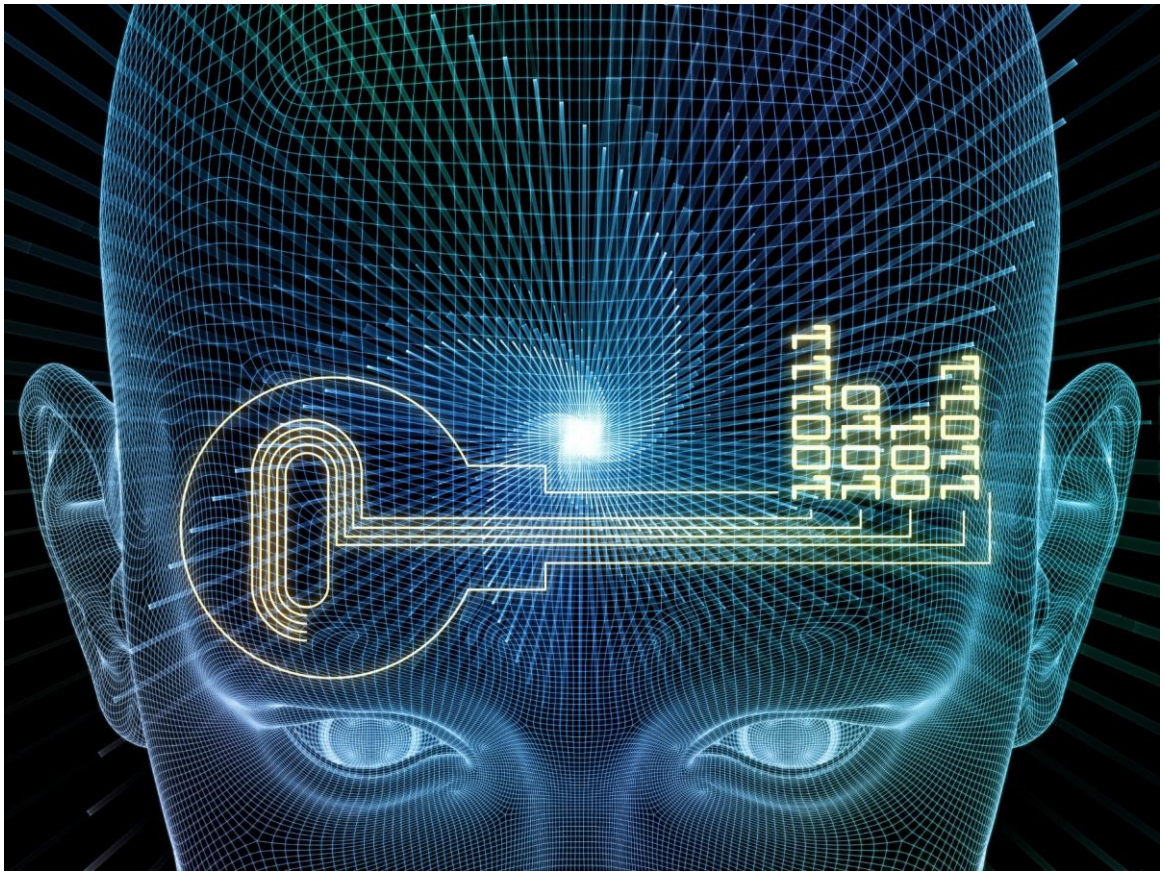
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА
И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РФ»
ВОЛГОГРАДСКИЙ ИНСТИТУТ УПРАВЛЕНИЯ

И. П. Михнев

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Учебное пособие



Волгоград 2019

УДК 004.056(0758)
ББК 32.972.53я73
М 69

Р е ц е н з е н т ы :

кандидат технических наук, доцент ***О.С. Власова,***
ФГБОУ ВО «Институт архитектуры и строительства ВолгГТУ»;

кандидат технических наук, доцент ***Н.А. Сальникова,***
Волгоградский институт управления – филиал ФГБОУ ВО «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации»

Михнев, И.П.

М 69 **Информационная безопасность:** учебное пособие / И.П. Михнев. – Волгоградский институт управления – филиал ФГБОУ ВО «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации». – Волгоград: Изд-во Волгоградского института управления – филиала РАНХиГС, 2019. – 1 электрон. опт. диск (CD-ROM). – Систем. требования: IBM PC с процессором 486; ОЗУ 64 Мб; CD-ROM дисковод; Adobe Reader 6.0. – Загл. с экрана.

Учебное пособие предназначено для студентов и слушателей высших учебных заведений, гуманитарных и экономических специальностей, а также может быть использовано специалистами в области проектирования и организации систем информационной безопасности. В пособии рассматриваются теоретические основы защиты информации, основы криптографии, защита информации, анализ и управление рисками в сфере информационной безопасности.

ISBN 978-5-7786-0776-7

ОГЛАВЛЕНИЕ

СПИСОК СОКРАЩЕНИЙ

ACL (Access Control List) – список управления доступом;

AD (Active Directory) – служба каталогов, являющаяся масштабируемой структурой домена управляемого ОС Windows;

AH (Authentication Header) – протокол аутентифицирующего заголовка;

ARP (Address Resolution Protocol) – протокол разрешения адресов;

ARPANET (Advanced Research Projects Agency Network) – глобальная сеть, которая являлась прообразом сети Internet;

CA (Certification Authority) – центр сертификации или удостоверяющий центр;

CBC (Cipher Block Chaining) – сцепление блоков шифра (режим шифра DES);

CFB (Cipher FeedBack) – обратная связь по шифртексту (режим шифра DES);

CRC (Cyclic Redundancy Code) – алгоритм вычисления контрольной суммы, предназначенный для проверки целостности передаваемых данных;

CRL (Certificate Revocation List) – список отозванных сертификатов;

ECB (Electronic Code Book) – электронная кодовая книга (режим шифра DES);

DES (Data Encryption Standard) – симметричный алгоритм шифрования;

DNS (Domain Name System) – система доменных имён;

DSL (Digital Subscriber Line) – цифровая абонентская линия;

EAP (Extensible Authentication Protocol) – расширяемый протокол аутентификации;

EFS (Encrypting File System) – шифрующая файловая система;

ESP (Encapsulating Security Payload) – протокол инкапсулирующей защиты данных;

FTP (File Transfer Protocol) – протокол передачи файлов;

GC (Global Catalog) – глобальный каталог в службе каталогов ОС Windows;

GSP (Generic Services Proxy) – технология модуля доступа прикладного уровня для поддержки внешних протоколов обеспечения безопасности;

HTTP (HyperText Transfer Protocol) – протокол передачи гипертекстовых Internet страниц;

HTTPS (Hypertext Transfer Protocol Secure) – расширение протокола, поддерживающее шифрование;

ID (Identification) – идентификатор;

IDS (Intrusion Detection System) – системы обнаружения вторжений;

IP (Internet Protocol Address) – уникальный сетевой адрес узла в компьютерной сети;

ISP (Internet Service Provider) – поставщик интернет-услуги (провайдер);

IT (Information Technology) – информационные технологии;

LSA (Local Security Authority) – локальный администратор безопасности используемый в ОС Windows;

MAC (Media Access Control) – адрес, по которому ведется доступ абонентов к общему каналу связи на канальном уровне OSI;

NFS (Network File System) – сетевая файловая система;

OFB (Output FeedBack) – обратная связь по выходу (режим шифра DES);

OSI (Open System Interconnection) – эталонная модель взаимодействия открытых систем;

PGP (Pretty Good Privacy) – протокол с открытым ключом для шифрования сообщений электронной почты;

PKI (Public Key Infrastructure) – инфраструктура открытых ключей;

RPC (Remote Procedure Call) – удалённый вызов процедур;

RSA – криптографический алгоритм с открытым ключом;

SA (Security Association) – контекст защиты или ассоциация безопасности;

SPI (Security Parameter Index) – индекс параметров защиты;

SRM (Security Reference Monitor) – диспетчер доступа ОС Windows;

SSL – Secure Socket Layer – протокол защищенной связи через Интернет по системе «клиент-сервер»;

TCP (Transmission Control Protocol) – протокол управления передачей;

TLS (Transport Layer Security) – протокол обеспечения безопасности транспортного уровня;

URL (Uniform Resource Locator) – формат символьного указателя ресурса в сети Internet;

VPN (Virtual Private Network) – виртуальная частная сеть;

Wi-Fi – беспроводная сеть стандарта IEEE 802.11;

WLAN (Wireless Local Area Network) – беспроводная локальная сеть;

АБС – автоматизированная банковская система;

АС – автоматизированная система;

БД – база данных;

ВК – виртуальный канал;

ВС – вычислительная система;

ВТ – виртуальный терминал;

ИБ – информационная безопасность;

ИС – информационная система;

ИТ – информационные технологии;

КС – компьютерная система;

ЛВС – локальная вычислительная сеть;

МЭ – межсетевой экран;

НСД – несанкционированный доступ;

ОЗУ – оперативное запоминающие устройство;

ПЗУ – постоянное запоминающие устройство;

ПИБ – политика информационной безопасности;

РВС – распределенная вычислительная система;

РПС – разрушающее программное средство;

СБИ – система безопасности информации;

СЗИ – средство защиты информации;

СФБ – стойкость функции безопасности;

ЭВМ – электронно-вычислительная машина;

ЭЦП – электронная цифровая подпись.

ВВЕДЕНИЕ

В настоящее время во всем мире резко повысилось внимание к проблеме информационной безопасности. Это обусловлено процессами стремительного расширения потоков информации, пронизывающих все сферы жизни общества. Современный специалист в области информационных технологий должен обладать знаниями и навыками обеспечения информационной безопасности. Связано это с тем, что в информационных системах предприятий и организаций хранится и обрабатывается критически важная информация, нарушение конфиденциальности, целостности или доступности которой может привести к нежелательным последствиям. Поэтому вопросам обеспечения информационной безопасности должно уделяться внимание на всех этапах разработки и эксплуатации информационных систем.

Информация давно перестала быть просто необходимым для производства вспомогательным ресурсом или побочным проявлением всякого рода деятельности. Она приобрела ощутимый стоимостной вес, который четко определяется реальной прибылью, получаемой при ее использовании, или размерами ущерба, с разной степенью вероятности наносимого владельцу информации. Однако создание индустрии переработки информации порождает целый ряд сложных проблем. Одной из таких проблем является надежное обеспечение сохранности и установленного статуса информации, циркулирующей и обрабатываемой в информационно-вычислительных системах и сетях.

Появление глобальных компьютерных сетей сделало простым получение доступа к информации, как для отдельных пользователей, так и для больших организаций. Но легкость и высокая скорость доступа к данным при помощи компьютерных сетей, таких как Internet, также сделали значительными следующие угрозы безопасности данных при отсутствии мер их защиты:

– неавторизованный доступ к информации;

– неавторизованное изменение информации;

– неавторизованный доступ к сетям и сервисам;

– другие сетевые атаки, например, повтор перехваченных ранее транзакций и атаки типа «отказ в обслуживании».

При обработке любой значимой информации при помощи отдельного

компьютера, а тем более в сети, возникает вопрос о ее защите от несанкционированного доступа и использования. Наиболее распространенный в компьютерных системах способ защиты – использование паролей – более пригоден для защиты доступа к вычислительным ресурсам, нежели для защиты информации. Это своеобразный экран, отгораживающий законных пользователей системы от посторонних, пройдя сквозь который, квалифицированный пользователь получает доступ практически ко всей информации.

В настоящее время исключительно важное значение в разных областях приобрели вопросы, связанные с сохранением и передачей конфиденциальной информации. Возникающие при этом задачи решает криптография – наука о методах преобразования информации в целях ее защиты от незаконных пользователей.

В представленном учебном пособии рассматриваются ключевые разделы курсов «Информационная безопасность» и «Основы информационной безопасности хозяйственной деятельности». В него включены как теоретические, так и практические разделы, направленные на развитие навыков анализа и совершенствования информационной безопасности объектов.

Главная цель книги – познакомить обучаемых с основами информационной безопасности, определить основные направления развития этой области знаний, в рамках образовательной программы попытаться сформировать у них элементы «информационной культуры». Обращаю внимание на то, что все без исключения определения и термины взяты мной из соответствующих законов РФ в области информации, защиты информации и информационной безопасности. Это освобождает автора от необходимости использовать определения других авторов, не всегда, на мой взгляд, корректные и точные. Кроме того, приведены наиболее употребляемые термины, используемые в области информационной безопасности, на английском языке и их перевод.

Настоящее учебное пособие написано по опыту преподавания автором дисциплин «Основы информационной безопасности хозяйственной деятельности» и «Обеспечение информационной безопасности компьютерных систем» в Волгоградском институте управления – филиале РАНХиГС при Президенте РФ и в первую очередь адресовано для студентов и слушателей высших учебных заведений гуманитарных и экономических специальностей. Также учебное пособие может быть использовано специалистами в области проектирования и организации систем информационной безопасности.

Учебное пособие учитывает требования государственного образовательного стандарта и структурно соответствует учебной программе и тематическому плану изучения дисциплины «Основы информационной безопасности хозяйственной деятельности». Отдельные части пособия соответствуют темам дисциплины, а отдельные главы – лекционным занятиям, а также могут быть использованы для проведения практических занятий и самостоятельно изучения студентами соответствующего материала с использованием ПК.

При написании пособия автор придерживался принципа необходимости дополнения общетеоретических и концептуальных основ информационной безопасности, изучение которых предусмотрено государственным образовательным стандартом, практическими сведениями по способам обеспечения безопасности ЭВМ и компьютерных сетей, которые являются актуальными для специалистов в информационной сфере. В связи с этим автор постарался расширить и дополнить текст, поэтому пособие содержит много дополнительных и справочных сведений о безопасности компьютерных сетей и ориентировано на читателя целью которого является более глубокое изучение вопросов информационной безопасности по сравнению с материалом, изучаемым на лекциях по дисциплине. При составлении учебного пособия автор ориентировался на известные учебные материалы в предметной области, а также использовал ресурсы сети Internet посвященные вопросам информационной безопасности.

Тематика курса разрабатывается многими авторами, ими к настоящему времени подготовлено достаточно много учебных пособий. Обилие этих книг говорит об огромной величине рассматриваемой области, ее постоянном изменении и увеличении. В качестве основы для курса были выбраны следующие книги:

- ✓ Нестеров С.А. Основы информационной безопасности: учебное пособие. – СПб.: Издательство «Лань», 2017. – 324 с.
- ✓ Макаренко С.И. Информационная безопасность: учебное пособие. – Ставрополь: СФ МГГУ им. М.А. Шолохова, 2009. – 372 с.
- ✓ Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие. – М.: ИД «ФОРУМ»: ИНФРА–М, 2008. – 416 с.
- ✓ Галатенко В.А. Основы информационной безопасности: курс лекций. – М.: ИНТУИТ. РУ, 2006. – 205 с.

- ✓ Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности: учебное пособие для вузов. – М.: Горячая линия – Телеком, 2006. – 544 с.
- ✓ Тихонов В.А., Райх В.В. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты: учебное пособие. – М.: Гелиос АРВ, 2006. – 528 с.

Все книги написаны известными специалистами в области информационной безопасности и во многом основаны на передовом зарубежном и отечественном опыте. Однако даже за прошедшее время с момента выхода книг произошли существенные изменения в данной области, например, вышли новые стандарты и рекомендации по вопросам информационной безопасности и новым технологиям, приняты новые законы и другие акты. В связи с этим должно быть переработано и дополнено содержание всех этих книг и курса на их основе. По-видимому, в последующем также надо будет учесть и процесс гармонизации международных и отечественных стандартов, особенности новых отраслевых стандартов.

Автор выражает благодарность рецензентам за кропотливый труд по поиску ошибок и неточностей, а также ценные замечания, которые помогли сделать материал пособия лучше и доступнее.

Глава 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. Базовые понятия

Начнем изучение дисциплины с определения ряда базовых понятий.

Информация – это сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления. Информация может существовать в различных формах в виде совокупностей некоторых знаков (символов, сигналов и т.д.) на носителях различных типов. Она может представлять ценность для отдельных лиц или организаций.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственниками информации. Собственниками информации могут быть государство, юридическое лицо, группа физических лиц, отдельное физическое лицо [1].

В последнее время все большие объемы информации, в том числе и критически важной для отдельных людей, организаций или государств, хранятся, обрабатываются и передаются с использованием автоматизированных систем (АС) обработки информации. *Система обработки информации* – совокупность технических средств и программного обеспечения, а также методов обработки информации и действий персонала, необходимых для выполнения автоматизированной обработки информации [2]. *Объект информатизации* – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров.

В зависимости от конкретных условий может решаться задача обеспечения комплексной безопасности объекта информатизации или защиты отдельных ресурсов – информационных, программных и т.д.

Информационные ресурсы (активы) – отдельные документы и отдельные массивы документов, документы и массивы документов, содержащиеся в информационных системах (библиотеках, архивах, фондах, банках данных, информационных системах других видов).

Рассматривая вопросы безопасности АС, можно говорить о наличии некоторых «желательных» состояний системы, через которые и описывается ее «защищенность» или «безопасность». Безопасность является таким же свойством системы, как надежность или производительность, и в последнее время ей уделяется все большее внимание. Чтобы указать на причины выхода системы из безопасного состояния, вводятся понятия «угроза» и «уязвимость».

Угроза (безопасности информации) – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Источник угрозы безопасности информации – субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации. По типу источника угрозы делят на связанные и несвязанные с деятельностью человека. Примерами могут служить, соответственно, удаление пользователем файла с важной информацией и пожар в здании. Угрозы, связанные с деятельностью человека, разделяют на угрозы случайного и преднамеренного характера. В последнем случае источник угрозы называют нарушителем или злоумышленником.

