В. В. Медведев, *ООО «Доктор Веб», Москва, v.medvedev@drweb.com*

Возможность выработки требований к системе защиты от вредоносных программ

Несмотря на то что вредоносные программы, а также средства защиты от них существуют уже несколько десятилетий, до сих пор не имеется правильных определений понятий «вредоносная программа» и «антивирус». В данной работе делается попытка выработки требований к антивирусной системе защиты, что позволит компаниям и частным пользователям реализовывать надежную защиту от современных угроз.

Ключевые слова: термины и определения, антивирус, вредоносная программа, информационная безопасность, стандарты, рекомендации.

Введение

Как ни странно, несмотря на огромное количество различных стандартов в области информационной безопасности, успешную деятельность ряда международных компаний и организаций, до сих пор единых определений в данной области не выработано. Нет даже такого базового определения, как вредоносная программа.

Отсутствие правильной терминологии дезориентирует как ИТ-специалистов, так и частных пользователей. Так, неверное понимание задач и возможностей антивируса не позволяет компаниям и организациям правильно оформить требования в ходе закупки и в процессе внедрения защитных мер. Системы защиты, построенные без понимания возможностей продуктов, не могут противостоять криминалитету.

Необходимо отметить, что правильное понимание возможностей и ограничений различных типов систем защиты позволяет оптимально использовать финансовые ресурсы компаний и организаций.

Более того, неверная терминология активно используется мошенниками для продвижения своих «решений».

Данная статья содержит:

1) анализ имеющихся терминов и определений в области антивирусной безопасности;

2) анализ ряда руководящих документов регуляторов в области антивирусной защиты в отношении возможностей систем защиты, построенных в соответствии с такими документами;

3) рекомендации, которых необходимо придерживаться при выборе систем антивирусной безопасности.

К сожалению, несмотря на огромное количество литературы по теме вредоносных программ, большая ее часть описывает сами вредоносные программы. Более того, имеется литература, содержащая советы, которые могут принести только вред. В ходе подготовки данной статьи автором не обнаружено литературы, посвященной анализу терминов и определений в области антивирусной защиты.

Анализ имеющихся определений термина «вредоносная программа»

Приведем лишь несколько определений из различных источников.

- «Вредоносная компьютерная программа — компьютерная программа либо иная компьютерная информация, заведомо предназначенная для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации»[1].

[1] Уголовный кодекс Российской Федерации. Ст. 273. URL: http://www.pravo.gov.ru/proxy/ips/?docbody=&link_id=1&nd=102041891

• «Вредоносный код — компьютерная программа, предназначенная для внедрения в автоматизированные системы, ПО, средства вычислительной техники, телекоммуникационное оборудование кредитной организации и ее клиентов — пользователей систем дистанционного банковского обслуживания, приводящая к уничтожению, созданию, копированию, блокированию, модификации и (или) передаче информации (в том числе защищаемой в соответствии с пунктом 2.1 Положения 382-П), а также к созданию условий для такого уничтожения, создания, копирования, блокирования, модификации и (или) передачи»[2].

• «Обеспечение программное вредоносное — программа, предназначенная для осуществления доступа несанкционированного к информации и (или) воздействия на информацию или ресурс системы информационной»[3].

• «Вредоносное программное обеспечение — программное обеспечение, целенаправленно приводящее к нарушению законных прав абонента и (или) пользователя, в том числе к сбору, обработке или передаче с абонентского терминала информации без согласия абонента и (или) пользователя, либо к ухудшению параметров функционирования абонентского терминала или сети связи»[4].

• «Вредоносную программу, известную также как вредоносный код и опасное программное обеспечение, относят к программам, которые внедряют в систему, обычно тайно, с целью нарушения конфиденциальности, целостности или доступности данных, приложений или операционной системы (ОС) жертвы или иным образом досаждающих владельцу устройства»[5].

Это далеко не все определения, но даже на их примере видно отсутствие единого мнения по поводу такого базового понятия, как вредоносная программа. Более того, нет даже единства насчет слова «вредоносный» — в ряде переводных документов используется понятие «защита от злонамеренных кодов»[6].

К сожалению, все известные определения (за исключением определения из NIST) отличаются либо четким перечислением конкретных функций (что исключает необходимость принятия мер по противодействию вредоносным программам с иным функционалам), либо нечеткостью понятий, что не позволяет на их основе сформулировать требования к антивирусной защите.

В качестве характерного примера рассмотрим программы удаленного управления. Они могут скрытно устанавливаться и системными администраторами, и злоумышленниками. Как антивирусная программа может определить, кто устанавливает программу? В определении выше используется слово «несанкционированно». Но кто именно должен санкционировать указанные действия над информацией?

