## Защита программного обеспечения на мобильных платформах. Недостатки технических методов защиты. Уязвимости современных методов защиты

### Защита программного обеспечения на мобильных платформах

Способы защиты программного обеспечения для мобильных платформ от копирования обычно основываются на невозможности рядового пользователя считывать/изменять хранящиеся в ППЗУ аппарата данные. Может также использоваться активация программного обеспечения.

**Устаревшие технические средства защиты**

В прошлом применялись и другие методы защиты ПО от ***нелегального использования***.

### Ключевая дискета

Метод был распространен во времена MS-DOS, сейчас, в силу устаревания технологии FDD, практически не применяется. Есть четыре основных способа создания некопируемых меток на дискетах:

* Считывание конкретного сектора дискеты (возможно, пустого или сбойного). Это самый простой способ защиты, и при копировании «дорожка в дорожку» дискета копируется.
* Запоминание сбойных секторов дискеты. Перед тем, как записать на дискету информацию, её царапают (или прожигают лазером), после этого записывают номера сбойных секторов. Для проверки подлинности дискеты программа пытается записать в эти сектора информацию, затем считать её.
* Нестандартное форматирование дискеты. Известна программа FDA (Floppy Disk Analyzer), которая могла проводить исследование и копирование таких дискет.
* «Плавающий бит». Один бит записывается так, что в некоторых случаях он читается как «0», в некоторых как «1». Проводится многократное считывание дискеты; среди результатов считывания должны быть и нули, и единицы.

### Запись некопируемых меток на жесткий диск

Некоторые старые программы для DOS создавали некопируемые метки на жёстком диске. Например, файл длиной 1 байт занимает на диске один кластер(не менее 512 байт), и в оставшиеся 511 байт можно записать некоторую информацию. Эта практика практически не используется, так как велик риск потери данных.

### Привязка к некоторому физическому объекту

Лицензия программы может привязываться к некоторому физическому объекту, к примеру

* к руководству пользователя. Например, программа выводит: «*Введите 5-е слово на 12-й сверху строке 26-й страницы*». Более изощрённый способ защиты — в руководстве находится важная информация, без которой невозможно пройти игру, этим известна серия Space Quest. Распространение сканеров и многозадачных операционных систем положило конец этой практике.
* к некоторому механическому устройству. Игра Another World поставлялась с «кодовым колесом». В системе защиты от копирования Lenslok, применявшейся в играх для ZX Spectrum, надо было, посмотрев на картинку через систему призм, увидеть двухбуквенный код.

## Недостатки технических методов защиты ПО

### Уязвимости современных методов защиты ПО

Уязвимости современных методов защиты можно достаточно строго классифицировать в зависимости от использованного метода защиты.

