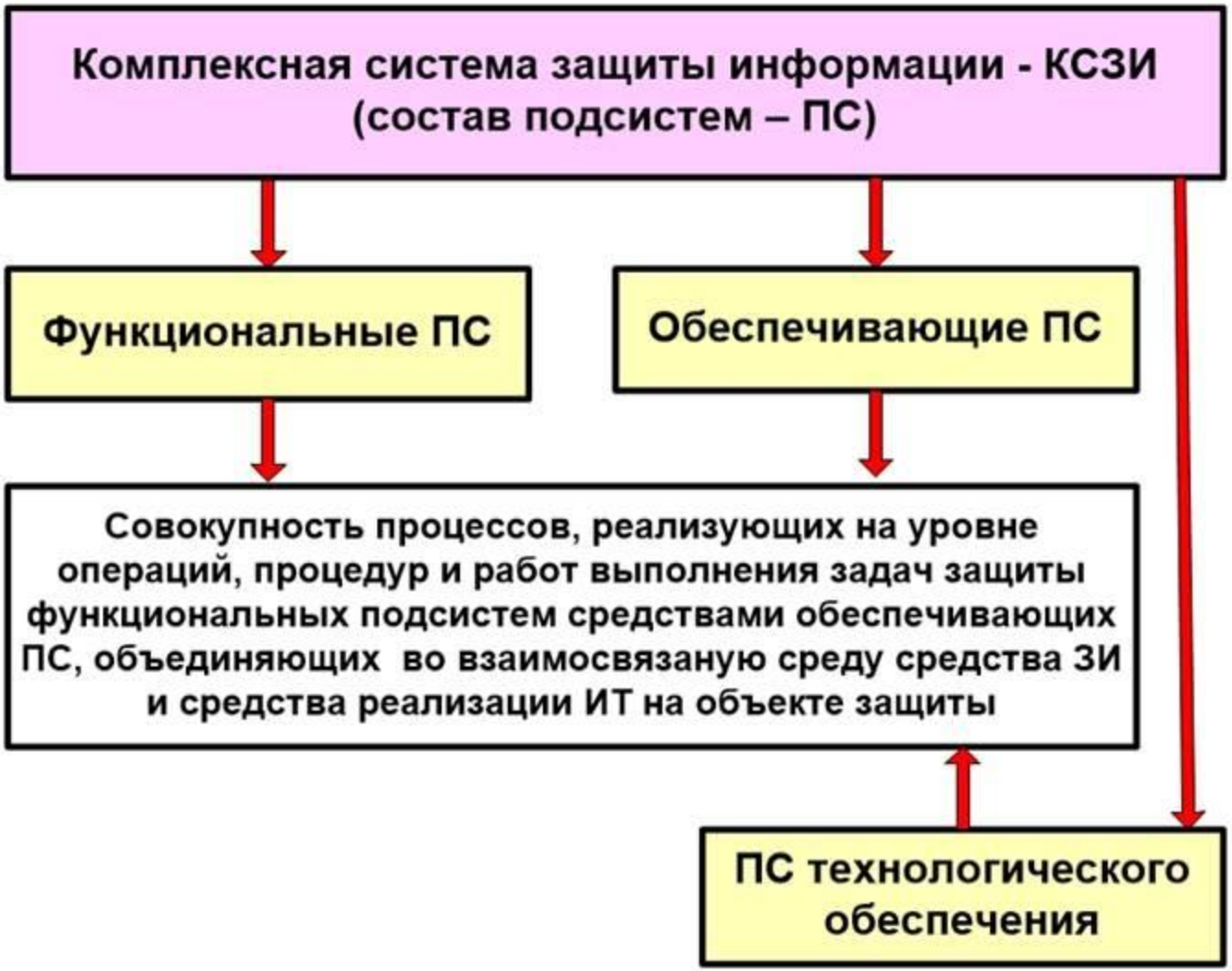
3.Способы защиты от воздействия ВП

4.Основные виды антивирусных средств

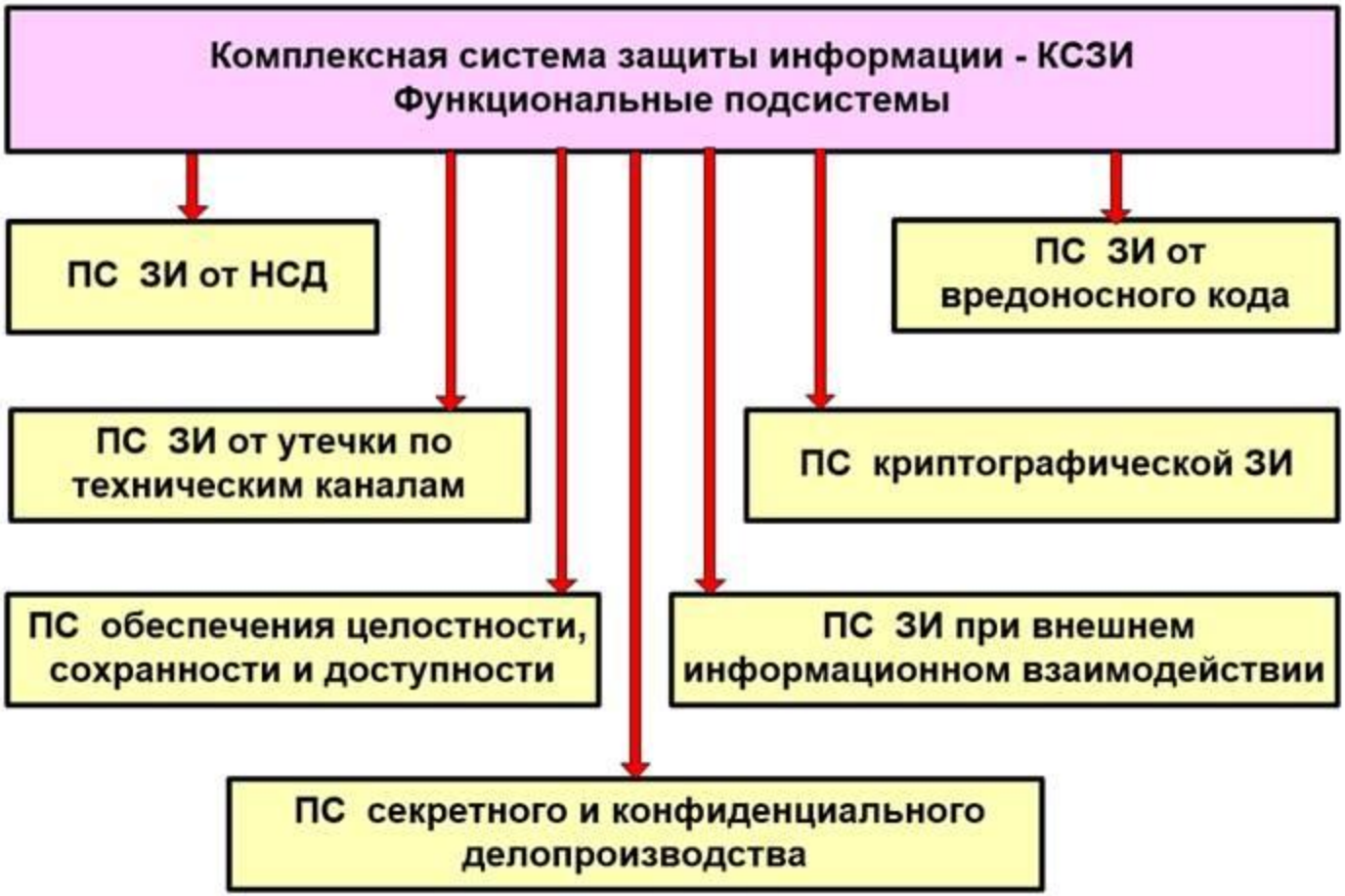
5.Общие требования по обеспечению ИБ от воздействия ВП

6.Основные навыки антивирусной защиты

***«Комплексная система защиты информации» (КСЗИ)*- совокупность различных подсистем.**



***«Комплексная система защиты информации» (КСЗИ)*- совокупность различных подсистем.**



ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности».

10.4 Защита от вредоносной и мобильной программы

Цель: Защита целостности программного обеспечения и информации.

Необходимо принимать меры предосторожности для предотвращения и обнаружения вредоносной программы и неавторизованной мобильной программы.

Угрозы безопасности информации (данные по материалам зарубежной печати)

№	Класс угроз	Размер ущерба %
1	Несанкционированный доступ извне	2
2	Проникновение вирусов	3
3	Технические сбои и отказы аппаратуры сети	20
4	Умышленные действия служащих	20
5	Ошибки персонала и пользователей, связанные с недостаточным уровнем их квалификации	55

Уголовный кодекс РФ:

Глава 28. Преступления в сфере компьютерной информации

Ст. 273. Создание, использование и распространение вредоносных программ для ЭВМ

1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами - наказываются лишением свободы на срок до трех лет со штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев.

2. Те же деяния, повлекшие по неосторожности тяжкие последствия,- наказываются лишением свободы на срок от трех до семи лет.

Вредоносная программа –

это программный код с потенциально опасными последствиями действия; это некоторая самостоятельная программа, которая способна выполнять непустое подмножество функций:

- **скрывать признаки своего присутствия в программной среде ЭВМ;**
- **обладать способностью к самодублированию, ассоциированию себя с другими программами и/или переносу своих фрагментов в иные области оперативной или внешней памяти ;**
- **разрушать код программ в оперативной памяти;**
