УДК 004.056

А.А. ЗАМУЛА, канд. техн. наук, А.П. ШУМАР

ЗАЩИТА ИНФОРМАЦИИ В ИНФОРМАЦИОННО-ТЕЛЕКОМУНИКАЦИОННОЙ СИСТЕМЕ ОТ ВНУТРЕННЕГО НАРУШИТЕЛЯ

Введение

Общепризнанным стратегическим фактором успешной деятельности банков, государственных предприятий, коммерческих компаний является эффективное применение информационных технологий. Информационно-телекоммуникационные системы (ИТС) становятся сегодня одним из главных инструментов управления бизнесом и фактически важнейшим средством производства современной компании. Современным ИТС доверяют решение самых разнообразных и важных задач: автоматизированное управление технологическими процессами и промышленными предприятиями, автоматизацию деятельности банков, финансовых бирж, страховых компаний, торговых компаний и т.д. Вместе с тем, возрастает уязвимость ИТС за счет повышения сложности элементов ИТС, появления новых технологий передачи и хранения данных, увеличения объема программного обеспечения. Расширился спектр угроз для ИТС из-за активного использования организациями открытых глобальных сетей для передачи сообщений.

Суть внутренних угроз информационной безопасности

Внутренний нарушитель (инсайдер) – сотрудник, который работает в организации и представляет собой потенциальную угрозу изнутри организации.

Долгое время компании предпринимали попытки предотвратить атаки несанкционированного доступа к конфиденциальной информации: защищали периметр межсетевыми экранами и системами предотвращения вторжений, внедряли VPN и другие инструменты против неавторизованного доступа. Защита от внешнего окружения достигла высокого уровня. Однако организации упустили из вида главную опасность – внутреннего нарушителя, собственного сотрудника, прошедшего все рубежи авторизации и получившего неограниченный доступ к корпоративной информации. Пока корпоративный периметр оборудовался новыми информационными технологиями, инсайдер беспрепятственно реализовал атаки на информационный ресурс организации (финансовую информацию и интеллектуальную собственность компании, персональные данные).

Классификация инсайдеров

Классификация инсайдеров представлена в таблице. Подробная характеристика и достоверная информация о злоумышленнике – это первое, что необходимо для эффективной защиты конфиденциальных данных. Особенно если дело касается информационной безопасности, в которой действия нарушителя, как ни в какой другой области, описываются поведенческими моделями. Понимая мотивацию внутреннего нарушителя и цели, можно принимать меры, которые всегда будут опережать его действия.

Тип	Умысел	Корысть	Постановка задачи
Сотрудники, халатно относящиеся к своим служебным обязанностям	нет	нет	нет
Манипулируемые сотрудники	нет	нет	нет
Сотрудники, которые считают себя обиженными	да	нет	сам
Сотрудники, нелояльно настроенные к организации	да	нет	сам
Сотрудники – совместители	да	да	сам/извне
Сотрудники, которые внедрены в организацию для выполнения целей по нарушению работоспособности системы	да	да	извне

Сотрудники, халатно относящиеся к своим служебным обязанностям

Такие внутренние нарушители являются наиболее распространенными типом внутренних нарушителей. Его нарушения носят немотивированный характер, не имеют конкретных целей, умысла, корысти.

Эти сотрудники создают незлонамеренные, ненаправленные угрозы, то есть они нарушают правила хранения конфиденциальных данных, действуя из лучших побуждений. Например, они могут вынести информацию из офиса для работы с ней дома, в командировке и т.д., потерять носитель или допустить членов семьи к этой информации. Против таких нарушителей действенными являются простые технические средства предотвращения утечек – фильтрация исходящего трафика в сочетании с работой менеджеров устройств ввода-вывода.

Манипулируемые сотрудники

Манипулируемые сотрудники – это чаще всего жертвы социальной инженерии. Социальная инженерия – вид мошенничества, основанный на человеческом факторе, на слабостях, комплексах, предрассудках человека [1].

Халатные сотрудники и манипулируемые –эти оба типа нарушителей объединяют в тип «незлонамеренных». Данные сотрудники, столкнувшись с техническим блокированием их попыток нарушить регламенты хранения и использования информации, обратятся за помощью к коллегам, техническому персоналу или руководству, которые укажут им на недоступность планируемых действий.