* Проверка оригинального носителя. Можно обойти при помощи копирования / эмуляции диска (специальная программа полностью копирует диск, затем создается драйвер виртуального дисковода, в который помещается образ, который программа принимает за лицензионный диск. Во многих играх применяется вариант этого метода под названием «Mini Image», когда подставной диск имеет маленький размер (несколько мегабайт, содержащие только лицензионную информацию), программа признаёт его лицензионным
* Ввод серийного номера. Основной уязвимостью является возможность беспрепятственного копирования и распространения дистрибутива вместе с серийным номером. Поэтому в настоящее время практически не используется (либо используется в совокупности с другими методами).
* Активация программного обеспечения. В отличие от предыдущего метода, активационный код генерируется с использованием уникальной информации (S/N оборудования, информации о пользователе) и является уникальным. В этом случае, в момент генерации кода активации в процессе установки программы есть риск эмуляции «универсального» аппаратного окружения (как то перехват обращений программы при считывании соответствующей информации, либо запуск программы изначально в виртуальной среде). Также, при неиспользовании запутывания кода защищенного приложения (или использовании слабых методов), злоумышленник может найти код генерации кода активации и вынести его в отдельную утилиту (т. н. «генератор ключей aka keygen»), ровно как и вырезать всю процедуру активации (что, однако, сложнее, так как он может вызываться в разных частях приложения)
* Использование электронных ключей. Часто встречается мнение о возможности эмуляции электронного ключа или библиотек интерфейса [API](https://ru.wikipedia.org/wiki/API), используемого при обращении к электронному ключу. Это действительно можно сделать при неграмотной реализации защиты на электронном ключе (к примеру, программа только проверяет наличие ключа и читает/пишет в него что-либо). Однако встроенные в программу защитные механизмы собственной разработки, основанные на вызове симметричных и асимметричных алгоритмов электронного ключа практически исключают возможность его эмуляции, так как обращения к ключу происходят каждый раз разные и накопить достаточное количество статистики для создания полного статистического аналога невозможно. Таким образом, стойкость защиты сильно зависит от реализации (в том числе от наличия уникальных защитных механизмов, реализованных разработчиком защиты). Тем не менее потенциально стойкость такой защиты может быть очень высока.
* «Отключение» защиты путём модификации программного кода (к примеру, удаления проверок лицензии). Может быть реализовано при неиспользовании (или использовании слабых) инструментов запутывания кода. В результате программа дизассемблируется (или даже декомпилируется, в худшем случае), код исследуется на наличие защитных механизмов, найденные проверки удаляются.

Многие защиты предоставляют инструменты противодействия взлому: дестабилизация отладчика; шифрование кода, исключающее изучение кода в статике при помощи дизассемблера; запутывание кода, «ложные ветви», сбивающие хакера с толку; проверка целостности файла, не дающая накладывать патчи; виртуализация кода с собственной системой команд. Все эти методы препятствуют изучению и анализу логики защиты, повышают её стойкость.

### Использование автоматических средств защиты

Существует проблема, связанная с недостатком ресурсов (в том числе временных) у разработчиков ПО. Им может не хватать времени, финансов или квалификации на реализацию собственной стойкой защиты. Они вынуждены пользоваться сторонними автоматическими средствами защиты ПО. Эти средства пристыковывают к скомпилированной программе защитный модуль. Преимущество такой защиты в том, что её можно установить на любую программу (даже без доступа к исходному коду программы). Недостаток в самом подходе — «шаблонности» метода. Стандартные защиты имеют большую вероятность быть взломанными, так как устанавливаются на несколько программ и тем самым обеспечивают спрос на рынке взлома.

Тем не менее, автоматические средства затрудняют взлом программы. Их иногда целесообразно использовать либо когда защиты нет вообще, либо в совокупности с реализацией собственной уникальной защиты.

### Проблема «лучше, чем легальное»

Это одна из фундаментальных проблем технических средств защиты. Заключается она в том, что система защиты неизбежно создаёт пользователю неудобства, и потому, с точки зрения пользователя, взломанная программа в каком-то смысле лучше, чем оригинальная. Например:

* Незащищенная программа работает, в общем случае, быстрее, чем защищенная
* Для работы «взломанной» программы не нужен оригинальный носитель. Если не использовать компакт-дисков, время работы [ноутбука](https://ru.wikipedia.org/wiki/%D0%9D%D0%BE%D1%83%D1%82%D0%B1%D1%83%D0%BA) существенно увеличивается. Кроме того на некоторых моделях ноутбуков устройство чтения компакт-дисков может отсутствовать вовсе
* При использовании USB-ключа может не хватить портов на всё нужное оборудование или не быть таковых вовсе (к примеру при использовании[виртуализации](https://ru.wikipedia.org/wiki/%D0%92%D0%B8%D1%80%D1%82%D1%83%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D0%BC%D0%B0%D1%88%D0%B8%D0%BD%D0%B0))
* Электронный ключ может создавать физические неудобства при работе с защищенной программой на ноутбуке
* J2ME-программа исчезнет после перепрошивки телефона, и нет возможности сделать её резервную копию.

