Содержание

Введение

Информационная безопасность (ИБ) является системообразующим фактором структуры национальной безопасности России. Иллюстрацией этому является рис. 1. Как видно из рисунка, сохраняя определенную самостоятельность, обусловленную спецификой содержания этой сферы деятельности, информационная безопасность естественным образом, в большей или меньшей мере, входит фактически во все компоненты национальной безопасности и является её системообразующим фактором.

Рис. 1. Роль и место информационной безопасности в обеспечении национальной безопасности России

Защита (обеспечение безопасности) информации является неотъемлемой частью общей проблемы информационной безопасности.

Для осуществления защиты информации к настоящему времени в России создана и функционирует государственная система защиты информации, базирующаяся на положениях Закона “О государственной тайне”, ряде Указов Президента Российской Федерации и постановлении Правительства Российской Федерации “О государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от её утечки по техническим каналам”.

Целями обеспечения информационной безопасности информационных систем (ИС) являются:

- достижение состояния защищенности жизненно важных интересов государства от различных угроз в сфере формирования, распространения и использования информационных ресурсов;

- обеспечение прав граждан на получение, использование и распространение информации;

- обеспечение информированности общества, необходимой для успешного функционирования всех его структур;

- предотвращение нарушений прав граждан и организаций на сохранение конфиденциальности и секретности информации;

- обеспечение условий, препятствующих преднамеренному искажению или сокрытию информации при отсутствии для этого законных оснований.

Задачами обеспечения информационной безопасности в ИС являются:

- выявление и прогнозирование внутренних и внешних угроз информационной безопасности, разработка и осуществление комплекса адекватных и экономически обоснованных мер по их предупреждению и нейтрализации;

- формирование единой политики государственной власти и субъектов России по обеспечению информационной безопасности в ИС;

- совершенствование и стандартизация применяемых методов и средств защиты информации в ИС;

- создание и реализация механизма государственного регулирования (лицензирования) деятельности в области защиты информации, а также обеспечение функционирования системы сертификации ИС и входящих в их состав защищенных технических средств, средств защиты информации и средств контроля эффективности принятых мер защиты.

Все эти аспекты и многое другое будет нами рассмотрено более подробно в ходе лекций, практических занятий и лабораторных работ.

Глава 1. Основы законодательства РФ в области информационной безопасности и защиты информации

1.1. Государственные стандарты и руководящие документы в области информационной безопасности.

Информационная сфера или среда - сфера деятельности, связанная с созданием, распространением, преобразованием и потреблением информации.

Основным объектом правоотношений в информационной сфере является *информация*. «Информация» в переводе с латинского означает ознакомление, разъяснение, изложение. С философской точки зрения информация — это не энергия и не материя. Так подходил к понятию «информация» Н. Винер. Простое и очевидное определение информации дал С.И. Ожегов:

1) сведения об окружающем мире и протекающих в нем процессах;

2) сообщения, осведомляющие о положении дел, о состоянии чего-либо.

Сегодня существует несколько подходов к определению понятия «информация». Подход, которого, по-видимому, придерживается большая часть специалистов и неспециалистов, сводится к тому, что существуют разные измерения (меры) информации: *техническая мера* - информация, которая передается по телеграфным линиям и отображается на экранах радиолокаторов.

При рассмотрении информации в качестве предмета правоотношений в правовой системе, предмета отношений государства, юридических и физических лиц, приходится возвращаться к определению информации в его исходном смысле: под *информацией* понимается *содержание сообщений, сведений и сигналов*. Это верно постольку, поскольку при движении информации в процессе ее создания, распространения, преобразования и потребления подавляющее большинство общественных отношений возникает именно по поводу информации в форме сведений или сообщений. Такой подход к определению понятия «информация» получил название антропоцентрический.

Федеральный закон «Об информации, информационных технологиях и о защите информации» определяет информацию как «сведения (сообщения, данные) независимо от формы их представления». Учитывая социальный аспект рассматриваемого объекта, добавим: включаемые в оборот в понятном для человека виде.

Закон вводит также термин документированная информация и определяет ее как «зафиксированную на материальном носителе путем документирования информацию с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель».

Понятие «*документированная информация*» основано на двуединстве информации - сведений и материального носителя, на котором она отражена в виде символов, знаков, букв, волн или других способов отображения. В результате документирования происходит как бы материализация и овеществление сведений.

Информация «закрепляется» на материальном носителе, «привязывается» к нему и тем самым обособляется от своего создателя. В итоге в качестве документированной информации мы получаем книгу, статью в журнале, сборник статей, фонд документов, банк данных или иной массив документов (данных) на бумажном, машиночитаемом или иных носителях. По сути документированная информация *представляет собой обыкновенные данные, а подход, отождествляющий информацию и данные, носит название техно-центрический.*

Несмотря на то что *документированная информация* (документ) есть по сути дела объект материальный, распространить право вещной собственности возможно только на сам носитель, но не на информацию.

Обеспечение безопасности информации, в том числе и в компьютерных системах, требует сохранения следующих ее свойств:

1) целостности;

2) доступности;

3) конфиденциальности.

Целостность информации заключается в ее существовании в неискаженном виде, неизменном по отношению к некоторому ее исходному состоянию.