Уязвимость (информационной системы) – свойство информационной системы, обуславливающее возможность реализации угроз безопасности обрабатываемой в ней информации. Например, угроза потери информации из-за сбоя в сети электропитания реализуется, если в АС не применяются источники бесперебойного питания или средства резервного электроснабжения (это является уязвимостью).

Если говорить об информационных ресурсах, то реализация угрозы может привести к таким последствиям, как получение информации людьми, которым она не предназначена, уничтожение или изменение информации, недоступность ресурсов для пользователей. Таким образом, мы подошли к определению трех основных угроз безопасности.

Угроза конфиденциальности (угроза раскрытия) – это угроза, в

результате реализации которой конфиденциальная или секретная информация становится доступной лицу, группе лиц или какой–либо организации, которой она не предназначалась. Здесь надо пояснить разницу между секретной и конфиденциальной информацией. В отечественной литературе «секретной» обычно называют информацию, относящуюся к разряду государственной тайны, а «конфиденциальной» – персональные данные, коммерческую тайну и т. п.

Угроза целостности – угроза, в результате реализации которой информация становится измененной или уничтоженной. Необходимо отметить, что и в нормальном режиме работы АС данные могут изменяться и удаляться. Являются ли эти действия легальными или нет, должно определяться политикой безопасности. *Политика безопасности* – совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

Угроза отказа в обслуживании (угроза доступности) – угроза, реализация которой приведет к отказу в обслуживании клиентов АС, несанкционированному использованию ресурсов злоумышленниками по своему усмотрению.

Ряд авторов дополняют приведенную классификацию, вводя *угрозу раскрытия параметров* АС, включающей в себя подсистему защиты. Угроза считается реализованной, если злоумышленником в ходе нелегального исследования системы определены все ее уязвимости. Данную угрозу относят к разряду опосредованных: последствия ее реализации не причиняют какой–либо ущерб обрабатываемой информации, но дают возможность для реализации первичных (непосредственных) угроз.

Таким образом, *безопасность информации* – это состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность. *Защита информации* может быть определена как деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию. Выделяются следующие направления защиты информации:

- *правовая защита информации* – защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением;

- *техническая защита информации* – защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств;
- *криптографическая защита информации* – защита информации с помощью ее криптографического преобразования;
- *физическая защита информации* – защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.

Защита информации осуществляется с использованием способов и средств защиты. *Способ защиты информации* – порядок и правила применения определенных принципов и средств защиты информации. *Средство защиты информации* – техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации. Отдельно выделяют:

- средства контроля эффективности защиты информации;
- средства физической защиты информации;
- криптографические средства защиты информации.

1.2. Общая схема процесса обеспечения безопасности

Рассмотрим теперь взаимосвязь основных субъектов и объектов обеспечения безопасности, как это предлагается в международном стандарте ISO/IEC–15408 (в России он принят как ГОСТ Р ИСО/МЭК 15408–2002 [4]).

Безопасность связана с защитой активов от угроз. Разработчики стандарта отмечают, что следует рассматривать все разновидности угроз, но в сфере безопасности наибольшее внимание уделяется тем из них, которые связаны с действиями человека. За сохранность активов отвечают их владельцы, для которых они имеют ценность. Существующие или предполагаемые нарушители также могут придавать значение этим активам и стремиться использовать их вопреки интересам их владельца. Действия нарушителей приводят к появлению угроз. Как уже отмечалось выше, угрозы реализуются через имеющиеся в системе уязвимости. Владельцы активов анализируют возможные угрозы, чтобы

определить, какие из них могут быть реализованы в отношении рассматриваемой системы. В результате анализа определяются риски (т. е. события или ситуации, которые предполагают возможность ущерба) и проводится их анализ.

Владельцы актива предпринимают контрмеры для уменьшения уязвимостей и выполнения политики безопасности. Но и после введения этих контрмер могут сохраняться остаточные уязвимости и соответственно – остаточный риск.

1.3. Идентификация, аутентификация, управление доступом. защита от несанкционированного доступа

В этом разделе будут рассмотрены вопросы, связанные с защитой информации от несанкционированного доступа (НСД).

Защита информации от несанкционированного доступа – защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации.

Для защиты от НСД, как правило, используется идентификация, аутентификация и управление доступом. В дополнение к перечисленным, могут применяться и другие методы.

Идентификация – присвоение пользователям идентификаторов (уникальных имен или меток) под которыми система «знает» пользователя. Кроме идентификации пользователей, может проводиться идентификация групп пользователей, ресурсов АС и т.д. Идентификация нужна и для других системных задач, например, для ведения журналов событий. В большинстве случаев идентификация сопровождается аутентификацией. *Аутентификация* – установление подлинности – проверка принадлежности пользователю предъявленного им идентификатора. Например, в начале сеанса работы в АС пользователь вводит имя и пароль. На основании этих данных система проводит идентификацию (по имени пользователя) и аутентификацию (сопоставляя имя пользователя и введенный пароль).

Управление доступом – метод защиты информации путем регулирования использования всех ресурсов системы.

Система идентификации и аутентификации является одним из ключевых

элементов инфраструктуры защиты от НСД любой информационной системы. Обычно выделяют 3 группы методов аутентификации.

1. Аутентификация по наличию у пользователя уникального объекта заданного типа. Иногда этот класс методов аутентификации называют по-английски “I have” («у меня есть»). В качестве примера можно привести аутентификацию с помощью смарт-карт или электронных USB-ключей.

2. Аутентификация, основанная на том, что пользователю известна некоторая конфиденциальная информация – “I know” («я знаю»). Например, аутентификация по паролю. Более подробно парольные системы рассматриваются далее в этом разделе.

3. Аутентификация пользователя по его собственным уникальным характеристикам – “I am” («я есть»). Эти методы также называются биометрическими. Биометрические методы аутентификации делят на статические и динамические.

Примеры аутентификации по статическим признакам – это проверка отпечатка пальца, рисунка радужной оболочки глаз, геометрии кисти руки, сравнение с фотографией и т.д. Достоинством этих методов является достаточно высокая точность. Но надо отметить, что подобные методы, как правило, требуют наличия специализированного оборудования (например, специальных сканеров) и имеют ограниченную область применения (например, при аутентификации по отпечатку пальца из-за грязи на руке человек может не пройти аутентификацию, т. е. подобные методы неприменимы на стройках и на многих производствах).

Примеры динамической аутентификации – аутентификация по голосу (при произнесении заранее определенной фразы или произвольного текста), аутентификация по «клавиатурному почерку» (проверяются особенности работы пользователя на клавиатуре, такие как время задержки при нажатии клавиш в различных сочетаниях) и т.д.

Нередко используются комбинированные схемы аутентификации, объединяющие методы разных классов. Например, двухфакторная аутентификация – пользователь предъявляет системе смарт-карту и вводит пин-код для ее активации.

Аутентификация может быть *односторонней,* когда одна сторона аутентифицирует другую (например, сервер проверяет подлинность клиентов), и *двусторонней*, когда стороны проводят взаимную проверку подлинности.

Также аутентификация может быть *непосредственной*, когда в процедуре

аутентификации участвуют только две стороны, или *с участием доверенной стороны.* В последнем случае в процессе аутентификации участвуют не только стороны, проверяющие подлинность друг друга, но и другая или другие, вспомогательные. Эту третью сторону иногда называют сервером аутентификации (англ. «authentication server») или арбитром (англ. «arbitrator»).

ПАРОЛЬНЫЕ СИСТЕМЫ АУТЕНТИФИКАЦИИ

Наиболее распространенными на данный момент являются парольные системы аутентификации. Определим ряд понятий, использующихся при описании подобных систем.

Идентификатор пользователя – уникальная информация, позволяющая различить отдельных пользователей парольной системы (провести идентификацию). Это может быть имя учетной записи пользователя в системе или специально генерируемые уникальные числовые идентификаторы.

Пароль пользователя – секретная информация, известная только пользователю (и возможно – системе), которая используется для прохождения аутентификации. В зависимости от реализации системы, пароль может быть одноразовым или многоразовым. При прочих равных условиях системы с одноразовыми паролями являются более надежными. В них исключаются некоторые риски, связанные с перехватом паролей – пароль действителен только на одну сессию и, если легальный пользователь его уже задействовал, нарушитель не сможет такой пароль повторно использовать. Но системы с многоразовыми паролями (в них пароль может быть использован многократно) проще реализовать и дешевле поддерживать, поэтому они более распространены.

Учетная запись пользователя – совокупность идентификатора, пароля и, возможно, дополнительной информации, служащей для описания пользователя. Учетные записи хранятся в базе данных парольной системы.

Парольная система – это программный или программно-аппаратный комплекс, реализующий функции идентификации и аутентификации пользователей компьютерной системы путем проверки паролей. В отдельных случаях подобная система может выполнять дополнительные функции, такие как генерация и распределение криптографических ключей и т.д. Как правило, парольная система включает в себя интерфейс пользователя, интерфейс администратора, базу учетных записей, модули сопряжения с другими компонентами подсистемы безопасности (подсистемой разграничения доступа, регистрации событий и т.д.).

Рассмотрим некоторые рекомендации по администрированию парольной системы, использующей многоразовые пароли.

1. Задание минимальной длины используемых в системе паролей. Это усложняет атаку путем подбора паролей. Как правило, рекомендуют устанавливать минимальную длину в 6–8 символов.

2. Установка требования использовать в пароле разные группы символов – большие и маленькие буквы, цифры, специальные символы. Это также усложняет подбор.

3. Периодическая проверка администраторами безопасности качества используемых паролей путем имитации атак[1], таких как подбор паролей «по словарю» (т. е. проверка на использование в качестве пароля слов естественного языка и простых комбинаций символов, таких как «1234»).

4. Установление максимального и минимального сроков жизни пароля, использование механизма принудительной смены старых паролей. При внедрении данной меры надо учитывать, что при невысокой квалификации пользователей от администратора потребуются дополнительные усилия по разъяснению пользователям того, что «от них требует система».

5. Ограничение числа неудачных попыток ввода пароля (блокирование учетной записи после заданного числа неудачных попыток войти в систему). Данная мера позволяет защититься от атак путем подбора паролей. Но при необдуманном внедрении также может привести к дополнительным проблемам – легальные пользователи из-за ошибок ввода паролей по невнимательности могут блокировать свои учетные записи, что потребует от администратора дополнительных усилий.

6. Ведение журнала истории паролей, чтобы пользователи после принудительной смены пароля не могли вновь выбрать себе старый, возможно скомпрометированный пароль.

1.4. Модели безопасности

Важным этапом процесса обеспечения безопасности АС является разработка политики безопасности. Если отсутствует политика безопасности,

[1] *Компьютерная атака* – целенаправленное несанкционированное воздействие на информацию, на ресурс автоматизированной информационной системы или получение несанкционированного доступа к ним с применением программных или программно-аппаратных средств.

невозможно даже четко провести разграничение между санкционированным (легальным) доступом к информации и НСД.

Политика безопасности может быть описана формальным или неформальным образом. Формальное описание политики безопасности производится в рамках модели безопасности. С этой точки зрения, модель безопасности можно определить как абстрактное описание поведения целого класса систем, без рассмотрения конкретных деталей их реализации.

Большинство моделей безопасности оперируют терминами «сущность», «субъект», «объект».

Сущность – любая именованная составляющая защищаемой АС.

Субъект – активная сущность, которая может инициировать запросы ресурсов и использовать их для выполнения каких-либо вычислительных операций. В качестве субъекта может выступать выполняющаяся в системе программа или «пользователь» (не реальный человек, а сущность АС).

Объект – пассивная сущность, используемая для хранения или получения информации. В качестве объекта может рассматриваться, например, файл с данными.

Обычно предполагается, что существует безошибочный способ различения объектов и субъектов.

Доступ – взаимодействие между субъектом и объектом, в результате которого производится перенос информации между ними. Два фундаментальных типа доступа: *чтение* – операция, результатом которой является перенос информации от объекта к субъекту; *запись* – операция, результатом которой является перенос информации от субъекта к объекту.

Также предполагается существование *монитора безопасности объектов,* т. е. такого субъекта, который будет активизироваться при любом обращении к объектам, может различать (на базе определенных правил) легальные и несанкционированные обращения и разрешать только легальный доступ.

В литературе выделяются три основных класса моделей политики безопасности: дискреционные, мандатные и ролевые.

Основу *дискреционной* (избирательной) политики безопасности составляет дискреционное управление доступом, которое характеризуется следующими свойствами [3]:

- все субъекты и объекты должны быть идентифицированы;
- права доступа субъекта к объекту системы определяются на основании некоторого внешнего по отношению к системе правила.

Правила дискреционного управления доступом часто задаются матрицей доступов. В подобной матрице строки соответствуют субъектам системы, столбцы – объектам, элементы матрицы описывают права доступа для соответствующей пары «субъект – объект».

Одной из наиболее известных дискреционных моделей является модель Харрисона-Рузо-Ульмана, часто называемая матричной моделью. Она будет подробно описана ниже.

Этот тип управления доступом наиболее часто используется в операционных системах в связи с относительной простотой реализации. В этом случае правила управления доступом часто описываются через *списки управления доступом* (англ. «Access Control List», сокр. ACL). Список связан с защищаемым объектом и хранит перечень субъектов и их разрешений на данный объект. В качестве примера можно привести использование ACL для описания прав доступа пользователей и групп к файлу в файловой системе NTFS в операционных системах семейства Windows NT.

Основу *мандатной* политики безопасности составляет мандатное управление доступом, которое подразумевает, что:

- все субъекты и объекты должны быть идентифицированы;
- задан линейно упорядоченный набор меток секретности;
- каждому объекту системы присвоена метка секретности, определяющая ценность содержащейся в нем информации – его *уровень секретности*;
- каждому субъекту системы присвоена метка секретности, определяющая уровень доверия к нему – его *уровень доступа*;
- решение о разрешении доступа субъекта к объекту принимается исходя из типа доступа и сравнения метки субъекта и объекта.

Чаще всего мандатную политику безопасности описывают в терминах модели Белла-ЛаПадула, которая будет рассмотрена ниже в данном разделе.

Управление доступом, основанное на ролях, оперирует в терминах «роль», «пользователь», «операция». Вся информация рассматривается как принадлежащая организации (а не пользователю, ее создавшему). Решения о разрешении или отказе в доступе принимаются на основе информации о той функции (роли), которую пользователь выполняет в организации. Роль можно понимать как множество действий, которые разрешены пользователю для выполнения его должностных обязанностей. Администратор описывает роли и авторизует пользователей на выполнение данной роли. Таким образом, ролевые модели содержат как признаки мандатных, так и признаки избирательных моделей.

1.4.1. Модель Харрисона-Рузо-Ульмана

Модель Харрисона-Рузо-Ульмана (матричная модель) используется для анализа системы защиты, реализующей дискреционную политику безопасности. При этом система представляется конечным автоматом, функционирующим согласно определенным правилам перехода.

С одной стороны, общая модель Харрисона-Рузо-Ульмана может выражать большое разнообразие политик дискреционного доступа, но при этом не существует алгоритма проверки их безопасности. С другой стороны, можно предпочесть монооперационную систему, для которой алгоритм проверки безопасности существует, но данный класс систем является слишком узким. Например, монооперационные системы не могут выразить политику, дающую субъектам права на созданные ими объекты, т. к. не существует одной операции, которая и создает объект, и одновременно помечает его как принадлежащий создающему субъекту.

1.4.2. Модель Белла-ЛаПадула

Классической мандатной моделью безопасности является модель Белла-ЛаПадула. В ней для описания системы используются:

S – множество субъектов (например, множество пользователей и программ);

O – множество объектов (например, множество файлов);

L – линейно упорядоченное множество уровней безопасности (например, «общий доступ», «для служебного пользования», «секретно», «совершенно секретно»).

Несмотря на достоинства модели Белла-ЛаПадула, при ее строгой реализации в реальных АС возникает ряд проблем.

1. *Завышение уровня секретности,* связанное с одноуровневой природой объектов и правилом безопасности по записи. Если субъект с высоким уровнем доступа хочет записать что-то в объект с низким уровнем секретности, то сначала приходится повысить уровень секретности объекта, а потом осуществлять запись. Таким образом, даже один параграф, добавленный в большой документ субъектом с высоким уровнем доступа, повышает уровень секретности всего этого документа. Если по ходу работы изменения в документ вносят субъекты со все более высоким уровнем доступа, уровень секретности документа также постоянно растет.

2. *Запись вслепую.* Эта проблема возникает, когда субъект производит операцию записи в объект с более высоким уровнем безопасности, чем его

собственный. В этом случае после завершения операции записи субъект не сможет проверить правильность выполнения записи при помощи контрольного чтения, так как ему это запрещено в соответствии с правилом безопасности по чтению.

3. *Проблема удаленного чтения-записи.* В распределенных системах при удаленном чтении файла создаются два потока: от субъекта к объекту (запросы на чтение, подтверждения, прочая служебная информация) и от объекта к субъекту (сами запрашиваемые данные). При этом, например, если F(s) > F(o), то первый поток будет противоречить свойству безопасности по записи. На практике для решения этой проблемы надо разделять служебные потоки (запросы, подтверждения) и собственно передачу информации.