По этой причине даже владельцы лицензионных копий иногда устанавливают взломанное программное обеспечение наравне с лицензионным.

**Методы и средства защиты от компьютерных вирусов**

В предыдущей статье, посвященной антивирусной защите, мы рассмотрели основные типы вирусов и способы их распространения. Теперь, основываясь на этих знаниях, мы займемся защитой от вирусов, троянских и других вредоносных программ. Мы расскажем о программно-технических и административно-технологических решениях и мероприятиях, необходимых для снижения риска вирусного заражения и уменьшения вреда, если такое заражение уже произошло.

## *Программно-технические методы обнаружения вирусов*

Основным средством борьбы с вирусами были и остаются антивирусные программы. Можно использовать антивирусные программы (антивирусы), не имея представления о том, как они устроены. Однако без понимания принципов устройства антивирусов, знания типов вирусов, а также способов их распространения, нельзя организовать надежную защиту компьютера. Как результат, компьютер может быть заражен, даже если на нем установлены антивирусы.

Сегодня используется несколько основополагающих методик обнаружения и защиты от вирусов:

         сканирование;

         эвристический анализ;

         использование антивирусных мониторов;

         обнаружение изменений;

         использование антивирусов, встроенных в BIOS компьютера.

Кроме того, практически все антивирусные программы обеспечивают автоматическое восстановление зараженных программ и загрузочных секторов. Конечно, если это возможно.

### Сканирование

Самая простая методика поиска вирусов заключается в том, что антивирусная программа последовательно просматривает проверяемые файлы в поиске сигнатур известных вирусов. Под сигнатурой понимается уникальная последовательность байт, принадлежащая вирусу, и не встречающаяся в других программах.

Антивирусные программы-сканеры способны найти только уже известные и изученные вирусы, для которых была определена сигнатура. Применение простых программ-сканеров не защищает Ваш компьютер от проникновения новых вирусов.

Для шифрующихся и полиморфных вирусов, способных полностью изменять свой код при заражении новой программы или загрузочного сектора, невозможно выделить сигнатуру. Поэтому простые антивирусные программы-сканеры не могут обнаружить полиморфные вирусы.

### Эвристический анализ

Эвристический анализ позволяет обнаруживать ранее неизвестные вирусы, причем для этого не надо предварительно собирать данные о файловой системе, как этого требует, например, рассмотренный ниже метод обнаружения изменений.

Антивирусные программы, реализующие метод эвристического анализа, проверяют программы и загрузочные секторы дисков и дискет, пытаясь обнаружить в них код, характерный для вирусов. Эвристический анализатор может обнаружить, например, что проверяемая программа устанавливает резидентный модуль в памяти или записывает данные  в исполнимый файл программы.

Практически все современные антивирусные программы реализуют собственные методы эвристического анализа. На рис. 1 мы показали одну из таких программ — сканер McAffee VirusScan, запущенный вручную для антивирусной проверки диска.

Когда антивирус обнаруживает зараженный файл, он обычно выводит сообщение на экране монитора и делает запись в собственном или системном журнале. В зависимости от настроек, антивирус может также направлять сообщение об обнаруженном вирусе администратору сети.

Если это возможно, антивирус вылечивает файл, восстанавливая его содержимое. В противном случае предлагается только одна возможность — удалить зараженный файл и затем восстановить его из резервной копии (если, конечно, она у Вас есть).

### Антивирусные мониторы

Существует еще целый класс антивирусных программ, которые постоянно находятся в памяти компьютера, и отслеживают все подозрительные действия, выполняемые другими программами. Такие программы носят название антивирусных мониторов или сторожей.

Монитор автоматически проверяет все запускаемые программы, создаваемые, открываемые и сохраняемые документы, файлы программ и документов, полученные через Интернет или скопированные на жесткий диск с дискеты и компакт диска. Антивирусный монитор сообщит пользователю, если какая-либо программа попытается выполнить потенциально опасное действие.