Доступность информации - это свойство, характеризующее ее способность обеспечивать своевременный и беспрепятственный доступ пользователей к интересующим их данным.

Конфиденциальность информации - это свойство, указывающее на необходимость введения ограничений на доступ к ней определенного круга пользователей.

Законодательство Российской Федерации в области информации и информационной безопасности

Вопросы правового обеспечения защиты информации занимают все более значительное место в законодательстве Российской Федерации. В приведенном далее списке указаны основные нормативные правовые акты в области информационной безопасности.

Конституция Российской Федерации:

- Закон РФ от 05.03.1992 № 2446-1 «О безопасности».
- Закон РФ от 23.09.1992 № 3521-1 «О правовой охране программ для электронных вычислительных машин и баз данных».
- Закон РФ от 23.09.1992 № 3526-1 «О правовой охране топологий интегральных микросхем».
- Закон РФ от 09.07.1993 № 5351-1 «Об авторском праве и смежных правах».
- Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне».
- Федеральный закон от 29.12.1994 № 77-ФЗ «Об обязательном экземпляре документов».
- Федеральный закон от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности».
- Федеральный закон от 10.01.2002 № 1-ФЗ «Об электронной цифровой подписи».
- Федеральный закон от 07.07.2003 № 126-ФЗ «О связи».
- Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне».
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

Государственные стандарты и руководящие документы:

• *по защите от НСД к информации:*

ГОСТ Р 50922-96. Защита информации. Основные термины и определения

ГОСТ Р 50739-95. Средства вычислительной техники. Защита от НСД к информации. Общие технические требования

ГОСТ Р 51275-99 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения

•*по криптографической защите и ЭЦП:*

ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования

ГОСТ Р 34.10-94 (2001). Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма

ГОСТ Р 34.11-94. Функция хеширования

•*по защите от утечки по техническим каналам:*

ГОСТ Р В50170-92. Противодействие иностранной технической разведке. Термины и определения

ГОСТ 29339-92. Защита информации от утечки за счет ПЭМИН. Общие технические требования

ГОСТ Р 50752-95. Информационная технология. Защита информации от утечки за счет побочных электромагнитных излучений при ее обработке средствами вычислительной техники. Методы испытаний

1.2. Виды информации, защищаемой законодательством РФ. Классификация информации по категориям доступа.

Объект защиты – обобщающий термин для всех форм существования информации, требующих защиты от технических разведок. По своему составу объекты защиты могут быть единичными и групповыми.

Средства защиты информации - технические, криптографические, программные и другие средства, предназначенные для защиты сведений конфиденциального характера, а также средства контроля эффективности защиты информации.

Российской Федерации *Федеральный закон «Об информации, информационных технологиях и о защите информации»* классифицирует информацию в зависимости от категории доступа к ней и от порядка ее предоставления или распространения. В соответствии со ст. 5 указанного закона *по категориям доступа* информация подразделяется на *общедоступную информацию и информацию ограниченного доступа*, т.е. такую информацию, доступ к которой ограничен федеральными законами.

По порядку предоставления или распространения информация подразделяется:

- *на свободно распространяемую;*

- *предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;*

- подлежащую предоставлению или распространению в соответствии с федеральными законами (например, сведения об имущественном положении кандидатов в депутаты);

- ограничиваемую или запрещаемую к распространению в Российской Федерации (например, разжигающую национальную, расовую или религиозную ненависть и вражду).

Статья 9 Федерального закона «Об информации, информационных технологиях и о защите информации» *устанавливает обязательность соблюдения конфиденциальности информации ограниченного доступа*, т.е. «обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя».

Информация ограниченного доступа подразделяется на сведения, представляющие собой:

- государственную тайну;
- коммерческую тайну;
- служебную тайну;
- *профессиональную тайну* - сведения, полученные гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности;
- персональные данные граждан (физических лиц).

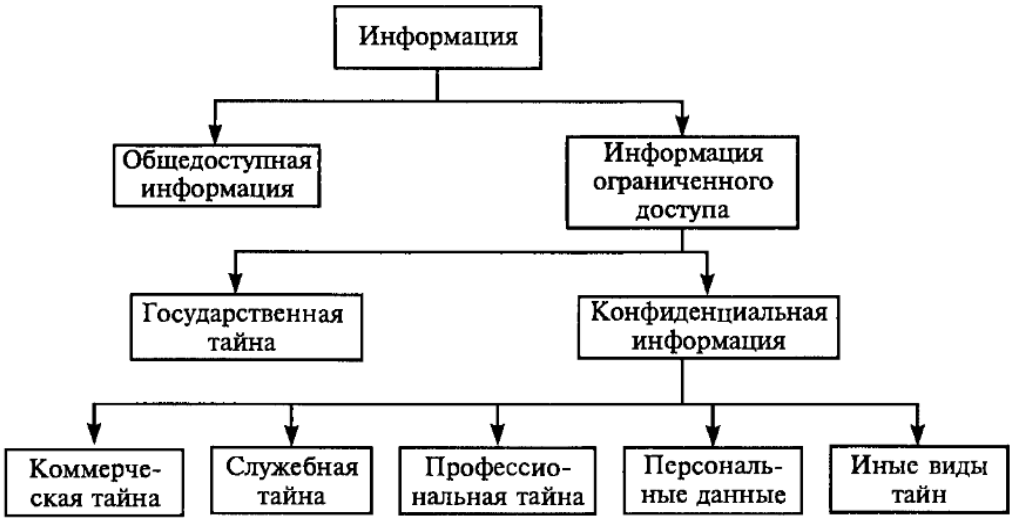

Рис. 2. Классификация информации по категориям доступа

В Указе Президента РФ от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» предпринята попытка упорядочить состав конфиденциальной информации.