Сотрудники, которые считают себя обиженными

Группы нарушителей – злонамеренные. В отличие от сотрудников, описанных выше, они осознают, что своими действиями наносят вред компании, в которой работают.

Обиженные сотрудники – это сотрудники, стремящиеся нанести вред компании по личным мотивам. Чаще всего мотивом такого поведения может быть обида, возникшая от недостаточной оценки их роли в компании, недостаточный размер оплаты, неподобающее место в корпоративной иерархии, отсутствие элементов моральной мотивации или отказ в выделении корпоративных статусных атрибутов (ноутбука, телефона, кабинета, машины, секретаря).

Сотрудники, нелояльно настроенные к организации

Следующий тип внутренних нарушителей – сотрудники, нелояльно настроенные к организации. Прежде всего, это сотрудники, принявшие решение сменить место работы. В последнее время увеличилось количество инцидентов, связанных с хищением интеллектуальной собственности в компаниях стажерами, поэтому временных сотрудников иногда также относят к этому типу. По направленности угроза, исходящая от таких нарушителей, является «неправильной» – нарушители стараются «унести» максимально возможное количество доступной информации, часто даже не подозревая о ее ценности и не имея представления, как они ее будут использовать. Обиженные и нелояльные сотрудники сами определяют объект хищения, уничтожения или искажения и место его сбыта.

Однако, если еще до похищения информации обиженный или нелояльный сотрудник выйдет на потенциального покупателя конкретной информации, будь то конкурент, пресса, криминальные структуры или спецслужбы, он становится самым опасным нарушителем – мотивируемым извне. Теперь его дальнейшая работа, благосостояние, а иногда жизнь и здоровье, напрямую зависят от полноты и актуальности информации, которую он сможет похитить.

Сотрудники-совместители

Сотрудники-совместители или подрабатывающие и внедренные нарушители – это сотрудники, цели которых определяет заказчик похищения информации. В особых случаях инсайдеры стремятся скрыть свои действия (по крайне мере, до момента успешного хищения), однако мотивация их все же различается. Данный тип нарушителя охватывает широкий пласт

сотрудников, ставших инсайдерами по разным причинам. К ним относят людей, решивших заработать. Нередки случаи инсайдеров поневоле: шантаж, вымогательство, давление извне буквально не оставляют им выбора и заставляют выполнять указания третьих сторон.

Анализ инсайдерских угроз

Экосистема внутренних нарушителей позволяет понять, кто является нарушителем и чем он руководствуется. Чтобы организовать эффективную систему защиты, следует знать, какие угрозы несут инсайдеры и какими средствами они располагают для их реализации.

Инсайдерские угрозы и средства их реализации удобнее всего рассматривать в виде сценариев, каждый из которых учитывает конкретную цель неправомерных действий и технические средства, используемые для ее достижения. В данной работе представляются основные инсайдерские сценарии:

-утечка конфиденциальной информации;
-использование уязвимостей средств защиты;
-нарушение конфиденциальности информации по неосторожности;
-нарушение авторских прав на информацию;
-мошенничество;
-нецелевое использование информационных ресурсов компании[2].

Средства защиты

К основным классам защиты от инсайдерских атак относятся:
-системы выявления и предотвращения утечек;
-средства внутреннего контроля;
-системы сильной аутентификации;
-предотвращение нецелевого использования почтовых ресурсов и Интернета;
-архивирование корпоративной корреспонденции.

Системы выявления и предотвращения утечек

Ключевыми элементами решений для борьбы с утечками являются: контентный анализ почтового и веб-трафика, контроль операций с документами на уровне рабочих станций, система централизованной установки и управления.

Средства внутреннего контроля

Система внутреннего контроля должна в первую очередь гарантировать целостность, точность и адекватность финансовой отчетности.

Предотвращение нецелевого использования ИТ-ресурсов

Системы предотвращения нецелевого использования сетевых ресурсов позволяют не допустить персонал компании к развлекательным сайтам и веб-почте, запретить скачивание музыки и видео на рабочем месте, пересылку писем с ненормативной, оскорбительной, грубой лексикой. Решения представляют собой два раздельных модуля, объединенных средством централизованного управления.