4. *Доверенные субъекты.* Модель Белла-ЛаПадула не учитывает, что в реальной системе, как правило, существуют субъекты, действующие в интересах администратора, а также системные процессы, например, драйверы. Жесткое соблюдение правил запрета чтения с верхнего уровня и запрета записи на нижний уровень в ряде случаев делает невозможной работу подобных процессов. Соответственно, их также приходится выделять.

1.4.3. Ролевая модель безопасности

Ролевая модель безопасности появилась как результат развития дискреционной модели. Однако она обладает новыми по отношению к исходной модели свойствами: управление доступом в ней осуществляется как на основе определения прав доступа для ролей, так и путем сопоставления ролей пользователям и установки правил, регламентирующих использование ролей во время сеансов.

В ролевой модели понятие «субъект» замещается понятиями «пользователь» и «роль». Пользователь – человек, работающий с системой и выполняющий определенные служебные обязанности. Роль – это активно действующая в системе абстрактная сущность, с которой связан набор полномочий, необходимых для выполнения определенной деятельности. Подобное разделение хорошо отражает особенности деятельности различных организаций, что привело к распространению ролевых политик безопасности. При этом как один пользователь может быть авторизован администратором на выполнение одной или нескольких ролей, так и одна роль может быть сопоставлена одному или нескольким пользователям.

При использовании ролевой политики управление доступом

осуществляется в две стадии:

– для каждой роли указывается набор полномочий (разрешений на доступ к различным объектам системы);

– каждому пользователю сопоставляется список доступных ему ролей.

При определении ролевой политики безопасности используются следующие множества:

U – множество пользователей;

R – множество ролей;

P – множество полномочий (разрешений) на доступ к объектам системы;

S – множество сеансов работы пользователя с системой.

Существует несколько разновидностей ролевых моделей управления доступом, различающихся видом функций *user* и *roles*, а также ограничениями, накладываемыми на множества *PA* и *UA*. В частности, может определяться иерархическая организация ролей, при которой роли организуются в иерархии, и каждая роль наследует полномочия всех подчиненных ей ролей.

Могут быть определены взаимоисключающие роли (т. е. такие роли, которые не могут быть одновременно назначены одному пользователю). Также может вводиться ограничение на одновременное использование ролей в рамках одной сессии, количественные ограничения при назначении ролей и полномочий, может производиться группировка ролей и полномочий.

1.5. Процесс построения и оценки системы обеспечения безопасности. Стандарт ISO/IEC 15408

Одним из наиболее распространенных современных стандартов в области информационной безопасности является международный стандарт ISO/IEC 15408. Он был разработан на основе стандарта «Общие критерии безопасности информационных технологий». В 2002 году этот стандарт был принят в России как ГОСТ Р ИСО/МЭК 15408–2002 «Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий» [4], часто называемый в литературе «Общие критерии».

Стандарт разработан таким образом, чтобы удовлетворить потребности трех групп специалистов: разработчиков, экспертов по сертификации и пользователей объекта оценки. Под объектом оценки (ОО) в стандарте понимаются «подлежащие оценке продукт информационных технологий (ИТ)

или система с руководствами администратора и пользователя». К таким объектам относятся, например, операционные системы, прикладные программы, информационные системы и т.д.

«Общие критерии» предусматривают наличие двух типов требований безопасности – функциональных и доверия. Функциональные требования относятся к сервисам безопасности, таким как управление доступом, аудит и т.д. Требования доверия к безопасности относятся к технологии разработки, тестированию, анализу уязвимостей, поставке, сопровождению, эксплуатационной документации и т.д.

Описание обоих типов требований выполнено в едином стиле: они организованы в иерархию «класс – семейство – компонент – элемент». Термин «класс» используется для наиболее общей группировки требований безопасности, а элемент – самый нижний, неделимый уровень требований безопасности. В стандарте выделены 11 классов функциональных требований:

- аудит безопасности;
- связь (передача данных);
- криптографическая поддержка (криптографическая защита);
- защита данных пользователя;
- идентификация и аутентификация;
- управление безопасностью;
- приватность (конфиденциальность);
- защита функций безопасности объекта;
- использование ресурсов;
- доступ к объекту оценки;
- доверенный маршрут/канал.

Основные структуры, определяемые «Общими критериями» – это профиль защиты и задание по безопасности. Профиль защиты – это независимая от реализации совокупность требований безопасности для некоторой категории ОО, отвечающая специфическим запросам потребителя. Профиль состоит из компонентов или пакетов функциональных требований и одного из уровней гарантированности. Профиль определяет «модель» системы безопасности или отдельного ее модуля. Количество профилей потенциально не ограничено, они разрабатываются для разных областей применения (например, профиль «Специализированные средства защиты от несанкционированного доступа к конфиденциальной информации»).

Профиль защиты служит основой для создания задания по безопасности, которое можно рассматривать как технический проект для разработки ОО. Задание по безопасности может включать требования одного или нескольких профилей защиты. Оно описывает также уровень функциональных возможностей средств и механизмов защиты, реализованных в ОО, и приводит обоснование степени их адекватности.

По результатам проводимых оценок, создаются каталоги сертифицированных профилей защиты и продуктов (операционных систем, средств защиты информации и т.д.), которые затем используются при оценке других объектов.

Глава 2. ОСНОВЫ КРИПТОГРАФИИ

2.1. Основные понятия. Классификация шифров

Исторически *криптография* (в переводе с греческого – «тайнопись») зародилась как способ скрытой передачи сообщений без сокрытия самого факта их передачи [3, 5]. Для этой цели сообщение, написанное с использованием какого-либо общепринятого языка, преобразовывалось под управлением дополнительной информации, называемой *ключом.* Результат преобразования, называемый *криптограммой,* содержит исходную информацию в полном объеме, однако последовательность знаков в нем внешне представляется случайной и не позволяет восстановить исходную информацию без знания ключа.

Процедура преобразования называется *шифрованием,* обратного преобразования – *расшифровыванием*.

Сейчас *криптографией* принято называть науку о математических методах обеспечения конфиденциальности и аутентичности (целостности и подлинности) информации. Задачей исследования методов преодоления криптографической защиты занимается *криптоанализ.* Для обозначения совокупности криптографии и криптоанализа используется термин «*криптология*».

Несмотря на то, что шифры применялись еще до нашей эры, как научное направление современная криптография относительно молода. Одной из важнейших работ в данной области является статья Клода Шеннона (Claude Shannon) «Теория связи в секретных системах», опубликованная в открытой печати в 1949 году. На стороне отправителя имеются два источника информации – источник сообщений и источник ключей. Источник ключей выбирает из множества всех возможных ключей один ключ *K*, который будет использоваться в этот раз. Ключ передается отправителю и получателю сообщения таким образом, что его невозможно перехватить.

Секретная система (или в современной терминологии – *шифр)* определяется как семейство однозначно обратимых отображений множества возможных сообщений во множество криптограмм.

Процесс расшифровывания сообщения для легального получателя информации состоит в применении криптографического отображения, обратного по отношению к отображению, использованному при шифровании. Процесс расшифровки для противника представляет собой попытку определить сообщение (или конкретный ключ), имея в распоряжении только криптограмму и априорные вероятности различных ключей и сообщений.

Существуют шифры, для которых любой объем перехваченной информации недостаточен для того, чтобы найти шифрующее отображение. Шифры такого типа называются *безусловно стойкими.* Иными словами, безусловно стойкими являются такие шифры, для которых криптоаналитик (даже если он обладает бесконечными вычислительными ресурсами) не может улучшить оценку исходного сообщения M на основе знания криптограммы C по сравнению с оценкой при неизвестной криптограмме.

Шифры другого типа характеризуются тем, что при определенном объеме перехваченных данных определить ключ (или расшифровать сообщение без знания ключа) становится теоретически возможно. Минимальный объем криптограммы, для которого существует единственное решение криптоаналитической задачи, называется *интервалом единственности.* Однако для криптоаналитика, обладающего ограниченными вычислительными ресурсами, вероятность найти это решение за время, в течение которого информация представляет ценность, чрезвычайно мала. Шифры такого типа называются *условно стойкими.* Их стойкость основана на высокой вычислительной сложности «взлома» шифра. Большинство применяемых сейчас шифров относятся к этому типу.

Доказано, что безусловно стойкие шифры существуют. Но для их построения необходимо использовать равновероятный случайный ключ, имеющий длину, равную длине сообщения. При соблюдении этого условия сама процедура преобразования может быть достаточно простой.

Рассмотрим, какими же свойствами должен обладать хороший шифр. Во–первых, шифрование и расшифровывание должно осуществляться достаточно быстро в тех условиях, в которых применяется шифр (с использованием ЭВМ, при шифровании вручную и т. п.). Во–вторых, шифр должен надежно защищать сообщение, т. е. быть стойким к раскрытию.

Криптостойкость – стойкость шифра к раскрытию методами криптоанализа. Она определяется вычислительной сложностью алгоритмов, применяемых для атаки на шифр. Вычислительная сложность измеряется временной и емкостной сложностями [6].

Для определения сложности алгоритма с конкретной задачей связывается число, называемое *размером задачи,* которое характеризует количество входных данных. Например, для задачи умножения чисел размером может быть длина наибольшего из сомножителей.

Временная сложность (или просто сложность) – это время, затрачиваемое алгоритмом для решения задачи, рассматриваемое как функция от размера задачи. Нередко сложность измеряют количеством некоторых элементарных операций. *Емкостная сложность* – объем памяти, необходимой для хранения полученных в ходе работы данных, как функция от размера задачи.

Очень важное требование к стойкому шифру было сформулировано в XIX веке голландским криптографом Огюстом Керкгоффсом (Auguste Kerckhoffs). В соответствии с ним, при оценке надежности шифрования необходимо предполагать, что противник знает все об используемой системе шифрования, кроме применяемых ключей. Данное правило отражает важный принцип организации защиты информации: защищенность системы не должна зависеть от секретности долговременных элементов (т. е. таких элементов, которые невозможно было бы быстро изменить в случае утечки секретной информации).

Существует несколько обобщенных постановок задачи криптоанализа. Все они формулируются в предположении, что криптоаналитику известны применяемый алгоритм шифрования и полученные криптограммы. Могут рассматриваться:

- атака при наличии только известной криптограммы;
- атака при наличии известного фрагмента открытого текста. В этом случае, криптоаналитик имеет доступ к криптограммам, а также к соответствующим некоторым из них исходным сообщениям. Задача – определить использующийся при шифровании ключ или расшифровать все остальные сообщения. Разновидность данного класса атак – атака с возможностью выбора открытого текста (когда криптоаналитик может навязать текст для шифрования и получить соответствующую ему криптограмму);
- атаки, использующие особенности реализации аппаратных шифраторов. В частности, может анализироваться тепловое и электромагнитное излучение от устройств, распространение ошибок после однократного воздействия на

аппаратуру (по цепи электропитания или иным образом) и т.д.;

- атака методом полного перебора множества возможных ключей. Данная атака также называется «атака методом грубой силы» (от англ. «brute force»).

ВИДЫ ШИФРОВ

Рассмотрим классификации шифров по разным признакам. По типу преобразований шифры можно разделить на следующие группы:

- шифры замены (подстановки);
- шифры перестановки;
- шифры гаммирования;
- шифры на основе аналитических преобразований.

При этом надо учитывать, что некоторые современные шифры совместно используют преобразования различных типов.

Шифры замены (подстановки): преобразование заключается в том, что символы шифруемого текста заменяются символами того или иного алфавита (алфавита криптограммы) в соответствии с заранее обусловленной схемой замены.

Подстановки разделяются на *одноалфавитные* и *многоалфавитные*. В первом случае определенному символу алфавита исходного сообщения всегда ставится в соответствие один и тот же символ алфавита криптограммы. Один из наиболее известных шифров данного класса – шифр Цезаря. В нем каждая буква алфавита заменялась на следующую через одну после нее. В случае русского алфавита, «а» меняется на «в», «б» на «г» и т.д. Алфавит «замыкался», поэтому «я» надо было заменять на «б». В качестве ключа в данном случае выступает число, на которое надо «сдвигать» символ алфавита, в нашем примере – 2. К достоинству таких шифров относится простота преобразования. Но они легко взламываются путем сравнения частоты появления различных символов в естественном языке и криптограмме.

При использовании многоалфавитных подстановок учитываются дополнительные параметры (например, положение преобразуемого символа в тексте), и в зависимости от них символ исходного алфавита может заменяться на один из нескольких символов алфавита шифртекста. Например, нечетные символы сообщения заменяются по одному правилу, четные – по-другому.

Шифры перестановок: шифрование заключается в том, что символы исходного текста переставляются по определенному правилу в пределах блока этого текста. При достаточной длине блока и сложном, неповторяющемся

порядке перестановки можно достичь приемлемой стойкости шифра.

Шифрование *гаммированием* заключается в том, что символы шифруемого текста складываются с символами некоторой случайной последовательности, называемой гаммой шифра или ключевой гаммой. Стойкость шифрования определяется длиной (периодом) неповторяющейся части гаммы шифра, а также сложностью предугадывания следующих элементов гаммы по предыдущим.

Шифрование *аналитическими преобразованиями* подразумевает использование аналитического правила (формулы) по которому преобразуется текст.

По типу использования ключей шифры делятся на:

- *симметричные,* использующие для шифрования и расшифровывания информации один и тот же ключ;
- *асимметричные,* использующие для шифрования и расшифровывания два различных ключа.

По размеру преобразуемого блока шифры делятся на блочные и потоковые.

Блочные шифры осуществляют преобразование информации блоками фиксированной длины. Если длина шифруемого сообщения некратна размеру блока, то его добавляют до нужной длины последовательностью специального вида. Например, это может быть последовательность 100...0. После расшифровки последний блок просматривают справа налево и отбрасывают «хвост» до первой единицы включительно. Чтобы подобное дополнение было применимо во всех случаях, если сообщение кратно длине блока, в его конец надо добавить целый блок указанного вида.

Потоковые шифры предназначены для преобразования сообщения поэлементно (элементом может быть бит, символ и т. п.). Примером такого вида шифров являются шифры гаммирования.

2.2. Симметричные шифры

2.2.1. Схема Фейстеля

Современные блочные шифры часто строятся на базе многократного повторения некоторого набора операций преобразования, называемых *раундом шифрования.*

В каждом раунде используется некоторая часть ключа, называемая

раундовым ключом. Порядок генерации и использования раундовых ключей называется *расписанием использования ключа шифрования.*

Для разработки итерационных блочных шифров широко используется схема, предложенная в начале 1970-х годов Хорстом Фейстелем (Horst Feistel). Данная схема, также называемая сетью Фейстеля. Ее достоинство заключается в том, что она позволяет использовать любые (в том числе необратимые) функции F для реализации обратимых шифрующих преобразований.

2.2.2. Шифр DES

Алгоритм шифрования DES (от англ. «Data Encryption Standard») был опубликован в 1977 году и предназначался для защиты важной, но несекретной информации в государственных и коммерческих организациях США. Реализованные в нем идеи были во многом позаимствованы в более ранней разработке корпорации IBM – шифре «Люцифер» (а как раз в IBM работал Хорст Фейстель, автор рассмотренной выше схемы). Но для своего времени «Люцифер» был слишком сложным, и его реализации отличались низким быстродействием.

Шифр DES является блочным – преобразования в нем проводятся блоками по 64 бита. Ключ также 64-битный, но значащими являются только 56 бит – каждый 8-й разряд использовался для контроля четности (шифр разрабатывался тогда, когда аппаратура была не слишком надежной и подобные проверки были необходимы).

Для того чтобы иметь возможность использовать шифр DES для решения различных криптографических задач, определены 4 режима его работы:

- электронная кодовая книга (англ. «Electronic Code Book» – ECB);
- сцепление блоков шифра (англ. «Cipher Block Chaining» – CBC);
- обратная связь по шифртексту (англ. «Cipher FeedBack» – CFB);
- обратная связь по выходу (англ. «Output FeedBack» – OFB).

При использовании *режима ECB* защищаемое сообщение разбивают на 64-битные блоки M_i. Каждый такой блок шифруют независимо от других, с использованием одного и того же ключа шифрования.

Достоинством данного режима является простота его реализации. Главный недостаток режима ECB заключается в том, что если в исходном сообщении есть повторяющиеся блоки, то и значения соответствующих блоков криптограммы будет совпадать. А это даст криптоаналитику противника дополнительную информацию о содержании сообщения. Поэтому режим ECB рекомендуют

использовать для защиты небольших объемов данных (например, криптографических ключей), где вероятность появления совпадающих блоков сообщения невелика.

Режим CBC используется для шифрования больших сообщений. Как легко заметить, последний блок криптограммы зависит от инициализирующего вектора, каждого бита открытого текста и значения секретного ключа. Поэтому его можно использовать для контроля целостности и аутентификации сообщений, задавая ему фиксированное значение и проверяя его после расшифровки.

Некоторое время шифр DES считался достаточно безопасным. Но по мере развития вычислительной техники короткий 56-битный ключ привел к тому, что атака путем полного перебора ключевого множества стала относительно легко реализуемой. Чтобы увеличить стойкость алгоритма и в то же время сохранить существующие наработки (в виде программных и аппаратных реализаций алгоритма), было использовано многократное шифрование.

Более надежной оказалась схема, включающая шифрование, расшифровывание и повторное шифрование на различных ключах. Данный шифр получил название Triple DES.

Использование в шифре Triple DES различных ключей и преобразований (шифрование и расшифровывание) позволяет противостоять атаке «встреча посередине». За счет более высокой надежности в настоящее время шифр Triple DES используется чаще, чем шифр DES.