Указом утвержден *перечень сведений конфиденциального характера*, в котором перечислены шесть видов информации:

1) сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;

2) сведения, составляющие тайну следствия и судопроизводства;

3) служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна);

4) сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее);

5) сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна);

6) сведения о сущности изобретения полезной модели или промышленного образца до официальной публикации информации о них.

1.3. Международное право в сфере защиты информации

До середины прошлого столетия авторское право не существовало как таковое. Право собственности могло распространяться лишь на конкретные произведения искусства (картины, скульптуры и т. п.). Начиная с середины XIX в. авторское право становится самостоятельной формой собственности - произведения интеллектуального труда стали отвечать всем признакам товара.

Бернская конвенция «Об охране литературных и художественных произведений» 1886 г. Работа по созданию правового инструмента по охране авторского права была начата в Брюсселе в 1858 г. на состоявшемся там конгрессе авторов произведений литературы и искусства. Затем последовали конгрессы в Антверпене 1861 и 1877 г.) и Париже 1878 г.), с 1883 г. работа была продолжена в Берне, где в 1886 г. после трех дипломатических конференций было выработано международное соглашение, получившее название Бернской конвенции об охране литературных и художественных произведений. *Соглашение было подписано девятью государствами: Бельгией, Великобританией, Испанией, Италией, Либерией, Гаити, Тунисом, Францией и Швейцарией. Конвенция вступила в силу 5 декабря 1887 г.*

Основные положения Конвенции подлежали обязательному включению в национальные законодательства стран-участниц в тех случаях, когда национальные законодательства обеспечивали менее благоприятный режим для обладателей авторских прав. В этом проявилось стремление создателей Конвенции к унификации основных положений авторского права.

Парижская конференция 1896 г. 15 апреля 1896 г. в Париже состоялась первая конференция по изменению Конвенции 1886 г. В конвенцию было

включено понятие *«публикация», определенное как выпуск копий.* Таким образом, представление и исполнение драматических, драматическо-музыкальных и музыкальных произведений, выставки произведений искусства к публикации не относились. Было также принято уточнение к ст. 3, в соответствии с которым охрана предоставлялась произведению, впервые опубликованному в стране - участнице Конвенции даже в том случае, когда автор был гражданином страны, не входящей в Бернский союз. Территориальный принцип Конвенции оставался неизменным, однако, акцент был перенесен с издателя на автора произведения.

Берлинская конференция 1908 г. Результатом работы конференции явился почти *полный пересмотр всех основных положений Бернской конвенции.* Новая редакция содержала 30 статей, и основные нововведения относились к следующим проблемам. Конвенция 1886 г. ставила охрану авторского права в зависимость от условий выполнения формальностей, предусмотренных в стране первой публикации. На Берлинской конференции было решено отказаться от всех формальностей даже в том случае, если в стране первой публикации они существуют.

Берлинский вариант Конвенции более полно определил и существенно расширил круг объектов охраны, включив в него произведения хореографии и пантомимы, кинематографии, фотографии и архитектуры. Были признаны права композиторов на разрешение адаптировать их произведения для исполнения аппаратами механического воспроизведения и их публичное исполнение. Правила, регламентирующие право перевода, были расширены. Берлинская конференция признала их действительность на протяжении всего срока действия авторского права без всяких ограничений.

Срок охраны авторского права был установлен равным 50 годам, исчисляемым со дня смерти автора. Правило не носило обязательный характер - допускались различия в сроках охраны авторских прав, определяемые законом страны, где ищется защита. Конвенция более четко определила *понятия литературного и художественного произведений и закрепила положение о том, что они должны охраняться во всех странах-участницах с обязательным отражением этого в национальных законодательствах*.

Римская конференция 1928 г. Римская конференция проходила в период бурного развития средств массовой информации и коммуникаций. Это нашло отражение в признании охраны прав авторов при трансляции по радио их произведений, в расширении числа объектов охраны, признании личных прав автора и т.п. *Уровень охраны авторского права был повышен в связи с включением в число объектов авторского права устных литературных произведений* (лекций, речей, проповедей и т.п.). К числу наиболее важных нововведений следует отнести признание так называемых *личных прав автора, которые сохраняются за ним и при отчуждении имущественных прав* (издание, публикация, постановка и т.п.).

Брюссельская конференция 1948г. Бернская конвенция подверглась существенным изменениям в Брюсселе в 1948 г.