Первый компонент продукта фильтрует трафик, передаваемый по протоколам HTTP и FTP, проверяет запрашиваемые веб-страницы по базе URL, авторизует пользователей при доступе к сети и протоколирует все их действия. Часто этот веб-фильтр может интегрироваться с антивирусными программами, чтобы обеспечить удаление вредоносного кода из HTTP - и FTP-потоков.

Второй компонент продукта фильтрует почтовый трафик и отсеивает запрещенные исходящие сообщения.

Системы сильной аутентификации

Решения класса сильной аутентификации (аутентификация, авторизация, безопасное администрирование) служат в основном для защиты от несанкционированного доступа к данным. В их основе лежит двух или трехфакторный процесс аутентификации, в результате которого пользователю может быть предоставлен доступ к запрашиваемым ресурсам.

Архивирование корпоративной корреспонденции

Вследствие постоянного обмена сообщениями личные ящики сотрудников очень быстро переполняются, происходит перегрузка системы. Программа для работы с корреспонденцией начинает медленнее работать. В результате служащие просто удаляют все сообщения полугодовой давности. Между тем, многие международные нормативные акты требуют, чтобы ИТ-инфраструктура организации обязательно включала централизованный архив корпоративной корреспонденции [3].

Представленные ниже продукты являются мировыми лидерами в области информационной безопасности и имеют высокий авторитет среди продуктов других компаний.

Защита информации от инсайдерских атак может быть реализована с использованием аппаратно-программного комплекса, представленного на рисунке. Такой комплекс предназначен для создания виртуальных частных сетей и обеспечения защиты информации, передаваемой по открытым каналам связи в корпоративных сетях, использующих протоколы семейства TCP/IP.

Комплекс включает следующие компоненты:

- криптографический шлюз;
- центр управления сетью криптографических шлюзов.

Аппаратно-программный комплекс обеспечивает:

-защиту внутренних сегментов сети от несанкционированного доступа со стороны пользователей сетей общего пользования;

-скрытие внутренней структуры защищаемых сегментов сети;

-криптографическую защиту данных, передаваемых сегментами сети(абонентскими пунктами);

-безопасный доступ пользователей VPN к ресурсам сетей общего пользования;

-централизованное управление настройками VPN-устройств сети;

-защищенное подключение удаленных и мобильных пользователей к защищаемым сегментам сети.

Примерами программно-аппаратных средств защиты от инсайдерских атак могут служить следующие средства [1].

Модуль VPN и удаленного доступа, разработанный компанией Cisco включает в себя:

-межсетевой экран Cisco Secure PIX Firewall;

-маршрутизатор Cisco 7100 IOS Router;

-концентратор Cisco VPN 3060 Concentrator;

-система Cisco Intrusion Detecting System;

-коммутаторы канального уровня Catalyst 3500.

Семейство Check Point Next Generation состоит из:

-FareWall 1;

-VPN 1;

-FloodGate 1;

-MetaIP;

-UserAuthority;

-ConnectControl;

-High Availability;

-SmartView Reporter;

