УДК 621.316

Печатается в порядке обсуждения

ЗАЩИТА ИНФОРМАЦИИ, ПЕРЕДАВАЕМОЙ ПО СЕТЯМ СВЯЗИ ОТКРЫТОГО ДОСТУПА

В. О. Шварцман, д.т.н.

Ключевые слова: *вирусные атаки, антивирусные устройства, информационная безопасность.*

Сегодня системы защиты информации и сетей связи от вирусных атак базируются на использовании антивирусных устройств, которые обнаруживают вирусы и по возможности уничтожают их. Исследования последних лет показали, что эффективность этих устройств весьма мала: они уничтожают только 20 % вирусов новых типов, причем просматривается тенденция к уменьшению этой величины. Кроме того, как следует из названия этих устройств, они рассчитаны только на борьбу с вирусами, между тем, как имеют место другие искажающие и мешающие факторы. Естественно возникает вопрос, почему такое противоестественное состояние с обеспечением информационной безопасности (ИБ) сетей связи и передаваемой по ним информации от воздействия вирусных атак существует многие годы, и почему никто не задает этого вопроса и не старается получить на него ответа?

Причины создавшегося положения. Существует несколько причин создавшегося положения. Основная — отсутствие до настоящего времени утвержденной количественной характеристики защищенности информации. А ведь такая характеристика предложена в [3]. Отсутствие этой характеристики и методики ее измерения в течение многих лет не позволяет судить об истинном положении дел в сфере информационной безопасности.

Важной причиной создавшегося положения является и то, что фирмы, осуществляющие защиту информации от вирусных атак, гарантируют своим заказчикам обеспечение «полной», «необходимой», «достаточной», «требуемой» защиты, зачастую не имея представления о том, насколько реально эффективны используемые ими методики и средства защиты. В результате у заказчиков возникает порой необоснованное состояние «самоуспокоенности». И кроме того, как в нашей стране, так и за рубежом, фирмы — владельцы информации часто скрывают ее потери от вирусных атак, опасаясь за свой престиж в глазах пользователей.

Такое ненормальное положение имеет место до сих пор, несмотря на то, что по сетям открытого доступа передается значительная часть всей передаваемой в стране информации, в том числе служебной.

Рассмотрим главную причину. Для этого выясним, почему до сих пор отсутствует количественная характеристика реальной величины степени защищенности от вирусов и других негативных факторов сетей связи. Для этого обратимся к директивным документам по данному вопросу.

В «Законе о связи» (2003 г.) сказано: «Федеральный орган исполнительной власти в области связи устанавливает требования к сетям электросвязи в отношении их защиты от несанкционированного доступа (НСД) и передаваемой посредством их информации».

Согласно утвержденному в 2004 г. «Положению о Министерстве информационных технологий и связи РФ» (сегодня Министерство связи и массовых коммуникаций РФ), на этот федеральный орган исполнительной власти возлагаются функции по выработке государственной политики и нормативное правовое регулирование в сфере информационных технологий и связи.

Согласно «Положению о Федеральном агентстве связи» в его полномочия входит размещение заказов на проведение НИР для государственных нужд в установленной сфере деятельности.

Таким образом, Минкомсвязи и его Федеральное агентство связи несут ответственность за комплекс требований к системам и сетям связи в отношении их защиты от НСД, а также за заказы на проведение соответствующих НИР по данной проблеме.

Эти общие положения конкретизированы в национальном стандарте РФ ГОСТ Р 52448 (2005 г): «Сеть электросвязи должна обеспечивать целостность передаваемых сообщений и своевременность их доставки адресату». Там же указано, что обеспечение безопасности сетей связи, в соответствии с установленными стандартами, возлагается на ее владельца и осуществляется его силами и средствами. Но ведь для того, чтобы министерство могло устанавливать нормы на ИБ для сетей и информации, необходимо иметь количественный показатель ИБ, который следует нормировать. А он до настоящего времени не утвержден, хотя предложения, касающиеся установления такого показателя, давно опубликованы [1—4].

По-видимому, такое положение вызвано тем, что задания на разработку такого показателя не было выдано, либо оно не было выполнено. Именно отсутствие утвержденной количественной характеристики ИБ и норм на ее допустимое значение не позволяет владельцам информации согласовывать с владельцами сетей связи свои требования в отношении качества защиты сетей от вирусных атак. Сложность этого согласования для владельца сети вызвана тем, что разные владельцы информации выдвигают различные требования по качеству и стоимости услуг, а реализовать их весьма непросто, особенно в условиях отсутствия утвержденных норм на ИБ. Да и работы по обеспечению ИБ владелец сети должен выполнять за свой счет и своими силами.