Основной целью конференции было стремление добиться более полной унификации правил Конвенции и национальных законодательств, а также учесть новые условия научного и технического развития. Унификация правил применения Конвенции была достигнута путем усиления принципа ее главенства над национальными законодательствами. Стокгольмская конференция 1967 году. К этому времени на международной арене появилось большое количество развивающихся стран с их специфическими нуждами и проблемами, которые стремились понизить уровень охраны авторских прав с целью получить свободный доступ к произведениям науки и культуры. Добившиеся высокого уровня охраны авторских прав развитые капиталистические страны боялись наметившейся тенденции и всячески ей противились. Для сохранения прежнего уровня охраны авторского права предполагалось пойти на сужение границ Бернского союза. Результатом сложной борьбы между двумя основными тенденциями в международном авторском праве явился протокол, отразивший в определенной мере проблемы развивающихся стран и предоставивший им значительные послабления.

К наиболее существенным изменениям следует отнести:

1) усовершенствование критериев применения конвенции и определение понятий страны происхождения и публикации;

2) признание права на воспроизведение;

3) особый режим кинематографических и приравненных к ним произведений (телефильмы и т.п.);

4) расширение личных прав автора (личные права существуют независимо от имущественных прав и даже после их отчуждения);

5) расширение сроков охраны авторских прав.

Конференция приняла специальную резолюцию, поощряющую стремления некоторых стран выработать особое соглашение о продлении срока действия авторского *права свыше установленных 50 лет*, исчисляемых со дня смерти автора. *Что касается России, то она присоединилась к Бернской концепции лишь спустя почти 100 лет после ее первого опубликования, в ноябре 1994 г.*

Глава 2. Информационная война

2.1.Основные понятия информационной войны

Первым использовал термин *"информационная война"* американский эксперт Томас Рона в отчете, подготовленным им в 1976 году для компании Boeing, и названный "Системы оружия и информационная война". Т. Рона указал, что информационная инфраструктура становится ключевым компонентом американской экономики. В то же самое время она становится и

уязвимой целью как в военное, так и в мирное время. Этот отчет и можно считать первым упоминанием термина "информационная война".

В конце 1996 г. Роберт Банкер, эксперт Пентагона, на одном из симпозиумов представил доклад, посвященный новой военной доктрине вооруженных сил США XXI столетия (концепции "Force XXI").

В ее основу было положено разделение всего театра военных действий на две составляющих – *традиционное пространство и киберпространство*, причем последнее имеет даже более важное значение. Р. Банкер предложил доктрину "кибермaневра", которая должна явиться естественным дополнением традиционных военных концепций, преследующих цель нейтрализации или подавления вооруженных сил противника.

В октябре 1998 года Министерство обороны США вводит в действие *"Объединенную доктрину информационных операций"*. Первоначально эта публикация называлась "Объединенная доктрина информационной войны". Позже она была переименована в "Объединенную доктрину информационных операций". Причина изменения состояла в том, чтобы разъяснить отношения понятий *информационных операций и информационной войны.*

Они были определены следующим образом:

- информационная операция: действия, предпринимаемые с целью затруднить сбор, обработку, передачу и хранение информации информационными системами противника при защите собственной информации и информационных систем;

- информационная война: комплексное воздействие (совокупность информационных операций) на систему государственного и военного управления противостоящей стороны, на ее военно-политическое руководство, которое уже в мирное время приводило бы к принятию благоприятных для стороны-инициатора информационного воздействия решений, а в ходе конфликта полностью парализовало бы функционирование инфраструктуры управления противника.

Какой бы смысл в понятие "информационная война" ни вкладывался, оно родилось в среде военных и обозначает прежде всего жесткую, решительную и опасную деятельность, сопоставимую с реальными боевыми действиями.

Многие страны вынуждены принимать специальные меры для защиты своих сограждан, своей культуры, традиций и духовных ценностей от чуждого информационного влияния. Следует постоянно помнить о защите национальных информационных ресурсов и сохранении конфиденциальности информационного обмена по мировым открытым сетям. Вполне вероятно, что на этой почве могут возникать политическая и экономическая конфронтация между рядом государств, новые кризисные ситуации в международных отношениях. Поэтому в настоящее время информационная безопасность, *информационная война и информационное оружие* оказались в центре внимания.

Методы информационной войны:

- *выброс дезинформации;*
- *представление информации в выгодном для себя ключе.*

В настоящее время в число сфер ведения боевых действий, помимо земли, моря, воздуха и космоса, добавилась и информационная сфера. Как подчеркивают военные эксперты, основными объектами поражения в новых войнах будут информационная инфраструктура и психология противника (появился даже термин «human network»).

2.2. Информационное оружие и его классификация

Информационное оружие (ИО) - это арсенал средств несанкционированного доступа к информации и выведения из строя электронных систем управления.

Информационная мишень - множество элементов информационной системы, принадлежащих или способных принадлежать сфере управления и имеющих потенциальные ресурсы для перепрограммирования на достижение целей, чуждых данной системе.

Для того чтобы повысить уязвимость противника, следует максимально расширить его информационную мишень, т.е. подтолкнуть его на включение в мишень как можно больше равноправных элементов, причем желательно открыть доступ в сферу управления таким элементам, которые легко поддаются перепрограммированию и внешнему управлению.

Информационное оружие стало одной из главных составляющих военного потенциала США, позволяющей выигрывать малые войны и разрешать военные конфликты без применения обычных вооруженных сил.

В войсках создаются специальные подразделения и структуры управления для ведения информационной войны.