- **сохранять фрагменты информации из оперативной памяти в некоторых областях внешней памяти (локальных или удаленных);**
- **искажать, блокировать и / или подменять выводимую информацию.**

Вредоносные программы – история («быль»)

•В начале 1970-х годов (предположительно в 1973-м) в прототипе современного Интернета — военной компьютерной сети ARPANET — был обнаружен вирус Creeper, который перемещался по серверам под управлением операционной системы Tenex.

• Creeper был в состоянии самостоятельно войти в сеть через модем и передать свою копию удаленной системе.

•На зараженных системах вирус обнаруживал себя сообщением I'M THE CREEPER: CATCH ME IF YOU CAN, которое ВЫВОДИЛОСЬ на дисплей или на принтер.

•Для удаления вируса Creeper была написана первая антивирусная программа Keeper, которая аналогичным образом распространялась по сети, удаляла обнаруженные копии Creeper и затем (предположительно — через определенный промежуток времени) самоликвидировалась.

•В начале 1970-х годов (предположительно в 1974-м) появилась программа, получившая название «Кролик» (Rabbit). Она клонировала себя, занимала системные ресурсы и таким образом снижала производительность системы. Достигнув определенного уровня распространения на зараженной машине, «Кролик» нередко вызывал сбой в ее работе. Скорее всего, «Кролики» не передавались от системы к системе и были сугубо местным явлением — ошибками или шалостями системных программистов, обслуживавших компьютер.

Основные источники ВП:

1.Глобальные сети - электронная почта, электронные конференции ….;

2.Локальные сети;

3.Пиратское программное обеспечение;

4.Носители информации;

5.Ремонтные службы.

Признаки (прямые) заражения компьютера:

- вывод на экран непредусмотренных сообщений или изображений;
- подача непредусмотренных звуковых сигналов;
- неожиданное открытие и закрытие лотка CD-ROM-устройства;
- произвольный, без вашего участия, запуск на компьютере каких-либо программ;
- при наличии на вашем компьютере межсетевого экрана, появление предупреждений о попытке какой-либо из программ вашего компьютера выйти в интернет, хотя вы это никак не инициировали.