2.2.3. Шифр ГОСТ 28147–89

Данный алгоритм симметричного шифрования был разработан и утвержден в качестве стандарта в 1989 году. Он считается достаточно стойким и широко используется в России теми предприятиями и организациями, которым, в силу особенностей сферы их деятельности, необходимо применять сертифицированные средства криптографической защиты данных (это государственные и военные структуры, организации банковской сферы и т.д.).

Этот шифр преобразует сообщение 64-битными блоками, преобразование осуществляется в соответствии со схемой Фейстеля в 32 раунда, размер ключа – 256 бит. Алгоритм предусматривает 4 режима работы:

- шифрование данных в режиме простой замены (аналог режима ECB для шифра DES);

- шифрование данных в режиме гаммирования (аналог режима OFB для шифра DES);
- шифрование данных в режиме гаммирования с обратной связью;
- выработка имитовставки.

По сравнению с шифром DES у ГОСТ 28147–89 есть следующие достоинства:

- существенно более длинный ключ (256 бит против 56 у шифра DES), атака на который путем полного перебора ключевого множества на данный момент представляется невыполнимой;
- простое расписание использования ключа, что упрощает реализацию алгоритма и повышает скорость вычислений.

2.2.4. Шифр Blowfish

Шифр Blowfish был разработан известным американским криптографом Брюсом Шнейером (Bruce Schneier) в 1993 году. Алгоритм ориентирован на программную реализацию на 32-разрядных микропроцессорах. Его отличают высокая скорость и криптостойкость. Также в качестве отличительной особенности можно назвать возможность использовать ключ переменной длины. Шифр блочный, размер входного блока равен 64 битам. Преобразование блока выполняется в 16 раундов (есть версия с 111-ю раундами). Ключ переменной длины, максимально 448 бит.

До начала шифрования или расшифровывания данных производится расширение ключа. В результате, на базе секретного ключа получают расширенный, который представляет собой массив из 18 раундовых ключей K_1, ..., K_{18} (размерность K – 32 бита) и матрицу подстановок Q с 4-мя строками, 256-ю столбцами и 32-битными элементами. Данная матрица используется для задания нелинейной функции шифрующего преобразования $F(X)$, где X – 32-битный аргумент.

Расширение ключа требует шифрования 521 блока данных. Эта процедура дополнительно осложняет атаку путем перебора ключевого множества, т. к. нарушитель будет вынужден проводить процедуру расширения для каждого возможного ключа.

2.3. Управление криптографическими ключами для симметричных шифров

Под *ключевой информацией* понимают совокупность всех ключей, действующих в системе. Если не обеспечено достаточно надежное и безопасное управление ключевой информацией, то эффект от применения криптографической защиты данных может быть сведен к нулю: завладев ключами нарушитель сможет получить доступ и к защищаемой информации. Процесс управления ключами включает в себя реализацию трех основных функций:

- генерация ключей;
- хранение ключей;
- распределение ключей.

Генерация ключей должна производиться таким образом, чтобы предугадать значение ключа (даже зная, как он будет генерироваться) было практически невозможно. В идеальном случае, вероятность выбора конкретного ключа из множества допустимых равна 1/N, где N – мощность ключевого множества (число его элементов).

Для получения ключей используют аппаратные и программные средства генерации случайных значений. Для систем с высокими требованиями к уровню безопасности более предпочтительными считаются аппаратные датчики, основанные на случайных физических процессах. В то же время, из-за дешевизны и возможности неограниченного тиражирования наиболее распространенными являются программные реализации. Но надо учитывать, что получаемая в этом случае последовательность будет псевдослучайной – если программный генератор повторно запустить с такими же начальными значениями, он выдаст ту же последовательность.

В программных генераторах ключей нередко используют алгоритмы шифрования и ключи, специально резервируемые для задач генерации. В качестве начальных значений могут браться, например, значения таймера вычислительной системы.

Рекомендуется регулярно проводить замену ключей, используемых в системе. В некоторых случаях вместо замены допустимо использовать процедуру модификации. *Модификация ключа* – генерация нового ключа из предыдущего значения с помощью односторонней функции (т. е. такой функции,

для которой обратное преобразование вычислить практически невозможно). Но в этом случае надо учитывать, что новый ключ безопасен в той же мере, что и прежний, т. к. противник может повторить всю цепочку модификаций.

При организации хранения ключей симметричного шифрования необходимо обеспечить такие условия работы, чтобы секретные ключи никогда были записаны в явном виде на носителе, к которому может получить доступ нарушитель. Например, это требование можно выполнить, создавая иерархии ключей. Трехуровневая иерархия подразумевает деление ключей на:

- главный ключ;
- ключ шифрования ключей;
- ключ шифрования данных (сеансовый ключ).

Сеансовые ключи – нижний уровень иерархии – используются для шифрования данных и аутентификации сообщений. Для защиты этих ключей при передаче или хранении используются *ключи шифрования ключей*, которые никогда не должны использоваться как сеансовые. На верхнем уровне иерархии располагается *главный ключ* (или мастер-ключ). Его применяют для защиты ключей второго уровня. Для защиты главного ключа в системах, использующих только симметричные шифры, приходится применять не криптографические средства, а, например, средства физической защиты данных (ключ записывается на съемный носитель, который после окончания работы изымается из системы и хранится в сейфе, и т. п.). В относительно небольших информационных системах может использоваться двухуровневая иерархия ключей (главный и сеансовые ключи).

При *распределении ключей* необходимо выполнить следующие требования:

- обеспечить оперативность и точность распределения ключей;
- обеспечить секретность распределения ключей.

Распределение ключей может производиться:

- с использованием одного или нескольких центров распределения ключей (централизованное распределение);
- прямым обменом сеансовыми ключами между пользователями сети (децентрализованное распределение ключей).

Децентрализованное распределение ключей симметричного шифрования требует наличия у каждого пользователя большого количества ключей (для связи с каждым из абонентов системы), которые необходимо сначала безопасно распределить, а потом обеспечивать их секретность в процессе хранения.

Централизованное распределение ключей симметричного шифрования

подразумевает, что у каждого пользователя есть только один основной ключ для взаимодействия с центром распределения ключей. Для обмена данными с другим абонентом, пользователь обращается к серверу ключей, который назначает этому пользователю и соответствующему абоненту сеансовый симметричный ключ. Одной из самых известных систем централизованного распределения ключей является Kerberos.

Протокол Kerberos был разработан в Массачусетском технологическом институте в середине 1980-х годов и сейчас является фактическим стандартом системы централизованной аутентификации и распределения ключей симметричного шифрования. Поддерживается операционными системами семейства Unix, Windows (начиная с Windows'2000), есть реализации для Mac OS.

Протокол Kerberos обеспечивает распределение ключей симметричного шифрования и проверку подлинности пользователей, работающих в незащищенной сети. Реализация Kerberos – это программная система, построенная по архитектуре «клиент-сервер». Клиентская часть устанавливается на все компьютеры защищаемой сети, кроме тех, на которые устанавливаются компоненты сервера Kerberos. В роли клиентов Kerberos могут, в частности, выступать и сетевые серверы (файловые серверы, серверы печати и т.д.).

Серверная часть Kerberos называется центром распределения ключей (англ. «Key Distribution Center», сокр. KDC) и состоит из двух компонент:

- сервер аутентификации (англ. «Authentication Server», сокр. AS);
- сервер выдачи разрешений (англ. «Ticket Granting Server», сокр. TGS).

Каждому субъекту сети сервер Kerberos назначает разделяемый с ним ключ симметричного шифрования и поддерживает базу данных субъектов и их секретных ключей.

2.4. Асимметричные шифры

2.4.1. Основные понятия

Несмотря на достижения в области симметричной криптографии, к середине 1970-х годов стала остро осознаваться проблема неприменимости данных методов для решения целого ряда задач.

Во-первых, при использовании симметричных шифров необходимо отдельно решать часто нетривиальную задачу распределения ключей. Несмотря на использование иерархий ключей и центров распределения, в какой-то

начальный момент ключ (или мастер-ключ) должен быть передан по безопасному каналу. Но такого канала может просто не быть, или он может быть достаточно дорогостоящим.

Во-вторых, при использовании методов симметричного шифрования подразумевается взаимное доверие сторон, участвующих во взаимодействии. Если это не так, совместное использование одного и того же секретного ключа может быть нежелательно.

Третья проблема связана с необходимостью проведения аутентификации информации и защиты от угроз, связанных с отказом отправителя (получателя) от факта отправки (получения) сообщений.

Перечисленные проблемы являются весьма существенными, и работа над их решением привела к появлению асимметричной криптографии, также называемой криптографией с открытым ключом.

В частности, односторонняя функция с секретом может быть использована для шифрования информации. Пусть M – исходное сообщение. Получатель выбирает одностороннюю функцию с секретом, и тогда любой, кто знает эту функцию, может зашифровать сообщение для данного получателя, вычислив значение криптограммы $C = F_k(M)$. Расшифровать данную криптограмму может только законный получатель, которому известен секрет k.

Первой публикацией в области криптографии с открытым ключом принято считать статью Уитфилда Диффи (Whitfield Diffie) и Мартина Хеллмана (Martin Hellman) «Новые направления в криптографии», вышедшую в свет в 1976 году.

В отличие от симметричных, в асимметричных алгоритмах ключи используются парами – открытый ключ (англ. «public key») и секретный или закрытый (англ. «private key»). Схема шифрования будет выглядеть следующим образом.

Получатель B генерирует пару ключей – открытый K_{Bpub} и секретный K_{Bpr}. Процедура генерация ключа должна быть такой, чтобы выполнялись следующие условия:

1) ключевую пару можно было бы легко сгенерировать;
2) сообщение, зашифрованное на открытом ключе, может быть расшифровано только с использованием секретного ключа;
3) зная только открытый ключ, невозможно рассчитать значение секретного.

Пересылка открытого ключа может осуществляться по незащищенному каналу связи. Нарушитель даже в том случае, если он смог перехватить криптограмму и открытый ключ, не может расшифровать криптограмму.

РАССМОТРИМ ТЕПЕРЬ ВОПРОС АУТЕНТИФИКАЦИИ СООБЩЕНИЙ

Электронная цифровая подпись (ЭЦП)[2] – это реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе, а также обеспечивать неотказуемость подписавшегося.

Функции ЭЦП аналогичны обычной рукописной подписи:

- удостоверить, что подписанный текст исходит от лица, поставившего подпись;
- не дать лицу, подписавшему документ, возможности отказаться от обязательств, связанных с подписанным текстом;
- гарантировать целостность подписанного текста.

Важное отличие ЭЦП заключается в том, что электронный документ вместе с подписью может быть скопирован неограниченное число раз, при этом копия будет неотличима от оригинала.

В ходе преобразований здесь используется пара ключей отправителя сообщения. Тот факт, что при вычислении ЭЦП применяется секретный ключ отправителя, позволяет доказать происхождение и подлинность сообщения. Получатель, имея открытый ключ отправителя, проверяет ЭЦП, и если подпись корректна, то он может считать, что сообщение подлинное.

2.4.2. Распределение ключей по схеме Диффи-Хеллмана

Основы асимметричной криптографии были заложены американскими исследователями У. Диффи и М. Хеллманом. Ими был предложен алгоритм, позволяющий двум абонентам, обмениваясь сообщениями по небезопасному каналу связи, распределить между собой секретный ключ шифрования. Нарушитель, который может перехватить передаваемые открытые ключи Y_A и Y_B, должен попытаться по ним вычислить общий секретный ключ без знания секретных ключей абонентов. На данный момент не найдено существенно лучшего пути решения данной задачи, чем дискретное логарифмирование, что и обеспечивает криптографическую стойкость алгоритма.

[2] Определение в соответствии федеральным законом Российской Федерации «Об электронной цифровой подписи».

2.4.3. Криптографическая система RSA

Алгоритм RSA был предложен в 1977 году и стал первым полноценным алгоритмом асимметричного шифрования и электронной цифровой подписи. Алгоритм назван по первым буквам фамилий авторов – Рональд Райвест (Ronald Rivest), Ади Шамир (Adi Shamir) и Леонард Адлеман (Leonard Adleman). Стойкость алгоритма основывается на вычислительной сложности задачи факторизации (разложения на множители) больших чисел и задачи дискретного логарифмирования.

2.4.4. Криптографическая система Эль-Гамаля

В 1984 году американским исследователем египетского происхождения Тахером Эль-Гамалем (Taher Elgamal) были опубликованы алгоритмы шифрования с открытым ключом и ЭЦП, получившие его имя. Криптографическая система Эль-Гамаля использует ту же математическую основу, что и рассмотренная ранее схема распределения ключей Диффи-Хеллмана: в качестве односторонней функции в этой криптосистеме используется возведение в степень по модулю большого простого числа.

2.4.5. Совместное использование симметричных и асимметричных шифров

Основным достоинством криптографических алгоритмов с открытым ключом является возможность решения таких задач, как распределение ключа по небезопасному каналу, аутентификации сообщения и отправителя и т.д. В то же время асимметричные шифры работают существенно более медленно, чем симметричные. Это связано с необходимостью производить операции над сверхбольшими числами. Поэтому симметричные и асимметричные алгоритмы часто используют вместе – для распределения ключей и ЭЦП используют криптографию с открытым ключом, данные шифруют с помощью симметричных алгоритмов.

При анализе системы, в которой совместно используются несколько алгоритмов, принято оценивать сложность ее взлома по сложности взлома самого слабого звена. В литературе [7] приводится примерное соответствие длин ключей для алгоритма симметричного шифрования (атака производится путем перебора ключевого множества) и алгоритма RSA, обеспечивающих сопоставимую стойкость. Например, 64-битному ключу симметричного шифрования примерно соответствует 512-битный ключ RSA, а 128-битному – ключ RSA длиной более 2300 бит.

2.5. Хэш-функции

В рассмотренных алгоритмах формирования ЭЦП длина подписи получается равной или даже большей, чем длина самого сообщения. Очевидно, что удостоверять подобным образом большой документ неудобно. Поэтому подписывается, как правило, не само сообщение, а его «дайджест» – значение фиксированной длины, зависящее от подписываемого сообщения. Для формирования дайджеста используется *хэш-функция* (от англ. «hash function») – односторонняя функция, преобразующая строку произвольной длины в строку фиксированной длины. В криптографии используются хэш-функции 2 классов:

- хэш-функции без ключа;
- хэш-функции с ключом.

2.5.1. Алгоритм SHA-1

Алгоритм SHA (Secure Hash Algorithm) разработан в США как часть стандарта SHS (Secure Hash Standard), опубликованного в 1993 году. Но в нем были обнаружены уязвимости, которые привели к необходимости модифицировать алгоритм. Через два года была опубликована новая версия – SHA-1, получившая на сегодняшний день широкое распространение.

Получая на входе сообщение произвольной длины менее 264 бит, SHA-1 формирует 160-битное выходное сообщение (дайджест). Вначале преобразуемое сообщение M дополняется до длины, кратной 512 битам. Заполнитель формируется следующим образом: в конец преобразуемого сообщения добавляется 1, потом – столько нулей, сколько необходимо для получения сообщения, которое на 64 бита короче, чем кратное 512, после чего добавляют 64-битное представление длины исходного сообщения. Например, если сообщение длиной 800 бит, то 801-й бит = 1, потом добавляем нули до 960 бит, после чего в оставшихся 64-разрядах записывается число «800», в итоге хэшируем 1024-битное сообщение.

Перед началом преобразований инициализируется пять 32-битных переменных:

A = 0x67452301;

B = 0xEFCDAB89;

C = 0x98BADCFE;

D = 0x10325476;

E = 0xC3D2E1F0.

Эти значения присваиваются также переменным a_0, b_0, c_0, d_0, e_0. Преобразование производится над блоком сообщения размером 512 бит в 80 раундов. В процессе преобразования используются нелинейные функции.

После преобразования очередного 512-битного блока полученные значения *a, b, c, d, e* складываются со значениями *A, B, C, D, E* соответственно, и начинается обработка следующего блока (или полученное значение в виде сцепления *a, b, c, d, e* подается на выход, если обработанный блок был последним). Таким образом, на выходе получаем 160-битный дайджест исходного сообщения.

2.5.2. Хэш-функции с ключом

Хэш-функцией с ключом называется односторонняя функция *H(k,x)* со следующими свойствами:

- аргумент *x* функции *H(k,x)* может быть строкой бит произвольной длины;
- значение функции должно быть строкой бит фиксированной длины;
- при любых данных *к* и *x* легко вычислить *H(k,x);*
- для любого *x* должно быть практически невозможно вычислить *H(k,x)*, не зная *к*.

Часто такие функции также называются *кодами аутентификации сообщений* (англ. «Message Authentication Code», сокр. MAC). В отечественной литературе используется также термин *имитозащитная вставка* (или просто *имитовставка*).

Хэш-функцию с ключом можно построить на базе криптографической хэш-функции без ключа или алгоритма шифрования.

2.6. Инфраструктура открытых ключей. Цифровые сертификаты

Использование методов асимметричной криптографии сделало возможным безопасный обмен криптографическими ключами между отправителем и получателем, которые никогда друг друга не встречали и, возможно, находятся за многие километры друг от друга.

Но возникает другая проблема – как убедиться в том, что имеющийся у Вас открытый ключ другого абонента на самом деле принадлежит ему. Иными

словами, возникает проблема аутентификации ключа. Без этого на криптографический протокол может быть осуществлена атака типа «человек посередине» (англ. «man in the middle»).

Для подтверждения подлинности открытых ключей создается инфраструктура открытых ключей (англ. «Public Key Infrastructure», сокр. PKI). PKI представляет собой набор средств, мер и правил, предназначенных для управления ключами, политикой безопасности и обменом защищенными сообщениями.