В комплект одного из наиболее совершенных сканеров Doctor Web (рис.2), разработанных Игорем Даниловым (http://www.drweb.ru) входит сторож Spider Guard, выполняющий функции антивирусного монитора.

### Обнаружение изменений

Когда вирус заражает компьютер, он изменяет содержимое жесткого диска, например, дописывает свой код в файл программы или документа, добавляет вызов программы-вируса в файл AUTOEXEC.BAT, изменяет загрузочный сектор, создает файл-спутник. Таких изменений, однако, не делают «бестелесные» вирусы, обитающие не на диске, а в памяти процессов ОС.

Антивирусные программы, называемые ревизорами диска, не выполняют поиск вирусов по сигнатурам. Они запоминают предварительно характеристики всех областей диска, которые подвергаются нападению вируса, а затем периодически проверяют их (отсюда происходит название программы-ревизоры). Ревизор может найти изменения, сделанные известным или неизвестным вирусом.

В качестве примеров ревизоров диска можно привести программу Advanced Diskinfoscope (ADinf), разработанную в ЗАО «ДиалогНаука» (http://www.dials.ru, http://www.adinf.ru) и ревизор AVP Inspector производства ЗАО «Лаборатория Касперского» (http://www.kaspersky.ru).

Вместе с ADinf применяется лечащий модуль ADinf Cure Module (ADinfExt), который использует собранную ранее информацию о файлах для восстановления их после поражения неизвестными вирусами. Ревизор AVP Inspector также имеет в своем составе лечащий модуль, способный удалять вирусы.

### Защита, встроенная в BIOS компьютера

В системные платы компьютеров тоже встраивают простейшие средства защиты от вирусов. Эти средства позволяют контролировать все обращения к главной загрузочной записи жестких дисков, а также к загрузочным секторам дисков и дискет. Если какая-либо программа попытается изменить содержимое загрузочных секторов, срабатывает защита и пользователь получает соответствующее предупреждение.

Однако эта защита не очень надежна. Существуют вирусы (например, Tchechen.1912 и 1914), которые пытаются отключить антивирусный контроль BIOS, изменяя некоторые ячейки в энергонезависимой памяти (CMOS-памяти) компьютера.

## *Особенности защиты корпоративной интрасети*

Корпоративня интрасеть может насчитывать сотни и тысячи компьютеров, играющих роль рабочих станций и серверов. Эта сеть обычно подключена к Интернету и в ней имеются почтовые серверы, серверы систем автоматизации документооборота, такие как Microsoft Exchange и LotusNotes, а также нестандартные информационные системы.

Для надежной защиты корпоративной интрасети необходимо установить антивируы на все рабочие станции и серверы. При этом на файл-серверах, серверах электронной почты и серверах систем документооборота следует использовать специальное серверное антивирусное программное обеспечение. Что же касается рабочих станций, их можно защитить обычными антивирусными сканерами и мониторами.

Разработаны специальные антивирусные прокси-серверы и брандмауэры, сканирующие проходящий через них трафик и удаляющие из него вредоносные программные компоненты. Эти антивирусы часто применяются для защиты почтовых серверов и серверов систем документооборота.

### Защита файловых серверов

Защита файловых серверов должна осуществляться с использованием антивирусных мониторов, способных автоматически проверять все файлы сервера, к которым идет обращение по сети. Антивирусы, предназначенные для защиты файловых серверов, выпускают все антивирусные компании, поэтому у Вас есть богатый выбор.

### Защита почтовых серверов

Антивирусные мониторы неэффективны для обнаружения вирусов в почтовых сообщениях. Для этого необходимы специальные антивирусы, способные фильтровать трафик SMTP, POP3 и IMAP, исключая попадание зараженных сообщений на рабочие станции пользователей.

Для защиты почтовых серверов можно приобрести антивирусы, специально предназначенные для проверки почтового трафика, или подключить к почтовому серверу обычные антивирусы, допускающие работу в режиме командной строки.

