Таким образом, расширение функциональных возможностей АМПДЗ и создание на их основе многофункциональных аппаратно-программных средств защиты информации обуславливают необходимость проведения дополнительных исследований подобных устройств на предмет оценивания корректности и надежности реализации дополнительных функциональных возможностей АМПДЗ в свете влияния их на функциональную безопасность АС ЗИ в целом [2].

В целях решения поставленной задачи разрабатываются частные методики тестирования различных функциональных подсистем многофункциональных аппаратно-программных средств защиты информации, обеспечивающие оценивание уровня функциональной безопасности всего устройства, в зависимости от архитектуры построения функциональных подсистем и параметров их настроек, а также технических характеристик данных устройств.

СПИСОК ЛИТЕРАТУРЫ:

1. Доктрина информационной безопасности Российской Федерации. Утверждена Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895.
2. *Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф.* Защита информации в компьютерных системах и сетях / Под ред. В. Ф. Шаньгина. 2-е изд., перераб. и доп. М.: Радио и связь, 2001.

Е. И. Гончаров

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОГО ОБМЕНА ПРИ ИСПОЛЬЗОВАНИИ ЭЛЕКТРОННОЙ ПОЧТЫ

С момента своего появления электронная почта была и остается важнейшим инструментом для организации информационного обмена как внутри организации, так и с ее внешними контрагентами. В то же время сам протокол, лежащий в основе ее работы, был создан без учета возможных угроз информационной безопасности. Но не только изначальные просчеты при проектировании протокола снижают уровень его безопасности — электронная почта также является удобнейшим средством Интернета для организации намеренной утечки защищаемой информации.

Основным протоколом электронной почты уже долгое время является ESMTP (Extended Simple Mail Transfer Protocol) [1]. Данный протокол, как и большинство подобных протоколов Интернета, является клиент-серверным и используется для отправки почты от отправителя до сервера и между серверами для дальнейшей пересылки к почтовому серверу получателя.

Сообщение электронной почты представляет собой текстовое сообщение, состоящее из двух обязательных частей: служебного заголовка и тела сообщения, разделенных пустой строкой. Сообщение может содержать только 7-битные символы, т. е. символы таблицы ASCII. При необходимости передать 8-битные данные, например русский текст или бинарные данные, производится их кодирование в печатные символы таблицы ASCII по схеме Base64. Никакого механизма защиты — шифрования сообщения, проверки подлинности отправителя — протокол не предусматривает.

На всех этапах передачи сообщения, кроме последнего — получения письма адресатом — используется один и тот же протокол (E)SMTP. На последнем шаге могут использоваться различные протоколы — POP3, IMAP. Процесс передачи сообщения выглядит следующим образом:

1. Клиентская почтовая программа формирует сообщение и передает его на указанный в ней почтовый сервер — обычно это внутренний почтовый сервер организации.

2. Почтовый сервер, получив сообщение, извлекает из служебного заголовка адрес получателя и ищет адрес почтового сервера, который должен принять письмо для указанного адресата. В случае если такой сервер найден, письмо передается дальше.

3. Шаг 2 повторяется до тех пор, пока письмо не достигнет почтового сервера, который непосредственно обслуживает указанного в письме адресата. Как правило, это внутренний почтовый сервер организации адресата.

4. Клиентская программа адресата забирает сообщение с сервера.

Стоит отметить, что на практике в процессе передачи сообщения обычно участвуют всего два почтовых сервера — отправителя и получателя, так как, будучи размещенными в Интернете, они доступны друг другу напрямую и необходимость в посредниках отсутствует. Между серверами сообщения передаются без использования какого-либо шифрования. Между клиентским почтовым ПО и сервером шифрование может использоваться. Как правило, почтовый сервер игнорирует значение заголовка адреса отправителя и иногда даже не проверяет наличие такого заголовка в письме, что позволяет указывать абсолютно произвольное значение адреса отправителя.

Таким образом, можно выделить следующие угрозы безопасности при использовании электронной почты для информационного обмена:

1. Перехват и несанкционированное прочтение;

2. Нарушение аутентичности;

3. Получение вредоносного ПО или несанкционированной рассылки;

4. Несанкционированная отправка защищаемой информации лицам, не участвующим в ее обработке.

