Висновки. Галузь телекомунікацій готова до впровадження запропонованої концепції інформаційної безпеки при умові вирішення таких проблем: врахування загроз антропогенного характеру, а не лише загроз телекомунікаціям техногенного й природного характеру, тобто врахувати загрози «людського фактору» та від потенційних противників; створення системи інформаційної безпеки та служби інформаційної безпеки ТМЗК (наприклад, в системі технічної експлуатації) та визначення її функцій згідно чинних нормативно-правових документів системи ТЗІ.

Напрямом подальшої роботи може бути дослідження оцінки економічної ефективності впровадження концепції інформаційної безпеки, розробка політики інформаційної безпеки та розробка методів оцінки досягнутого рівня захищеності інформаційних ресурсів ТМЗК.

Список літератури:

1. Тардаскін М.Ф., Кононович В.Г., Вараксін О.О., Тардаскіна Т.М. Механізми забезпечення інформаційної безпеки телекомунікаційних мереж загального користування // Зв'язок. – 2005.- № 7 - 8. – С. 30-35.

2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» в редакції від 31 травня 2005 року, № 2599-IV.

3. "Концепція технічного захисту інформації в галузі зв'язку України", від 24.09.1999 р.

4 Леваков А. Анатомия информационной безопасности США. Jet Info online #6(109), 2002, http://daily.sec.ru/dailypblshow.cfm?rid=9&pid=5503&pos=13&stp=10. – С. 74.

5. Ліцензійні умови провадження діяльності у сфері телекомунікацій з надання послуг фіксованого міжнародного міжміського, місцевого зв'язку з правом технічного обслуговування та експлуатації телекомунікаційних мереж і надання в користування каналів електрозв'язку. Наказ Держкомзв'язку та інформатизації України від 17.06.2004 № 132. – С.25.

6. Ліцензійні умови провадження діяльності у сфері телекомунікацій з технічного обслуговування і експлуатації мереж ефірного теле- та радіомовлення та телемереж, надання в користування каналів електрозв'язку. Наказ Міністерства транспорту та зв'язку України від 10.11.200, № 984. – С.20.

7. ITU-T Recommendation X.805. Security architecture for system providing end-to-end communications. – С. 28.

УДК 681.003.4

В.В.Овсянников

ЗАЩИТА ИНФОРМАЦИИ ОТ АТАК ИЗ ИНТЕРНЕТ

Чтобы справиться со стремительно нарастающим потоком информации, вызванным научно-техническим прогрессом, субъекты предпринимательской деятельности, организации вынуждены постоянно пополнять свой арсенал различными техническими средствами и системами, предназначенными для приема, передачи, обработки и хранения информации. При этом следует учитывать, что главными носителями информации являются:

- знающие люди;
- документы;
- средства беспроводной и проводной связи;
- электронные системы обработки информации;
- разные отслеживаемые факторы (поведение, разговоры, результаты действий).

Центральной проблемой защиты информации является проблема защиты от несанкционированного доступа. Всем известен тезис, что главную угрозу для информации представляют собственные сотрудники. На основании этого тезиса некоторые пессимисты делают вывод о том, что не стоит предпринимать какие-либо шаги, в силу их бесполезности. На самом деле бесполезным в защите информации является только формальное выполнение

отдельных требований, вместо осмысления - каким образом циркулирует в организации информация с ограниченным доступом, понимания возможных каналов ее утечки и принятия разумных мер защиты.

Методы и средства несанкционированного получения информации из корпоративной сети (КС) можно классифицировать, исходя из разных признаков: по виду доступа, по уровню доступа, по характеру действий злоумышленника, по многократности доступа, по направленности действий злоумышленника, по тяжести последствий.

По виду доступа все методы и средства можно разделить на две большие группы. К первой группе относятся методы и средства, используемые при локальном (физическом) доступе к КС, а по второй – методы и средства, используемые при удаленном доступе (по компьютерной сети). Как правило, любая, даже самая надежная КС при наличии злоумышленника локального доступа, достаточных сил и средств и достаточного времени, не сможет обеспечить сохранности информации. При удаленном доступе КС может быть достаточно надежно защищена, но, с другой стороны, абсолютной безопасности КС, имеющей физическое подключение к сетчм передачи данных, гарантировать также нельзя.