• Работа администраторов на компьютерах сети, как правило, проходит скрытно для пользователей. Пользователь не санкционирует установку программы и не контролирует ее.

• Пользователи в своей массе не являются специалистами по ИБ и не в курсе, что и почему работает у них на компьютере. И как правило, соглашаются на предложения различных всплывающих окон (т.е. санкционируют). Можно ли считать установившу-

---

[2] Письмо Банка России от 24.03.2014 №49-Т «О рекомендациях по организации применения средств защиты от вредоносного кода при осуществлении банковской деятельности». URL: http://www.garant.ru/products/ipo/prime/doc/70526030

[3] ГОСТ Р 50922–2006. URL: http://www.glossary.ibbank.ru/solution/605

[4] Постановление Правительства РФ от 10.09.2007 №575. URL: http://base.garant.ru/12155536

[5] NIST SP 800–83. URL: http://csrc.nist.gov/publications/drafts/800–83-rev1/draft_sp800-83-rev1.pdf

[6] ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности, ISO/IEC 27002 Информационные технологии. Свод правил по управлению защитой информации. URL: http://docs.cntd.ru/document/gost-r-iso-13335-4-2007

юся таким образом программу заведомо невредоносной?

Еще одна проблема возникает, когда наряду с определением вредоносной программы в стандарты проникают определения частных типов вредоносных программ. Так, например, NIST, кроме понятия *malware* параллельно вводит понятие *spyware*.

«Программное обеспечение, которое тайно или незаметно устанавливается в систему обработки информации для сбора данных о людях или организациях без их согласия; тип вредоносного кода»[7].

Формально *spyware* описывается как один из типов *malware*, но почему тогда не описать все остальные типы *malware*? В результате такого акцентирования внимания даже солидные журналы рекомендуют устанавливать в дополнение к антивирусу еще и антируткит с антишпионом, тогда как любой антивирус способен перехватывать и уничтожать любые типы вредоносных программ. И наоборот, программы, называющие себя антишпионами и антируткитами, нередко сами относятся к вредоносным программам.

Определение термина «вредоносная программа»

Необходимо понимать, что в подавляющем большинстве случаев состав программного обеспечения, а также его версии достаточно слабо контролируются не только самими пользователями, но и системными администраторами. И если автоматические обновления ранее установленного ПО еще могут контролироваться, то, например, ряд типов программ запускается без уведомления пользователя (точнее, не уведомляя об этом пользователя, если не были сделаны соответствующие настройки). К таким программам могут быть отнесены скрипты, запускаемые в браузере, макросы программ, входящих в состав офисного пакета, и многие другие. Ряд программ устанавливается в ходе установки иных программ (с предупреждением или без предупреждения об этом на соответствующих этапах инсталляции основной программы). Следует ли эти программы и компоненты программ относить к вредоносным? Теоретически любой браузер можно настроить на то, что на каждый запуск чего-либо будет выдаваться запрос. Но насколько опытным должен быть пользователь, чтобы на лету определять степень вредоносности действия?

Особые проблемы возникают с предустановленным ПО. Пользователь получает уже готовые к работе системы и компоненты, соглашаясь на их использование. Но насколько он уверен, что знает все функции полученного им ПО?

В связи с вышеизложенным введем определение вредоносного ПО.

Вредоносными являются программы, которые устанавливаются без разрешения или выполняют действия, не обозначенные в соответствующей документации или лицензии.

Можно отметить, что в категорию вредоносных в данном случае попадают любые программы, имеющие неописанный функционал. Но такой функционал так или иначе приносит вред (работой с информацией, расходом ресурсов, наличием уязвимостей или иначе). Соответственно, отнесение такого ПО к вредоносному достаточно логично.

Наиболее близко к данному нами определению (наряду с определением от NIST) лежит определение Положения Банка России от 09.06.2012 № 382-П (с изменениями согласно Указанию Банка России от 05.06.2013 № 3007-У и Указанию Банка России от 14.08.2014 № 3361-У) «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении денежных переводов»:

«программные коды, приводящие к нарушению штатного функционирования сред-

[7] NIST Special Publication 800–53 rev. 4. URL: http://csrc.nist.gov/publications/drafts/800–53-rev4/sp800-53-rev4-ipd.pdf

ства вычислительной техники (далее — вредоносный код)»[8].

К сожалению, данное определение делает акцент на вредоносном коде, что связывает его с определенным типом вредоносных программ — вирусами, тогда как на данный момент бóльшая часть вредоносных программ — это троянцы. Минусом этого определения является то, что согласно ему вредоносными не считаются программы, не нарушающие установленных правил функционирования системы. Например, системы кражи персональной информации.