Демон антивируса Doctor Web можно интегрировать со всеми наиболее известными почтовыми серверами и системами, такими как DoctorComminiGatePro, Sendmail, Postfix, Exim, QMail и Zmailer. Аналогичные средства предоставляются и Лабораторией Касперского в составе пакета Kaspersky Corporate Suite.

Почтовый сервер MERAK Mail Server допускает подключение внешних антивирусов различных типов, имеющих интерфейс командной строки. Некоторые почтовые серверы (например, EServ) поставляются со встроенным антивирусом.

Можно также дополнительно проверять трафик POP3 и на рабочих станциях пользователей. Это позволяет сделать, например, антивирусный прокси-сервер SpIDer Mail для протокола POP3, который можно приобрести вместе с антивирусом Doctor Web.

### Защита серверов систем документооборота

Серверы систем документооборота, такие как Microsoft Exchange и Lotus Notes, хранят документы в базах данных собственного формата. Поэтому использование обычных файловых сканеров для антивирусной проверки документов не даст никаких результатов.

Существует ряд антивирусных программ, специально предназначенных для антивирусной защиты подобных систем. Это Trend Micro ScanMailдля Lotus Notes, McAfee GroupScan и McAfee GroupShield, Norton Antivirus для Lotus Notes, антивирус Касперского Business Optimal для MS ExchangeServer и некоторые другие.

Эти программы сканируют почту и файлы вложений, удаляя в реальном времени все вредоносные программы, обнаруживают макрокомандные вирусы  и троянские программы в формах и макросах, в файлах сценариев и в объектах OLE. Проверка выполняется в режиме реального времени, а также по требованию.

### Защита нестандартных информационных систем

Для антивирусной защиты нестандартных информационных систем, хранящих данные в собственных форматах, необходимо либо встраивать антивирусное ядру в систему, либо подключать внешний сканер, работающий в режиме командной строки.

Например, ядро антивируса Doctor Web было использовано ФГУП «НПО машиностроения» для защиты системы документооборота, созданной на базе собственной технологии Sapiens (http://www.npomit.ru). Вся информация, сохраняемая этой системой в базе данных, проверяется антивирусным ядром Doctor Web.

Как разработчики информационных систем для ответственного применения, «НПО машиностроения» снабдило антивирусной защитой такие свои разработки, как Sapiens Регистрация и Контроль Исполнения Документов, Sapiens Мониторинг Вычислительных Ресурсов, Sapiens Электронный Архив Конструкторской Документации.

### Сетевой центр управления антивирусами

Если интрасеть насчитывает сотни и тысячи компьютеров, то необходимо централизованное удаленное управление антивирусными программами и контроль их работы. Выполнение в «ручном» режиме таких операций, как отслеживание обновлений антивирусной базы данных и загрузочных модулей антивирусных программ, контроль эффективности обнаружения вирусов на рабочих станциях и серверах и т.п., малоэффективно, если в сети имеется большое количество пользователей или если сеть состоит из территориально удаленных друг от друга сегментов.

Если же не обеспечить своевременное и эффективное выполнение перечисленных выше операций, технология антивирусной защиты корпоративной сети обязательно будет нарушена, что рано или поздно приведет к вирусному заражению. Например, пользователи могут неправильно настроить автоматическое обновление антивирусной базы данных или просто выключать свои компьютеры в то время, когда такое обновление выполняется. В результате автоматическое обновление не будет выполнено и возникнет потенциальная угроза заражения новыми вирусами.

В современных антивирусных системах реализованы следующие функции удаленного управления и контроля:

         установка и обновление антивирусных программ, а также антивирусных баз данных;

         централизованная дистанционная установка и настройка  антивирусов;

         автоматическое обнаружение новых рабочих станций, подключенных к корпоративной сети, с последующей автоматической установкой на эти станции антивирусных программ;

         планирование заданий для немедленного или отложенного запуска (таких как обновление программ, антивирусной базы данных, сканирование файлов и т.п.) на любых компьютерах сети;

         отображение в реальном времени процесса работы антивирусов на рабочих станциях и серверах сети.