Наибольшее распространение получили цифровые сертификаты, формат которых определен стандартом X.509. На данный момент принята третья версия стандарта.

Серийный номер – уникальный номер, присваиваемый каждому сертификату.

Алгоритм подписи – идентификатор алгоритма, используемого при подписании сертификата. Должен совпадать с полем *Алгоритм ЭЦП.*

Изготовитель – имя центра сертификации, выдавшего сертификат. Записывается в формате Relative Distinguished Name – RDN (варианты перевода названия – «относительное отдельное имя», «относительное характерное имя»). Данный формат используется в службах каталога, в частности, в протоколе LDAP. При записи Relative Distinguished Name используются специальные ключевые слова: CN (англ. «Common Name») – общее имя; OU (англ. «Organization Unit») – организационная единица; DC (англ. «Domain Component») – составная часть доменного имени.

Субъект – имя владельца сертификата, представленное в том же формате RDN.

Период действия описывает временной интервал, в течение которого центр сертификации гарантирует отслеживание статуса сертификата (сообщит абонентам сети о факте досрочного отзыва сертификата и т.д.). Период задается датами начала и окончания действия.

Открытый ключ – составное поле, содержащее идентификатор алгоритма, для которого предназначается данный открытый ключ, и собственно сам открытый ключ в виде набора битов.

ID Изготовителя и *ID Субъекта* содержат уникальные идентификаторы центра сертификации и пользователя (на случай совпадения имен различных CA или пользователей).

Расширения – дополнительный атрибут, связанный с субъектом,

изготовителем или открытым ключом и предназначенный для управления процессами сертификации. Более подробно он описан ниже.

Алгоритм электронной цифровой подписи (ЭЦП) – идентификатор алгоритма, используемый для подписи сертификата. Должен совпадать со значением поля *Алгоритм подписи*.

ЭЦП – само значение электронно-цифровой подписи для данного сертификата.

Расширения могут определять следующие дополнительные параметры:

- идентификатор пары открытый/секретный ключ центра сертификации (изготовителя), если центр имеет несколько различных ключей для подписи сертификатов;
- идентификатор конкретного ключа пользователя (субъекта), если пользователь имеет несколько сертификатов;
- назначение ключа, например, ключ для шифрования данных, проверки ЭЦП данных, для проверки ЭЦП сертификатов и т.д.;
- уточнение периода использования – можно сократить время действия сертификата, указанное в поле *Период действия* (период, в течение которого статус сертификата отслеживается, станет больше, чем разрешенное время использования сертификата);
- политики использования сертификата;
- выбор соответствия политик использования сертификата для центра сертификации и пользователя, если имеются различные варианты;
- альтернативное имя пользователя и центра сертификации;
- указания, является ли пользователь сам центром сертификации, и насколько глубоко разрешается разворачивать сертификационный путь.

Номер версии определяет номер версии формата CRL. Текущая используемая версия – вторая.

Алгоритм подписи – идентификатор алгоритма, с помощью которого подписан CRL. Должен совпадать по значению с полем *Алгоритм ЭЦП.*

Изготовитель – имя центра сертификации в формате RDN.

Выпущен – дата выпуска CRL.

Следующий – дата, до которой будет выпущен следующий CRL.

Отозванный сертификат – таких полей будет столько, сколько сертификатов отзывается – содержит номер отзываемого сертификата, дату, с которой сертификат отозван, описание причины отзыва.

Алгоритм ЭЦП – идентификатор алгоритма ЭЦП, используемого для

подписи списка.

ЭЦП – сама электронная цифровая подпись.

Проблемы с CRL заключаются в том, что может возникнуть ситуация, когда ключ уже отозван, но CRL еще не выпущен, т. е. пользователи не могут получить информацию о компрометации ключа.

Кроме того, распространение CRL идет по запросу клиента, и нарушитель может препятствовать их получению.

Другая проблема PKI – самоподписанные сертификаты. Сертификат корневого ЦС должен раздаваться всем абонентам сети в начале работы и сохраняться в защищенном от подделки хранилище. Иначе нарушитель может попробовать навязать свой сертификат в качестве сертификата корневого центра.

Мы рассмотрели случай реализации *иерархической модели* PKI, при которой центры сертификации организованы в древовидную структуру с корневым центром сертификации на верху иерархии. На практике также встречаются другие варианты организации:

- *одиночный центр сертификации,* который выдает себе само–подписанный сертификат – данная модель часто реализуется в небольших организациях, но она имеет отмеченный выше недостаток, связанный с самоподписанными сертификатами;
- *одноранговая модель,* при которой независимые центры сертификации взаимно сертифицируют друг друга.

Надо отметить, что сфера применения цифровых сертификатов сейчас достаточно широка. В частности, они используются для распределения открытых ключей в протоколах защиты электронной почты S/MIME или PGP, с помощью цифровых сертификатов проверяется подлинность участников соединения по протоколу SSL и т.д.

Глава 3. ЗАЩИТА ИНФОРМАЦИИ В IP-СЕТЯХ

На сегодняшний день стек сетевых протоколов TCP/IP является наиболее широко используемым как в глобальных, так и в локальных компьютерных сетях. Именно поэтому методы и средства защиты передаваемых данных в IP-сетях представляют особый интерес.

В этом разделе будут рассмотрены криптографические протоколы, позволяющие защищать электронную почту, передаваемые данные на транспортном и сетевом уровне. Кроме того, учитывая большую роль межсетевых экранов в решении задач обеспечения сетевой безопасности, будет рассмотрен этот класс средств защиты.

3.1. Протокол защиты электронной почты S/MIME

Протокол Secure Multipurpose Internet Mail Extensions (S/MIME) предназначен для защиты данных, передаваемых в формате MIME, в основном – электронной почты. Он был предложен в 1995 году компанией RSA Data Security Inc. Дальнейшие работы над протоколом велись рабочей группой организации Internet Engineering Task Force (IETF), разрабатывающей стандарты сети Интернет. На данный момент последней является версия 3.1 этого протокола, описываемая в документах RFC 3850, 3851, 3852. Протокол S/MIME предоставляет следующие криптографические услуги безопасности (криптографические сервисы):

- проверка целостности сообщения;
- установление подлинности отправителя (аутентификация);
- обеспечение секретности передаваемых данных (шифрование).

Нужно отметить, что сам по себе формат MIME описывает порядок форматирования писем, содержащих различные типы данных (обычный текст, текст в формате html, видео и графические файлы различный типов и т.д.). При использовании S/MIME добавляются новые типы (например, application/pkcs7–mime и application/pkcs7– signature). Это позволяет указать на то, что данные в этом разделе являются зашифрованными, подписанными и т.д. Протокол позволяет обычным почтовым клиентам защищать исходящую почту и

интерпретировать криптографические сервисы, добавленные во входящую почту (расшифровывать сообщения, проверять их целостность и т.д.).

Стандарт определяет использование симметричных криптоалгоритмов для шифрования содержимого почтовых сообщений и алгоритма с открытым ключом для защиты передаваемого вместе с письмом ключа симметричного шифрования.

Протокол S/MIME позволяет использовать различные криптоалгоритмы, причем их список может расширяться. Изначально из симметричных шифров могли использоваться RC2, DES или TripleDES. Для формирования дайджестов – алгоритмы MD5 и SHA1, причем версия 3 стандарта рекомендует использовать именно последний алгоритм (из-за того, что он формирует более длинный дайджест и считается более надежным). Защита симметричного ключа шифрования и ЭЦП в версии 2 осуществляется с помощью алгоритма RSA с ключом от 512 до 1024 бит. Версия 3 добавляет возможность использовать другие алгоритмы, например алгоритм Диффи-Хеллмана с ключом длиной до 2048 бит. Распределение и аутентификация открытых ключей производится с помощью цифровых сертификатов формата X.509. Таким образом, чтобы защищать переписку с помощью этого протокола, оба абонента должны сгенерировать ключевые пары и удостоверить открытые ключи с помощью сертификатов.

S/MIME поддерживается многими почтовыми клиентами: Microsoft Outlook, Mozilla, The Bat! и т.д. Более широкое применение протокола сдерживается необходимостью наличия сертификатов у абонентов и плохой совместимостью с системами Web–почты.

Альтернативой S/MIME является PGP (англ. «Pretty Good Privacy») – компьютерная программа, созданная Филиппом Циммерманном (Philip Zimmermann) в 1991 году. Данная программа положила основу работе над стандартом OpenPGP, последняя версия которого описана в RFC 4880. По функциональности S/MIME и PGP во многом схожи.

3.2. Протоколы SSL и TLS

Протокол Secure Sockets Layer (SSL) был разработан корпорацией Netscape Communications для обеспечения аутентификации, целостности и секретности трафика на сеансовом уровне модели OSI (с точки зрения четырехуровневой

модели стека протоколов TCP/IP – на прикладном уровне). В январе 1999 года на смену SSL v3.0 пришел протокол TLS v1.0 (Transport Layer Security) последняя версия TLS v.1.2 описывается в RFC 5246. С точки зрения выполняемых действий, различия между этими протоколами SSL и TLS весьма невелики, в то же время, они несовместимы друг с другом [8].

SSL обеспечивает защищенное соединение, которое могут использовать протоколы более высокого уровня – HTTP, FTP, SMTP и т.д. Наиболее широко он используется для защиты данных, передаваемых по HTTP (режим HTTPS). Для этого должны использоваться SSL-совместимые web-сервер и браузер.

Протокол предусматривает два этапа взаимодействия клиента и сервера:

1) установление SSL-сессии (процедура «рукопожатия», от англ. «handshake»), на этом этапе может производиться аутентификация сторон соединения, распределение ключей сессии, определяются настраиваемые параметры соединения;

2) защищенное взаимодействие.

Протоколом SSL используются следующие криптоалгоритмы:

- асимметричные алгоритмы RSA и Диффи-Хеллмана;
- алгоритмы вычисления хэш-функций MD5 и SHA1;
- алгоритмы симметричного шифрования RC2, RC4, DES, TripleDES, IDEA.

В протоколе SSL v 3.0 и TLS перечень поддерживаемых алгоритмов является расширяемым. Для подтверждения подлинности открытых ключей используются цифровые сертификаты формата X.509.

Протокол SSL позволяет проводить следующие варианты аутентификации сторон взаимодействия:

- аутентификация сервера без аутентификации клиента (односторонняя аутентификация) – это наиболее часто используемый режим, позволяющий установить подлинность сервера, но не проводящий проверки клиента (ведь подобная проверка требует и от клиента наличия сертификата);
- взаимная аутентификация сторон (проверяется подлинность как клиента, так и сервера);
- отказ от аутентификации – полная анонимность; в данном случае SSL обеспечивает шифрование канала и проверку целостности, но не может защитить от атаки путем подмены участников взаимодействия.

Рассмотрим более подробно процедуру рукопожатия в режиме аутентификации сервера без аутентификации клиента. Она включает следующие шаги [9].

1. Клиент посылает серверу запрос на установление защищенного соединения, в котором передает, в частности, следующие параметры:

- дату и текущее время;
- сгенерированную клиентом случайную последовательность;
- перечень поддерживаемых клиентом алгоритмов шифрования, хеширования и сжатия (если сжатие используется).

2. Сервер обрабатывает запрос от клиента и передает ему согласованный набор параметров:

- идентификатор SSL-сессии;
- идентификаторы криптографических алгоритмов из числа предложенных клиентом, которые будут использоваться в данной сессии (если по какой-либо причине предложенные алгоритмы или их параметры не удовлетворяют требованиям сервера, сессия закрывается);
- цифровой сертификат сервера формата X.509;
- случайную последовательность (RAND_SERV).

3. Клиент проверяет полученный сертификат и соответствие роли ключа его назначению, описанному в сертификате. При отрицательном результате проверки сессия закрывается, а при положительном клиент выполняет следующие действия:

- генерирует случайную 48-байтную последовательность, называемую Pre_MasterSecret, предназначенную для расчета общего секретного ключа;
- шифрует значение Pre_MasterSecret с использованием открытого ключа сервера, взятого из сертификата, и посылает криптограмму серверу;
- с помощью согласованной с сервером хэш-функции формирует общий секретный ключ (MasterSecret), используя в качестве параметров последовательность Pre_MasterSecret, посланную ранее серверу случайную последовательность RAND_CL и полученную от него случайную последовательность RAND_SERV;
- используя значение MasterSecret, вычисляет криптографические параметры SSL-сессии: формирует общие с сервером сеансовые секретные ключи для симметричного шифрования и вычисления хэш-функций;
- переходит в режим защищенного взаимодействия.

4. Сервер, используя свой секретный ключ, расшифровывает полученное значение Pre_MasterSecret и выполняет те же операции, что и клиент:

- с помощью согласованной с клиентом хэш-функции формирует общий секретный мастер-ключ (MasterSecret), используя в качестве параметров

значение Pre_MasterSecret, а также посланную клиенту случайную последовательность RAND_SERV и полученную от него случайную последовательность RAND_CL;

- используя значение MasterSecret, вычисляет криптографические параметры SSL-сессии: формирует общие с клиентом сеансовые секретные ключи для симметричного шифрования и вычисления хэш-функций;
- переходит в режим защищенного взаимодействия.

Так как при формировании параметров SSL-сессии и клиент, и сервер пользовались одними и теми же исходными данными (согласованными алгоритмами, общей секретной последовательностью Pre_MasterSecret и случайными последовательностями RAND-CL и RAND-SERV), то очевидно, что в результате описанных выше действий они выработали одинаковые сеансовые секретные ключи. Для проверки идентичности параметров SSL-сессии клиент и сервер посылают друг другу тестовые сообщения, содержание которых известно каждой из сторон:

- клиент формирует сообщение из собственных посылок в адрес сервера на шаге 1 и посылок, полученных от сервера на шаге 2, внося элемент случайности в виде последовательности MasterSecret, уникальной для данной сессии; формирует код для проверки целостности сообщения (MAC), шифрует сообщение на общем сеансовом секретном ключе и отправляет серверу;
- сервер, в свою очередь, формирует сообщение из собственных посылок в адрес клиента на шаге 2, посылок, полученных от клиента на шаге 1, и последовательности MasterSecret; формирует код для проверки целостности сообщения (MAC), шифрует сообщение на общем сеансовом секретном ключе и отправляет клиенту;
- в случае успешной расшифровки и проверки каждой из сторон целостности полученных тестовых сообщений SSL-сессия считается установленной, и стороны переходят в штатный режим защищенного взаимодействия.

Необязательная вторая фаза рукопожатия позволяет аутентифицировать клиента. Она заключается в том, что сервер шлет запрос клиенту, клиент аутентифицирует себя, возвращая подписанное сообщение (запрос сервера) и свой цифровой сертификат.

В процессе защищенного взаимодействия с установленными криптографическими параметрами SSL-сессии выполняются следующие действия:

- каждая сторона при передаче сообщения формирует имитовставку (MAC) для последующей проверки целостности сообщения и затем зашифровывает исходное сообщение вместе с MAC по сеансовому секретному ключу;
- каждая сторона при приеме сообщения расшифровывает его и проверяет на целостность (вычисляется текущее значение MAC и сверяется со значением, полученным вместе с сообщением); в случае обнаружения нарушения целостности сообщения, SSL-сессия закрывается.

Протоколы SSL и TLS получили широкое распространение, прежде всего благодаря их использованию для защиты трафика, передаваемого по протоколу HTTP в сети Интернет. В то же время предоставляемые SSL услуги не являются прозрачными для приложений, т. е. сетевые приложения, которые хотят воспользоваться возможностями SSL, должны включать в себя реализацию протокола (или подключать ее в виде каких-то внешних модулей).

3.3. Протоколы IPSec и распределение ключей

Протокол IPSec или, если точнее, набор протоколов, разработан организацией IETF как базовый протокол обеспечения безопасности на уровне IP-соединения. Он является дополнением к использующемуся сейчас протоколу IP ver.4 и составной частью IP ver.6. Возможности, предоставляемые протоколами IPSec:

- контроль доступа;
- контроль целостности данных;
- аутентификация данных;
- защита от повторений;
- обеспечение конфиденциальности.

Основная задача IPSec – создание между двумя компьютерами, связанными через общедоступную (небезопасную) IP-сеть, безопасного туннеля, по которому передаются конфиденциальные или чувствительные к несанкционированному изменению данные. Подобный туннель создается с использованием криптографических методов защиты информации. Протокол работает на сетевом уровне модели OSI, и, соответственно, он «прозрачен» для приложений. Иными словами, на работу приложений (таких как web-сервер, браузер, СУБД и т.д.) не влияет, используется ли защита передаваемых данных с помощью IPSec или нет.

Архитектура IPSec является открытой, что позволяет использовать для защиты передаваемых данных новые криптографические алгоритмы, например, соответствующие национальным стандартам. Для этого необходимо, чтобы взаимодействующие стороны поддерживали эти алгоритмы, и они были бы стандартным образом зарегистрированы в описании параметров соединения.

Процесс защищенной передачи данных регулируется правилами безопасности, принятыми в системе. Параметры создаваемого туннеля описывает информационная структура, называемая контекст защиты или ассоциация безопасности (от англ. «Security Association», сокр. SA). Как уже отмечалось выше, IPSec является набором протоколов, и состав контекста защиты может различаться. В зависимости от конкретного протокола в него входит:

- IP-адрес получателя;
- указание на протоколы безопасности, используемые при передаче данных;
- ключи, необходимые для шифрования и формирования имитовставки (если это требуется);
- указание на метод форматирования, определяющий, каким образом создаются заголовки;
- индекс параметров защиты (от англ. «Security Parameter Index», сокр. SPI) – идентификатор, позволяющий найти нужный SA.