Анализ имеющихся определений терминов «антивирус» и «антивирусная система защиты»

Поскольку отсутствует единое определение вредоносной программы, естественно, отсутствует и единое мнение по поводу определения антивируса и антивирусной системы защиты. Вот несколько вариантов.

- «Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации»[9].
- «Защита информационной системы, включающая обнаружение компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации»[10].
- «Программа, которая выявляет, предотвращает и выполняет определенные действия, чтобы блокировать или удалять вредоносные программы, такие как вирусы и черви»[11].

Забегая вперед, можно сказать, что определения как минимум не учитывают момент, когда система защиты должна обнаруживать вредоносную программу. Опасность также представляет акцент в определении на каких-либо конкретных действиях. Так, модификация в настоящее время является устаревшей мерой защиты. Также распространенной ошибкой является включение в определение системы защиты перечисления типов вредоносных программ или их действий. В связи с этим появление новых типов вредоносных программ или их действий автоматически выводит их из-под действия нормативных документов.

Анализ требований регуляторов в области антивирусной защиты

Прежде чем ввести определение системы антивирусной защиты, определим возможности вредоносных программ по ее обходу (уровень риска). Сейчас основную проблему для компаний составляют вредоносные программы, не обнаруживаемые системами защиты, что связано с особенностями разработки современных вредоносных программ.

---

[8] О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств (с изменениями на 14 августа 2014 года). URL: http://docs.cntd.ru/document/902352532

[9] Приказ ФСТЭК № 17. URL: http://www.rg.ru/2013/06/26/gostajna-dok.html

[10] Методический документ ФСТЭК. Меры защиты информации в государственных информационных системах. URL: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/805-metodicheskij-dokument

[11] URL: http://www.microsoft.com/ru-ru/security/resources/antivirus-whatis.aspx

На данный момент антивирус должен обеспечивать:

1) защиту от проникновения **всех** уже известных типов вредоносных программ (в том числе с помощью технологий, позволяющих обнаруживать модификации ранее найденного);

2) поддержание системы защиты в контролируемом состоянии;

3) гарантированное получение обновлений;

4) после получения обновлений — обнаружение и уничтожение (но не откат действий) ранее запущенных вредоносных программ.

Определения антивирусной защиты, данные в нормативных документах, не указывают на необходимость лечения ранее неизвестных вредоносных программ и функционирования в условиях попыток дискредитации системы защиты. В связи с этим реализованные на основе этих определений системы антивирусной защиты не способны противостоять современным угрозам.

Необходимо отметить, что требовать обязательного использования в системе защиты именно антивируса — необоснованно. Так, например, классический файловый антивирус не может использоваться в системах, близких к системам реального времени, к которым можно отнести практически все системы, управляющие технологическими процессами. Также система защиты на основе антивируса не может быть использована в системах, в которых отсутствует достаточное количество ресурсов для запуска антивируса.

В связи с вышеизложенным давать определение и задавать требования необходимо к антивирусной системе защиты, в которой непосредственно антивирус может выполнять лишь определенную функцию.

В качестве примера рассмотрим требования ФСТЭК России, данные в методическом документе «Меры защиты информации в государственных информационных системах», и узнаем, что думает регулятор о функциях антивируса.

«3.6. АНТИВИРУСНАЯ ЗАЩИТА (АВЗ)

АВЗ. 1 РЕАЛИЗАЦИЯ АНТИВИРУСНОЙ ЗАЩИТЫ

Требования к реализации АВЗ.1: Оператором должна обеспечиваться антивирусная защита информационной системы, включающая обнаружение компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

Реализация антивирусной защиты должна предусматривать:

• применение средств антивирусной защиты на автоматизированных рабочих местах, серверах, периметральных средствах защиты информации (средствах межсетевого экранирования, прокси-серверах, почтовых шлюзах и других средствах защиты информации), мобильных технических средствах и иных точках доступа в информационную систему, подверженных внедрению (заражению) вредоносными компьютерными программами (вирусами) через съемные машинные носители информации или сетевые подключения, в том числе к сетям общего пользования (вложения электронной почты, веб- и другие сетевые сервисы)»[12].

Данное положение абсолютно правильно требует установки антивирусной защиты на всех компьютерах и устройствах, подверженных заражению (в том числе на личных устройствах и домашних компьютерах, с которых осуществляется доступ в информационную систему). Однако, как уже отмечалось, установка антивируса на всех устройствах и компьютерах, подверженных заражению, невозможна.

[12] Методический документ ФСТЭК. Меры защиты информации в государственных информационных системах. URL: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/805-metodicheskij-dokument

Не учитывается также, что защита серверов может не подразумевать защиту сервисов, работающих на них. Так, установка постоянной антивирусной защиты сервера (файлового монитора) не будет означать проверки почты, проходящей через MS Exchange, или трафика через MS ISA/TMG.