По уровню доступа методы и средства несанкционированного получения информации обычно разделяют на методы и средства гостевого, пользовательского, административного, системного и неограниченного уровня. Во многих современных операционных системах имеются встроенные учетные записи, которые предоставляют их владельцам все перечисленные выше уровни доступа. При создании дополнительных учетных записей в большинстве современных операционных систем можно указать любой уровень доступа, но изменять его для встроенных учетных записей зачастую невозможно.

По характеру действий злоумышленника используемые им методы и средства могут быть направлены на копирование, модификацию, уничтожение или внедрение информации. В последнем случае появляется особенность КС, отсутствующая у традиционных средств накопления информации, связанная с тем, что в КС хранятся не только данные, но и программные средства, обеспечивающие их обработку и обмен информацией. Эта особенность интенсивно используется злоумышленниками, которые часто стремятся получить доступ к той или иной КС не ради несанкционированного доступа и хранящейся в ней информации, а для внедрения программной закладки, т.е. для несанкционированного создания в КС новой информации, представляющей собой активный компонент самой КС, либо для скрытого хранения собственной информации без ведома владельца КС.

По многократности доступа выделяют методы и средства, направленные на разовое получение несанкционированного доступа и многократное.

По направленности действий злоумышленника методы и средства несанкционированного получения информации из КС подразделяются на методы и средства, направленные на получение системной информации и собственно прикладной информации. Многих злоумышленников, проникающих в КС, подключенные к глобальным сетям, вообще не интересует хранящаяся в этих КС прикладная информация или интересует лишь в той степени, в какой она позволяет получить доступ к системной информации. Обычно такие злоумышленники используют подобные КС в качестве промежуточных узлов для проникновения в другие КС.

По тяжести последствий используемые злоумышленниками методы и средства несанкционированного получения информации можно разделить на неопасные, потенциально опасные, опасные и чрезвычайно опасные.

Если доступ к компьютеру строго регламентирован, но жесткий диск выделен в общее пользование в локальной сети, то информация может быть бесконтрольно считана из любого места в этой сети. Соответственно, и приобрести такую информацию для ваших конкурентов становится проще и дешевле. Иногда мы сами отдаем ценнейшую информацию в руки злоумышленников. Например, можно передать компьютер в ремонт, оставив при этом жесткий диск с информацией ограниченного доступа.

Но настоящая опасность подстерегает вашу информацию, когда компьютер, на жестком

диске которого она хранится, подключается к сети Интернет. Информация с жесткого диска может быть считана или уничтожена из любой точки земного шара. И дело тут не в уникальных умственных способностях хакеров, как это зачастую преподносится, а в том, что их в Интернете много, у них уйма свободного времени, и как все увлеченные люди они тратят его на поиски способов - как бы еще куда-нибудь забраться. Если нарушителю удается получить определенные права на каком-либо компьютере вашей сети, то он, как правило, сможет путешествовать по всей локальной сети от имени данного компьютера. Чаще же успешная атака завершается записью на жесткий диск специальной программы - «троянского коня», которая в дальнейшем и выполняет необходимые шпионские действия. Поэтому сейчас никого уже не удивишь такими мудреными словами, как «файервол» («брандмауэр»). В Солидных организациях это отдельное весьма дорогое устройство. В большинстве средних и даже малых офисов подключение к Интернет осуществляется через так называемый «Прокси-сервер» (сервер-посредник). Все современные прокси-сервера имеют развитые возможности файервола. Существуют также «персональные» файерволы, устанавливаемые на одиночных компьютерах. Весьма развитые функции файервола имеют даже операционные Системы, например, Windows-XP. Тем не менее, Интернет приносит очень много хлопот. Главная из них - это сложность настройки файервола, зачастую помноженная на отсутствие в организации четко определенных правил, какая информация все же может или не может поступать из Интернет и каким образом.

Не следует также забывать, что любой файервол это, по сути, специализированный компьютер, принципиально не отличающийся от любого другого компьютера в локальной сети. Поэтому существуют способы получения доступа к этому компьютеру, а дальше - как и не было файервола. Безусловно, захватить управление над операционной системой файервола значительно труднее, чем над операционной системой обычного компьютера. Но периодически находятся бреши в защите любого файервола. Производители выпускают новые патчи, и опять толпы хакеров бросаются искать новые бреши.

