Лекция

«Защита от вредоносного программного обеспечения»

1. Методы и средства защиты от вредоносного ПО.
2. Организация системы антивирусной защиты.

Методы и средства защиты от вредоносного ПО

Независимо от того, какое влияние на ИС оказывает вредоносное ПО, пользователю всегда необходимо знать основные методы и средства защиты от его воздействия.

- Общие средства и методы защиты информации, которые полезны как страховка от порчи носителей этой информации, неправильно работающих программ или ошибочных действий пользователя.
- Профилактические меры, позволяющие уменьшить вредоносное влияние подобного ПО.
- Специальные методы и средства защиты от подобного ПО (в том числе специальные программы защиты и обнаружения действия вредоносного ПО).

Общие средства и методы защиты:

- копирование информации (создание копий файлов и системных областей диска);
- разграничение доступа (предотвращает несанкционированное использование информации, в частности, защиту от изменений программ и данных, неправильно работающими программами и ошибочными действиями пользователя).

Профилактические меры:

- использование современных ОС;
- своевременное установление патчей;
- работа на персональном компьютере исключительно под правами пользователя, а не администратора, что не позволит большинству вредоносных программ инсталлироваться;
- ограничение физического доступа к компьютеру посторонних лиц;
- использование внешних носителей информации только от проверенных источников;
- отключение автозапуска со сменных носителей и т.д.

Методы и средства защиты от вредоносного ПО

Специальные методы и средства защиты от вредоносного ПО

Борьба с фишингом

Некоторые правила, позволяющие противостоять атаке фишеров:

1) Никогда не отвечайте на письма, запрашивающие вашу конфиденциальную информацию.
2) В случае получения информации, вызывающей у вас недоверие к ее источнику, посетите веб-сайт предполагаемого источника полученной информации (например, банка) путем ввода его URL-адреса через адресную строку браузера.
3) Регулярно проверяйте состояние своих онлайн счетов.
4) Проверяйте уровень защиты посещаемого вами сайта.
5) Проявляйте осторожность, работая с электронными письмами и конфиденциальными данными.
6) Обеспечьте защиту своему компьютеру.
7) Всегда сообщайте об обнаруженной подозрительной активности.

Другим направлением борьбы с фишингом является создание списка фишинговых сайтов и последующая сверка с ним. Подобная система существует в современных браузерах.

Одним из простейших средств проверки состояния счета является *SMS*-банкинг.
Другой распространенный способ связан с ограничением операций (в таком случае клиенту достаточно установить сумму предельно возможного снятия наличности либо платежа в торговой точке, и банк не позволит ни ему, ни мошеннику выйти за установленные рамки).

Методы и средства защиты от вредоносного ПО

Специальные методы и средства защиты от вредоносного ПО

Защита от DoS-атак

Методы обнаружения DoS-атак:

- ✓ *сигнатурные* – основанные на качественном анализе трафика;
- ✓ *статистические* – основанные на количественном анализе трафика;
- ✓ *гибридные* – сочетающие в себе достоинства двух предыдущих методов.

Методы противодействия DoS-атакам :

- ✓ *пассивные*;
- ✓ *активные*.

Среди них:

- ❑ *Предотвращение.* Профилактика причин, побуждающих тех или иных лиц организовывать DoS-атаки. Очень часто атаки являются следствиями личной обиды, политических, религиозных разногласий, провоцирующего поведения жертвы и т.п.
- ❑ *Фильтрация.*
- ❑ *Устранение уязвимостей.*
- ❑ *Наращивание ресурсов.*
- ❑ *Рассредоточение.* Построение распределённых и продублированных систем, которые не прекратят обслуживать пользователей даже если некоторые их элементы станут недоступны из-за атаки.
- ❑ *Уклонение.* Увод непосредственной цели атаки (доменного имени или IP-адреса) подальше от других ресурсов, которые часто также подвергаются воздействию вместе с непосредственной целью.
- ❑ *Активные ответные меры.* Воздействие на источники, организатора или центр управления атакой, как технического, так и организационно-правового характера.

Методы и средства защиты от вредоносного ПО

Защита от сниффинга

Суть данной атаки – пассивное прослушивание сети.

Методы определения наличия запущенного сниффера в локальной сети:

- метод пинга,
- метод ARP,
- метод DNS,
- метод ловушки и т.д.

Метод пинга (Ping method)

Использует уловку, заключающуюся в отсылке «ICMP Echo request» (*Internet Control Massage Protocol* эхо-запроса) не на MAC-адрес (*Media Access Control*) компьютера, а на ее IP-адрес (*Internet Protocol*).

1) Допустим, хост, который мы подозреваем на использование сниффера, имеет IP-адрес 10.1.1.1 и MAC-адрес 00-40-05-A7-77-**37**.
2) Ваш компьютер должен находиться в том же сегменте локальной вычислительной сети, что и подозреваемый компьютер.
3) Вы посылаете «ICMP Echo request», указав в запросе IP-адрес подозреваемого хоста и его слегка измененный MAC-адрес, например, 00-40-05-A7-77-**38**.
4) Каждый хост, получив данный запрос, сравнивает указанный в запросе MAC-адрес со своим MAC-адресом. В случае совпадения MAC-адресов, хост отвечает источнику запроса с помощью «*ICMP Echo Reply*», иначе пакет игнорируется. В данном случае, ни один из хостов в ЛВС не должен увидеть данный пакет.
5) Если же получен ответ от какого-либо хоста, это значит что у него не используется фильтр MAC-адресов, т.е. его сетевой адаптер находится в «беспорядочном режиме». Следовательно, на данном хосте используется сниффер.

Метод пинга может быть перенесен на другие протоколы, которые генерируют ответы на запросы, например, запрос на установление TCP-соединения или запрос по протоколу UDP (*User Datagram Protocol* – протокол датаграмм пользователя) на порт 7 (эхо).

Методы и средства защиты от вредоносного ПО

Защита от сниффинга

Метод ARP

Использует похожую технику, а также особенности реализации протокола ARP (*Address Resolution Protocol* – протокол распознавания адреса) в Windows и Linux.

Действие данного метода на примере определения хоста под управлением Windows с запущенным сниффером.