Все перечисленные выше функции или многие из них реализованы в сетевых центрах управления ведущих корпоративных антивирусных продуктов, созданных компаниями Sophos (http://www.sophos.com), Symantec (http://www.symanteс.ru), Network Associates (http://www.nai.com) и Лаборатория Касперского.

Сетевые центры управления позволяют управлять антивирусной защитой всей сети с одной рабочей станции системного администратора. При этом для ускорения процесса установки антивирусов в удаленных сетях, подключенных к основной сети медленными каналами связи, в этих сетях создаются собственные локальные дистрибутивные каталоги.

При использовании клиент-серверной архитектуры основой сетевого центра управления является антивирусный сервер, установленный на одном из серверов корпоративной сети. С ним взаимодействуют, с одной стороны, программы-агенты, установленные вместе с антивирусами на рабочих станциях сети, а с другой стороны — управляющая консоль администратора антивирусной защиты

Антивирусный сервер выполняет управляющие и координирующие действия. Он хранит общий журнал событий, имеющих отношение к антивирусной защите и возникающих на всех компьютерах сети, список и расписание выполнения заданий. Антивирусный сервер отвечает за прием от агентов и передачу администратору антивирусной защиты сообщений о возникновении тех или иных событий в сети, выполняет периодическую проверку конфигурации сети с целью обнаружения новых рабочих станций или рабочих станций с изменившейся конфигурацией антивирусных средств и т.д.

Помимо агентов, на каждой рабочей станции и сервере корпоративной сети устанавливается антивирус, выполняющий сканирование файлов и проверку файлов при их открытии (функции сканера и антивирусного монитора). Результаты работы антивируса передаются через агентов антивирусному серверу, которых их анализирует и протоколирует в журнале событий.

Управляющая консоль может представлять собой стандартное приложение Microsoft Windows с оконным интерфейсом или аплет (snap-in) управляющей консоли Control Panel операционной системы Microsoft Windows. Первый подход реализован, например, а управляющей системе антивирусов Sophos, а второй — в управляющей системе Norton AntiVirus.

Пользовательский интерфейс управляющей консоли позволяет просматривать древовидную структуру корпоративной сети, получая при необходимости доступ к отдельным компьютерам тех или иных групп пользователей или доменов.

### Многоуровневые системы с Web-интерфейсом

Архитектура многоуровневых систем с Web-интерфейсом предполагает использование Web-сервера в качестве ядра системы. Задачей этого ядра является, с одной стороны, организация диалогового интерактивного взаимодействия с пользователем, а с другой — с программными модулями той или иной системы.

Преимущества такого подхода заключаются в унификации способов управления различными системами сети, а также в отсутствии необходимости устанавливать на рабочую станцию администратора какие-либо управляющие программы или консоли. Администрирование может выполняться с любого компьютера сети, а если сеть подключена к Интернету, то из любого места земного шара, где есть Интернет и компьютер с браузером.

Для защиты управляющей информации при ее передаче по Интернету или корпоративной интрасети применяются протоколы SSH или другие аналогичные средства (например, собственные защищенные модификации протокола HTTP).

На рабочих станциях устанавливается антивирус (PC-cillin, Server Protect, InterScan VirusWall, ScanMail и т.д.). Этот антивирус управляется антивирусным сервером через агента.

На компьютере, играющем роль антивирусного сервера, устанавливается Web-сервер Microsoft IIS. Специальное Web-приложение, работающее на этом сервере, управляет антивирусным сервером. Оно также предоставляет администратору пользовательский интерфейс для управления системой антивирусной защиты.

С целью обеспечения максимальной независимости от компьютерных платформ сервер Trend VCS Server и клиентское приложение написаны на языке программирования Java и других языках, применяющихся для разработки приложений Интернета.

Что же касается извещений о возникновении событий в корпоративной системе антивирусной защиты, то они передаются программами-агентами серверу Trend VCS Server и рассылаются по электронной почте, по пэйджинговым сетям, через системы SMS и т.п.