Обычно контекст защиты является однонаправленным, а для передачи данных по туннелю в обе стороны задействуются два SA. Каждый хост имеет свою базу контекстов защиты, из которой выбирается нужный элемент либо на основании значения SPI, либо по IP-адресу получателя.

Два протокола, входящие в состав IPSec, это:

1) протокол аутентифицирующего заголовка – AH (от англ. «Authentication Header»), обеспечивающий проверку целостности и аутентификацию передаваемых данных; последняя версия протокола описана в документе RFC 4302 (предыдущие – RFC 1826, 2402);

2) протокол инкапсулирующей защиты данных – ESP (от англ. «Encapsulating Security Payload»), обеспечивающий конфиденциальность и, опционально, проверку целостности и аутентификацию; описан в RFC 4303 (предыдущие версии – RFC 1827, 2406).

Оба эти протокола имеют два режима работы – транспортный и туннельный, последний определен в качестве основного. Туннельный режим используется, если хотя бы один из соединяющихся узлов является шлюзом безопасности. В

этом случае создается новый IP-заголовок, а исходный IP-пакет полностью инкапсулируется в новый.

Транспортный режим ориентирован на соединение хост-хост. При использовании ESP в транспортном режиме защищаются только данные IP-пакета, заголовок не затрагивается. При использовании AH защита распространяется на данные и часть полей заголовка.

3.4. Межсетевые экраны

Межсетевой экран (МЭ) – это средство защиты информации, осуществляющее анализ и фильтрацию проходящих через него сетевых пакетов. В зависимости от установленных правил МЭ пропускает или уничтожает пакеты, разрешая или запрещая таким образом сетевые соединения. МЭ является классическим средством защиты периметра компьютерной сети: он устанавливается на границе между внутренней (защищаемой) и внешней (потенциально опасной) сетями и контролирует соединения между узлами этих сетей. Но бывают и другие схемы подключения, которые будут рассмотрены ниже.

Английский термин, используемый для обозначения МЭ – «firewall». Поэтому в литературе межсетевые экраны иногда также называют файервол или брандмауэр (немецкий термин, аналог firewall).

Как уже было отмечено, фильтрация производится на основании правил. Наиболее безопасным при формировании правил для МЭ считается подход «запрещено все, что явно не разрешено». В этом случае сетевой пакет проверяется на соответствие разрешающим правилам, а если таковых не найдется – отбрасывается. Но в некоторых случаях применяется и обратный принцип: «разрешено все, что явно не запрещено». Тогда проверка производится на соответствие запрещающим правилам, и если таких не будет найдено, пакет будет пропущен.

Фильтрацию можно производить на разных уровнях эталонной модели сетевого взаимодействия OSI. По этому признаку МЭ делятся на следующие классы [10]:

- экранирующий маршрутизатор;
- экранирующий транспорт (шлюз сеансового уровня);
- экранирующий шлюз (шлюз прикладного уровня).

Экранирующий маршрутизатор (или пакетный фильтр) функционирует на сетевом уровне модели OSI, но для выполнения проверок может использовать информацию и из заголовков протоколов транспортного уровня. Соответственно, фильтрация может производиться по ip-адресам отправителя и получателя, а также по TCP и UDP портам. Такие МЭ отличает высокая производительность и относительная простота – функциональностью пакетных фильтров обладают сейчас даже наиболее простые и недорогие аппаратные маршрутизаторы. В то же время, они не защищают от многих атак, например, связанных с подменой участников соединений.

Шлюз сеансового уровня работает на сеансовом уровне модели OSI и также может контролировать информацию сетевого и транспортного уровней. Соответственно, в дополнение к перечисленным выше возможностям подобный МЭ может контролировать процесс установки соединения и проводить проверку проходящих пакетов на принадлежность разрешенным соединениям.

Шлюз прикладного уровня может анализировать пакеты на всех уровнях модели OSI от сетевого до прикладного, что обеспечивает наиболее высокий уровень защиты. В дополнение к ранее перечисленным появляются такие возможности, как аутентификация пользователей, анализ команд протоколов прикладного уровня, проверка передаваемых данных (на наличие компьютерных вирусов, соответствие политике безопасности) и т.д.

Рассмотрим теперь вопросы, связанные с установкой МЭ. МЭ устанавливается после маршрутизатора и защищает всю внутреннюю сеть. Такая схема применяется, если требования в области защиты от несанкционированного межсетевого доступа примерно одинаковы для всех узлов внутренней сети. Например, «разрешать соединения, устанавливаемые из внутренней сети во внешнюю, и пресекать попытки подключения из внешней сети во внутреннюю».

В случае если требования для разных узлов различны (например, нужно разместить почтовый сервер, к которому могут подключаться «извне»), подобная схема установки межсетевого экрана не является достаточно безопасной. Если в нашем примере нарушитель в результате реализации сетевой атаки получит контроль над указанным почтовым сервером, через него он может получить доступ и к другим узлам внутренней сети.

В подобных случаях иногда перед МЭ создается открытый сегмент сети предприятия, а МЭ защищает остальную внутреннюю сеть. Недостаток данной схемы заключается в том, что подключения к узлам открытого сегмента МЭ не контролирует.

Более предпочтительным в данном случае является использование МЭ с тремя сетевыми интерфейсами.

МЭ с тремя сетевыми интерфейсами конфигурируется таким образом, чтобы правила доступа во внутреннюю сеть были более строгими, чем в открытый сегмент. В то же время, и те, и другие соединения могут контролироваться МЭ. Открытый сегмент в этом случае иногда называется «демилитаризованной зоной» – DMZ.

Еще более надежной считается схема, в которой для защиты сети с DMZ задействуются два независимо конфигурируемых МЭ. В этом случае МЭ 2 реализует более жесткий набор правил фильтрации по сравнению с МЭ 1. И даже успешная атака на первый МЭ не сделает внутреннюю сеть беззащитной.

В последнее время стал широко использоваться вариант установки программного МЭ непосредственно на защищаемый компьютер. Иногда такой МЭ называют «персональным». Подобная схема позволяет защититься от угроз исходящих не только из внешней сети, но из внутренней. Особенно актуально применение персональных МЭ при непосредственном подключении компьютера к потенциально опасной сети. Например, при подключении домашнего компьютера к Интернет.

Глава 4. АНАЛИЗ И УПРАВЛЕНИЕ РИСКАМИ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1. Введение в проблему

Целью данного раздела является изучение современных методик анализа и управления рисками, связанными с информационной безопасностью (ИБ).

Риском в сфере ИБ будем называть потенциальную возможность понести убытки из-за нарушения безопасности информационной системы (ИС). Зачастую понятие риска смешивают с понятием угрозы. Необходимо отметить, что от угрозы риск отличает наличие количественной оценки возможных потерь и (возможно) оценки вероятности наступления нежелательного события.

Разберемся, зачем нужно исследовать риски в сфере ИБ, и что это может дать при разработке системы обеспечения ИБ для ИС. Для любого проекта, требующего финансовых затрат на его реализацию, весьма желательно уже на начальной стадии определить, что мы будем считать признаком завершения работы и как будем оценивать результаты проекта. Для задач, связанных с обеспечением ИБ, это также весьма актуально.

На практике наибольшее распространение получили два подхода к обоснованию проекта подсистемы обеспечения безопасности.

Первый из них основан на проверке соответствия уровня защищенности ИС требованиям одного из стандартов в области информационной безопасности. Это может быть класс защищенности в соответствии с требованиями руководящих документов Гостехкомиссии РФ (сейчас это ФСТЭК России), профиль защиты, разработанный в соответствии со стандартом ISO-15408, или какой–либо другой набор требований. Тогда критерий достижения цели в области безопасности – это выполнение заданного набора требований. Критерий эффективности – минимальные суммарные затраты на выполнение поставленных функциональных требований.

Основной недостаток данного подхода заключается в том, что в случае,

когда требуемый уровень защищенности жестко не задан (например, через законодательные требования), определить «наиболее эффективный» уровень защищенности ИС достаточно сложно.

Второй подход к построению системы обеспечения ИБ связан с оценкой и управлением рисками. Изначально он произошел из принципа «разумной достаточности», примененного к сфере обеспечения ИБ. Этот принцип быть описан следующим набором утверждений:

- абсолютно непреодолимую систему защиты создать невозможно;
- необходимо соблюдать баланс между затратами на защиту и получаемым эффектом, в т. ч. и экономическим, заключающимся в снижении потерь от нарушений безопасности;
- стоимость средств защиты не должна превышать стоимости защищаемой информации (или других ресурсов – аппаратных, программных);
- затраты нарушителя на несанкционированный доступ к информации должны превышать тот эффект, который он получит, осуществив подобный доступ.

Но вернемся к рискам. В данном случае, рассматривая ИС в ее исходном состоянии, мы оцениваем размер ожидаемых потерь от инцидентов, связанных с информационной безопасностью (как правило, берется определенный период времени, например, год). После этого делается оценка того, как предлагаемые средства и меры обеспечения безопасности влияют на снижение рисков, и сколько они стоят.

По мере того, как затраты на защиту растут, размер ожидаемых потерь падает. К сожалению, на практике точные зависимости между затратами и уровнем защищенности определить не представляется возможным, поэтому аналитический метод определения минимальных затрат в представленном виде неприменим.

Для того чтобы перейти к рассмотрению вопросов описания риска, введем еще одно определение. *Ресурсом* или *активом* будем называть именованный элемент ИС, имеющий (материальную) ценность и подлежащий защите.

Тогда риск может быть идентифицирован следующим набором параметров:

- угроза, с возможной реализацией которой связан данный риск;
- ресурс, в отношении которого может быть реализована угроза (ресурс может быть информационный, аппаратный, программный и т.д.);
- уязвимость, через которую может быть реализована данная угроза в отношении данного ресурса.

Важно также определить то, как мы узнаем, что нежелательное событие произошло. Поэтому в процессе описания рисков, обычно также указывают события – «триггеры», являющиеся идентификаторами рисков, произошедших или ожидающихся в скором времени (например, увеличение время отклика web–сервера может свидетельствовать о производимой на него одной из разновидностей атак на «отказ в обслуживании»).

Исходя из сказанного выше, в процессе оценки риска надо оценить стоимость ущерба и частоту возникновения нежелательных событий и вероятность того, что подобное событие нанесет урон ресурсу. Размер ущерба от реализации угрозы в отношении ресурса зависит от стоимости ресурса, который подвергается риску, и степени разрушительности воздействия на ресурс, выражаемой в виде коэффициента разрушительности. Как правило, указанный коэффициент лежит в диапазоне от 0 до 1. Таким образом, получаем оценку потери от разовой реализации угрозы, представимую в виде произведения:

$$\text{Потери} = (\text{Стоим. Рес.}) \times (\text{Коэфф. Разруш.}) \qquad (4.1)$$

Далее необходимо оценить частоту возникновения рассматриваемого нежелательного события (за какой–то фиксированный период времени, например, за год) и вероятность успешной реализации угрозы. В результате, стоимость риска может быть вычислена по формуле:

$$\text{Стоим. Риска} = (\text{Частота}) \times (\text{Вероятн.}) \times (\text{Стоим. Рес.}) \times (\text{Коэфф. Разруш}) \qquad (4.2)$$

Примерно такая формула используется во многих методиках анализа рисков, некоторые из которых будут рассмотрены в дальнейшем. Ожидаемый ущерб сравнивается с затратами на меры и средства защиты, после чего принимается решение в отношении данного риска. Он может быть:

- принят;
- снижен (например, за счет внедрения средств и механизмов защиты, уменьшающих вероятность реализации угрозы или коэффициент разрушительности);
- устранен (за счет отказа от использования подверженного угрозе ресурса);
- перенесен (например, застрахован, в результате чего в случае реализации угрозы безопасности потери будет нести страховая компания, а не владелец ИС).

4.2. Управление информационной безопасностью. Стандарты ISO/IEC 17799/27002 и 27001

Международные стандарты ISO/IEC 17799 (новая версия вышла под номером 27002) и 27001 посвящены вопросам управления информационной безопасностью, и так как они взаимосвязаны, рассматривать их будем в одном разделе.

В 1995 году Британским институтом стандартов (BSI) был опубликован стандарт BS 7799 Part 1 «Code of Practice for Information Security Management» (название обычно переводится как «Практические правила управления информационной безопасностью»). На его основе в 2000 году был принят уже международный стандарт ISO/IEC 17799:2000 «Information technology. Code of practice for information security management». Следующая дополненная версия была принята в 2005 году и обозначается ISO/IEC 17799:2005. А в 2007-м году данный стандарт был переиздан под номером ISO/IEC 27002. Как следует из названия, он описывает рекомендуемые меры в области управления информационной безопасностью и, в целом, не предназначался для проведения сертификации систем на его соответствие.

В 2000 году была опубликована вторая часть стандарта: BS 7799 Part 2 «Information Security Management Systems – Specification with guidance for use» (Системы управления информационной безопасностью – спецификации с руководством по использованию). На его базе был разработан стандарт ISO/IEC 27001:2005 «Information Technology. Security techniques. Information security management systems. Requirements», на соответствие которому может проводиться сертификация.

В России на данный момент действуют стандарты ГОСТ Р ИСО/МЭК 17799–2005 «Информационная технология. Практические правила управления информационной безопасностью» (аутентичный перевод ISO/IEC 17799:2000) и ГОСТ Р ИСО/МЭК 27001–2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» (перевод ISO/IEC 27001:2005). Несмотря на некоторые внутренние расхождения, связанные с разными версиями и особенностями перевода, наличие стандартов позволяет привести систему управления информационной безопасностью в соответствие их требованиям и, при необходимости, сертифицировать.

4.2.1. ГОСТ Р ИСО/МЭК 17799:2005 «Информационная технология. Практические правила управления информационной безопасностью»

Рассмотрим теперь содержание стандарта ИСО/МЭК 17799. Указывается, что «информация, поддерживающие ее процессы, информационные системы и сетевая инфраструктура являются существенными активами организации. Конфиденциальность, целостность и доступность информации могут существенно способствовать обеспечению конкурентоспособности, ликвидности, доходности, соответствия законодательству и деловой репутации организации». Таким образом, можно говорить о том, что данный стандарт рассматривает вопросы информационной безопасности, в том числе, и с точки зрения экономического эффекта.

Указываются три группы факторов, которые необходимо учитывать при формировании требований в области информационной безопасности:

- оценка рисков организации. Посредством оценки рисков происходит выявление угроз активам организации, оценка уязвимости соответствующих активов и вероятности возникновения угроз, а также оценка возможных последствий;
- юридические, законодательные, регулирующие и договорные требования, которым должны удовлетворять организация, ее торговые партнеры, подрядчики и поставщики услуг;
- специфический набор принципов, целей и требований, разработанных организацией в отношении обработки информации.

После того как определены требования, идет этап выбора и внедрения мероприятий по управлению информационной безопасностью, которые обеспечат снижение рисков до приемлемого уровня. Выбор мероприятий по управлению информационной безопасностью должен основываться на соотношении стоимости их реализации, эффекта от снижения рисков и возможных убытков в случае нарушения безопасности. Также следует принимать во внимание факторы, которые не могут быть представлены в денежном выражении, например, потерю репутации. Возможный перечень мероприятий приводится в стандарте, но отмечается, что он может быть дополнен или сформирован самостоятельно исходя из потребностей организации.

Кратко перечислим разделы стандарта и предлагаемые в них мероприятия по защите информации. Первая их группа касается политики безопасности.

Требуется, чтобы она была разработана, утверждена руководством организации, издана и доведена до сведения всех сотрудников. Она должна определять порядок работы с информационными ресурсами организации, обязанности и ответственность сотрудников. Политика периодически пересматривается, чтобы соответствовать текущему состоянию системы и выявленным рискам.

Следующий раздел затрагивает организационные вопросы, связанные с обеспечением информационной безопасности. Стандарт рекомендует создавать управляющие советы (с участием высшего руководства компании) для утверждения политики безопасности, назначения ответственных лиц, распределения обязанностей и координации внедрения мероприятий по управлению информационной безопасностью в организации. Также должен быть описан процесс получения разрешений на использование в организации средств обработки информации (в т. ч. нового программного обеспечения и аппаратуры), чтобы это не привело к возникновению проблем с безопасностью. Требуется определить и порядок взаимодействия с другими организациями по вопросам информационной безопасности, проведения консультаций с «внешними» специалистами, независимой проверки (аудита) информационной безопасности.

При предоставлении доступа к информационным системам специалистам сторонних организаций необходимо особое внимание уделить вопросам безопасности. Должна быть проведена оценка рисков, связанных с разными типами доступа (физическим или логическим, т. е. удаленным) таких специалистов к различным ресурсам организации. Необходимость предоставления доступа должна быть обоснована, а в договоры со сторонними лицами и организациями должны быть включены требования, касающиеся соблюдения политики безопасности. Аналогичным образом предлагается поступать и в случае привлечения сторонних организаций к обработке информации (аутсорсинга).

Следующий раздел стандарта посвящен вопросам классификации и управления активами. Для обеспечения информационной безопасности организации необходимо, чтобы все основные информационные активы были учтены и закреплены за ответственными владельцами. Начать предлагается с проведения инвентаризации. В качестве примера приводится следующая классификация активов:

- информационные (базы данных и файлы данных, системная документация и т.д.);
- программное обеспечение (прикладное программное обеспечение,

системное программное обеспечение, инструментальные средства разработки и утилиты);

- физические активы (компьютерное оборудование, оборудование связи, носители информации, другое техническое оборудование, мебель, помещения);
- услуги (вычислительные услуги и услуги связи, основные коммунальные услуги).