Не очень удачно использование слов «*внедрению (заражению)*», так как заражение подразумевает запуск и активацию вредоносной программы, а внедрение может осуществляться простым размещением файла — в том числе на ОС, заражение которых данной вредоносной программой невозможно (например, размещением вредоносной программы на файловом сервере Linux);

• «проверку в масштабе времени, близком к реальному, объектов (файлов) из внешних источников (съемных машинных носителей информации, сетевых подключений, в том числе к сетям общего пользования, и других внешних источников) при загрузке, открытии или исполнении таких файлов»[13].

Ключевая ошибка в определении задач защиты. Требуется перепроверка не только для ранее полученных объектов в случае их получения из внешних источников, но и для иных файлов/объектов (в том числе имевшихся в момент установки и/или размещенных злоумышленниками в обход систем безопасности). Проверка необходима в связи с тем, что на момент проникновения (внедрения) вредоносная программа может быть неизвестна антивирусной системе — но станет известной после очередного обновления.

Более того. Нужно проверять и уже запущенные процессы — там также могут находиться ранее неизвестные угрозы.

Требования к усилению АВ3.1:

«4) в информационной системе должно обеспечиваться использование на разных уровнях информационной системы средств антивирусной защиты разных производителей»[14].

Типичное заблуждение. Требование основано на том, что в связи с достаточно большим объемом потока создаваемых вредоносных программ в произвольный момент времени каждый из антивирусов знает только часть из них. В развернутом виде правило подразумевает, что любой документ, получаемый пользователем, должен проходить проверку двух антивирусов: 1) при получении документа с файлового сервера или хранилища — антивирусом на файловом сервере и антивирусом на рабочей станции; 2) при получении или отправке сообщения — антивирусом на почтовом сервере и антивирусом на рабочей станции; 3) при получении или отправке файла в Интернет — антивирусом на шлюзе и антивирусом на рабочей станции.

Однако данное требование не учитывает изменившуюся систему разработки вредоносных программ — в реальности основную опасность представляют протестированные на актуальных версиях систем защиты вредоносные программы, не обнаруживаемые ими. В связи с этим количество антивирусов существенной роли не играет (при условии использования систем защиты равного уровня).

Однако использование двух антивирусов необходимо для периодических проверок на еще не известные производителю вредоносные файлы.

«В информационной системе должна обеспечиваться проверка объектов файловой системы средством антивирусной защиты до загрузки операционной системы»[15].

Также требование из прошлого. Полная проверка может занимать достаточно длительное время и действительно оправдана либо в случае подозрений на заражение, либо при отсутствии средств постоянной антивирусной защиты.

«ЗСВ. 9. РЕАЛИЗАЦИЯ И УПРАВЛЕНИЕ АНТИВИРУСНОЙ ЗАЩИТОЙ В ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРЕ

[13] Там же.

[14] Там же.

[15] Там же.

Требования к реализации ЗСВ.9:

В информационной системе должны обеспечиваться реализация и управление антивирусной защитой в виртуальной инфраструктуре в соответствии с АВЗ.1, АВЗ.2.

При реализации соответствующих мер должны обеспечиваться:

• проверка наличия вредоносных программ (вирусов) в хостовой операционной системе, включая контроль файловой системы, памяти, запущенных приложений и процессов;

• проверка наличия вредоносных программ в гостевой операционной системе в процессе ее функционирования, включая контроль файловой системы, памяти, запущенных приложений и процессов»[16].

Пример из того же документа, но иного размера, демонстрирует более правильный подход к защите — АВЗ.1 контроля памяти и запущенных процессов не требуют.

Интересно отметить, что список мер, которые могут согласно документу применяться для защиты локальной сети компании, в большей своей части также будет выполнять требования по защите от вредоносных программ.

«В информационной системе подлежат реализации следующие меры защиты информации:

• идентификация и аутентификация субъектов доступа и объектов доступа;

• управление доступом субъектов доступа к объектам доступа;

• ограничение программной среды;

• защита машинных носителей информации;

• регистрация событий безопасности;

• обнаружение (предотвращение) вторжений;

• обеспечение целостности информационной системы и информации;

• защита информационной системы, ее средств и систем связи и передачи данных»[17].

Требования к антивирусной системе защиты, позволяющие обеспечить безопасность локальной сети

Перейдем к описанию требований по организации антивирусной защиты на конкретных узлах сети. Инфраструктура типичной организации включает:

• рабочие станции и файловые серверы (как правило, на основе ОС Windows) — включая в данном случае файловые серверы, серверы баз данных, серверы приложений, терминальные серверы и т. д.;

• почтовые серверы (как правило, на основе MS Exchange);

• мобильные устройства и ноутбуки руководителей организации и ее сотрудников;

• интернет-шлюзы и межсетевые шлюзы.