Во всех военных учебных заведениях США введены специальные курсы по информационным войнам и налажен выпуск офицеров по специальности этого профиля.

Классификация ИО включает в себя:

- СМИ;
- психотронные генераторы;
- психотропные препараты;
- средства РЭБ;
- средства СПТВ.

Глава 3. Способы несанкционированного доступа к ресурсам и объектам информационной безопасности

3.1. Несанкционированный доступ

Под безопасностью ИС понимается отсутствие (устранение) условий, представляющих потенциальную возможность нанесения ущерба ИС.

Известны четыре типа угроз для ИС:

- прерывание: при прерывании компонент системы утрачивается (например, в результате похищения), становится недоступным (например, в результате блокировки - физической или логической), либо теряет работоспособность;
- перехват: некоторая третья неавторизованная сторона (злоумышленник) получает доступ к компоненту. Примерами перехвата являются незаконное копирование программ и данных, неавторизованное чтение данных из линии связи компьютерной сети и т.д.;
- модификация: некоторая третья неавторизованная сторона не только получает доступ к компоненте, но и манипулирует с ним. Например, модификациями является несанкционированное изменение данных в базах данных или вообще в файлах компьютерной системы, изменение алгоритмов используемых программ с целью выполнения некоторой дополнительной незаконной обработки;
- подделка: злоумышленник может добавить некоторый фальшивый процесс в систему для выполнения нужных ему, но не учитываемых системой, действий, либо подложные записи в файлы системы или других пользователей.

Таким образом, проблема безопасности ИС сводится главным образом к задаче управления доступом множества субъектов системы ко множеству компонент системы.

Основных видов защищенного доступа два: разделенный доступ (администратор дает субъектам права доступа к объектам, создается матрица доступа) и мандатный доступ (метки безопасности и метки конфиденциальности, важность объекта, больше метка безопасности).

3.2. Несанкционированный доступ к программам

Под “программой” понимают:

- обычные программы пользователей;
- специальные программы, рассчитанные на нарушение безопасности системы;
- разнообразные системные утилиты и прикладные программы, которые отличаются более высоким профессиональным уровнем разработки и, тем не менее, могут содержать отдельные недоработки, позволяющие противнику воздействовать на системы.

Программы могут порождать проблемы двух видов:

- могут *перехватывать и модифицировать данные* в результате действий пользователя;
- используя упущения в защите ИС, программы могут или *обеспечивать доступ к системе пользователям, не имеющим на это право*, или *блокировать доступ к системе законных пользователей.*

К сожалению, количество возможных слабых точек, которые могут содержаться в той или иной программе, значительно превышает число известных технологий устранения последствий воздействий злоумышленника.

Это обусловлено двумя причинами:

- *качество программы всегда не превышает квалификации ее разработчика (очевидные потери и нарушения могут быть выявлены и устранены достаточно легко, однако, чем выше уровень подготовки программиста, тем более неявными, даже для него, становятся допускаемые им ошибки и тем более тщательно и надежно он способен скрыть умышленные механизмы, разработанные для нарушения защищенности системы);*

- *имеет место трудно разрешимый компромисс между эффективностью и удобством ИС в работе и степенью обеспечения в ней требований по защищенности.*

Чем более высокие требования предъявляются к защищенности системы, тем больше ресурсов системы затрачивается на обеспечение этих требований, тем сильнее снижается производительность системы и увеличиваются сроки решения задач, наконец, тем неудобнее работать в данной системе пользователям. С другой стороны, чем больше ресурсов выделяется для решения текущих задач, тем меньше возможностей по обеспечению требуемого уровня безопасности. В основном нарушение безопасности программ состоит в том, что они могут быть использованы как средства получения “критичной” информации (данных), циркулирующей в системе, тем более, что данные в ИС обычно хранятся в виде, непонятном для большинства людей.

Целью НСД могут быть и сами программы. Причины этому:

1. *Программы могут быть товаром*, приносящим прибыль, особенно тому, кто первым начнет тиражировать программу в коммерческих целях и оформит авторские права на нее.

2. *Программы могут становиться также объектом НСД*, имеющего целью модифицировать эти программы некоторым образом, что позволило бы в будущем провести воздействия на другие объекты системы.

Рассмотрим несколько видов программ и приемы, которые наиболее часто используются для НСД в программы и данные.

3.2.1. Проникновение в программу

Проникновение в программу предполагает использование “люка”. “Люком” называется не описанная в документации на программный продукт возможность работы с программным продуктом.

Сущность использования “люков” состоит в том, что при выполнении пользователем не описанных в документации действий он получает доступ к возможностям и данным, которые в обычных условиях для него закрыты (в частности - выход в привилегированный режим).

Причинами появления “люков” являются действия разработчиков по созданию временных механизмов, облегчающих ведение отладки за счет прямого доступа к отлаживаемым частям программы. Например, для начала работы с программой требуется выполнить некоторую последовательность

действий, предусмотренных алгоритмом: ввести пароль, установить значения некоторых переменных и т.п. При нормальной работе программы эти действия имеют определенный смысл. Но во время отладки, когда разработчику приходится тестировать некоторые части программы по несколько раз, программист использует специальные дополнительные механизмы, включенные в программу.