Виды вредоносных программ

Виды вредоносных программ

Один из способов классификации ВП – это разделение их по следующим основным признакам:

- **среда обитания;**
- **особенности алгоритма;**
- **способы заражения (резидентные и нерезидентные);**
- **степень воздействия (безвредные, опасные, очень опасные).**

Виды вредоносных программ

Один из способов классификации ВП – это разделение их по следующим основным признакам:

- **среда обитания;**
- **особенности алгоритма;**
- **способы заражения (резидентные и нерезидентные);**
- **степень воздействия (безвредные, опасные, очень опасные).**

Классификация ВП по среде обитания

1. **Программные ВП** - поражают программные файлы с расширением .COM и .EXE;
2. **Загрузочные ВП** – поражают не программные файлы, а загрузочный сектор магнитных носителей (гибких и жестких дисков);
3. **Макровирусы** – поражают документы, которые созданы в прикладных программах, имеющих средства для исполнения макрокоманд (документы текстового процессора WORD, табличного процессора Excel);
4. **Сетевые ВП -** пересылаются с компьютера на компьютер, используя для своего распространения компьютерные сети, электронную почту и другие каналы.

Виды вредоносных программ

Один из способов классификации ВП – это разделение их по следующим основным признакам:

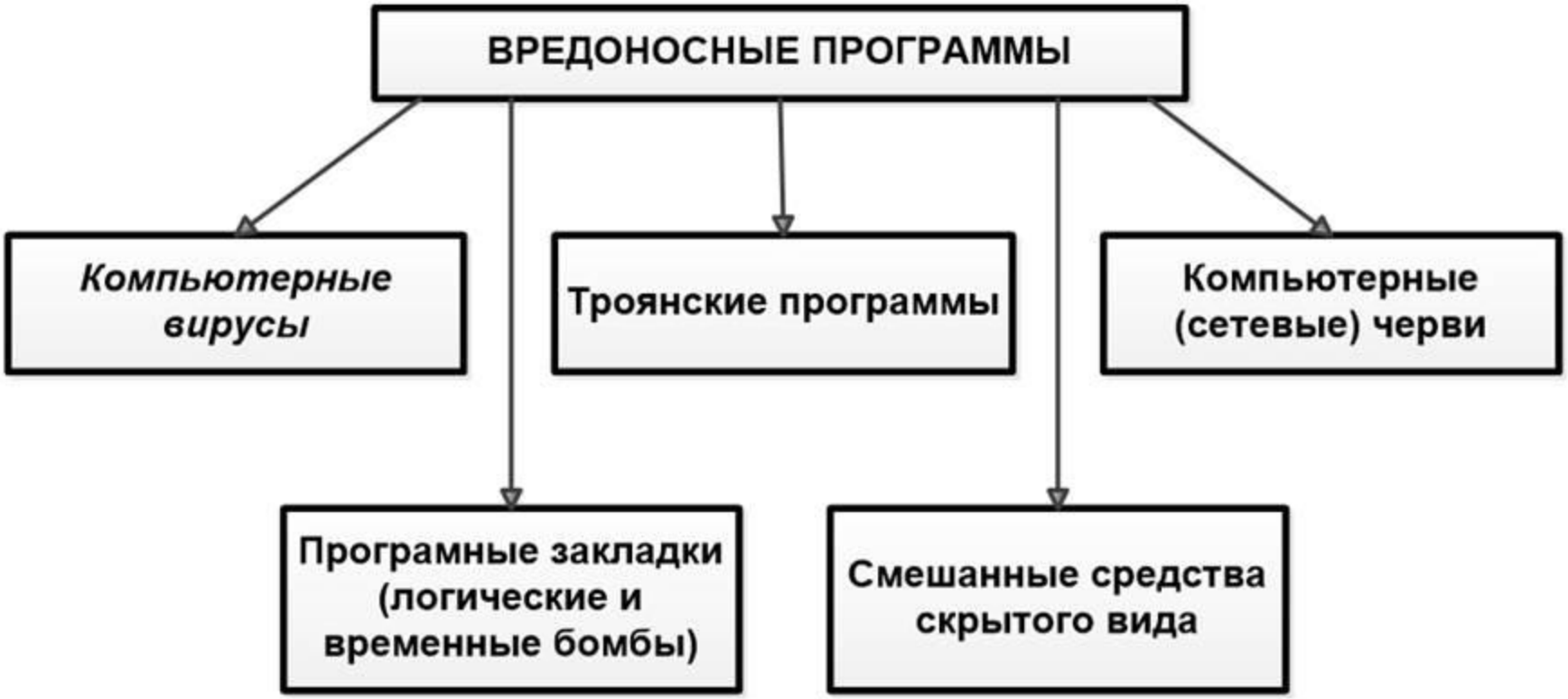
- **среда обитания;**
- **особенности алгоритма;**
- **способы заражения (резидентные и нерезидентные);**
- **степень воздействия (безвредные, опасные, очень опасные).**

Виды вредоносных программ

Один из способов классификации ВП – это разделение их по следующим основным признакам:

- **среда обитания;**
- **особенности алгоритма;**
- **способы заражения (резидентные и нерезидентные);**
- **степень воздействия (безвредные, опасные, очень опасные).**

Виды вредоносных программ (особенности алгоритма)



Вредоносные программы: компьютерные вирусы

Синонимы: Вирус, Классический вирус

Это вредоносные программы, распространяющие свои копии по ресурсам локального компьютера с целью:

- последующего запуска своего кода при каких-либо действиях пользователя;
- дальнейшего внедрения в другие ресурсы компьютера.