В серьезных системах обработка информации различной категории конфиденциальности осуществляется в отдельных изолированных друг от друга и, тем более, от Интернет, физически не связанных между собой сегментах локальной сети. При таком построении сети проблем с безопасностью почти не возникает.

Однако сейчас трудно представить себе деятельность любой организации без электронной почты. Выполняя требования по физическому разделению локальной сети и сети Интернет, приходится внедрять громоздкие схемы переноса информации между сетями с участием различных администраторов или устанавливать сотрудникам по два компьютера.

Для обеспечения защиты информации от атак из Интернет компания ЕПОС разработала специализированное автоматизированное рабочее место (АРМ «МЕЖА»), предназначенное для работы в двух физически разделенных сетях. Принцип защиты достаточно прост (см. рис. 1).

АРМ «МЕЖА» имеет, по крайней мере, два жестких диска и две сетевые карты. Питание на эти элементы подается от специального коммутатора. Управление коммутатором осуществляется - в простейшем случае (домашний компьютер) - обычным переключателем. В более серьезных решениях управление осуществляется с помощью ключа.

При работе в сети Интернет отключается питание от жесткого диска и сетевой карты, предназначенных для работы во внутренней локальной сети. При работе во внутренней локальной сети отключается питание от сетевой карты и жесткого диска, предназначенного для работы в сети Интернет. При таком построении работы в сети Интернет, даже в случае полного захвата управления операционной системой, нарушитель может видеть только «несекретный» жесткий диск, не содержащий важной информации.

Опыт применения АРМ «МЕЖА» в различных организациях показал высокую надежность защиты от атак из Интернет. Однако ориентированный на персональное

применение АРМ не всегда удобен для защиты корпоративных ресурсов. В частности, для защиты электронной почты необходимо, чтобы и почтовый сервер был физически отделен от сети Интернет. Таким образом, возникает задача автоматического переноса электронных почтовых сообщений из определенного почтового сервера сети Интернет в почтовый сервер, расположенный в локальной сети.

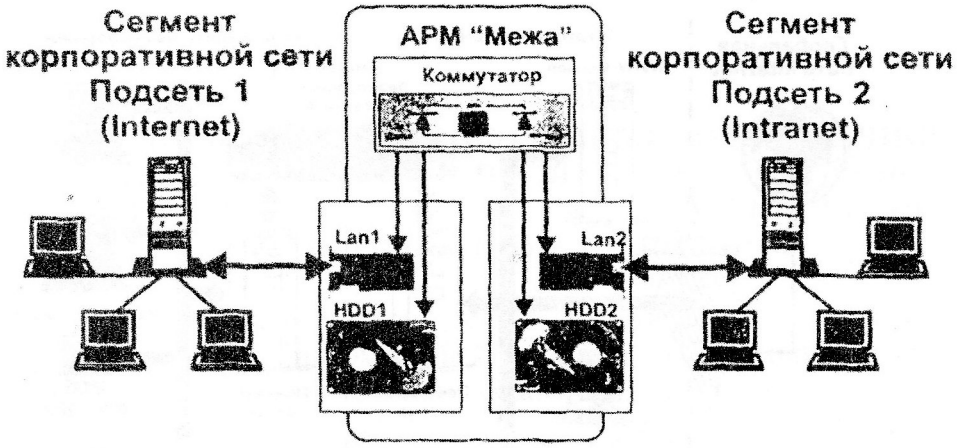

Рис. 1.Принцип работы АРМ «МЕЖА»

Для реализации данной задачи ЕПОС проводит работы по модернизации АРМ «МЕЖА» с целью реализации автоматического шлюза для переноса почтовых сообщений из сети Интернет в локальную сеть. Общий принцип построения остался практически таким же, как и раньше. Однако, теперь физическое подключение элементов (сетевых карт и жестких дисков) осуществляется под управлением специально разработанного микропроцессорного устройства - блока управления и регистрации. Блок управления и регистрации подключает поочередно одну из сетевых карт и соответствующий жесткий диск. После загрузки операционной системы управление передается специальной программе, осуществляющей почтовый обмен с заданным почтовым сервером. Почтовые сообщения проверяются на соответствие установленным в организации правилам разграничения доступа. Сетевое соединение с сервером защищается встроенным файерволом. Такое построение шлюза гарантирует, что в каждый момент времени шлюз подключен только к одной из сетей, т.е. сети остаются физически не объединенными.