1) Вы подозреваете, что на хосте (A) с IP-адресом 192.168.87.19 запущен сниффер. Если вы разошлете широковещательный ARP-запрос, которому соответствует Ethernet-адрес «FF:FF:FF:FF:FF:**FF**», с целью выяснения MAC-адреса хоста (A), все хосты должны получить ваш запрос, но ответит только тот, чей IP-адрес указан в ARP-запросе (т.е. подозреваемый). Однако было обнаружено, что если на хосте запущен сниффер, то в некоторых случаях он неправильно обрабатывает ARP-запросы.
2) Используя предложенный метод, вы посылаете точно такой же ARP-запрос, но где вместо широковещательного адреса «FF:FF:FF:FF:FF:FF» указан адрес «FF:FF:FF:FF:FF:**FE**» (ложный широковещательный адрес, из которого вычли один бит). Поскольку адрес не является широковещательным, теоретически ни один из хостов не должен ответить на такой запрос. Однако практические эксперименты показали, что Windows 2000/XP/2003 при условии, что сетевой адаптер, работает в беспорядочном режиме, посчитает такой запрос широковещательным. Соответственно хост (A), на котором запущен сниффер, сравнив IP-адрес в запросе со своим IP-адресом, пошлет ответ ARP-reply. Таким образом, хост (A) выдаст, что он прослушивает весь сетевой трафик.

Экспериментальным путем были созданы таблицы аномальных ответов на различные ARP-запросы для современных ОС – Windows и Linux, в которых запущены снифферы.

Некоторые программы, удаленно определяющих наличие снифферов:
L0pth Antisniff, Cain&Abel и PMD (*Promiscuous Mode Detector* – детектор беспорядочного режима).

Методы и средства защиты от вредоносного ПО

Массовое распространение вирусов (сегодня число известных вредоносных программ для ОС Windows исчисляется миллионами, для ОС Android – тысячами), серьезность последствий их воздействия на ресурсы компьютерных систем вызвали необходимость разработки и использования специальных антивирусных средств и методов их применения.

Методы и средства борьбы с вирусами

Антивирусные средства применяются для решения следующих задач:

- обнаружение вирусов в ИС;
- блокирование работы программ-вирусов;
- устранение последствий воздействия вирусов.

Методы и средства защиты от вредоносного ПО

Методы обнаружения вирусов

- сканирование;
- обнаружение изменений;
- эвристический анализ;
- использование резидентных сторожей;
- вакцинирование программ;
- аппаратно-программная защита от вирусов.

Сканирование осуществляется *программой-сканером* (*детектором*), которая просматривает файлы в поисках опознавательной части вируса – *сигнатуры*. Программа фиксирует наличие уже известных вирусов, за исключением полиморфных вирусов, которые применяют шифрование тела вируса, изменяя при этом каждый раз и сигнатуру. Программы-сканеры могут хранить не сигнатуры известных вирусов, а их контрольные суммы (*CRC-сканеры*).

Метод сканирования применим для обнаружения вирусов, сигнатуры которых уже выделены и являются постоянными. Для эффективного использования метода необходимо регулярное обновление сведений о новых вирусах.

К достоинствам сканеров относится их универсальность,

к недостаткам – размеры антивирусных баз и относительно небольшая скорость поиска вирусов.

Методы и средства защиты от вредоносного ПО

Метод *обнаружения изменений* базируется на использовании *программ-ревизоров* (*инспекторов*).

Эти программы определяют и запоминают характеристики всех областей на дисках, в которых могут размещаться вирусы (предполагается, что в этот момент программы и системные области дисков не заражены).

Программы-ревизоры запоминают в специальных файлах образы главной загрузочной записи, загрузочных секторов логических дисков, характеристики всех контролируемых файлов, каталогов и номера дефектных кластеров. Могут контролироваться также объем установленной ОП, количество подключенных к компьютеру дисков и их параметры.

При периодическом выполнении программ-ревизоров сравниваются хранящиеся характеристики и характеристики, получаемые при контроле областей дисков. По результатам ревизии программа выдает сведения о предположительном наличии вирусов. Это позволяет обнаружить заражение компьютерным вирусом, когда он еще не успел нанести большого вреда.

Главным достоинством метода является возможность обнаружения вирусов всех типов, а также новых неизвестных вирусов (в том числе стелс-вирусов).

Доктора-ревизоры - программы, которые не только обнаруживают изменения в файлах и системных областях дисков, но и могут в случае изменений автоматически вернуть их в исходное состояние.

Недостатки метода:

- С помощью программ-ревизоров невозможно определить вирус в файлах, которые поступают в систему уже зараженными(вирусы будут обнаружены только после размножения в системе).
- Программы-ревизоры непригодны для обнаружения заражения макровирусами, так как документы и таблицы очень часто изменяются.

Эвристический анализ

Данный метод позволяет определять неизвестные вирусы, но не требует предварительного сбора, обработки и хранения информации о файловой системе.

Сущность эвристического анализа заключается в проверке возможных сред обитания вирусов и выявление в них команд (групп команд), характерных для вирусов. Такими командами могут быть команды создания резидентных модулей в оперативной памяти, команды прямого обращения к дискам, минуя ОС.

Эвристические анализаторы при обнаружении подозрительных команд в файлах или загрузочных секторах выдают сообщение о возможном заражении. После получения таких сообщений необходимо тщательно проверить предположительно зараженные файлы и загрузочные сектора всеми имеющимися антивирусными средствами.

Впервые эвристический анализ был использован в *Norton antivirus* фирмы Symantec.

Методы и средства защиты от вредоносного ПО

Метод резидентных сторожей

Метод основан на применении программ, которые постоянно находятся в оперативной памяти и отслеживают все действия остальных программ.
Такие программы также называют *программами-фильтрами* или *мониторами*.

Мониторы представляют собой небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вирусов, и оповещения о них пользователей.

Такими действиями могут являться:

- ✓ попытки коррекции файлов с расширениями COM, EXE;
- ✓ изменение атрибутов файла;
- ✓ прямая запись на диск по абсолютному адресу;
- ✓ запись в загрузочные сектора диска;
- ✓ запись в системные области операционной системы (например, где располагаются драйверы);
- ✓ загрузка резидентной программы.

Преимущества использования программ-фильтров (мониторов, сторожей) – они позволяют обнаружить многие вирусы на самой ранней стадии, когда вирус еще не успел размножиться и что-либо испортить.

Недостатком данного метода является значительный процент ложных тревог.

Методы и средства защиты от вредоносного ПО

Под ***вакцинацией*** программ понимается создание специального модуля для контроля ее целостности. В качестве характеристики целостности файла обычно используется контрольная сумма.

Программы-вакцины или *иммунизаторы* – это резидентные программы, предотвращающие заражение файлов. Вакцины применяют, если отсутствуют программы-доктора, «лечащие» этот вирус. Вакцинация возможна только от известных вирусов. В настоящее время программы-вакцины имеют ограниченное применение.