Пути заражения:

- из доступных дисков вирус проник в файлы, расположенные на сетевом ресурсе;
- вирус скопировал себя на съёмный носитель или заразил файлы на нем;
- пользователь отослал электронное письмо с зараженным вирусом вложением.

Некоторые компьютерные вирусы содержат в себе свойства других разновидностей ВП

Вредоносные программы:
компьютерные черви
Синоним: Червь

Черви являются в некотором роде вирусами, так как созданы на основе саморазмножающихся программ.

Черви не могут заражать существующие файлы.

Червь поселяется в компьютер отдельным файлом и ищет уязвимости в сети или системе для дальнейшего распространения себя.

Черви подразделяются по способу заражения: электронная почта, мессенджеры, обмен файлами и пр.

Некоторые черви существуют в виде сохраненных на жестком диске файлов, а некоторые поселяются лишь в оперативной памяти компьютера.

Вредоносные программы:

Троянские программы

Синоним: Троянец, Троян

Исторические корни названия

Это программы, осуществляющие различные несанкционированные действия: сбор информации и ее передачу злоумышленнику, ее разрушение или злонамеренную модификацию, нарушение работоспособности компьютера, использование ресурсов компьютера в неблаговидных целях.

Отдельные категории троянских программ наносят ущерб удаленным компьютерам и сетям, не нарушая работоспособность зараженного компьютера (например, троянские программы, разработанные для распределенных DoS-атак на удаленные ресурсы сети).

Троян: по своему действию является противоположностью вирусам и червям.

Его предлагают загрузить под видом законного приложения, однако вместо заявленной функциональности он делает то, что нужно злоумышленникам.

Трояны не самовоспроизводятся и не распространяются сами по себе.

С увеличением вала информации и файлов в Интернете трояна стало довольно легко подцепить!

Троян: по своему действию является противоположностью вирусам и червям.

Нынешние трояны эволюционировали до таких сложных форм, как, например, «хакерские программы»:

Бэкдор или RAT (remote administration tool, средство удаленного администрирования) - это приложение, которое позволяет хакеру управлять вашим компьютером на расстоянии (брать на себя контроль за компьютером и информацией жертвы):

установить и запустить на компьютере жертвы любое программное обеспечение;

сохранять все нажатия клавиш;

загружать и сохранять любые файлы;

включать микрофон или камеру.

Трояны – хакерские программы.

Руткит – специально разработанная ВП, тесно интегрированная с ОС, предназначена для скрытия присутствия (в том числе и от СЗИ) и действия вредоносного кода.

Буткит – это Руткит, который начинает свою работу прежде, чем загрузится ОС.

Троян-загрузчик - небольшая часть кода, используемая для дальнейшей загрузки и установки полной версии ВП. После того как загрузчик попадает в систему путем сохранения вложения электронного письма или, например, при просмотре зараженной картинки, он соединяется с удаленным сервером и загружает всю ВП.

Вредоносные программы:
Программные закладки
Синонимы: Логические бомбы, Временные бомбы

Программные закладки – преднамеренно внесенные в ПО функциональные объекты, которые при определенных условиях (входных данных) инициируют выполнение не описанных в документации функций ПО, приводящих к нарушению конфиденциальности, доступности или целостности обрабатываемой информации.

Закладка активизируется при выполнении условий:

Она должна находиться в оперативной памяти до начала работы программы, которая является целью воздействия закладки, т.е.:

Она должна быть загружена до или одновременно с программой.

Закладка должна активизироваться по некоторому общему как для закладки, так и для программы событию, по наступлении которого управление получит закладка (например – время).

Возможна программно-аппаратная закладка

Примеры ВП:

Почтовые (черви) – распространяются путем рассылки своих копий по электронной почте, при этом они могут указывать чужой обратный адрес. Адреса для рассылки почтовый червь получает путем сканирования содержимого ряда файлов зараженного компьютера, например, файлов адресных книг Windows, html-файлы и др.

Сетевые (черви)– для распространения активно используют протоколы и возможности локальных и глобальных сетей. Основным принципом работы сетевого червя является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию. "Полноценные" сетевые черви при этом обладают еще и возможностью запустить на выполнение свой код на удаленном компьютере или.

Примеры ВП:

Parasitic – вирусы, которые при распространении своих копий обязательно изменяют содержимое заражаемых файлов, оставляя сами файлы при этом полностью или частично работоспособными. Основными типами таких вирусов являются вирусы, записывающиеся в начало файлов, в конец файлов и в середину файлов.

Overwrite – вирусы записывают свой код вместо кода заражаемого файла, уничтожая его содержимое. Естественно, что при этом пораженный файл восстановить невозможно. Такие вирусы очень быстро обнаруживают себя, так как операционная система и приложения довольно быстро перестают работать.

Companion – алгоритм работы вирусов данной группы состоит в том, что для заражаемого файла создается файл-двойник, являющийся вирусом. Содержимое заражаемых файлов остается неизменным, однако, при их запуске управление получает файл-двойник, т.е. вирус.

Примеры ВП:

Link – вирусы, которые, как и companion-вирусы, не изменяют физического содержимого файлов, однако при запуске зараженного файла "заставляют" ОС выполнить свой код. Этой цели они достигают модификацией необходимых полей файловой системы.

Destruct – троянские программы данной группы портят информацию на компьютере: форматируют диски, переписывают существующие файлы, удаляют файлы в каталогах или на диске, "съедают" свободное место в компьютере, забивая его мусором;

Backdoor – открывают несанкционированный доступ к пораженному компьютеру и предоставляют контроль над его работой.