Далее предлагается классифицировать информацию, чтобы определить ее приоритетность, необходимость и степень ее защиты. При этом можно оценить соответствующую информацию с учетом того, насколько она критична для организации, например, с точки зрения обеспечения ее целостности и доступности. После этого предлагается разработать и внедрить процедуру маркировки при обработке информации. Для каждого уровня классификации следует определять процедуры маркировки, для того чтобы учесть следующие типы обработки информации:

- копирование;
- хранение;
- передачу по почте, факсом и электронной почтой;
- передачу голосом, включая мобильный телефон, голосовую почту, автоответчики;
- уничтожение.

Стандартом определяется, чтобы обязанности по соблюдению требований безопасности распределялись на стадии подбора персонала, включались в трудовые договоры, и проводился их мониторинг в течение всего периода работы сотрудника. В частности, при приеме в постоянный штат рекомендуется проводить проверку подлинности представляемых претендентом документов, полноту и точность резюме, представляемые им рекомендации. Рекомендуется, чтобы сотрудники подписывали соглашение о конфиденциальности, уведомляющее о том, какая информация является конфиденциальной или секретной. Должна быть определена дисциплинарная ответственность сотрудников, нарушивших политику и процедуры безопасности организации. Там, где необходимо, эта ответственность должна сохраняться и в течение определенного срока после увольнения с работы.

Пользователей необходимо обучать процедурам безопасности и правильному использованию средств обработки информации, чтобы

минимизировать возможные риски. Кроме того, должен быть определен порядок информирования о нарушениях информационной безопасности, с которым необходимо ознакомить персонал. Аналогичная процедура должна задействоваться в случаях сбоев программного обеспечения. Подобные инциденты требуется регистрировать и проводить их анализ для выявления повторяющихся проблем.

Следующий раздел стандарта посвящен вопросам физической защиты и защиты от воздействия окружающей среды. Указывается, что «средства обработки критичной или важной служебной информации необходимо размещать в зонах безопасности, обозначенных определенным периметром безопасности, обладающим соответствующими защитными барьерами и средствами контроля проникновения. Эти зоны должны быть физически защищены от неавторизованного доступа, повреждения и воздействия». Кроме организации контроля доступа в охраняемые зоны, должны быть определены порядок проведения в них работ и, при необходимости, процедуры организации доступа посетителей. Необходимо также обеспечивать безопасность оборудования (включая и то, что используется вне организации), чтобы уменьшить риск неавторизованного доступа к данным и защитить их от потери или повреждения. К этой же группе требований относится обеспечение защиты от сбоев электропитания и защиты кабельной сети. Также должен быть определен порядок технического обслуживания оборудования, учитывающий требования безопасности, и порядок безопасной утилизации или повторного использования оборудования. Например, списываемые носители данных, содержащие важную информацию, рекомендуется физически разрушать или перезаписывать безопасным образом, а не использовать стандартные функции удаления данных.

С целью минимизации риска неавторизованного доступа или повреждения бумажных документов, носителей данных и средств обработки информации рекомендуется внедрить политику «чистого стола» в отношении бумажных документов и сменных носителей данных, а также политику «чистого экрана» в отношении средств обработки информации. Оборудование, информацию или программное обеспечение можно выносить из помещений организации только на основании соответствующего разрешения.

В разделе «Управление передачей данных и операционной деятельностью» требуется, чтобы были установлены обязанности и процедуры, связанные с функционированием всех средств обработки информации. Например, должны

контролироваться изменения конфигурации в средствах и системах обработки информации. Требуется реализовать принцип разграничения обязанностей в отношении функций управления, выполнения определенных задач и областей.

Рекомендуется провести разделение сред разработки, тестирования и промышленной эксплуатации программного обеспечения (ПО). Правила перевода ПО из статуса разрабатываемого в статус принятого к эксплуатации должны быть определены и документально оформлены.

Дополнительные риски возникают при привлечении сторонних подрядчиков для управления средствами обработки информации. Такие риски должны быть идентифицированы заранее, а соответствующие мероприятия по управлению информационной безопасностью согласованы с подрядчиком и включены в контракт.

Для обеспечения необходимых мощностей по обработке и хранению информации необходим анализ текущих требований к производительности, а также прогноз будущих. Эти прогнозы должны учитывать новые функциональные и системные требования, а также текущие и перспективные планы развития информационных технологий в организации. Требования и критерии для принятия новых систем должны быть четко определены, согласованы, документально оформлены и опробованы.

Необходимо принимать меры предотвращения и обнаружения внедрения вредоносного программного обеспечения, такого как компьютерные вирусы, сетевые «черви», «троянские кони» и логические бомбы. Отмечается, что защита от вредоносного программного обеспечения должна основываться на понимании требований безопасности, соответствующих мерах контроля доступа к системам и надлежащем управлении изменениями.

Должен быть определен порядок проведения вспомогательных операций, к которым относится резервное копирование программного обеспечения и данных, регистрация событий и ошибок и, где необходимо, мониторинг состояния аппаратных средств. Мероприятия по резервированию для каждой отдельной системы должны регулярно тестироваться для обеспечения уверенности в том, что они удовлетворяют требованиям планов по обеспечению непрерывности бизнеса.

Для обеспечения безопасности информации в сетях и защиты поддерживающей инфраструктуры требуется внедрение средств контроля безопасности и защита подключенных сервисов от неавторизованного доступа.

Особое внимание уделяется вопросам безопасности носителей информации

различного типа: документов, компьютерных носителей информации (лент, дисков, кассет), данных ввода/вывода и системной документации от повреждений. Рекомендуется установить порядок использования сменных носителей компьютерной информации (порядок контроля содержимого, хранения, уничтожения и т.д.). Как уже отмечалось выше, носители информации по окончании использования следует надежно и безопасно утилизировать.

С целью обеспечения защиты информации от неавторизованного раскрытия или неправильного использования необходимо определить процедуры обработки и хранения информации. Эти процедуры должны быть разработаны с учетом категорирования информации и действовать в отношении документов, вычислительных систем, сетей, переносных компьютеров, мобильных средств связи, почты, речевой почты, речевой связи вообще, мультимедийных устройств, использования факсов и любых других важных объектов, например, бланков, чеков и счетов. Системная документация может содержать определенную важную информацию, поэтому тоже должна защищаться.

Процесс обмена информацией и программным обеспечением между организациями должен быть под контролем и соответствовать действующему законодательству. В частности, должна обеспечиваться безопасность носителей информации при пересылке, определена политика использования электронной почты и электронных офисных систем. Следует уделять внимание защите целостности информации, опубликованной электронным способом, например, информации на Web-сайте. Также необходим соответствующий формализованный процесс авторизации, прежде чем такая информация будет сделана общедоступной.

Следующий раздел стандарта посвящен вопросам контроля доступа. В нем требуется, чтобы правила контроля доступа и права каждого пользователя или группы пользователей однозначно определялись политикой безопасности. Пользователи и поставщики услуг должны быть оповещены о необходимости выполнения данных требований.

При использовании парольной аутентификации необходимо осуществлять контроль в отношении паролей пользователей. В частности, пользователи должны подписывать документ о необходимости соблюдения полной конфиденциальности паролей. Требуется обеспечить безопасность процесса получения пароля пользователем и, если это используется, управления пользователями своими паролями (принудительная смена пароля после первого входа в систему и т.д.).

Доступ как к внутренним, так и к внешним сетевым сервисам должен быть контролируемым. Пользователям следует обеспечивать непосредственный доступ только к тем сервисам, в которых они были авторизованы. Особое внимание должно уделяться проверке подлинности удаленных пользователей. Исходя из оценки риска, важно определить требуемый уровень защиты для выбора соответствующего метода аутентификации. Также должна контролироваться безопасность использования сетевых служб.

Многие сетевые и вычислительные устройства имеют встроенные средства удаленной диагностики и управления. Меры обеспечения безопасности должны распространяться и на эти средства.

В случае, когда сети используются совместно несколькими организациями, должны быть определены требования политики контроля доступа, учитывающие это обстоятельство. Также может потребоваться внедрение дополнительных мероприятий по управлению информационной безопасностью, чтобы ограничивать возможности пользователей по подсоединению.

На уровне операционной системы следует использовать средства информационной безопасности для ограничения доступа к компьютерным ресурсам. Это относится к идентификации и аутентификации терминалов и пользователей. Рекомендуется, чтобы все пользователи имели уникальные идентификаторы, которые не должны содержать признаков уровня привилегии пользователя. В системах управления паролем должны быть предусмотрены эффективные интерактивные возможности поддержки необходимого их качества. Использование системных утилит должно быть ограничено и тщательным образом контролироваться.

Желательно предусматривать сигнал тревоги на случай, когда пользователь может стать объектом насилия[3] (если такое событие оценивается как вероятное). При этом необходимо определить обязанности и процедуры реагирования на сигнал такой тревоги.

Терминалы, обслуживающие системы высокого риска, при размещении их в легкодоступных местах должны отключаться после определенного периода их бездействия для предотвращения доступа неавторизованных лиц. Также может вводиться ограничение периода времени, в течение которого разрешены подсоединения терминалов к компьютерным сервисам.

[3] В качестве примера можно назвать пароли для входа «под принуждением». Если пользователь вводит такой пароль, система отображает процесс обычного входа пользователя, после чего имитируется сбой, чтобы нарушители не смогли получить доступ к данным.

На уровне приложений также необходимо применять меры обеспечения информационной безопасности. В частности, это может быть ограничение доступа для определенных категорий пользователей. Системы, обрабатывающие важную информацию, должны быть обеспечены выделенной (изолированной) вычислительной средой.

Для обнаружения отклонения от требований политики контроля доступа и обеспечения доказательства на случай выявления инцидентов нарушения информационной безопасности необходимо проводить мониторинг системы. Результаты мониторинга следует регулярно анализировать. Журнал аудита может использоваться для расследования инцидентов, поэтому достаточно важной является правильная установка (синхронизация) компьютерных часов.

При использовании переносных устройств, например, ноутбуков, необходимо принимать специальные меры противодействия компрометации служебной информации. Необходимо принять формализованную политику, учитывающую риски, связанные с работой с переносными устройствами, в особенности в незащищенной среде.

Десятый раздел стандарта называется «Разработка и обслуживание систем». Уже на этапе разработки информационных систем необходимо обеспечить учет требований безопасности. А в процессе эксплуатации системы требуется предотвращать потери, модификацию или неправильное использование пользовательских данных. Для этого в прикладных системах рекомендуется предусмотреть подтверждение корректности ввода и вывода данных, контроль обработки данных в системе, аутентификацию сообщений, протоколирование действий пользователя.

Для обеспечения конфиденциальности, целостности и аутентификации данных могут быть использованы криптографические средства защиты.

Важную роль в процессе защиты информации играет обеспечение целостности программного обеспечения. Чтобы свести к минимуму повреждения информационных систем, следует строго контролировать внедрение изменений. Периодически возникает необходимость внести изменения в операционные системы. В этих случаях необходимо провести анализ и протестировать прикладные системы с целью обеспечения уверенности в том, что не оказывается никакого неблагоприятного воздействия на их функционирование и безопасность. Насколько возможно, готовые пакеты программ рекомендуется использовать без внесения изменений.

Связанным вопросом является противодействие «троянским» программам и использованию скрытых каналов утечки. Одним из методов противодействия является использование программного обеспечения, полученного от доверенных поставщиков, и контроль целостности системы.

В случаях, когда для разработки программного обеспечения привлекается сторонняя организация, необходимо предусмотреть меры по контролю качества и правильности выполненных работ.

Следующий раздел стандарта посвящен вопросам управления непрерывностью бизнеса. На начальном этапе предполагается идентифицировать события, которые могут быть причиной прерывания бизнес–процессов (отказ оборудования, пожар и т. п.). При этом нужно провести оценку последствий, после чего разработать планы восстановления. Адекватность планов должна быть подтверждена тестированием, а сами они должны периодически пересматриваться, чтобы учитывать происходящие в системе изменения.

Заключительный раздел посвящен вопросам соответствия требованиям. В первую очередь, это касается соответствия системы и порядка ее эксплуатации требованиям законодательства. Сюда относятся вопросы соблюдения авторского права (в том числе, на программное обеспечение), защиты персональной информации (сотрудников, клиентов), предотвращения нецелевого использования средств обработки информации. При использовании криптографических средств защиты информации, они должны соответствовать действующему законодательству. Также должна быть досконально проработана процедура сбора доказательств на случай судебных разбирательств, связанных с инцидентами в области безопасности информационной системы.

Сами информационные системы должны соответствовать политике безопасности организации и используемым стандартам. Безопасность информационных систем необходимо регулярно анализировать и оценивать. В то же время требуется соблюдать меры безопасности и при проведении аудита безопасности, чтобы это не привело к нежелательным последствиям (например, сбой критически важного сервера из-за проведения проверки).

Подводя итог можно отметить, что в стандарте рассмотрен широкий круг вопросов, связанных с обеспечением безопасности информационных систем, и по ряду направлений даются практические рекомендации.

4.2.2. ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»

Разработчики стандарта отмечают, что он был подготовлен в качестве модели для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения системы менеджмента информационной безопасности (СМИБ). СМИБ (англ. – information security management system; ISMS) определяется как часть общей системы менеджмента, основанная на использовании методов оценки бизнес-рисков для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения информационной безопасности. Система менеджмента включает в себя организационную структуру, политики, деятельность по планированию, распределение ответственности, практическую деятельность, процедуры, процессы и ресурсы.

Стандарт предполагает использование процессного подхода для разработки, внедрения, обеспечения функционирования, мониторинга, анализа, поддержки и улучшения СМИБ организации. Он основан на модели «Планирование (Plan) – Осуществление (Do) – Проверка (Check) – Действие (Act)» (PDCA), которая может быть применена при структурировании всех процессов СМИБ. Показано, как СМИБ, используя в качестве входных данных требования ИБ и ожидаемые результаты заинтересованных сторон, с помощью необходимых действий и процессов выдает выходные данные по результатам обеспечения информационной безопасности, которые соответствуют этим требованиям и ожидаемым результатам.

На этапе «Разработка системы менеджмента информационной безопасности» *организация должна осуществить следующее:*

- определить область и границы действия СМИБ;
- определить политику СМИБ на основе характеристик бизнеса, организации, ее размещения, активов и технологий;
- определить подход к оценке риска в организации;
- идентифицировать риски;
- проанализировать и оценить риски;
- определить и оценить различные варианты обработки рисков;
- выбрать цели и меры управления для обработки рисков;
- получить утверждение руководством предполагаемых остаточных рисков;
- получить разрешение руководства на внедрение и эксплуатацию СМИБ;
- подготовить Положение о применимости.

Этап «Внедрение и функционирование системы менеджмента информационной безопасности» *предполагает, что организация должна:*

- разработать план обработки рисков, определяющий соответствующие действия руководства, ресурсы, обязанности и приоритеты в отношении менеджмента рисков ИБ;
- реализовать план обработки рисков для достижения намеченных целей управления, включающий в себя вопросы финансирования, а также распределение функций и обязанностей;
- внедрить выбранные меры управления;
- определить способ измерения результативности выбранных мер управления;
- реализовать программы по обучению и повышению квалификации сотрудников;
- управлять работой СМИБ;
- управлять ресурсами СМИБ;
- внедрить процедуры и другие меры управления, обеспечивающие быстрое обнаружение событий ИБ и реагирование на инциденты, связанные с ИБ.

Третий этап «Проведение мониторинга и анализа системы менеджмента информационной безопасности» *требует:*

- выполнять процедуры мониторинга и анализа;
- проводить регулярный анализ результативности СМИБ;
- измерять результативность мер управления для проверки соответствия требованиям ИБ;
- пересматривать оценки рисков через установленные периоды времени, анализировать остаточные риски и установленные приемлемые уровни рисков, учитывая изменения;
- проводить внутренние аудиты СМИБ через установленные периоды времени;
- регулярно проводить руководством организации анализ СМИБ в целях подтверждения адекватности ее функционирования и определения направлений совершенствования;
- обновлять планы ИБ с учетом результатов анализа и мониторинга;
- регистрировать действия и события, способные повлиять на результативность или функционирование СМИБ.

И наконец, этап *«Поддержка и улучшение системы менеджмента информационной безопасности»* предполагает, что организация должна регулярно проводить следующие мероприятия:

- выявлять возможности улучшения СМИБ;
- предпринимать необходимые корректирующие и предупреждающие действия, использовать на практике опыт по обеспечению ИБ, полученный как в собственной организации, так и в других организациях;
- передавать подробную информацию о действиях по улучшению СМИБ всем заинтересованным сторонам, при этом степень ее детализации должна соответствовать обстоятельствам и, при необходимости, согласовывать дальнейшие действия;
- обеспечивать внедрение улучшений СМИБ для достижения запланированных целей.

Далее в стандарте приводятся требования к документации, которая должна включать положения политики СМИБ и описание области функционирования, описание методики и отчет об оценке рисков, план обработки рисков, документирование связанных процедур. Также должен быть определен процесс управления документами СМИБ, включающий актуализацию, использование, хранение и уничтожение.

Для предоставления свидетельств соответствия требованиям и результативности функционирования СМИБ необходимо вести и поддерживать в рабочем состоянии учетные записи и записи о выполнении процессов. В качестве примеров называются журналы регистрации посетителей, отчеты о результатах аудита и т. п.

Стандарт определяет, что руководство организации ответственно за обеспечение и управление ресурсами, необходимыми для создания СМИБ, а также организацию подготовки персонала.