### *Административно-технологические методы защиты*

Для того чтобы антивирусные программы эффективно выполняли свои функции, необходимо строго соблюдать рекомендации по их применению, описанные в документации. Особое внимание следует обратить на необходимость регулярного обновления вирусных баз данных и программных компонент антивирусов. Современные антивирусы умеют загружать файлы обновлений через Интернет или по локальной сети. Однако для этого их необходимо настроить соответствующим образом.

Однако даже без применения антивирусных программ можно постараться предотвратить проникновение вирусов в компьютер и уменьшить вред, который они нанесут в случае заражения. Вот что следует для этого сделать в первую очередь:

         блокируйте возможные каналы проникновения вирусов: не подключайте компьютер к Интернету и локальной сети компании, если в этом нет необходимости, отключите устройства внешней памяти, такие как дисководы для дискет и устройства CD-ROM;

         настройте параметры BIOS таким образом, чтобы загрузка ОС выполнялась только с жесткого диска, но не с дискет;

         запретите программное изменение содержимого энергонезависимой памяти BIOS;

         изготовьте системную загрузочную дискету, записав на нее антивирусы и другие системные утилиты для работы с диском, а также диск аварийного восстановления Microsoft Windows;

         проверяйте все программы и файлы документов, записываемые на компьютер, а также дискеты с помощью антивирусных программ новейших версий;

         устанавливайте программное обеспечение только с лицензионных компакт-дисков;

         установите на всех дискетах защиту от записи и снимайте ее только в случае необходимости;

         ограничьте обмен программами и дискетами;

         регулярно выполняйте резервное копирование данных;

         устанавливайте минимально необходимые права доступа к каталогам файлового сервера, защищайте от записи каталоги дистрибутивов и программных файлов;

         составьте инструкцию для пользователей по антивирусной защите, описав в ней правила использования антивирусов, правила работы с файлами и электронной почтой, а также опишите действия, которые следует предпринять при обнаружении вирусов.

### *Проблема домашних компьютеров*

Часто сотрудники компаний работают не только в офисе, но и дома, обмениваясь файлами между домашним компьютером и офисной рабочей станцией. Системный администратор компании не в состоянии защитить от вирусов все домашние компьютеры сотрудников. Вирусы могут попасть на домашний компьютер из Интернета, а также в результате обмена игровыми программами. Зачастую это происходит, если к домашнему компьютеру имеют доступ другие члены семьи и дети.

Все файлы, которые сотрудники приносят из дома на работу, следует рассматривать как потенциально опасные. В ответственных случаях такой обмен следует полностью запретить, либо сильно ограничить. Потенциально опасные «домашние» файлы необходимо проверять перед открытием антивирусными программами.

### *Установка персональных брандмауэров*

Корпоративная сеть, подключенная к Интернету, должна быть защищена от атак хакеров при помощи брандмауэра. Однако помимо этого можно дополнительно защитить рабочие станции и серверы сети, установив на них персональные брандмауэры, такие как AtGuard

Помимо фильтрации нежелательного трафика, некоторые персональные брандмауэры способны защитить компьютер от троянских аплетов Java и элементов управления ActiveX. Такие компоненты могут быть встроены в почтовые сообщения формата HTML и в страницы троянских Web-сайтов.

Персональные брандмауэры, находящиеся в так называемом режиме обучения, могут оказать помощь в обнаружении трафика от троянских программ, логических бомб и других нежелательных вредоносных компонентов. Когда такой компонент попытается установить связь с компьютером хакера, брандмауэр отобразит на экране предупреждающее сообщение.

Следует заметить, что в настройках браузера Вы также можете отключить возможность использования активных компонентов, таких как аплетыJava и элементов управления ActiveX. Однако персональные брандмауэры более универсальны, и позволяют блокировать использование таких компонентов любыми программами, например, почтовыми клиентами