Примеры ВП:

Spy – отсылают с компьютера конфиденциальную информацию (имя пользователя, параметры удаленного доступа, пароли, данные, набираемый на клавиатуре и т.п.). Основной целью в данном случае является сбор информации (в первую очередь, паролей доступа), с последующей пересылкой злоумышленнику.

BadJoke – программы данной группы не причиняют компьютеру прямого вреда, однако сопровождаются графическими или звуковыми эффектами, которые пользователь не может прекратить. Например, программы могут "пугать" пользователя сообщениями о форматировании диска (хотя никакого форматирования на самом деле не происходит), находить вирусы в незараженных файлах, выводить странные вирусоподобные сообщения, изображения, от которых невозможно избавиться и т.д. – в зависимости от чувства юмора автора такой программы.

Примеры ВП:

DDoS – программы, реализующие атаки удаленных компьютеров, используя для этого зараженный компьютер-посредник, с целью вызвать на атакуемом компьютере отказ в обслуживании. Злоумышленник при этом остается незамеченным, так как в качестве атакующей машины выступает компьютер "жертвы-посредника".

DoS (Denial of Service – отказ в обслуживании) – программы данной группы атакуют серверы, инициируя множественные подключения к серверу, которые он не в состоянии обслужить, что приводит к его отказу (DoS-атаки). В отличие от DDoS атака осуществляется напрямую с компьютера злоумышленника без привлечения посредников.

Nuker – программы этой группы реализуют DoS-атаки (см. DoS) на удаленные компьютеры, используя ошибки в легальном сетевом программном обеспечении, установленном на атакуемом компьютере.

Примеры ВП:

HackTool – программы, предназначенные для нанесения вреда удаленным компьютерам. Программы данного класса сами по себе не являются ни вирусами, ни троянцами и не причиняют никакого вреда локальным компьютерам, на которых они установлены. Владелец компьютера знает, что у него установлен HackTool и, более того, целенаправленно его устанавливает и использует.

Virtool – специальные программы для создания, модификации и изучения вирусов. Программы данной группы, по сути, являются конструкторами вирусов/троянцев и позволяют генерировать исходные и хорошо откомментированные тексты вирусов/троянцев, объектные модули и непосредственно зараженные файлы.

Примеры ВП:

Flooder – программы инициируют массированную рассылку сообщений (SMS, ICQ, E-maile и пр.) с целью нанесения морального вреда какому-то пользователю, вывода из строя удаленного компьютера или канала связи, по которому осуществляется рассылка.

Exploit – программы, с помощью которых злоумышленник, используя ошибки в программном обеспечении, получает управление над удаленным компьютером-жертвой, или запускает программный код на этом компьютере. В отличие от Nuker программы данной группы не пытаются нарушить работоспособность атакуемого компьютера.

Joke – программы –шутки, которые проявляются только какими-либо графическими или звуковыми эффектами и не несут ни морального вреда пользователю, ни ущерба зараженному компьютеру.

Примеры ВП:

Вирус CIH (1998 г.) - способен перепрограммировать BIOS.

Троянская программа, способная заражать BIOS (2010 г.).

Ботнет Hlux – проведение DDoS-атак, массовая загрузка на компьютеры жертв различных вредоносных программ. На момент закрытия (2011 г.) объединял более 40 000 компьютеров и был способен рассылать ежедневно десятки миллионов спам-писем.

2011 г. - 680 новых модификаций ВП для различных мобильных платформ. Среди них 559 – ВП для ОС Android.

ZitMo и SpitMo - мобильные троянцы, нацеленные на перехват банковских SMS-сообщений.

Примеры ВП:

Червь Win32/Stuxnet - распространяется через бреши в компьютерных системах, которые раньше не были известны. Он умеет хорошо скрываться, выявить его чрезвычайно сложно.

В конце сентября 2010 г. стало известно, что вирус Stuxnet нанес серьезный урон иранской ядерной программе. Используя уязвимости операционной системы и пресловутый «человеческий фактор».
Stuxnet успешно поразил 1368 из 5000 центрифуг на заводе по обогащению урана в Натанзе, а также сорвал сроки запуска ядерной АЭС в Бушере.
Заказчик – неизвестен.
Исполнитель – нерадивый сотрудник Siemens, вставивший инфицированный флэш-накопитель в рабочую станцию.
Ущерб, нанесенный ядерным объектам Ирана, сопоставим с ущербом от атаки ВВС.

TOP 10 ВП в интернете

1	Blocked	89,37%
2	UFO:Blocked	3,45%
3	Trojan.Script.Iframer	2,27%
4	Trojan.Script.Generic	1,79%
5	AdWare.Win32.Eorezo.heur	1,47%
6	Exploit.Script.Generic	1,02%
7	Trojan.Win32.Generic	0,90%
8	Trojan-Downloader.Script.Generic	0,74%
9	WebToolbar.Win32.MyWebSearch.gen	0,65%
10	AdWare.Win32.Shopper.ee	0,45%

TOP 10 стран, на ресурсах кот.размещены ВП

1	United States	22,14%
2	Russian Federation	15,18%
3	Germany	14,37%
4	Netherlands	7,27%
5	United Kingdom	4,92%
6	Ukraine	4,56%
7	China	2,84%
8	Virgin Islands, British	2,51%
9	France	2,28%
10	Romania	1,97%

TOP 10 вредоносных хостингов

1	ru-download.in	13.94%
2	jimmok.ru	10.54%
3	ak.imgfarm.com	10.15%
4	72.51.44.90	9.05%
5	lxtraffic.com	7.77%
6	literedirect.com	5.90%
7	adult-se.com	5.87%
8	jimmmedia.com	4.70%
9	best2banners.com	3.76%
10	h1.ripway.com	3.75%

Лаборатория Касперского 2011

Основные направления защиты от ВП:

- *предупреждение проникновения ВП в ЭВМ;*
- *обнаружение уже существующих ВП.*

Меры защиты:

- *Применение организационных мер защиты;*
- *Использование специализированных программных средств («антивирусных средств»);*
- *Использование программно-аппаратных средств (специализированных межсетевых экранов, систем предупреждения вторжения);*
- *Проведение «специсследований» (программно-аппаратные закладки)*
- *Выбор операционной системы*

Организационные меры защиты:

1. *Закрепление ЭВМ за сотрудниками или назначение ответственных за организацию работ на ЭВМ (администратора ИБ).*
2. *Ведение фондов страховых и эталонных копий программного и информационного обеспечения с целью использования их при ликвидации*
3. *Учет и тщательное изучение всех нештатных ситуаций.*
4. *Проверка всего поступающего программного обеспечения и создание с этой целью стенда на предмет выявления возможного заражения ВП.*
5. *Учет и контроль доступа к носителям информации.*
6. *Назначение администратора ИБ, выполняющего следующие виды работ:*

- *проверка программного обеспечения на наличие в нем ВП;*
- *анализ нештатных ситуаций в работе вычислительных систем, предположительно связанных с воздействием ВП;*
- *выяснение источников проникновения ВП в ЭВМ подразделения;*
- *информирование сотрудников о появлении новых типов ВП, проведение разъяснительной работы об опасностях ВП, а также мерах борьбы с ними.*

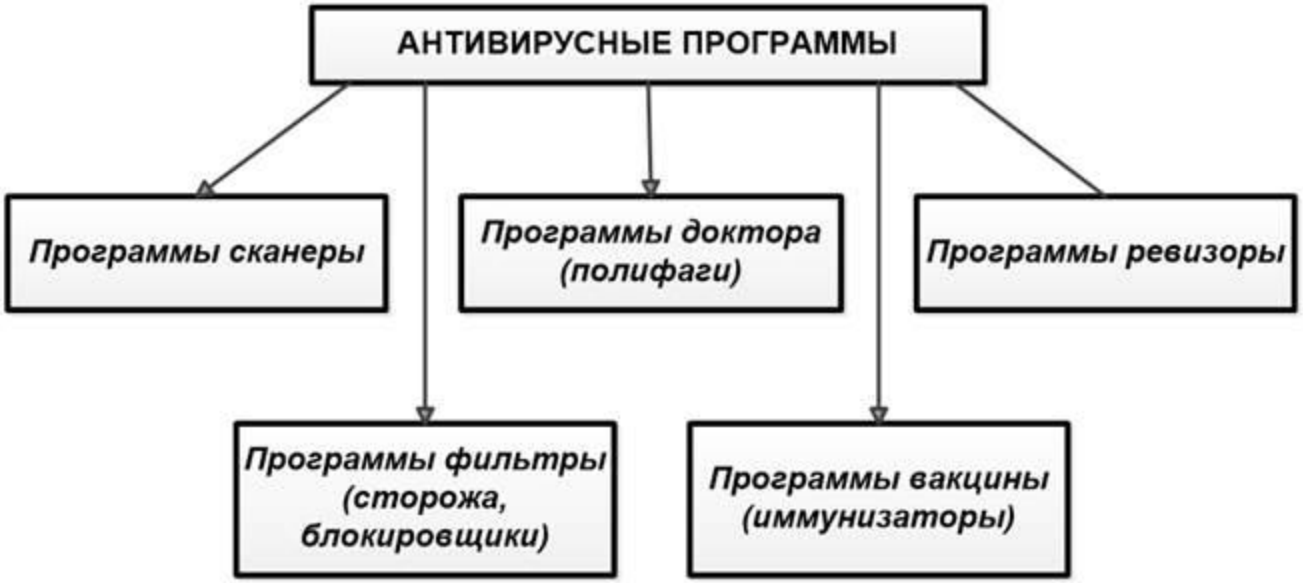
7. *Создание доверенной среды*

Организационные меры защиты:

7.Создание доверенной среды:

- В системе только разрешенное, сертифицированное ПО.
  - Отсутствуют средства разработки.
- Четко реализовано разграничение доступа.
  - Штатное ПО сосредоточено на логическом диске и защищено от записи.
- Изменяемые файлы сосредоточены в отдельном разделе диска.
  - На рабочих станциях отсутствуют съемные носители.
- Проверенное ПО не запускается вне проверенной среды.

Виды антивирусных средств (АВС):



Базовый принцип организации АВС: проактивная защита

Реализация АВС:

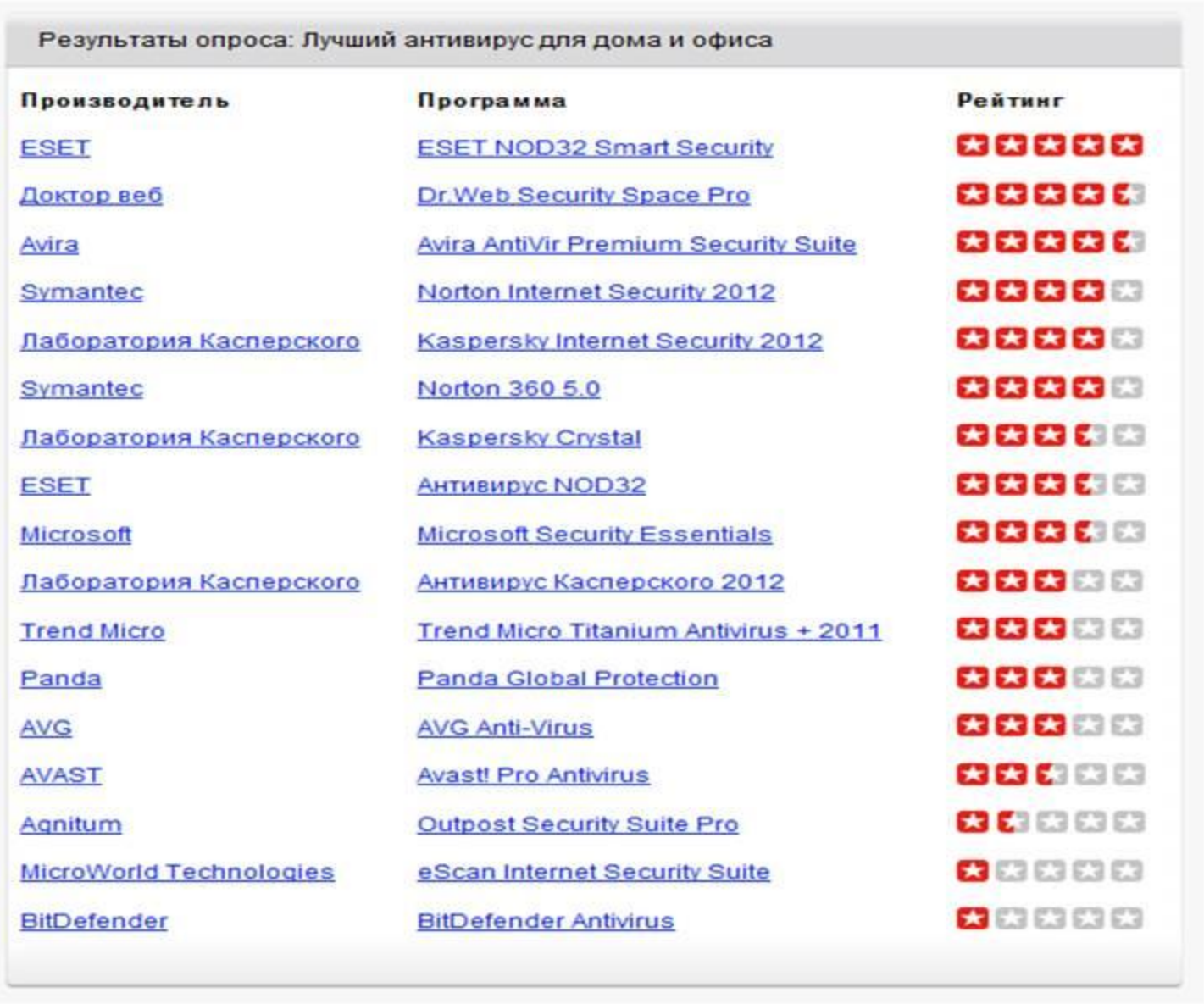
- Эвристические анализаторы.
- Системы предупреждения вторжений.
- Поведенческие блокираторы.
- Нейронные сети.

Потребительские свойства АВС:

1. Надежность и удобство работы.
2. Качество обнаружения вирусов всех распространенных типов. Отсутствие «ложных срабатываний».
3. Существование версий антивируса под все популярные платформы.
4. Скорость работы и прочие полезные особенности и функции.
5. Взаимодействие со средствами управления доступом

Специализация АВС:

1. Для домашних и офисных компьютеров.
2. Для корпоративных сетей
3. Для мобильных устройств.



Результаты опроса: Лучший антивирус для дома и офиса

Производитель	Программа	Рейтинг
ESET	ESET NOD32 Smart Security	★★★★★
Доктор веб	Dr.Web Security Space Pro	★★★★½
Avira	Avira AntiVir Premium Security Suite	★★★★½
Symantec	Norton Internet Security 2012	★★★★☆
Лаборатория Касперского	Kaspersky Internet Security 2012	★★★★☆
Symantec	Norton 360 5.0	★★★★☆
Лаборатория Касперского	Kaspersky Crystal	★★★½☆
ESET	Антивирус NOD32	★★★½☆
Microsoft	Microsoft Security Essentials	★★★½☆
Лаборатория Касперского	Антивирус Касперского 2012	★★★☆☆
Trend Micro	Trend Micro Titanium Antivirus + 2011	★★★☆☆
Panda	Panda Global Protection	★★★☆☆
AVG	AVG Anti-Virus	★★★☆☆
AVAST	Avast! Pro Antivirus	★★½☆☆
Agnitum	Outpost Security Suite Pro	★½☆☆☆
MicroWorld Technologies	eScan Internet Security Suite	★☆☆☆☆
BitDefender	BitDefender Antivirus	★☆☆☆☆

сайт Anti-Malware.ru, декабрь 2012

Корпоративный: антивирус для корпоративных сетей

Производитель	Программа	Рейтинг
Доктор веб	Dr.Web Enterprise Suite	★★★★★
Лаборатория Касперского	Kaspersky Business Space Security	★★★★★
ESET	ESET NOD32 Smart Security Business Edition	★★★★★
Avira	Avira AntiVir NetWork Bundle	★★★★½
Symantec	Symantec Endpoint Protection	★★★★½
Kerio	Kerio Control 7	★★★★
Доктор веб	Антивирус Dr.Web для Windows	★★★★
Trend Micro	Trend Micro OfficeScan	★★★½
AVAST	Avast! 4 Professional Edition	★★★½
Agnitum	Outpost Security Suite Pro	★★★
AVG	AVG Anti-Virus Business Edition	★★½
eEye Digital Security	Blink Enterprise	★★
McAfee	McAfee Active VirusScan	★½
Sophos	Sophos Endpoint Security	★
F-Secure	F-Secure Anti-Virus for Windows Servers	★