Самым надежным *методом* защиты от вирусов является использование ***аппаратно-программных антивирусных средств*.**

В настоящее время для защиты компьютерных систем используются специальные контроллеры и их программное обеспечение. Контроллер устанавливается в разъем расширения и имеет доступ к общей шине. Это позволяет ему контролировать все обращения к дисковой системе. При выполнении запретных действий любой программой контроллер выдает соответствующее сообщение пользователю и блокирует работу компьютера.

Достоинства аппаратно-программных антивирусных средства:

- ✓ работают постоянно;
- ✓ обнаруживают все вирусы, независимо от механизма их действия;
- ✓ блокируют неразрешенные действия, являющиеся результатом работы вируса или неквалифицированного пользователя.

Недостаток этих средств – зависимость от аппаратных средств компьютера. Изменение последних ведет к необходимости замены контроллера.

Примером аппаратно-программной защиты от вирусов может служить комплекс *Sheriff*.

Методы удаления последствий заражения вирусами

Первый метод предполагает восстановление системы после воздействия известных вирусов (разработчик программы-фага, удаляющей вирус, должен знать структуру вируса и его характеристики размещения в среде обитания).

Второй метод позволяет восстанавливать файлы и загрузочные сектора, зараженные неизвестными вирусами (для восстановления файлов программа восстановления должна заблаговременно создать и хранить информацию о файлах, полученную в условиях отсутствия вирусов).

Профилактика заражения вирусами

1. Использование программных продуктов, полученных законным официальным путем.

Вероятность наличия вируса в пиратской копии во много раз выше, чем в официально полученном программном обеспечении. С другой стороны различные производители антивирусов стали сообщать о широком распространении нового типа антивирусов - *ложные антивирусы* или *лже-антивирусы* (*rogueware*).

2. Дублирование информации.

Прежде всего, необходимо сохранять дистрибутивные носители программного обеспечения. При этом запись на носители, допускающие выполнение этой операции, должна быть, по возможности, заблокирована. При этом может копироваться либо весь файл, либо только вносимые изменения. Последний вариант применим, например, при работе с базами данных.

3. Регулярно использовать антивирусные средства.

Антивирусные средства должны регулярно обновляться.

4. Особую осторожность следует проявлять при использовании новых съемных носителей информации и новых файлов.

Профилактика заражения вирусами

5. Пользователи компьютеров *не должны всё время работать с правами администратора*.
Если бы они пользовались режимом доступа обычного пользователя, то некоторые разновидности вирусов не смогли бы распространяться (или, по крайней мере, ущерб от действия вирусов был бы меньше). Это одна из причин, по которым вирусы в Unix-подобных системах относительно редкое явление.

6. При работе в распределенных системах или в системах коллективного пользования целесообразно новые сменные носители информации и вводимые в систему файлы проверять на специально выделенных для этой цели компьютерах.
Целесообразно для этого использовать автоматизированное рабочее место администратора системы или лица, отвечающего за безопасность информации. Только после всесторонней антивирусной проверки дисков и файлов они могут передаваться пользователям системы.

7. Если не предполагается осуществлять запись информации на носитель, то необходимо заблокировать выполнение этой операции.

Порядок действий пользователя при обнаружении заражения компьютера вирусами

1. Не паниковать и попытаться, используя антивирусные средства, обезвредить вирус путем "лечения" файлов, а лучше удалить зараженные файлы, если они не представляют большой ценности или, если имеются их копии.

Если имеются опасения, что активизирован резидентный вирус, то необходимо перезагрузить (*"холодная перезагрузка"* - с выключением питания и повторным включением) компьютер. Если таких опасений нет, можно работать далее, при этом лучше запустить одну из антивирусных программ (сканеров) на предмет внеочередной проверки всех логических, физических жестких дисков и памяти.

2. Если же последствия более серьезные, чем указаны в п.1, то необходимо попытаться сохранить важные файлы, не имеющие резервных копий, в том числе и на сменных носителях информации (даже если они будут заражены, потом разберетесь, чем потеряете их навсегда).

После чего необходимо выключить компьютер и осуществить перезагрузку, если не удастся загрузиться с жесткого диска, то воспользуйтесь эталонной операционной системы со сменного носителя информации, в которой отсутствуют вирусы.

3. Для удаления вирусов и восстановления файлов, областей памяти используйте антивирусные средства.

Если работоспособность компьютера восстановлена, то осуществляется переход на п.7, иначе – п.4.

Порядок действий пользователя при обнаружении заражения компьютера вирусами

4. Необходимо осуществить полное стирание и форматирование жесткого диска (в первую очередь системного).

Для этого могут быть использованы различные программы. При этом, например, необходимо помнить, что некоторые программы форматирования (например, *FORMAT*) не удаляют главную загрузочную запись на жестком диске, в которой может находиться загрузочный вирус. Поэтому, в этом случае, необходимо выполнить иные программы. (Например, используя программу *FDISK*, можно создать разделы и логические диски на жестком диске, после чего исполнить программу *FORMAT* для всех логических дисков.)

5. Восстановите ОС, другие программные системы и файлы с дистрибутивов и резервных копий, созданных до заражения.

6. Тщательно проверьте файлы, сохраненные после обнаружения заражения, и, при необходимости, удалить вирусы и восстановите файлы.

7. Завершите восстановление информации всесторонней проверкой компьютера с помощью всех имеющихся в распоряжении пользователя антивирусных средств.

Методы и средства защиты от вредоносного ПО

Антивирусы можно также разделить *по способу их воздействия на вирусы*:

- ✓ чистые антивирусы;
- ✓ антивирусы двойного назначения.

Чистый антивирус

Чистый антивирус отличается наличием антивирусного ядра, которое выполняет функцию сканирования по образцам. Принципиальная особенность в этом случае заключается в возможности лечения.

Программа двойного назначения

Программы двойного назначения – это программы, используемые и в антивирусах и в ПО, которое не является антивирусом.

Разновидностью программ двойного назначения являются *поведенческие блокираторы*, которые анализируют поведение других программ и при обнаружении подозрительных действий блокируют их.

От классического антивируса с антивирусным ядром, «узнающим» и лечащим от вирусов, поведенческие блокираторы отличаются тем, что лечить от вирусов не умеют, поскольку ничего о них не знают. Это свойство блокираторов полезно тем, что они могут работать с любыми вирусами, в том числе и с неизвестными.

Организация системы антивирусной защиты

Критерием выбора антивируса достаточно часто является не качество и надежность, а доступность пиратской копии, малый объем, низкая стоимость!!!