3.2.2. Деструктивные функции закладок и работа прикладных программ

Исполнение кода закладки может быть сопровождено операциями несанкционированной записи (например, для сохранения некоторых фрагментов информации) и несанкционированного считывания, которое может происходить отдельно от операций чтения прикладной программы или совместно с ними. Под операциями считывания и записи понимаются любые обращения к внешнему устройству (возможно и несвязанные с получением информации, например, считывание параметров устройства или его инициализация; закладка может использовать для своей работы такие операции, в частности, для инициирования сбойных ситуаций или переназначения ввода-вывода).

Перенос информации в оперативную память не является опасным, поскольку извлечение ее требует вывода на внешний носитель или устройство вывода, что предопределяет необходимость НСЗ закладкой.

Несанкционированная запись закладкой может происходить в:

- массив данных, не совпадающий с пользовательской информацией (сохранение информации);

- массив данных, совпадающий с пользовательской информацией или ее подмножеством (искажение, уничтожение или навязывание информации закладкой).

Основные группы деструктивных функций, которые могут выполняться закладками:

- сохранение фрагментов информации, возникающей при работе пользователя, прикладных программ, вводе-выводе данных, во внешней памяти (локальной или удаленной) сети или выделенной ПЭВМ;

- разрушение функций самоконтроля или изменение алгоритмов функционирования прикладных программ;

- навязывание некоторого режима работы (например, при уничтожении информации блокирования записи на диск, при этом информация, естественно, не уничтожается), либо замена записываемой информации навязанной закладкой.

Процесс размножения закладки качественно не отличается от процесса размножения вируса.

3.2.3. Способы реализации функций закладок. Общие положения

Для того чтобы закладка смогла выполнить какие-либо функции по отношению к прикладной программе, она должна получить управление на себя, т.е. процессор должен начать выполнять инструкции (команды), относящиеся к коду закладки.

Это возможно только при одновременном выполнении двух условий:

1) закладка должна находиться в оперативной памяти до начала работы программы, которая является целью воздействия закладки, следовательно, она должна быть загружена раньше или одновременно с этой программой;

2) закладка должна активизироваться по некоторому общему как для закладки, так и для программы событию, т.е. при выполнении ряда условий в программно-аппаратной среде управление должно быть передано на «программу – закладку».

Это достигается путем анализа и обработки закладкой общих относительно закладки и прикладной программы воздействий (как правило, прерываний). Причем прерывания должны сопровождать работу прикладной программы или работу всей ПЭВМ.

В качестве таких прерываний можно выделить:

- прерывания от таймера ПЭВМ;
- прерывания от внешних устройств;
- прерывания от клавиатуры;
- прерывания при работе с диском;
- прерывания операционной среды (в том числе прерывания при работе с файлами и запуск исполняемых модулей).

Возможен случай, когда при запуске программы закладка разрушает некоторую часть кода программы, уже загруженной в оперативную память, и, возможно, систему контроля целостности кода или контроля иных событий и на этом заканчивает свою работу.

Можно выделить закладки:

1. Резидентного типа - которые находятся в памяти постоянно с некоторого момента времени до окончания сеанса работы персонального компьютера (выключения питания или перегрузки).

2. Нерезидентного типа - которые начинают работу по аналогичному событию, но заканчивают ее самостоятельно по истечении некоторого промежутка времени или некоторому событию, при этом выгружая себя из памяти целиком.

3.2.4. Несанкционированный доступ в базы данных

Основные требования по безопасности, предъявляемые к базам данных, а также к системам управления базами данных (СУБД), практически совпадают с требованиями, предъявляемыми к другим элементам ИС. Это управление доступом, устойчивость к занесению ложных данных, аутентификация

показателей, достоверность и т.д. Тем не менее из них можно выделить основные требования:

1. *Целостность физической базы данных* - хранимые в базе данные должны быть устойчивы по отношению к неблагоприятным физическим воздействиям (например, сбоям питания).

2. *Целостность логической базы данных* - устойчивой должна быть логическая структура базы данных. Условие логической целостности базы данных состоит в том, что изменение значения одного элемента данных не должно влиять на интерпретацию другого элемента.

3. *Целостность отдельного элемента* - т.е. в каждый элемент данных информации заносится точно в соответствии с описанием этого элемента. Должны быть предусмотрены механизмы обеспечения устойчивости элементов данных к ошибкам или неквалифицированным действиям пользователей.

4. *Возможность контроля доступа* - должна существовать возможность установления лица, осуществившего тот или иной доступ к конкретному элементу данных, а также тип, соответствующий конкретному элементу данных, а также тип осуществленного доступа. Во многом это требование обусловлено необходимостью иметь средства восстановления базы данных после искажения.

5. *Управление доступом* - пользователь должен иметь доступ только к тем данным, для работы с которыми он авторизован; при этом пользователи могут быть ограничены различными типами доступа к данным.

6. *Доступность данных* - пользователи, которые авторизованы для работы с базой данных, должны иметь гарантированный доступ к данным.

При работе с данными могут быть искажены сами значения данных, что, в свою очередь, сделает их непригодными для использования.