Антивирусная защита веб-серверов является темой отдельного исследования и здесь не рассматривается.

На практике же антивирусная защита большинства организаций включает в себя установку антивируса на рабочие станции и файловые серверы (как правило, файловые серверы Windows).

На организацию локальной сети также сильно влияет род деятельности компании, в связи с чем она может попадать под те или иные требования законодательных актов. Так, в организации могут использоваться секретные документы, она может сотрудничать с определенными учреждениями (наиболее частый случай последнего — институты и НИИ, работающие с Министерством обороны). Кроме того, организация может относиться к обслуживающим критически важные инфраструктуры (железные дороги, атомные станции и т. д.) — и тем самым попадать под требования их защиты. Как правило, в локальных сетях таких компаний внутренняя сеть отделена от внешней и большая часть сотрудников компании не должна

[16] Методический документ ФСТЭК. Меры защиты информации в государственных информационных системах. URL: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/805-metodicheskij-dokument

[17] Там же.

иметь доступа в Интернет или имеет доступ только к определенным сервисам.

Начнем с рабочих станций.

Система антивирусной защиты рабочих станций (а также желательно домашних компьютеров сотрудников) должна включать, кроме собственно файлового антивируса, также файервол (как ни странно, но в компаниях не переводятся любители пошарить по сети), поведенческий анализатор — для отслеживания подозрительных действий, средства офисного/родительского контроля, систему резервирования. Как минимум.

При этом необходимо выполнение ряда требований:

1) антивирус должен иметь систему самозащиты, не позволяющую неизвестной вредоносной программе нарушить нормальную работу антивируса, — антивирусное решение должно нормально функционировать до поступления обновления, позволяющего пролечить заражение;

2) весь входящий трафик должен проверяться до момента его поступления в соответствующие клиентские приложения, что не позволит вредоносным программам использовать незакрытые по тем или иным причинам уязвимости;

3) как система управления, так и система обновления антивирусного решения должны находиться под контролем системы самозащиты. Крайне нежелательно использовать для обновления и управления сторонние по отношению к антивирусу системы (WSUS, Windows Update, консоли Microsoft и т. д.);

4) должна иметься система автоматического сканирования ранее запущенных процессов.

Поскольку система разработки вредоносных программ подразумевает тестирование на типовых установках систем защиты, то в обязательном порядке после развертывания системы защиты должна проводиться ее настройка. Это необходимо в связи с тем, что многие модули антивируса по умолчанию не настроены, но именно они во многом определяют качество антивирусной защиты — защиты от неизвестных вредоносных программ.

В первую очередь необходима настройка компонентов превентивной защиты и офисного контроля. Модуль офисного контроля позволяет контролировать доступ (попытки проникновения) к различным областям компьютерной станции. Естественно, что при полном контроле возможны конфликты с различным ПО, используемым в системе. Поэтому уровень контроля по умолчанию минимален. Соответственно, администратор имеет возможность, зная список используемого ПО, настроить более высокий уровень контроля. Еще более важно осуществить настройку систем ограничения доступа. Работа этой подсистемы не позволит вредоносному файлу запуститься или получить необходимые для работы компоненты.

В качестве рекомендации можно указать на необходимость минимизации использования широко распространенного ПО, уязвимости в котором интересуют злоумышленников. В первую очередь к такому ПО можно отнести такие продукты, как Adobe Flash и Adobe Acrobat.

На данный момент сотрудники компаний широко используют сервисы хранения документов. В данном случае принимаемые документы, поступающие по защищенному каналу, минуют средства безопасности компании, но при этом никакой гарантии их безопасности и неизменности за время хранения на внешних сервисах не существует.

Еще одним заблуждением является то, что в силу относительно малого количества вредоносных программ для операционных систем типа Mac OS X, Linux/Unix необходимо защищать только рабочие станции и серверы, работающие с использованием операционных систем типа Windows. В результате такого подхода вредоносные программы получают безопасное убежище на незащищенных машинах — даже если они не могут заразить сами операционные системы (ОС) и работающие приложения, они могут использовать их в качестве источника заражения — например, через открытые для общего доступа сетевые ресурсы.

Более того, на данный момент есть тенденция роста количества вредоносных программ для этих ОС. Фактически их незащищенность провоцирует злоумышленников на поиск путей заражения.

Защита этих операционных систем осложнена невозможностью реализации полноценной системы самозащиты, в связи с чем вредоносная программа, проникшая на такие машины, получает очень большие возможности.