Как уже ранее отмечалось, организация должна в соответствии с утвержденным графиком проводить внутренние аудиты СМИБ, позволяющие оценить ее функциональность и соответствие стандарту. А руководство должно проводить анализ системы менеджмента информационной безопасности.

Также должны проводиться работы по улучшению системы менеджмента информационной безопасности: повышению ее результативности и уровня соответствия текущего состояния системы и предъявляемым к ней требованиям.

В приложении к стандарту перечисляются рекомендуемые меры управления, взятые из ранее рассмотренного стандарта ISO/IEC 17799:2005.

4.3. Методики построения систем защиты информации

4.3.1. Модель Lifecycle Security

Роль анализа рисков для создания корпоративной системы защиты информации в компьютерной сети предприятия можно наглядно показать на примере модели Lifecycle Security [5] (название можно перевести как «жизненный цикл безопасности»), разработанной компанией Axent, впоследствии приобретенной Symantec.

Lifecycle Security – это обобщенная схема построения комплексной защиты компьютерной сети предприятия. Выполнение описываемого в ней набора процедур позволяет системно решать задачи, связанные с защитой информации, и дает возможность оценить эффект от затраченных средств и ресурсов. С этой точки зрения, идеология Lifecycle Security может быть противопоставлена тактике «точечных решений», заключающейся в том, что все усилия сосредотачиваются на внедрении отдельных частных решений (например, межсетевых экранов или систем аутентификации пользователей по смарт–картам). Без предварительного анализа и планирования подобная тактика может привести к появлению в компьютерной системе набора разрозненных продуктов, которые не стыкуются друг с другом и не позволяют решить проблемы предприятия в сфере информационной безопасности.

Lifecycle Security включает в себя 7 основных компонентов, которые можно рассматривать как этапы построения системы защиты.

Политики безопасности, стандарты, процедуры и метрики. Этот компонент определяет рамки, в которых осуществляются мероприятия по обеспечению безопасности информации, и задает критерии оценки полученных результатов. Стоит отметить, что под стандартами здесь понимаются не только государственные и международные стандарты в сфере информационной безопасности, но и корпоративные стандарты, которые в ряде случаев могут оказать очень существенное влияние на создаваемую систему защиты информации. Также хочется остановиться на обязательном введении метрики, позволяющей оценить состояние системы до и после проведения работ по защите информации. Метрика определяет, в чем и как измеряется защищенность системы, и позволяет соотнести сделанные затраты и полученный эффект.

Анализ рисков. Этот этап является отправной точкой для установления и

поддержания эффективного управления системой защиты. Проведение анализа рисков позволяет подробно описать состав и структуру информационной системы (если по каким-то причинам это не было сделано ранее), расположить имеющиеся ресурсы по приоритетам, основываясь на степени их важности для нормальной работы предприятия, оценить угрозы и идентифицировать уязвимости системы.

Стратегический план построения системы защиты. Результаты анализа рисков используются как основа для разработки стратегического плана построения системы защиты. Наличие подобного плана помогает распределить по приоритетам бюджеты и ресурсы и в последующем осуществить выбор продуктов и разработать стратегию их внедрения.

Выбор и внедрение решений. Хорошо структурированные критерии выбора решений в сфере защиты информации и наличие программы внедрения уменьшают вероятность приобретения продуктов, становящихся «мертвым грузом», мешающим развитию информационной системы предприятия. Кроме непосредственно выбора решений, также должно учитываться качество предоставляемых поставщиками сервисных и обучающих услуг. Кроме того, необходимо четко определить роль внедряемого решения в выполнении разработанных планов и достижении поставленных целей в сфере безопасности.

Обучение персонала. Знания в области компьютерной безопасности и технические тренинги необходимы для построения и обслуживания безопасной вычислительной среды. Усилия, затраченные на обучение персонала, значительно повышают шансы на успех мероприятий по защите сети.

Мониторинг защиты. Он помогает обнаруживать аномалии или вторжения в ваши компьютеры и сети и является средством контроля над системой защиты, чтобы гарантировать эффективность программ защиты информации.

Разработка методов реагирования в случае инцидентов и восстановление. Без наличия заранее разработанных и «отрепетированных» процедур реагирования на инциденты в сфере безопасности невозможно гарантировать, что в случае обнаружения атаки ей будут противопоставлены эффективные меры защиты, и работоспособность системы будет быстро восстановлена.

Все компоненты программы взаимосвязаны и предполагается, что процесс совершенствования системы защиты идет непрерывно.

Остановимся более подробно на этапе анализа рисков. По мнению разработчиков модели Lifecycle Security, он должен проводиться в следующих случаях:

- до и после обновления или существенных изменений в структуре системы;
- до и после перехода на новые технологии;
- до и после подключения к новым сетям (например, подключения локальной сети филиала к сети головного офиса);
- до и после подключения к глобальным сетям (в первую очередь, Интернет);
- до и после изменений в порядке ведения бизнеса (например, при открытии электронного магазина);
- периодически, для проверки эффективности системы защиты.

Ключевые моменты этапа анализа рисков:

1. Подробное документирование компьютерной системы предприятия. При этом особое внимание необходимо уделять критически важным приложениям.
2. Определение степени зависимости организации от нормального функционирования фрагментов компьютерной сети, конкретных узлов, от безопасности хранимых и обрабатываемых данных.
3. Определение уязвимых мест компьютерной системы.
4. Определение угроз, которые могут быть реализованы в отношении выявленных уязвимых мест.
5. Определение и оценка всех рисков, связанных с эксплуатацией компьютерной системы.

Особо хочется обратить внимание на связь анализа рисков с другими компонентами модели. С одной стороны, наличие метрики защищенности и определение значений, характеризующих состояние системы до и после мероприятий по защите информации, накладывают определенные требования на процедуру анализа рисков. Ведь на базе полученных результатов и оценивается состояние системы. С другой стороны, они дают те начальные условия, исходя из которых разрабатывается план построения системы защиты сети. И результаты анализа рисков должны быть сформулированы в виде, пригодном для выполнения как первой, так и второй функции.

4.3.2. Модель многоуровневой защиты

Понятие многоуровневой защиты или эшелонированной обороны (от англ. «Defense in depth») пришло в информационные технологии из военных руководств.

С точки зрения информационной безопасности, модель многоуровневой защиты определяет набор уровней защиты информационной системы. Модель часто используется корпорацией Майкрософт в руководствах по безопасности. Корректная организация защиты на каждом из выделенных уровней позволяет уберечь систему от реализации угроз информационной безопасности.

Политика безопасности должна описывать все аспекты работы системы с точки зрения обеспечения информационной безопасности. Поэтому *уровень политики безопасности* можно рассматривать как базовый. Этот уровень также подразумевает наличие документированных организационных мер защиты (процедур) и порядка информирования о происшествиях, обучение пользователей в области информационной безопасности и прочие меры аналогичного характера (например, рекомендуемые стандартом ISO/IEC 17799).

Уровень физической защиты включает меры по ограничению физического доступа к ресурсам системы – защита помещений, контроль доступа, видеонаблюдение и т.д. Сюда же относятся средства защиты мобильных устройств, используемых сотрудниками в служебных целях.

Уровень защиты периметра определяет меры безопасности в «точках входа» в защищаемую сеть из внешних, потенциально опасных. Классическим средством защиты периметра является межсетевой экран, который на основании заданных правил определяет, может ли проходящий сетевой пакет быть пропущен в защищаемую сеть. Другие примеры средств защиты периметра – системы обнаружения вторжений, средства антивирусной защиты для шлюзов безопасности и т.д.

Уровень защиты внутренней сети «отвечает» за обеспечение безопасности передаваемого внутри сети трафика и сетевой инфраструктуры. Примеры средств и механизмов защиты на этом уровне – создание виртуальных локальных сетей (VLAN) с помощью управляемых коммутаторов, защита передаваемых данных с помощью протокола IPSec и т.д. Нередко внутри сети также используют средства, характерные для защиты периметра, например, межсетевые экраны, в том числе и персональные (устанавливаемые на защищаемый компьютер). Связано это с тем, что использование беспроводных сетевых технологий и виртуальных частных сетей (VPN) приводит к «размыванию» периметра сети. Например, если атакующий смог подключиться к точке беспроводного доступа внутри защищаемой сети, его действия уже не будут контролироваться межсетевым экраном, установленным «на границе» сети, хотя формально атака будет производиться с внешнего по отношению к

нашей сети компьютера. Поэтому иногда при анализе рассматривают «*уровень защиты сети*», включающий и защиту периметра, и внутренней сети.

Следующим на схеме идет *уровень защиты узлов.* Здесь рассматриваются атаки на отдельный узел сети и, соответственно, меры защиты от них. Может учитываться функциональность узла и отдельно рассматриваться защита серверов и рабочих станций. В первую очередь, необходимо уделять внимание защите на уровне операционной системы – настройкам, повышающим безопасность конфигурации (в том числе, отключению не использующихся или потенциально опасных служб), организации установки исправлений и обновлений, надежной аутентификации пользователей. Исключительно важную роль играет антивирусная защита.

Уровень защиты приложений отвечает за защиту от атак, направленных на конкретные приложения – почтовые серверы, web– серверы, серверы баз данных. В качестве примера можно назвать SQL-инъекции – атаки на сервер БД, заключающиеся в том, что во входную текстовую строку включаются операторы языка SQL, что может нарушить логику обработки данных и привести к получению нарушителем конфиденциальной информации. Сюда же можно отнести модификацию приложений компьютерными вирусами. Для защиты от подобных атак используются настройки безопасности самих приложений, установка обновлений, средства антивирусной защиты.

Уровень защиты данных определяет порядок защиты обрабатывающихся и хранящихся в системе данных от несанкционированного доступа и других угроз. В качестве примеров контрмер можно назвать разграничение доступа к данным средствами файловой системы, шифрование данных при хранении и передаче.

В процессе идентификации рисков определяется, что является целью нарушителя, и на каком уровне или уровнях защиты можно ему противостоять. Соответственно выбираются и контрмеры. Защита от угрозы на нескольких уровнях снижает вероятность ее реализации, а значит, и уровень риска.

4.3.3. Методика управления рисками, предлагаемая Майкрософт

Ниже представлено краткое описание подхода к управлению рисками, предлагаемого корпорацией Майкрософт. Данное описание базируется на материалах «Руководства по управлению рисками» [6].

Управление рисками рассматривается как одна из составляющих общей программы управления, предназначенной для руководства компаний и позволяющей контролировать ведение бизнеса и принимать обоснованные решения.

Процесс управления рисками безопасности, предлагаемый Майкрософт, включает следующие четыре этапа:

Этап «оценка рисков» включает в себя следующие мероприятия:

- *планирование сбора данных:* обсуждение основных условий успешной реализации и подготовка рекомендаций;
- *сбор данных о рисках:* описание процесса сбора и анализа данных;
- *выделение наиболее приоритетных рисков:* подробное описание шагов по качественной и количественной оценке рисков.

Этап «поддержка принятия решений»:

- *определение функциональных требований:* определение функциональных требований для снижения рисков;
- *выбор возможных решений для контроля:* описание подхода к выбору решений по нейтрализации риска;
- *экспертиза решения:* проверка предложенных элементов контроля на соответствие функциональным требованиям;
- *оценка снижения риска*: оценка снижения подверженности воздействию или вероятности рисков;
- *оценка стоимости решения*: оценка прямых и косвенных затрат, связанных с решениями по нейтрализации риска;
- *выбор стратегии нейтрализации риска:* определение наиболее экономически эффективного решения по нейтрализации риска путем анализа соотношения затрат и получаемого результата. Этап «реализация контроля» включает мероприятия по развертыванию и использованию решений для контроля (например, внедрение новых средств защиты), снижающих риск для организации:
- *поиск целостного подхода:* включение персонала, процессов и технологий в решение по нейтрализации риска.
- *организация по принципу многоуровневой защиты*: упорядочение решений по нейтрализации риска в рамках предприятия.

Этап «оценка эффективности программы» предполагает проведение анализа эффективности процесса управления рисками и проверки того, обеспечивают ли элементы контроля надлежащий уровень безопасности:

- разработка системы показателей рисков: *оценка уровня и изменения риска.*

- *оценка эффективности программы:* оценка программы управления рисками для выявления возможностей усовершенствования.

В руководстве [5, 7] особо отмечается, что термины «управление рисками» и «оценка рисков» не являются взаимозаменяемыми. Под управлением рисками понимаются общие мероприятия по снижению риска в рамках организации до приемлемого уровня. Управление рисками представляет собой непрерывный процесс, но производимые оценки чаще всего делаются для годичного интервала. Под оценкой рисков понимается процесс выявления и приоритизации рисков для бизнеса, являющийся составной частью управления рисками.

На начальном этапе проведения оценки рискам присваиваются значения в соответствии со шкалой: «высокий», «средний» и «низкий». После этого для выявленных наиболее существенных рисков проводится количественная оценка.

Организациям, в которых отсутствуют формальные политики или процессы, относящиеся к управлению рисками безопасности, будет очень трудно сразу внедрить все аспекты рассматриваемого процесса. Если окажется, что уровень зрелости является достаточно низким, рассматриваемый процесс можно внедрять последовательными этапами на протяжении нескольких месяцев (например, начав с пилотного проекта в отдельном подразделении). Продемонстрировав эффективность процесса управления рисками безопасности на примере пилотного проекта, группа управления рисками безопасности может перейти к внедрению данного процесса в других подразделениях, постепенно охватывая всю организацию.

ЗАКЛЮЧЕНИЕ

Проблема обеспечения информационной безопасности становится все более актуальной для российских компаний. Это связано и с обострением конкурентной борьбы на внутренних рынках, и с выходом компаний на международный уровень. Многие из них уже не могут обеспечить защиту коммерческой информации собственными силами и вынуждены пользоваться услугами профильных профессиональных IT-консультантов.

Обеспечение информационной безопасности является не только российской, но и мировой проблемой. Так в первые годы внедрения корпоративных локальных сетей головной болью компаний был несанкционированный доступ к коммерческой информации путем внешнего взлома. Сейчас с точки зрения информационной безопасности многие компании напоминают крепости, окруженные несколькими периметрами мощных стен – программными и аппаратными платформами ИБ. Однако практика показывает, что информация все равно утекает. При этом основной предпосылкой к утечке информации являются отсутствие единого системного подхода к обеспечению ИБ в компаниях.

В течение многих лет компании отчаянно боролись с вирусными эпидемиями, обносили периметр межсетевыми экранами и системами предотвращения вторжений, внедряли мощные инструменты против неавторизованного доступа. Однако компании упустили из вида главную опасность. Отсутствие единой политики информационной безопасности, а также единой концепции построения профиля информационной защиты компании зачастую обесценивает многомиллионные затраты на программные и аппаратные комплексы ИБ. Еще пару лет назад IT-службы отвечали за защиту от внешних угроз, а с внутренними угрозами разбиралась служба безопасности. Сегодня она просто физически не может контролировать перемещение информации по электронным сетям и с помощью переносных носителей. Для этого нужны специально разработанные регламенты, ликбез сотрудников, специально подготовленные сотрудники безопасности и технические средства для выявления попыток несанкционированного доступа или перемещения информации. Все эти меры должны реализоваться специалистом ИБ в рамках единой концепции.

Бурное развитие IT технологий и направления ИБ приводит к росту спроса на профессиональных специалистов в данной области. Это актуализирует получение образования в области ИБ и широкой востребованности полученных профильных знаний на рынке труда.

Хочется надеяться, что данное учебное пособие поможет будущим профессионалам в сфере IT получить тот общий набор знаний и умений в области ИБ, чтобы оказаться востребованными и высокооплачиваемыми сотрудниками престижных компаний.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. ГОСТ Р 50922–2006. Защита информации. Основные термины и определения. – М.: Стандартинформ, 2008. – 12 с.
2. ГОСТ Р 51275–2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. – М.: Стандартинформ, 2007. – 11 с.
3. Михнев, И.П. Основы информационной безопасности хозяйственной деятельности: учебное пособие / И.П. Михнев; Волгоградский филиал ФГБОУ ВПО «Российская академия народного хозяйства и государственной службы». – Волгоград: Изд-во Волгоградского филиала ФГБОУ ВПО РАНХиГС, 2013. – 144 с.
4. ГОСТ Р ИСО/МЭК 15408–1–2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. – М.: Госстандарт России, 2002. – 40 с.
5. Нестеров, С.А. Основы информационной безопасности: учебное пособие / С.А. Нестеров. – СПб.: Издательство «Лань», 2017. – 324 с.
6. Макаренко, С.И. Информационная безопасность: учебное пособие / С.И. Макаренко. – Ставрополь: СФ МГГУ им. М.А. Шолохова, 2009. – 372 с.
7. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В.Ф. Шаньгин. – М.: ИД «ФОРУМ»: ИНФРА-М, 2008. – 416 с.
8. Галатенко, В.А. Основы информационной безопасности: курс лекций / В.А. Галатенко. – М.: ИНТУИТ. РУ, 2006. – 205 с.
9. Белов, Е.Б. Основы информационной безопасности: учебное пособие для вузов / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. – М.: Горячая линия – Телеком, 2006. – 544 с.
10. Тихонов, В.А. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты: учебное пособие / В.А. Тихонов, В.В. Райх. – М.: Гелиос АРВ, 2006. – 528 с.

Михнев Илья Павлович

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Учебное пособие

Электронное издание

Издательство Волгоградского института управления –
филиала ФГБОУ ВО «РАНХиГС»
400078, Волгоград, ул. Герцена, 10.