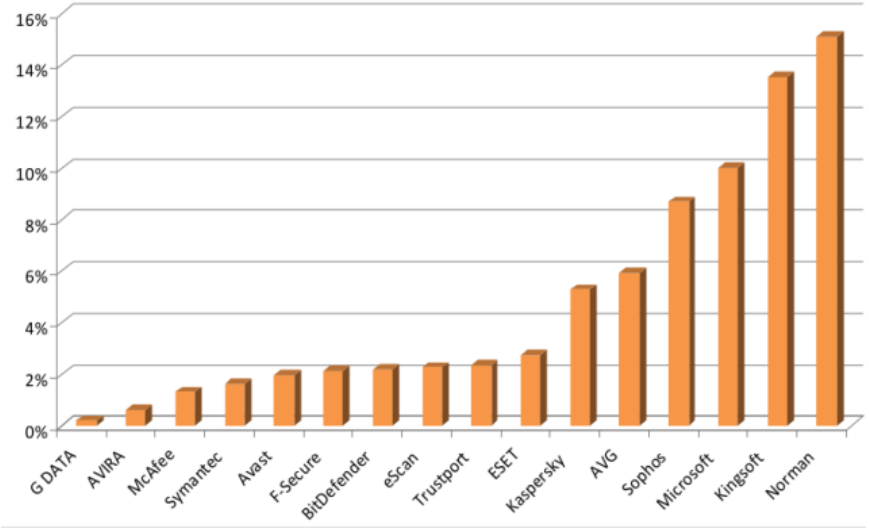
Профессиональный подход к выбору конкретного программного продукта – это оценка его эффективности.

Основные учитываемые факторы при выборе:

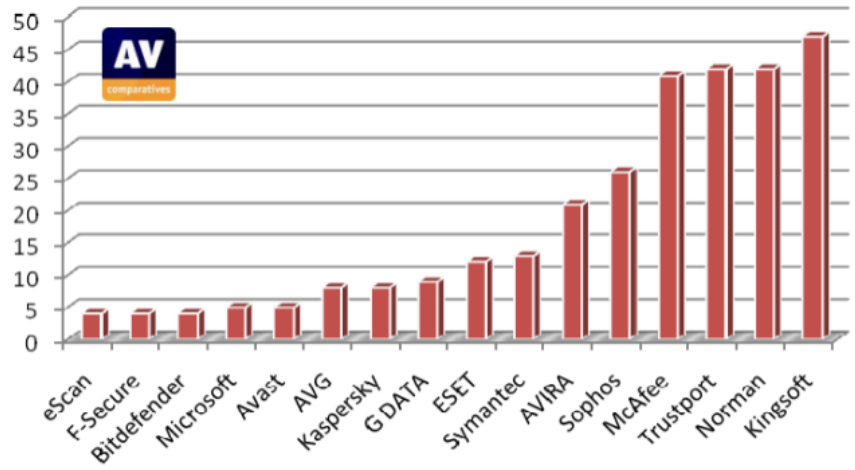
- ✓ величина списка вирусов в текущей базе;
- ✓ оперативность обновления базы поставщиком;
- ✓ способ доставки обновленных баз распознавания вирусов до потребителя;
- ✓ на каком этапе антивирус может распознать вирус и предотвратить его распространение;
- ✓ требуемые ресурсы (вычислительные, ОП) для антивируса от хоста, на котором он будет установлен;
- ✓ архитектура работы программы (отдельный программный модуль или сервер и агенты);
- ✓ Совокупную стоимость владения и некоторые другие.

Организация системы антивирусной защиты

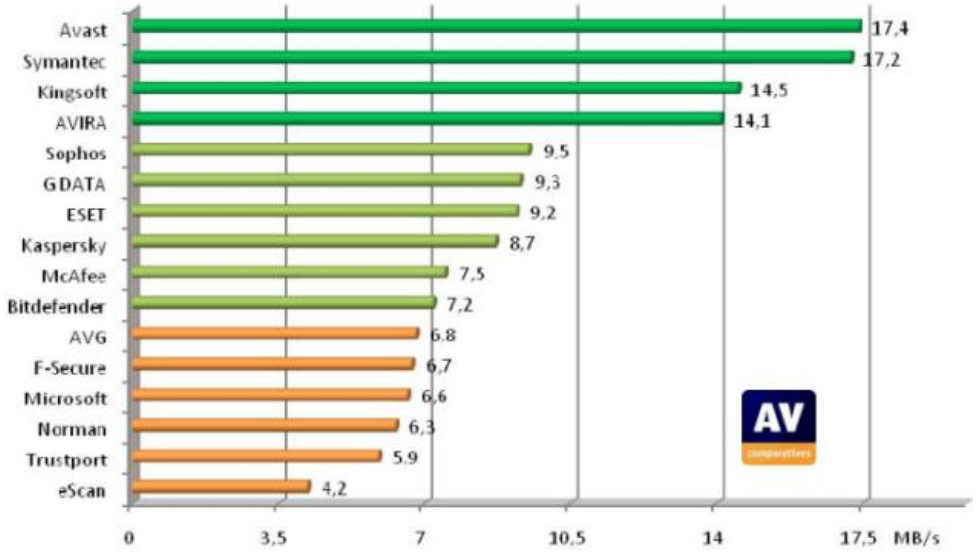
Результаты тестирования (отчет), проведенные компанией AV-Comparatives