Эти трудности усугубляются и тем, что отдельные участки сети открытого доступа используются в качестве вставок в корпоративные сети. В результате оказывается, что ни владелец информации, ни владелец сети, ни оператор системы, ни получатель информации, ни заказчик системы ИБ, ни организация, контролирующая ИБ системы, не знают, каково же реальное состояние с защищенностью от вирусных атак.

Очевидно, что назрела острая необходимость в разработке и утверждении подзаконных актов, содержащих подробные указания о порядке разработки и нормирования характеристик защищенности сетей и информации от вирусных атак.

С появлением такого показателя и методики его измерения [3, 4] представляется возможность провести измерения величины защищенности систем связи от вирусов и дать обоснованный ответ на вопрос о состоянии информационной безопасности систем связи сегодня.

Предложенная характеристика величины ИБ сети и информации от вирусных атак позволяет количественно определить эффективность систем защиты информации от вирусов и разработать принципы функционирования устройства непрерывного контроля состояния информации с позиций ее защищенности.

Устройство непрерывного контроля с расширенными возможностями. Исследования показали, что предлагаемое устройство, кроме своей основной функции, указанной выше, должно выполнять ряд дополнительных функций. Поэтому такое устройство будем называть многоцелевым. Оно позволит:

- оценивать величину защищенности информации от влияния таких непреднамеренных влияний, как хроматическая дисперсия, попутный поток и др.;
- определять, какое из вышеуказанных явлений вызывает снижение достоверности и до какого уровня;
- определять место возникновения причины снижения достоверности — в информации или в сети.

Проведенные исследования показали, что многоцелевое устройство отличается от общепринятых устройств для измерения уровня сигналов рядом дополнительных функций. Это вызвано тем, что многоцелевое устройство действует в условиях влияния на сети связи не одного фактора (полезного сигнала или вирусной атаки), а целого ряда непреднамеренных мешающих воздействий и суммы некоторых из них. Такими воздействиями могут быть попутный поток — ПП, хроматическая дисперсия — ХД, поляризованная модовая дисперсия, вирусы.

В случаях, когда система контроля показывает снижение достоверности передачи в канале, необходимо знать, что является причиной снижения достоверности. Разработанная методика решения этой задачи включает три этапа: первый заключается в определении того вида помех и искажений, которые предполагается обнаруживать; второй — в определении признаков, присущих принимаемым сигналам; третий — в отнесении искажений к определенному классу помех и искажений или к непреднамеренным воздействиям.

Для владельца сообщения и оператора сети причины снижения достоверности и определение мест их возникновения облегчают выявление местонахождения злоумышленников.

Предложенные универсальное устройство и методика контроля достоверности получаемой информации должны обслуживать множество пользователей, и поэтому целесообразно создавать устройство не в виде персональных подсистем, а включать его в состав компонентов единой системы контроля и управления, которые в настоящее время отслеживают выполнение ряда других характеристик качества услуг: времени задержки пакетов и ячеек, времени установления соединения и т. п. Конечно, при этом не исключено создание устройств индивидуального пользования, например, для владельцев наиболее важных систем связи.

Поскольку нет необходимости устанавливать требования к степени защищенности информации и сетей от вирусов более жесткими, чем нормы на защищенность от непреднамеренных воздействий, можно рекомендовать, чтобы между этими нормами имелось такое соотношение: например, если норма достоверности принята 10^{-6}, то норму на защищенность от НСД можно рекомендовать $0{,}5 \cdot 10^{-6}$–10^{-7}. Такие нормы можно рекомендовать владельцам информации при согласовании требований к защищенности информации и сетей связи с операторами сетей связи.

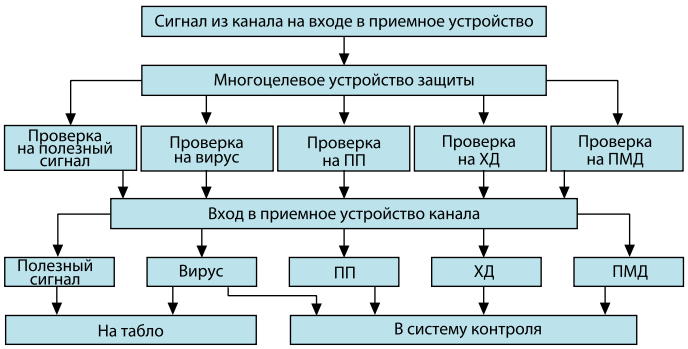
Принципы работы многоцелевого устройства. Основной принцип заключается в том, что многоцелевое устройство включается в анализируемую сеть и измеряет уровень сигнала на входе в приемное устройство. Далее устройство анализирует этот сигнал (полезный сигнал, вирусная атака, та или иная несанкционированная помеха).