Кроме того, большинство прикладных программ будут работать только в том случае, если данные размещены в файлах со строго определенными именами и в определенном порядке. Важным является то, что элементы данных самостоятельно существуют и обрабатываются довольно редко. Чаще обрабатываются группы взаимосвязанных данных. Собственно целостность данных и означает, что в каждый момент времени корректны и сами значения всех элементов данных, и взаимосвязи между элементами данных.

Глава 4. Защитные механизмы, используемые в ИС

4.1. Система защиты информации

Система защиты информации - совокупность специальных мер правового и административного характера, организационных мероприятий, физических и технических средств защиты, а также специального персонала, предназначенных для обеспечения безопасности ИС.

Основные принципы построения систем обеспечения информационной безопасности:

- *законность;*
- *системность;*
- *комплексность;*
- *непрерывность защиты;*
- *минимизации полномочий;*
- *разделения функций;*
- *гибкость управления;*
- *открытость алгоритмов и механизмов защиты;*
- *простота применения защитных мер и средств.*

Принцип системности. Системный подход к защите компьютерных систем предполагает необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности ИС.

Принцип комплексности. Комплексный подход предполагает согласованное применение разнородных мер, методов и средств при построении целостной системы защиты, перекрывающей все существенные каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов.

Принцип разумной достаточности. Создать абсолютно непреодолимую систему защиты принципиально невозможно. Поэтому имеет смысл вести речь только о некотором приемлемом уровне безопасности. Высокоэффективная система защиты стоит дорого, использует при работе существенную часть мощности и ресурсов компьютерной системы и может создавать ощутимые дополнительные неудобства пользователям.

Важно правильно выбрать тот достаточный уровень защиты, при котором затраты на защиту и остаточный риск нанесения ущерба были бы приемлемыми (задача анализа риска).

Принцип непрерывности защиты. Защита информации - это не разовое мероприятие и даже не определенная совокупность проведенных мероприятий и установленных средств защиты, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла ИС, начиная с самых ранних стадий проектирования, а не только на этапе ее эксплуатации.

Принцип минимизации полномочий. Означает предоставление пользователям минимальных прав доступа в строгом соответствии с производственной необходимостью.

Доступ к информации должен предоставляться только в том случае и объеме, в каком это необходимо сотруднику для выполнения его должностных обязанностей.

Принцип разделения функций. Ни один сотрудник организации не должен иметь полномочий, позволяющих ему единолично осуществлять выполнение критичных операций.

Все такие операции должны быть разделены на части, и их выполнение должно быть поручено различным сотрудникам. Кроме того, необходимо предпринимать специальные меры по недопущению сговора и разграничению ответственности между этими сотрудниками.

Принцип гибкости системы защиты. Часто приходится создавать систему защиты в условиях большой неопределенности. Поэтому принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты.

Для обеспечения возможности варьирования уровнем защищенности, средства защиты должны обладать определенной гибкостью. Особенно важным это свойство является в тех случаях, когда установку средств защиты необходимо осуществлять на работающую систему, не нарушая процесса ее нормального функционирования.

Принцип открытости алгоритмов и механизмов защиты. Безопасность не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования системы защиты. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления (даже ее авторам). Однако это вовсе не означает, что информация о конкретной системе защиты должна быть общедоступна.

Принцип простоты применения. Механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе законных пользователей, а также не должно требовать от них выполнения рутинных малопонятных ему операций (ввод нескольких паролей и имен и т.д.).

4.2. Идентификация и аутентификация

Идентификация (субъекта или объекта):

1) именование (присвоение имен-идентификаторов);

2) опознавание (выделение конкретного из множества).

Аутентификация (субъекта или объекта) - подтверждение подлинности (доказательство того, что он именно тот, кому предоставлены права).

Три способа аутентификации:

1. Знать что-либо, чего не знают другие (разделяемый секрет - пароль, ключ).

Аутентификация по паролю предполагает решение следующих проблем: хранения, перехвата и повторного использования пароля и проблемы доставки.

Пути решения: одноразовые пароли, одноразовые свертки пароля и случайного ключа, аутентификация по ключу, многократная аутентификация.

2. Иметь что-либо, чего нет у других (что сложно отнять или передать).

Аутентификация по биометрическим параметрам, проблемы: получения ключа из биометрических параметров, хранения, неоднозначного сравнения с эталоном, доставки. Однократный ввод пароля *(Single Sign-On):*схема с шифрованием паролей и схема с сервером аутентификации.

3. Иметь рекомендации от доверенного посредника (которому верит проверяющий)

Использование инфраструктуры открытых ключей – базируется на асимметричной криптографии и служит для обеспечения подлинности открытого ключа.

4.3. Разграничение доступа к ресурсам ИС

Основная проблема – санкционирование доступа к ресурсам.

Три подхода к управлению доступом субъектов к объектам.

1. Избирательное (дискреционное, произвольное, добровольное):

- управление доступом к файлам, каталогам, устройствам;
- матрица избирательного управления доступом;
- политики доступа;
- списки управления доступом;
- списки полномочий пользователей;
- наследование прав доступа.

2. Полномочное (мандатное, принудительное) управление доступом к файлам и каталогам:

- иерархия меток (грифов) конфиденциальности;
- неиерархическая система меток конфиденциальности.