Количество пропущенных экземпляров вредоносного ПО в процентном соотношении



Статистика ложных срабатываний средствами обеспечения безопасности ПК

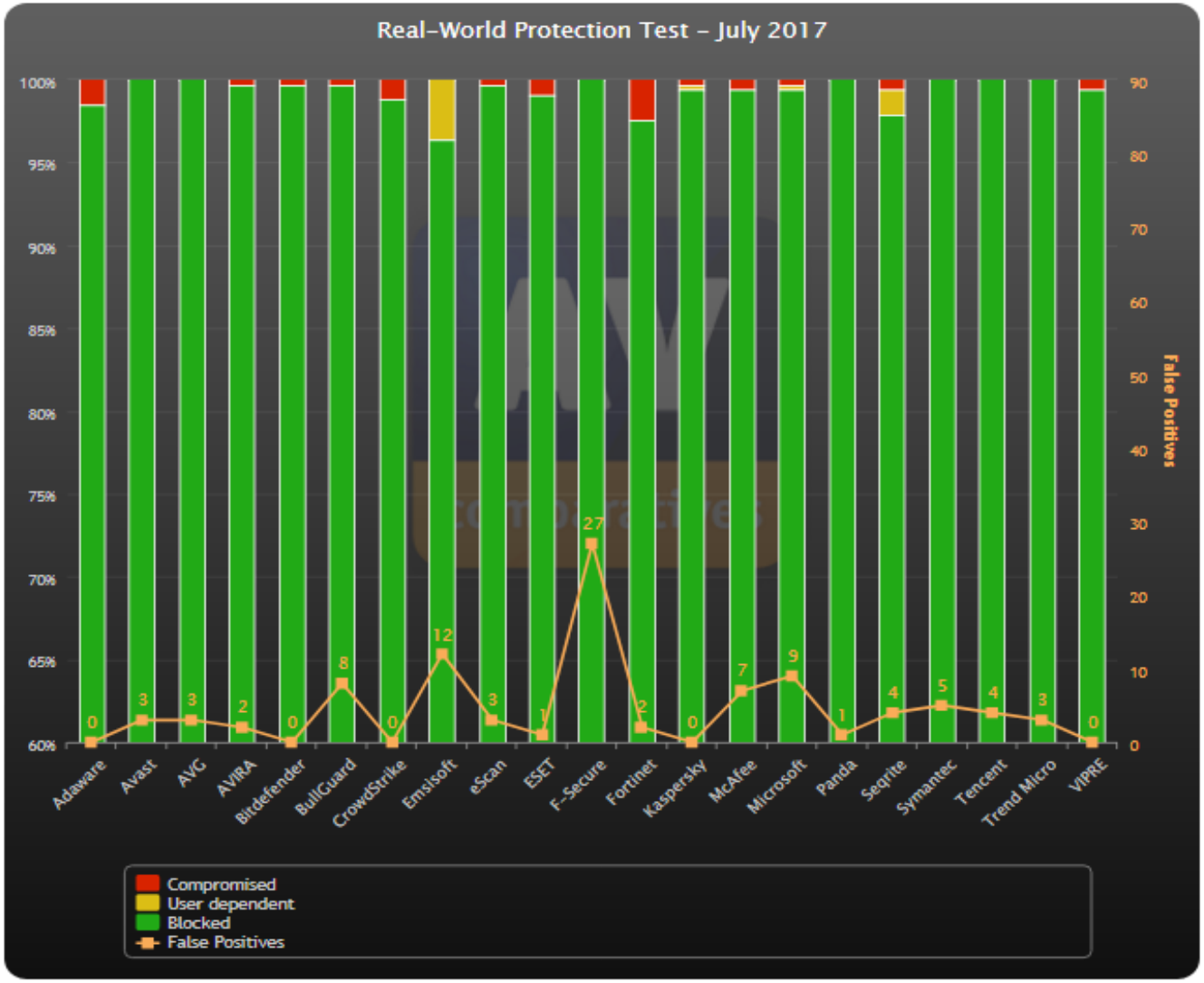


Количество пропущенных экземпляров вредоносного ПО в процентном соотношении

Организация системы антивирусной защиты

Результаты тестирования (отчет), проведенные компанией AV-Comparatives

Test: Real-World Protection Test ▼ Year: 2017 ▼ Month: Jul ▼ Sort: by vendor ▼ Zoom: 60 - 100% ▼

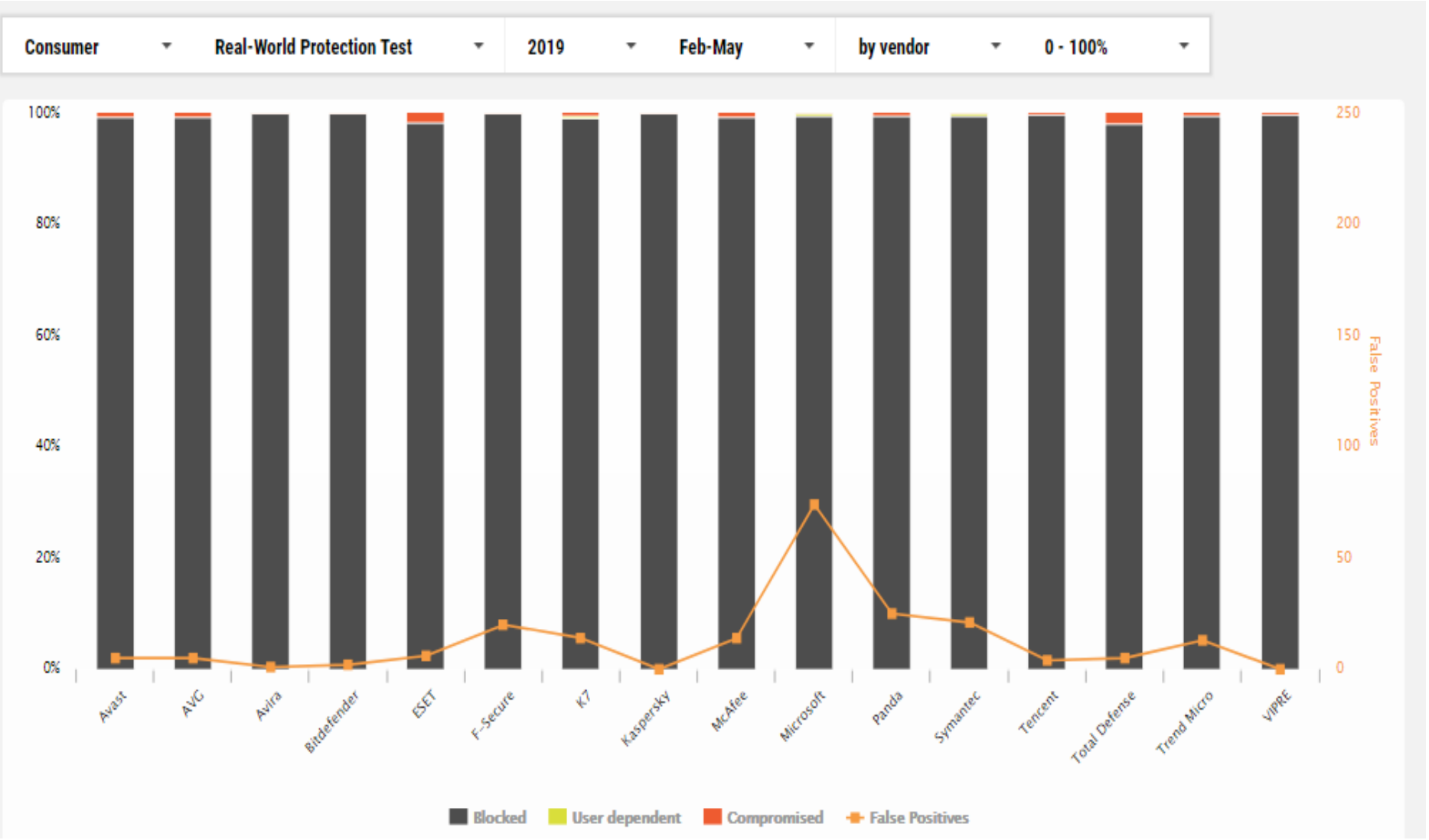


Compromised – скомпрометированы (пропущенные угрозы);
Blocked – заблокированные угрозы (в состоянии заблокировать вредоносное ПО);
User dependent – действие над угрозой зависит от решения пользователя;
False positives – ложные срабатывания.