Все измерения устройство осуществляет последовательно и автоматически, что позволяет оператору установить, относятся ли они к вирусу или нет. Если результаты показывают наличие вируса, то оператор получает сигнал о произведенных измерениях его величины. В других случаях — сигнал о том, что результаты измерений относятся к тому или иному виду непреднамеренных воздействий.

Алгоритм работы анализатора позволяет оператору определить, к какому классу относится измеренная величина: к вирусам, к полезному сигналу или непреднамеренным искажениям.

Отметим, что многоцелевое устройство может кроме предоставления вышеизложенных услуг выполнять и другие важные функции, например, определять место нахождения причины снижения достоверности: в сети, в устройствах сети или непосредственно в информации.

Структурная схема прохождения сигналов через универсальное устройство показана на рисунке.



Введение в устройство всех отмеченных алгоритмов повысит величину защищенности сетей связи и передаваемой по ним информации. Следует иметь ввиду, что технология антивирусной защиты сетей связи открытого доступа и передаваемой по ним информации включает три этапа: первый — проверка уязвимости рассматриваемых сетей; второй — локализация и приостановление распространения вирусов до того, как будет введена в действие система их уничтожения; третий — само устранение вирусов. Далее предусматривается удаление антивирусным устройством следов проникновения в систему вирусов, которые остаются после чистки.

Рассмотренное выше устройство использует новые алгоритмы, и поэтому при его разработке следует по возможности учитывать имеющиеся подобные устройства или их компоненты. Весьма полезно использовать многочисленные разработки устройств контроля появления в сети вирусных атак, антивирусов, устройств управления системами связи и ряда других. Такого вида устройства выпускаются отечественной и зарубежной промышленностью. Сведения о них можно найти, например в [5, 6, 10] и многих других источниках.

Пути выхода из создавшегося положения. На основании вышеизложенного, можно заключить, что положение с защитой сетей связи открытого доступа и передаваемой по ним информации считается неудовлетворительным. Для иллюстрации этого приведем высказывание крупнейшего специалиста в области защиты информации Е. Касперского. Оценивая сложившуюся ситуацию, на вопрос: «неужели проблема компьютерной преступности неразрешима?» он ответил так: «Выход есть — это полная идентификация пользователей сети. Необходимо, чтобы, входя в Интернет, пользователь вставил в компьютер пластиковую карту и ввел пин-код. Тогда при необходимости можно будет найти злоумышленника и привлечь его к ответственности. Реализация такого проекта будет стоить очень дорого, но к этому все равно придут». Однако предложение Е. Касперского направлено не на непосредственную защиту информации и сетей, а на выявление злоумышленников, вводящих вирусы в канал связи. Такое предложение должно заставить злоумышленника задуматься о последствиях для него раскрытия его адреса. И в этом отношении оно заслуживает внимания.

Между тем это предложение действенно только в том случае, если в роли злоумышленника выступает человек, которого можно найти и привлечь к ответственности. Но он может быть недосягаем, если его действия относятся лишь к дистан-

ционному управлению вводом вирусов в каналы связи, а непосредственный их ввод осуществляется автоматически.

Естественно возникает вопрос, что же делать в создавшейся ситуации, есть ли какой-нибудь выход из нее? В процессе ответа на этот вопрос следует рассмотреть еще один вариант решения, который предложен д. т.н., проф. А. Ю. Щегловым. Это — принцип проверки импульсной последовательности, поступающей на вход приемного устройства на наличие специального «разрешения». Теория этой системы изложена в [6], где со ссылкой на сообщение на сайте (www.it.sec от 24.07.2006 г) Г. Ингрема, главного управляющего австралийского подразделения Группы оперативного реагирования на чрезвычайные ситуации в компьютерной области (Aus CERT), говорится, что распространенные антивирусные средства блокируют лишь около 20 % недавно появившихся вирусных атак. А что будет при более сложных атаках? Особенно с учетом того, что средства нападения (в том числе вирусы) развиваются быстрее, чем средства защиты.

В статье А. Г. Щеглова со ссылкой на публикацию от 01.02.2006 г на сайте www.it.sec указывается, что компания Ernst@Young провела ежегодный глобальный опрос руководителей ИТ-компаний о проблемах ИБ и выпустила очередную, восьмую версию своего ежегодного отчета «Global Information Security 2005». В опросе принимали участие топ-менеджеры более 1,3 тыс. коммерческих и государственных организаций из 55 стран мира, включая Россию. Основную массу респондентов составили директора информационных служб и отделов IT-безопасности.