Более того, жесткий диск с операционной системой аппаратно защищен от записи. Поэтому даже в случае, если нарушитель преодолеет защиту встроенного файервола и захватит управление операционной системой шлюза, он не в состоянии будет изменить содержимое жесткого диска. Нарушителю может быть доступна только информация, полученная с почтового сервера сети Интернет, которую проще получить непосредственно с почтового сервера. При следующем подключении к Интернет, поскольку операционная система грузится с защищенного от записи жесткого диска, результаты предыдущей атаки не влияют на безопасность работы.

Применение микропроцессорного блока управления и регистрации позволило решить еще одну важную для применения в корпоративных системах задачу: он выполняет функции встроенной аппаратной системы защиты от несанкционированного доступа, что позволяет применять такой шлюз как элемент комплексной защиты информации, в том числе и в автоматизированных системах государственных учреждений. Общий принцип построения сети при применении шлюза «МЕЖА-ША» показан на Рис.2.

Если автоматизированная система не подключена к Интернет, но в ней осуществляется

обработка информации с различным грифом секретности, то и в этом случае целесообразно разделить локальную сеть на ряд физически не связанных сегментов с различной политикой безопасности. Перенос информации между сегментами сети можно также осуществлять с помощью автоматических шлюзов «МЕЖА-ША» с проверкой выполнения правил разграничения доступа к информации, передаваемой из одного сегмента сети в другой (рис.3.)

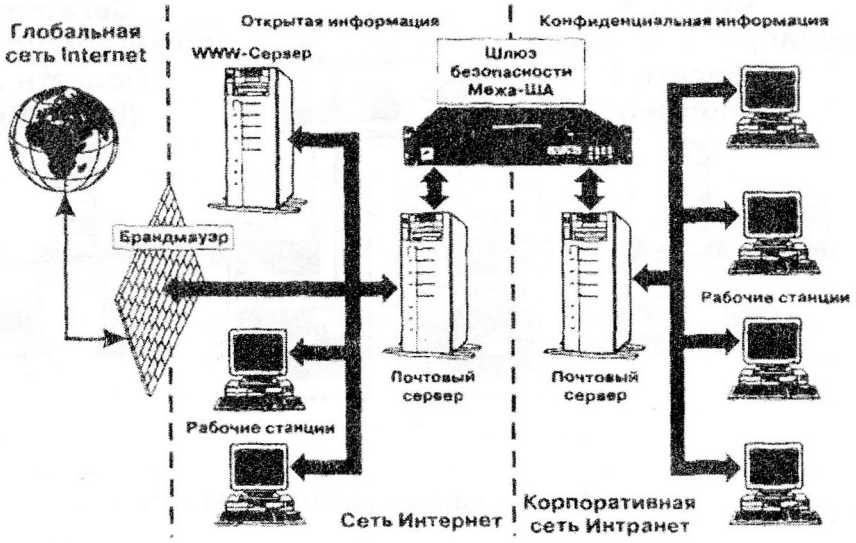

Рис. 2. Пример конфигурации сети с применением шлюза «МЕЖА-ША».

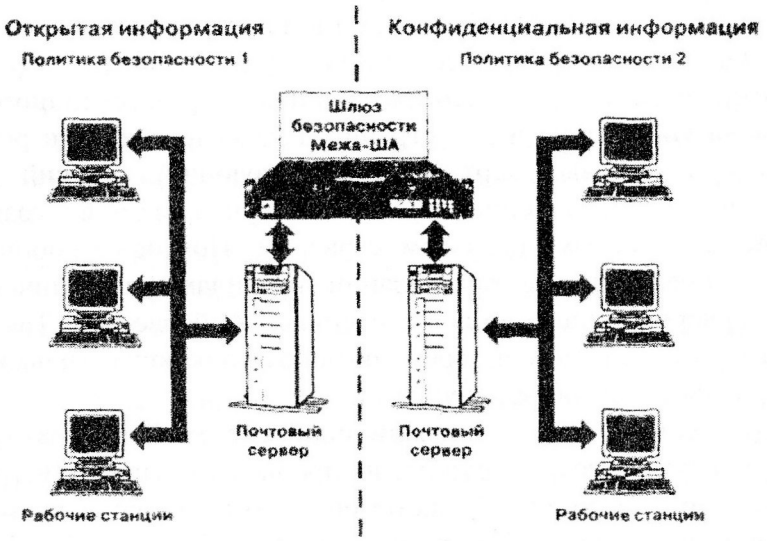

Рис. 3. Применение шлюза «МЕЖА-ША» в локальной сети.