Динамическое тестирование (Real World Protection Test) антивирусов от AV-Comparatives является наиболее полным и комплексным из доступных сравнительных тестов, в котором используется большое количество тестовых образцов

Организация системы антивирусной защиты

Результаты тестирования (отчет), проведенные компанией AV-Comparatives
(Platform OS – Microsoft Windows)



https://www.av-comparatives.org/comparison/

Организация системы антивирусной защиты

Результаты тестирования (отчет), проведенные компанией AV-Comparatives

Протестированные продукты

Vendor	Product	Version February	Version March	Version April	Version May
Avast	Free Antivirus	19.2	19.3	19.4	19.4
AVG	Free Antivirus	19.2	19.3	19.4	19.4
AVIRA	Antivirus Pro	15.0	15.0	15.0	15.0
Bitdefender	Internet Security	23.0	23.0	23.0	23.0
ESET	Internet Security	12.0	12.1	12.1	12.1
F-Secure	SAFE	17.215	17.5	17.5	17.6
K7	Total Security	15.1	15.1	15.1	15.1
Kaspersky	Internet Security	19.0	19.0	19.0	19.0
McAfee	Internet Security	22.2	22.2	22.2	22.3
Microsoft	Windows Defender	4.18	4.18	4.18	4.18
Panda	Free Antivirus	18.6	18.6	18.7	18.7
Symantec	Norton Security	22.16	22.17	22.17	22.17
Tencent	PC Manager	12.3	12.3	12.3	12.3
Total Defense	Essential Anti-Virus	11.5	11.5	11.5	11.5
Trend Micro	Internet Security	15.0	15.0	15.0	15.0
VIPRE	Advanced Security	11.0	11.0	11.0	11.0

Организация системы антивирусной защиты

Результаты тестирования (отчет), проведенные компанией AV-Comparatives

Итоговые результаты (февраль-май)

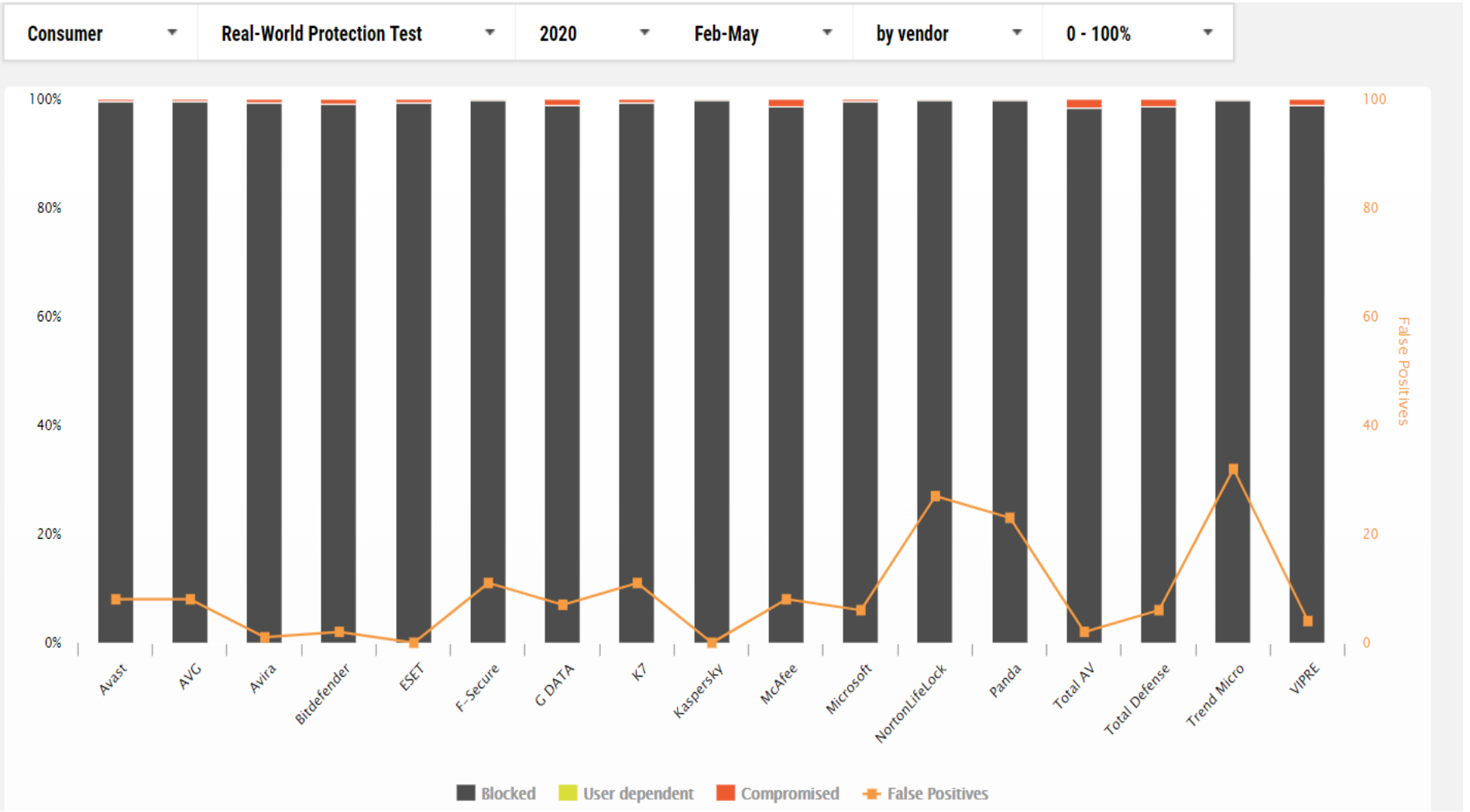
Test period: February – May 2019 (752 Test cases)