Вторым по важности узлом сети являются файловые серверы, к которым в связи с одинаковым подходом к обеспечению антивирусной защиты также относятся серверы баз данных, терминальные серверы и т. д. Здесь в первую очередь необходимо отметить разницу в обеспечении антивирусной защиты серверов, работающих под управлением ОС Windows и ОС типа Unix. В первом случае защита доступных пользователю областей сервера совмещается с защитой всей файловой системы, во втором защита файловой системы и папок, доступных пользователю, осуществляется разными продуктами.

Необходимо отметить, что реализация защиты на уровне файловой системы не обеспечивает защиты проходящей почты, обрабатываемой почтовыми серверами, содержимого баз данных различных сервисов и т. д. Антивирусные продукты не способны лечить базы данных.

После установки антивирусной защиты серверов необходимо также произвести их настройку. В первую очередь рекомендуется исключить из проверки часто проверяемые области файловой системы — базы данных, объекты, к которым постоянно обращаются работающие сервисы. При этом должен соблюдаться баланс между быстродействием и безопасностью.

Важно отметить, что защита файловых серверов на данный момент является необходимостью в связи с тем, что наиболее опасные вредоносные программы, в том числе направленные на хищения денежных средств, после заражения рабочих станций осуществляют сканирование сети и попытки заражения серверов — в том числе с целью проникновения на банкоматы и терминалы.

Защита банкоматов и терминалов фактически должна повторять систему защиты файловых серверов и включать, помимо файлового антивируса, также файервол, систему проверки интернет-трафика, а также систему ограничения доступа (офисный контроль).

Почтовые серверы (точнее, почтовые сервисы) оснащаются защитой гораздо реже, чем вышеперечисленные узлы сети. Это связано в первую очередь с тем, что компании считают достаточным иметь защиту почты на уровне рабочих станций. Это является типичной ошибкой. Дело в том, что решения для защиты почтовых серверов имеют в своем составе функционал периодической проверки почтовых баз, а также функцию проверки почты при обращении. Данный функционал позволяет удалить из почтовых папок пользователей ранее неизвестные вредоносные программы. Наличие данного функционала критично при реализации в компании технологии BYOD, при которой сотрудники используют для работы собственные устройства. Функционал гарантирует непопадание известного вредоносного ПО на незащищенные личные устройства.

Необходимо отметить, что большинство решений для защиты почтовых сервисов действует в режиме плагинов к соответствующим программам (Kerio, Lotus, Exchange и т. д.). Это достаточно сильно ограничивает возможности по антивирусной проверке сообщений. Вплоть до того, что антивирусные плагины проверяют сообщения по частям — в том виде, в каком они их получают от почтового сервиса. Гораздо больше возможностей получают решения, реализуемые в форме почтового шлюза. В данном случае антивирус имеет доступ непосредственно к процедуре приема и передачи сообщения, может выявлять отклонения от известных протоколов передачи, проверять подлинность отправителей и получателей и т. д.

Как правило, такие почтовые шлюзы реализуются в виде решений на базе ОС Unix,

а также в виде программно-аппаратных решений.

Необходимо отметить, что сами сотрудники компаний и организаций используют платные и бесплатные облачные сервисы — почтовые, хранения документов и т. д. (google.docs, google.mail, google.disk и аналогичные) в обход почтовых серверов организации, в результате чего доступ к ним не контролируется системами безопасности компании. Использование данных сервисов также несет определенные риски. Наличие антивирусных почтовых шлюзов позволяет проверять (при возможности проверки защищенных протоколов) также и этот трафик.

Еще одним сильно недооцененным решением антивирусной защиты является антивирусный шлюз. Его функционал также сильно похож на функционал проверки трафика в решениях для рабочих станций, и аналогично системам для защиты почты им пренебрегают. Однако назначение системы защиты на уровне шлюзов совершенно иное. Такая защита обеспечивает безопасность тех устройств и компьютеров, установка системы защиты на которые по тем или иным причинам невозможна.

В отношении организации локальной сети необходимо отметить возможность использования в ней так называемых облачных сервисов. Вопреки общему мнению внедрение облачных сервисов существенно увеличивает ряд рисков, связанных с информационной безопасностью. В первую очередь перенос инфраструктуры из контролируемого системой безопасности компании периметра во внешнюю среду вызывает соответствующий рост рисков:

- доступа к корпоративным данным на удаленных серверах (со стороны сотрудников подрядчика, злоумышленников, вредоносных программ, в том числе проникших через виртуальные машины, не имеющие адекватной защиты);
- перехвата и модификации информации во время ее передачи с удаленных серверов и на них;
- возможности отказа удаленной инфраструктуры или потери доступа к ней.