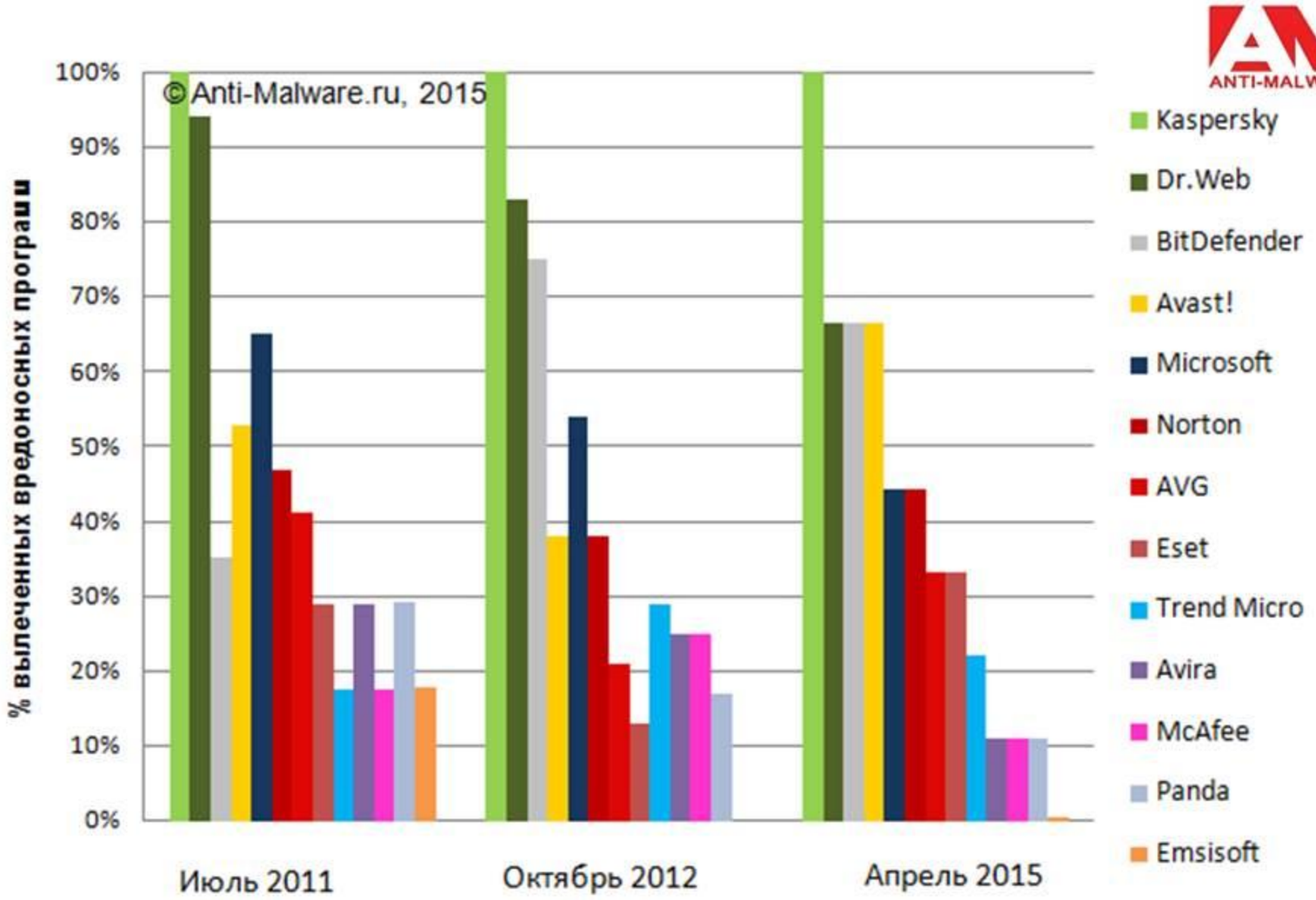
сайт Anti-Malware.ru, декабрь 2012

Мобильная версия: защита мобильных устройств

Производитель	Программа	Рейтинг
Лаборатория Касперского	Kaspersky Mobile Security	5
ESET	Антивирус ESET NOD32 Mobile	4.5
Доктор веб	Dr.Web Mobile Security Suite	4.5
Symantec	Symantec Mobile Security Suite	4
Avira	Avira AntiVir Mobile	3.5
AVAST	Avast! 4 PDA Edition	1.5
Sophos	Sophos Mobile Security	1

сайт Anti-Malware.ru, декабрь 2012

4.Основные виды антивирусных средств



Правила компьютерной гигиены

Главное:

- ***Регулярно обновляйте операционную систему.***
- ***Пользуйтесь легальными программами известных компаний.***
- ***Не открывайте письма с неизвестных адресов или со знакомых, если вы их не ждете.***
- ***Не переходите по неизвестным завлекательным ссылкам, не бродите в Интернете, если на компьютере хранятся важные документы.***
- ***Как можно реже выходите в Интернет с телефона и ни в коем случае не открывайте неизвестные сайты: телефоны являются вашими «маленькими кошельками», злоумышленники часто их атакуют.***

Помните: ***Интернет знает о нас многое – где мы находимся, чем интересуемся, кто наши друзья. Удалить эту информацию, если она попала в Сеть, в принципе невозможно, и ее могут использовать птив нас.***

Правила компьютерной гигиены

Банковские карточки:

- Не храните все деньги на карточке, выводите их на депозит.
- Имейте отдельную (не зарплатную!) карточку для платежей в Интернете.
- Нужно запомнить **CVV-код** (три цифры на обратной стороне карты) и закрасить их или стереть.
- Выбирайте банк, который правильно реагирует на инциденты с карточками и хищениями, где хорошая служба поддержки.

Помните: Согласно ст.9 закона «О национальной платежной системе», если клиент не позднее следующего дня уведомил банк о краже, ему должны вернуть деньги.

Благодарю за внимание!

Толстой Александр Иванович

AlTolstoj@mephi.ru