Самым значительным выводом этого исследования стал тот, что пропасть между угрозами IT-безопасности и мерами защиты от них стала еще шире!

Автор цитируемой статьи делает заключение относительно бессмысленности использования для защиты компьютера установки на его входе любого средства, фильтрующего сетевой трафик. Он предлагает вход в него ограничить только теми программами, которые отнесены к санкционированным. Именно реализации технологии этого предложения посвящено основное внимание в цитируемой статье.

Заметим, что принципиальное отличие предлагаемого метода защиты от используемых, заключается в том, что она производится не в оконечном устройстве, а на его входе, где вирусы опознаются и не пропускаются в оконечное устройство. Таким образом, возникла противоречивая и опасная ситуация: с одной стороны, многие годы для защиты информации в сетях связи от вирусов используют принятые методику и устройства, а с другой — появилась информация об их практической несостоятельности.

Естественно возникают следующие вопросы:

- насколько обоснованы выводы авторитетных международных организаций?
- почему многочисленные владельцы и операторы традиционных систем и устройств защиты информации, а также поставщики систем защиты не обращали внимание на очень высокий процент (80 %) поражаемой информации?
- может быть, вышеизложенное относится только к каким-то новым типам вирусов?
- распространяется ли выявившаяся ситуация не только на безопасность информации, но и на безопасность сетей связи?
- какое же положение в этой сфере существует сегодня?

Представляется, что разрешить эту опасную ситуацию можно только путем экспериментальной, сравнительной проверки эффективности традиционной методики и устройств защиты информации от вирусов с предложением, приведенным в цитируемой статье.

Достоинства предложенной автором статьи методики заключаются в том, что она базируется на принципиально новом подходе — непрерывном контроле передачи сообщений. Тем самым методика свободна от недостатков существующих способов обнаружения действия НСД, которые показали в последнее время низкий процент (20 %) защиты от новых видов вирусов.

Кроме того, методика позволяет:

- определить количественную величину степени защищенности линий связи и передаваемой по ним информации, что было недоступно ни одной из существующих систем контроля. Это коренным образом изменяет существующее положение, при котором было неизвестно истинное состояние сетей и систем связи в отношении их защищенности от НСД и истинная эффективность систем и средств связи в отношении их возможностей;
- вычислить реальную степень защищенности сетей и информации от действия как вирусов, так и преднамеренных искажающих факторов –попутного потока, хроматической дисперсии, поляризационной модовой дисперсии, а может быть и от других негативных воздействий (это покажут дальнейшие исследования);
- определить, где находится источник снижения защищенности;
- непрерывно контролировать появление вирусных и других атак и выдавать соответствующие сигналы в систему управления;
- устанавливать нормы на величину защищенности, характеризующие требуемую степень защиты от НСД;
- своевременно, с помощью системы управления, принимать меры по ликвидации последствий различных помех, искажений и НСД.

Следует отметить, что предложенная методика особенно актуальна в связи с опубликованными новыми данными о низкой эффективности действующих методик защиты информации от вирусных атак.

Заключение. Проведенные теоретические исследования позволяют сделать следующие выводы:

- существующая система и средства защиты сетей и информации от вирусов обеспечивают защиту только в 20 % случаев, что совершенно недостаточно;
- основная причина создавшегося положения — отсутствие утвержденных показателей реальной величины защищенности сетей и информации в результате чего неизвестно положение дел в этой области;
- предложенные в данной статье подходы оценки ИБ позволяют выявить реальное количественное положение с реальной защищенностью сетей и информации.

ЛИТЕРАТУРА

1. **Шварцман В. О.** Информационная безопасность систем и сетей передачи данных общего пользования//Вестник связи. — 2005. — № 12.
2. **Шварцман В. О.** Актуальные вопросы теории и практики обеспечения информационной безопасности систем (сетей) общего пользования//Электросвязь. — 2007. — № 4.
3. **Шварцман В. О.** Методика количественной оценки защищенности информации от вирусов//Электросвязь. — 2007. — № 9.
4. **Шварцман В. О.** Количественная оценка защищенности информации и сетей связи от несанкционированных действий//Электросвязь. — 2008. — № 5.
5. «Антивирус Касперского»//Аргументы и факты. — 2008. — № 1—2.
6. **Щеглов А. Ю.** Защита компьютера от сетевых атак//Информост. — 2007. — № 3.

Получено 26.03.09.