В связи с этим при использовании облачных сервисов необходимо предусматривать меры, противодействующие:

- получению доступа, хищению и/или модификации данных на удаленных серверах, а также во время передачи данных между удаленными серверами и серверами и рабочими станциями, находящимися в локальной сети компании;
- внедрению вредоносных программ на удаленные серверы и во время передачи данных;
- простоям на время отсутствия доступа к удаленным серверам.

В качестве таких мер могут быть использованы:

- системы шифрования, а также системы создания каналов VPN;
- почтовые шлюзы на стороне ЦОД и на стороне локальной сети или локальные почтовые серверы, проверяющие входящую почту и накапливающие почтовые сообщения во время отсутствия доступа к ЦОД;
- файловые серверы и сервисы, синхронизирующие содержание с удаленными серверами.

В связи с этим всегда и для любой компании можно предлагать как минимум защиту рабочих станций, почтовых серверов и интернет-шлюза — но нужно учесть, что любое такое предложение должно быть обосновано ссылками на положения законодательства или факты, указывающие на недостаточность частичной защиты. При этом желательно выяснять реальный состав используемых серверов и рабочих станций — в том числе и тех, защита которых клиентом на данный момент не предполагается.

Заключение

В качестве вывода отметим следующее.

1. Антивирусная подсистема (именно как система обнаружения вредоносных файлов и их обработки) должна рассматриваться не только (и даже не столько) как система,

предотвращающая попадание вредоносных программ в локальную сеть (как показывает практика, эту роль могут выполнять и иные решения), но в первую очередь как система лечения уже активных заражений. Кроме антивируса, эту задачу не может выполнить никто (удаление вредоносных файлов в ручном режиме в качестве меры противодействия рассматривать нельзя в связи с отсутствием нужного количества специалистов). При этом:

а) антивирусное решение должно иметь систему сбора информации, позволяющую максимально быстро передавать в антивирусную лабораторию всю необходимую для решения проблемы информацию. Должен быть исключен случай, когда в каждом случае заражения необходимую информацию нужно собирать вручную — в том числе и на удаленных рабочих станциях и серверах;

б) используемое антивирусное решение должно иметь систему самозащиты, не позволяющую неизвестной вредоносной программе нарушить нормальную работу антивируса, — тот должен нормально функционировать до поступления обновления, позволяющего пролечить заражение;

в) система управления антивирусной защитой должна обеспечивать максимально быстрое получение обновлений защищаемыми рабочими станциями и серверами — антивирусные агенты должны быть по возможности постоянно подключены к серверу защиты;

г) как система управления, так и система обновления антивирусного решения должны быть независимы от соответствующих механизмов, используемых в операционных системах, и включены в систему самозащиты антивируса, что позволяет исключить возможность перехвата системы обновления вредоносной программой. Недопустимо использование антивирусом системных компонентов, не помещаемых под защиту системы самозащиты;

д) используемое антивирусное решение должно уметь лечить не только поступающие (неактивные) вредоносные программы, но и уже запущенные — ранее неизвестные.

2. Антивирусная система не должна использовать компоненты, которые так или иначе могут быть скомпрометированы и использованы злоумышленниками для заражения защищаемой системы.

3. Используемое антивирусное решение должно проверять все поступающие из локальной сети файлы до момента получения их используемыми приложениями, что исключает использование вредоносными приложениями неизвестных уязвимостей данных приложений.

4. С целью защиты от проникновения неизвестных на момент заражения вредоносных программ антивирусное решение должно дополняться:

а) персональным брандмауэром, обеспечивающим невозможность сканирования локальной сети, а также защиту от внутрисетевых атак;

б) системой ограничения доступа к сменным носителям и внутрисетевым ресурсам;

в) централизованной системой периодического сканирования на отсутствие неактивных вредоносных программ и известных уязвимостей.

В ходе выбора системы антивирусной защиты могут использоваться исключительно тесты на совместимость с используемым ПО, на обнаружение активных заражений, а также на самозащиту. Остальные существующие виды тестов (в том числе тесты на больших коллекциях и динамические тесты) не отражают возможности, которыми должна обладать система защиты.