Приведенные примеры показывают, что надежно защититься можно и от атак из сети Интернет. В настоящее время на рынке предлагается достаточно много надежных средств для решения конкретных проблем.

Единственная проблема, трудно поддающаяся решению - это непонимание того, что самая сложная техника не решает проблем защиты информации. Защита информации - это кропотливая повседневная работа, направленная на s непрерывный анализ всех изменений в составе сотрудников, изменении стоящих перед организацией задач, «залатывании» вновь обнаруженных брешей в своей системе защиты и т.д. И уж, тем более, недопустимо выделять какую-либо «главную задачу» и бросать все силы только на ее решение. Нельзя, например, бросать силы только на защиту от утечки информации по каналу ПЭМИН (за счет

собственных излучений компьютера), не уделяя должного внимания защите от несанкционированного доступа. Нельзя бросать все силы на защиту от атак из Интернет, не принимая мер по разграничению доступа к информации для своих сотрудников. Как бы лояльны и проверены не были ваши сотрудники, но исторический опыт показал, что самая конфиденциальная, жизненно важная информация иногда продается и за тридцать серебренников. И единственный путь уменьшить свои потери за счет утечки информации - это серьезное отношение к ее защите.

УДК 004.621

И.В.Васюков

СВЕДЕНИЕ НЕЛИНЕЙНОГО ВЗАИМНООДНОЗНАЧНОГО ПРЕОБРАЗОВАНИЯ В ПОЛЯХ ГАЛУА К СИСТЕМЕ АЛГЕБРАИЧЕСКИХ УРАВНЕНИЙ ДЛЯ РЕШЕНИЯ ЗАДАЧИ РАНДОМИЗАЦИИ СООБЩЕНИЙ.

Одним из направлений повышения криптостойкости систем, использующих блочные шифры с предварительной рандомизацией входных сообщений, является введение нелинейности между этапами рандомизации и собственно криптографического преобразования [1]. В качестве нелинейности можно выбрать операцию обращения элементов, поскольку для любого элемента x конечного поля обратный элемент y существует по определению (за исключением лишь нулевого элемента). При этом следует понимать, что элемент y является обратным по отношению к x в смысле равенства единице произведения этих элементов.

$$x \cdot y = 1 \tag{1}$$

Тогда процедура нахождения элемента

$$y = \frac{1}{x}$$

может состоять в решении уравнения (1) при известном x. Для аналитического описания векторов данных в задачах криптографии обычно используются полиномы над полем Галуа $GF(2^n)$, коэффициенты которых совпадают с битовыми значениями соответствующих компонентов блока входных данных. Так двоичному вектору блока данных $\bar{x}$

$$\bar{x} = \{ x_{n-1}, \quad x_{n-2}, \quad \text{K}, \quad x_i, \quad \text{K}, \quad x_2, \quad x_1, \quad x_0 \}$$

в поле $GF(2^n)$ соответствует полином $X(z)$:

$$X(z) = x_{n-1}z^{n-1} \oplus x_{n-2}z^{n-2} \oplus \Lambda \oplus x_i z^i \oplus \Lambda \oplus x_2 z^2 \oplus x_1 z^1 \oplus x_0 z^0,$$

а двоичному вектору блока данных $\bar{y}$ соответствует полином $Y(z)$:

$$Y(z) = y_{n-1}z^{n-1} \oplus y_{n-2}z^{n-2} \oplus \Lambda \oplus y_i z^i \oplus \Lambda \oplus y_2 z^2 \oplus y_1 z^1 \oplus y_0 z^0.$$

Построение обратного элемента $Y(z)$ по известному элементу $X(z)$ можно выполнить, например, с помощью алгоритма Евклида для нахождения наибольшего общего делителя [2] или с помощью метода индексного обращения [3].

Следует отметить, что использование алгоритма Евклида предполагает необходимость выполнения последовательности операций деления с остатком над полиномами, т.е. в плане вычислительной сложности этот алгоритм не проще операции деления полиномов, которая в явном виде присутствует в операции их обращения:

$$Y(z) = \frac{1}{X(z)}. \tag{2}$$

Использование метода индексного обращения основано на учете конечности поля