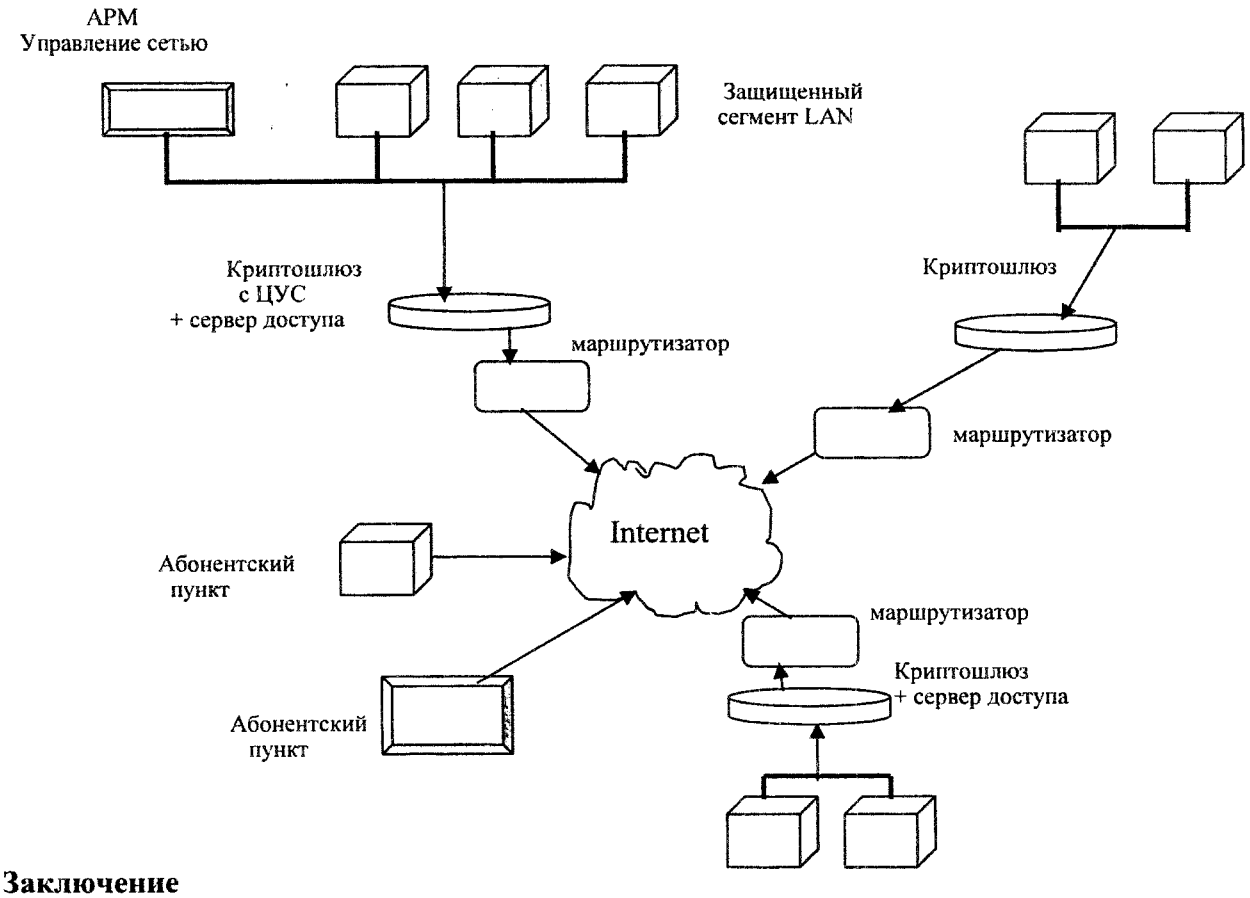
-SmartUpdate.

Для решения пятого класса – архивирования корпоративной корреспонденции – можно использовать продукты следующих компаний:

-Symantec Enterprise Vault 7.0 (компания производитель Symantec);

-Sunbelt Exchange Archive 4.0 (компания производитель Sunbelt Software);

-InfoWatch Mail Storage (компания производитель InfoWatch).



Заключение

Результатом данной работы является подробное изложение сути угроз внутренней ИТ-безопасности и существующих способов защиты от этих угроз. С использованием представленных материалов появляется возможность минимизировать риски утечки конфиденциальной информации организации, сформулировать требования к необходимым для этого техническим решениям. Также представлены примеры защиты информации от инсайдерских атак. Эффективное внедрение средств защиты конфиденциальной информации невозможно без проведения мероприятий организационного характера. В частности, организации-заказчику необходимо создать ряд документов, описывающих политику обращения с электронной конфиденциальной информацией, и проводить регулярные тренинги персонала. Политика должна описывать виды информации, хранящейся и обрабатываемой в информационной системе заказчика, присваивать каждому виду информации категорию ее конфиденциальности и определять правила работы с ней. В результате этих действий создается нормативная база комплексной системы защиты от внутренних угроз.

Список литературы: 1.*Скиба В.Ю., Кубатов В.А.* Руководство по защите от внутренних угроз информационной безопасности. – Питер; М. : Наука, 2008. – 320с. 2. *В.Ф. Шаньгин* Информационная безопасность компьютерных систем и сетей : учеб. пособие. – М. : ИД «Форум» ИНФА, 2008. – 416 с. 3.*А.В. Галицкий, Рябко С.Д., Шаньгин В.Ф.* Защита информации в сети – анализ и синтез решений. – М. : ДМК, 2007. - 615с.

Харьковский национальный
университет радиоэлектроники

Поступила в редколлегию 12.02.2011