Список литературы

1. *Безруков Н. Н.* Компьютерная вирусология. Киев: УРЕ, 1991. URL: http://vx.netlux.org/lib/anb00.html
2. *Белоусов С. А., Гуц А. К., Планков М. С.* Троянские кони. Принципы работы и методы защиты. Омск: Наследие: Диалог-Сибирь 2003. — 33 с.
3. Вирусы и средства борьбы с ними. Учебный курс. URL: www.intuit.ru
4. *Гульев И. А.* Компьютерные вирусы. Взгляд изнутри. М.: ДМК, 1999. — 304 с.
5. *Исаева Е. В.* Специфика формирования терминосистемы компьютерной вирусологии. URL: http://

cyberleninka.ru/article/n/spetsifika-formirovaniya-terminosistemy-kompyuternoy-virusologii6
6. *Касперский Е. В.* Компьютерные вирусы в MSDOS. М.: Эдель, 1992. — 175 с.
7. *Касперский Е. В.* Компьютерные вирусы, что это такое и как с ними бороться. М.: Издательство «СК Пресс», 1998. — 288 с.
8. *Касперски Крис.* Азбука хакера 3. Компьютерная вирусология. М.: Майор, 2006. — 512 с.
9. *Касперски Крис.* Записки исследователя компьютерных вирусов. СПб: Питер, 2005. — 316 с.
10. Компьютерная контрразведка или кто следит за нами URL: http://www.zahist.narod.ru/analytic. htm
11. *Парфенов В. И.* Защита информации: Словарь. Воронеж: НП РЦИБ «Факел», 2003. — 292 с.

References

1. Bezrukov N. N. *Komp'juternaja virusologija* [Computer virology]. Kiev, URE Publ., 1991.
2. Belousov C. A., Guc A. K., Plankov M. S. *Trojanskie koni. Principy raboty i metody zashhity* [Principles of work and methods of protection]. Omsk: Nasledie: Dialog-Sibir' Publ., 2003. 33p.
3. *Virusy i sredstva bor'by s nimi. Uchebnyj kurs* [Viruses and means of fight against them. Training course]. URL: www.intuit.ru
4. Gul'ev I. A. *Komp'juternye virusy. Vzgljad iznutri* [Computer viruses. Look from within.]. Moscow, DMK Publ., 1999. 304 p.
5. Isaeva E. V. *Specifika formirovanija terminosistemy komp'juternoj virusologii* [Spetsifik of formation of a terminosistema of computer virology]. URL: http://cyberleninka.ru/article/n/spetsifika-formirovaniya-terminosistemy-kompyuternoy-virusologii
6. Kasperskij E. V. *Komp'juternye virusy v MSDOS* [Computer viruses in MSDOS]. Moscow, Jedel' Publ., 1992. 75 p.
7. Kasperskij E. V. *Komp'juternye virusy, chto jeto takoe i kak s nimi borot'sja*. [Computer viruses, what is it and as to struggle with them]. Moscow, Izdatel'stvo «CK Press», 1998. 288 p.
8. Kasperski Kris. *Azbuka hakera 3. Komp'juternaja virusologija* [Alphabet of the hacker 3. Computer virology]. Moscow, Major Publ., 2006. 512 p.
9. Kasperski Kris. *Zapiski issledovatelja komp'juternyh virusov* [Notes of the researcher of computer viruses]. Saint Petersburg, Piter Publ., 2005. 316 p.
10. *Komp'juternaja kontrrazvedka ili kto sledit za nami* [Computer counterintelligence or who watches us the]. URL: http://www.zahist.narod.ru/analytic. htm
11. Parfenov V. I. *Zashhita informacii: Slovar'* [Information security: Dictionary]. Voronezh, NP RCIB «Fakel», 2003. 292 p.

V. Medvedev, *Doctor Web, Ltd., Moscow, Russia, v.medvedev@drweb.com*

Possibility of working out requirements for the protection system against malware

Although, both malware and security software already exists for several decades, there are still no correct definitions for «malware» and «anti-virus».

Sometimes existing standards and regulators' documents show completely opposite approach to terminology in this field. A fundamental difference between «anti-virus» and «anti-virus protection system» has not been defined — as a result, the anti-virus is assigned functions which this subsystem cannot perform even theoretically.

Lack of proper terminology makes it impossible to work out the requirements to the anti-virus protection system in whole as well as its components — current standards contain points, which at least do not raise the level of security, but increase expanses of companies and organizations.

As a result, statistics shows that about 19 of 20 companies do not know anything either about the role of the anti-virus in security system or the requirements that must be met by products which are supposed to use — when drawing up requirements for the anti-virus subsystem, IT specialists rely on set myths (e.g., claiming that all malware is created by anti-virus authors).

This paper attempts to develop requirements for the anti-virus protection system and directly to the anti-virus as a part of the anti-virus protection system. The proposed requirements will allow companies and home users to implement a reliable protection against the latest threats.

Keywords: terms and definitions, anti-virus, malware, information security, standards, recommendations.

For citation: Medvedev V. Possibility of working out requirements for the protection system against malware. *Prikladnaya Informatika* — Journal of Applied Informatics, 2015, vol. 10, no. 3 (57), pp. 76–87 (in Russian).