	Blocked	User dependent	Compromised	Protection Rate*	Cluster
AVIRA, F-Secure, Kaspersky	752	-	-	100%	1
Bitdefender	751	-	1	99.9%	1
Microsoft	749	3	-	99.8%	1
Tencent, VIPRE	750	-	2	99.7%	1
Symantec	749	2	1	99.7%	1
Trend Micro	749	-	3	99.6%	1
Panda	748	-	4	99.5%	1
K7	745	3	4	99.3%	2
Avast, AVG, McAfee	746	-	6	99.2%	2
ESET	740	-	12	98.4%	3
Total Defense	738	-	14	98.1%	3

Организация системы антивирусной защиты

Итоговые результаты (февраль-май)

Test period: February – May 2020 (754 Test cases)



https://www.av-comparatives.org/comparison/

Организация системы антивирусной защиты

Итоговые результаты (февраль-май)

Test period: February – May 2020 (754 Test cases)

Tested Products

- Avast Free Antivirus
  19.8 | 20.1 | 20.2 | 20.3
- AVG Free Antivirus
  19.8 | 20.1 | 20.2 | 20.3
- Avira Antivirus Pro
  15.0 | 15.0 | 15.0 | 15.0
- Bitdefender Internet Security
  24.0 | 24.0 | 24.0 | 24.0
- ESET Internet Security
  13.0 | 13.0 | 13.1 | 13.1
- F-Secure SAFE
  17.7 | 17.7 | 17.7 | 17.7
- G DATA Internet Security
  25.5 | 25.5 | 25.5 | 25.5
- K7 Total Security
  16.0 | 16.0 | 16.0 | 16.0
- Kaspersky Internet Security
  20.0 | 20.0 | 20.0 | 20.0
- McAfee Total Protection
  22.7 | 23.0 | 23.0 | 23.0
- Microsoft Windows Defender
  4.18 | 4.18 | 4.18 | 4.18
- NortonLifeLock Norton 360 Deluxe
  22.20 | 22.20 | 22.20 | 22.20
- Panda Free Antivirus
  20.0 | 20.0 | 20.0 | 20.0
- Total AV Antivirus Pro
  5.4 | 5.5 | 5.5 | 5.6
- Total Defense Essential Antivirus
  12.0 | 12.0 | 12.0 | 12.0
- Trend Micro Internet Security
  16.0 | 16.0 | 16.0 | 16.0
- VIPRE Advanced Security
  11.0 | 11.0 | 11.0 | 11.0

Итоговые результаты (февраль-май)

Test period: February – May 2020 (754 Test cases)

	Blocked	User dependent	Compromised	Protection Rate*	Cluster
F-Secure, NortonLifeLock, Trend Micro	754	–	–	100%	1
Kaspersky, Panda	753	–	1	99.9%	1
Avast, AVG, Microsoft	752	–	2	99.7%	1
Avira	751	–	3	99.6%	1
ESET	750	–	4	99.5%	1
K7	749	1	4	99.4%	1
Bitdefender	749	–	5	99.3%	1
G Data, Vipre	747	–	7	99.1%	2
McAfee, Total Defense	746	–	8	98.9%	2
Total AV	743	–	11	98.5%	3

Организация системы антивирусной защиты

Уровни наград, достигнутые в этом тесте (Real World Protection Test)

Test period: February – May 2020 (754 Test cases)

ADVANCED+	ADVANCED	STANDARD	TESTED
Kaspersky	F-Secure*	Total AV	-
Microsoft	NortonLifeLock*		
Avast	Trend Micro*		
AVG	Panda*		
Avira	K7*		
ESET	G Data		
Bitdefender	Vipre		
	Total Defense		
	McAfee		

* эти продукты получили более низкие награды из-за ложных срабатываний

Организация системы антивирусной защиты

Но даже, когда антивирусное программное обеспечения выбрано, угроза вирусных атак по-прежнему присутствует.

Почему?

Причины:

- установлено разрозненное антивирусное ПО, нет единой системы центрального управления и сбора информации о вирусных атаках;
- отсутствует техническая поддержка поставленного ПО, библиотека сигнатур (образов вирусов) устарела и антивирусное ПО не выявляет новые вирусы;
- отсутствует программы действий в экстремальных ситуациях, ликвидация последствий вирусной атаки происходит медленно и некачественно, утерянные данные не восстанавливаются;
- отсутствует связь с производителем антивирусного ПО при возникновении новых вирусов.

Организация системы антивирусной защиты

Какой должна быть антивирусная защита, и что должно лежать в ее основе?

В основе защиты от вирусов должны лежать знание и понимание правил безопасности, надлежащие средства управления доступом к системам. А именно:

- организация должна проводить политику, требующую установки только лицензированного программного обеспечения;
- противовирусные программные средства должны регулярно обновляться и использоваться для профилактических проверок (желательно ежедневных);
- необходимо проводить регулярную проверку целостности критически важных программ и данных. Наличие лишних файлов и следов несанкционированного внесения изменений должно быть зарегистрировано в журнале и расследовано;
- дискеты, диски, флэш-носители неизвестного происхождения следует проверять на наличие вирусов до их использования;
- необходимо строго придерживаться установленных процедур по уведомлению о случаях поражения ИС компьютерными вирусами и принятию мер по ликвидации последствий от их проникновения;
- следует иметь планы обеспечения бесперебойной работы организации для случаев вирусного заражения, в том числе планы резервного копирования всех необходимых данных и программ и их восстановления. Эти меры особенно важны для сетевых файловых серверов, поддерживающих большое количество рабочих станций.

Организация системы антивирусной защиты

Какой должна быть антивирусная защита, и что должно лежать в ее основе?

В общем случае, антивирусная защита корпоративной информационной системы должна *строиться по иерархическому принципу*:

I. службы общекорпоративного уровня - 1-й уровень иерархии;
II. службы подразделений или филиалов - 2-й уровень иерархии;
III. службы конечных пользователей - 3-й уровень иерархии.

Службы всех уровней объединяются в единую вычислительную сеть (образуют единую инфраструктуру), посредством локальной вычислительной сети.

Службы общекорпоративного уровня должны функционировать в непрерывном режиме.

Управление всех уровней должно осуществляться специальным персоналом, для чего должны быть предусмотрены средства централизованного администрирования.