Для обеспечения безопасности информационного обмена от указанных выше угроз необходимо:

1. При наличии инфраструктуры открытых ключей (или другой системы распространения ключевой информации) или возможности ее создания использовать электронные подписи и шифрование содержимого почтовых сообщений. В противном случае необходимо внедрить: защиту каналов клиент-сервер и сервер-сервер, предпочтительно с помощью протокола TLS [2] или IPSec (и подобных), расширение SMTP-протокола SPF [3] и/или DKIM [4], ведение расширенных журналов почтового сервера и привязку клиентского оборудования к IP-адресу.

2. Составить список адресатов, получателей и типов файлов-вложений, которые для них разрешены. Внедрить фильтр почтовых сообщений на его основе. Если же данный метод нереализуем, то внедрить, по крайней мере, общий список разрешенных адресатов и получателей.

Автору не удалось найти готового программного продукта, реализующего все указанные меры, поэтому для их реализации были использованы: ПО Microsoft Certification Authority в качестве удостоверяющего центра, почтовое ПО Postfix и самостоятельно разработанный для этого ПО фильтр почты. В результате проведенных испытаний полученного комплекса ни одна из рассматриваемых угроз не была успешно реализована.

СПИСОК ЛИТЕРАТУРЫ:

1. *Klensin J.* Simple Mail Transfer Protocol // RFC 5321. Network Working Group. October 2008.
2. *Dierks T., Rescorla E.* The Transport Layer Security (TLS) Protocol // Network Working Group. August 2008.

3. *Wong M., Schlitt W.* Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail // Network Working Group. April 2006.
4. *Allman E., Callas J., Delany M., Libbey M., Fenton J., Thomas M.* DomainKeys Identified Mail (DKIM) Signatures // Network Working Group. May 2007.

Н. В. Гришина

АНАЛИЗ ВЗАИМОДЕЙСТВИЯ СУБЪЕКТОВ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ С ЦЕЛЬЮ ВЫЯВЛЕНИЯ УГРОЗ ДЛЯ ИХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Коротко суть проблемы можно сформулировать следующим образом: субъектами информационных отношений являются юридические и физические лица, находящиеся в едином информационном конкурентном пространстве. У каждого из них есть свои цели и задачи. Каждый из них решает проблему безопасности информации, необходимой для обеспечения непрерывности бизнес-процессов. Однако часто причины и источники информационных рисков лежат за пределами конкретного субъекта, являются результатом взаимодействия субъектов. А вот эффекту «взаимодействия» должного внимания не уделяется.

Несмотря на важность изучения проблем обеспечения информационной безопасности при различного рода взаимодействиях субъектов информационных отношений, данный объект исследования не выделялся в самостоятельную проблему. Тем не менее исследования, прямо или опосредованно касающиеся данной проблематики, довольно обширны по объему и разнообразны с точки зрения конкретного предмета исследования.

Следует выделить несколько важнейших направлений научно-исследовательской деятельности, в рамках которых затрагиваются отдельные аспекты проблем взаимодействия субъектов информационных отношений:

– анализ понятия, принципов и методов обеспечения информационной безопасности отдельных субъектов информационных отношений;

– анализ подходов к выявлению и нейтрализации информационных рисков субъектов единого информационного поля и угроз информационной безопасности;

– изучение особенностей конкурентной среды как единого информационного пространства, в котором происходит взаимодействие субъектов информационных отношений, нуждающихся в обеспечении защиты информации и информационной безопасности.

Выделенные блоки проблем отчасти смыкаются друг с другом, однако, как правило, рассматриваются отдельно специалистами в разных областях экономики, менеджмента, защиты информации и т. д. Одной из задач данного исследования является объединение ряда таких подходов в рамках интеграции различных научно-исследовательских направлений в целях решения теоретических и практических задач построения модели взаимодействия субъектов информационных отношений.

Выводы

Тематика данного исследования лежит на стыке различных направлений, таких как управление рисками, анализ конкурентной среды, управление информационными рисками, информационная безопасность и др. Изучение выделенного предмета исследования должно представлять собой комплексный анализ экономических, правовых, организационных и технических проблем в различных областях научно-исследовательских знаний.