Организация системы антивирусной защиты

Антивирусная система должна предоставлять следующие виды сервисов:

на общекорпоративном уровне:

- ✓получение и обновления программного обеспечения и антивирусных баз;
- ✓управление распространением антивирусного программного обеспечения;
- ✓управление обновлением антивирусных баз;
- ✓контроль за работой системы в целом (получение предупреждений об обнаружении вируса, регулярное получение комплексных отчетов о работе системы в целом);

на уровне подразделений:

- ✓обновление антивирусных баз конечных пользователей;
- ✓обновление антивирусного программного обеспечения конечных пользователей;
- ✓управление локальными группами пользователей;

на уровне конечных пользователей:

- ✓автоматическая антивирусная защита данных пользователя.

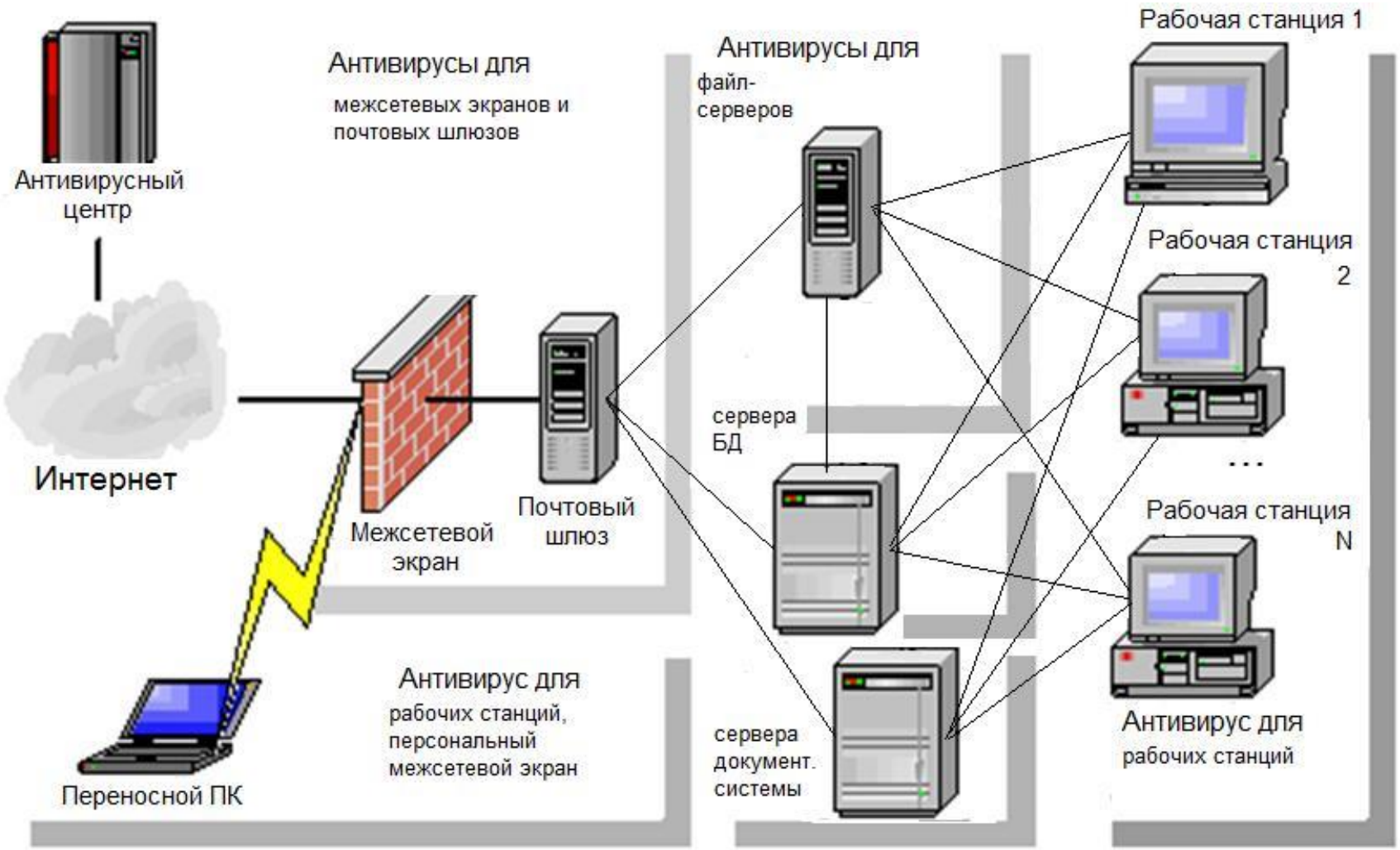
Организация системы антивирусной защиты

Программно-технические компоненты системы антивирусной защиты должны обеспечивать:

- ***надежность***:
  - система антивирусной защиты не должна нарушать логику работы остальных используемых приложений;
  - система должна обеспечивать возможность вернуться к использованию предыдущей версии антивирусных баз;
  - система должна функционировать в режиме функционирования объекта (рабочая станция/сервер) на котором она установлена;
  - система должна обеспечивать оповещение администратора системы при сбоях или обнаружении вирусов и отразить все сбои и факты обнаружения вирусов в специальных журналах (файлах);
- ***масштабируемость***:
  - система антивирусной защиты должна формироваться с учетом роста числа защищенных объектов;
- ***открытость****:*
  - система должна формироваться с учетом возможности пополнения и обновления ее функций и состава, без нарушения функционирования вычислительной среды в целом;
- ***совместимость****:*
  - поддержка антивирусным программным обеспечением максимально возможного количества сетевых ресурсов. В структуре и функциональных особенностях компонент должны быть представлены средства взаимодействия с другими системами;
- ***унифицированность*** (однородность):
  - компоненты должны представлять собой стандартные, промышленные системы и средства, имеющие широкую сферу применения и проверенные многократным использованием.

Организация системы антивирусной защиты

Возможный вариант структуры построения антивирусной защиты



Организация системы антивирусной защиты

Средства сетевого экранирования в первую очередь призваны обеспечить защиту мобильных пользователей при работе через Интернет, а также защиту рабочих станций ЛВС компании от внутренних нарушителей политики безопасности.

Сетевые экраны для рабочих станций:

- ✓ контролируют подключения в обе стороны;
- ✓ позволяют известным приложениям получить доступ в Интернет без вмешательства пользователя;
- ✓ делают компьютер невидимым в Интернете (прячет порты);
- ✓ предотвращают известные хакерские атаки и троянские кони;
- ✓ извещают пользователя о попытках взлома;
- ✓ записывают информацию о подключениях в лог файл;
- ✓ предотвращают отправку конфиденциальных данных без предварительного уведомления;
- ✓ не дают серверам получать информацию без разрешения пользователя.