3. Механизм создания индивидуальной ограниченной замкнутой программной среды:

- замкнутая программная среда – для этого необходимо выполнить требования: «запрещено все, что явно не разрешено», указание полных путей доступа к исполняемым файлам, запрет модификации (защита от подмены) файлов, формирование списка по журналам регистрации, наличие «мягкого» режима работы.

Управление доступом

Средства управления доступом позволяют определять и контролировать действия, которые субъекты (пользователи и процессы) могут выполнять над объектами (информацией или другими компьютерными ресурсами). Логическое управление доступом - это основной механизм многопользовательских систем, призванный обеспечить конфиденциальность и целостность объектов.

Если дается разрешение на выполнение затребованного действия, говорят, что объект, осуществляющий запрос, имеет полномочия по отношению к указанному элементу данных. Элементом данных может быть файл, запись, поле, отношение или некоторая другая структура.

При принятии решения о предоставлении доступа обычно анализируется следующая информация:

- Идентификатор субъекта (идентификатор субъекта, сетевой адрес компьютера и т.д.). Подобные идентификаторы являются основой произвольного управления доступом.

- Атрибуты субъекта (метка безопасности, группа пользователя).

Метки безопасности являются основой принудительного управления доступом.

- Место действия (системная консоль, узел в сети и т.п.).

- Время действия (большинство действий целесообразно разрешать только в рабочее время).

- Внутренние ограничения сервиса (число одновременно работающих пользователей, сумма денег, которую разрешено выдавать наличными и пр.).

Матрица доступа (полномочий) представляет собой матрицу, в которой столбец соответствует объекту системы, а строка - субъекту. На пересечении столбца и строки матрицы указывается тип разрешенного доступа субъекта к объекту. Обычно выделяют такие типы доступа субъекта к объекту, как "доступ на чтение", "доступ на запись", "доступ на исполнение" и т.п.

Текущее состояние прав доступа (профиль полномочий) описывается матрицей полномочий: по строкам перечислены субъекты, в столбцах - объекты, на пересечении записываются способы доступа, допустимые для субъекта по отношению к объекту. Каждый элемент A(i,j) в матрице установления полномочий определяет права доступа i-го пользователя к j-му ресурсу.

Таблица 1

Место расположения терминала	Имя служа-щего	Адрес служа-щего	Таб. № служа-щего	Квалифи кация служа-щего	Данные об окладе	Прогноз объема продаж	Цена закупки
Отдел кадров	11	11	11	11	11	00	00
Касса	01	00	01	00	11	00	00
Отдел сбыта	00	00	00	01	00	11	01
Снабжение	00	00	00	00	00	00	11
Отдел маркетинга	00	00	01	01	00	00	01

01 - означает право ЧИТАТЬ;

10 - означает право ПИСАТЬ;

00 - в i-строке и j-м столбце означает, что терминалу из i-й строки запрещены все виды доступа к элементу данных, описанному в j-м столбце.

11 - означает, что с терминала можно как читать, так и записывать элемент данных.

Глава 5. Основные этапы разработки политики информационной безопасности

5.1. Регламентация процесса функционирования ИС

Этапы построения защищенной ИС:

1. *Предпроектный этап.*
2. *Проектирование подсистемы ИБ.*
3. *Ввод в действие подсистемы ИБ.*
4. *Аттестация ИС.*
5. *Ввод ИС в эксплуатацию.*

Предпроектный этап:

- Назначение и подготовка должностных лиц, ответственных за организацию системы ОИБ.
- Обследование объекта, анализ исходных данных.
- Формирование общих требований к подсистеме ИБ.
- Разработка концепции ИБ.
- Разработка ТЗ на создание подсистемы ИБ.

Проектирование подсистемы ИБ - заключается в разработке политики ИБ в виде совокупности документируемых программных, аппаратных, организационных, административных, юридических, физических решений, набора правил и инструкций, четко регламентирующих все аспекты деятельности компании в области ИБ.

Основная цель политики ИБ - информирование пользователей ИС о наложенных на них обязательных требованиях по защите информационных ресурсов.

Эффективная система ИБ должна обеспечивать *разумный баланс* между политикой ИБ и техническими средствами защиты информации.

Политика безопасности – совокупности правил и ограничений (регламентов), направленных на обеспечение безопасности организации при использовании ИС. Определяет КАК ДОЛЖНО БЫТЬ. Термин политика ИБ имеет различное содержание для различных категорий пользователей ИС организации: сотрудников, системных и сетевых администраторов, администраторов безопасности. Все сотрудники организации должны быть ознакомлены с политикой ИБ в части их касающейся. Основные положения политики ИБ организации должны быть изложены в “Концепции ИБ”.

Основные составляющие политики ИБ:

1. Определение ИБ, ее общие цели и область действия, а также сведения о важности ИБ в качестве механизма, делающего возможным совместное использование информации.
2. Принципы обеспечения и границы применяемости политики безопасности. Краткое разъяснение политики безопасности.

3. Определение общих и частных обязанностей по управлению ИБ, в том числе предоставление сведений об инцидентах.

4. Соответствие законодательным актам и стандартам.

5. Политика доступности и обеспечения непрерывности работы и восстановления ИС.

6. Политика аутентификации, которая устанавливает эффективную политику паролей, рекомендации по аутентификации удаленных субъектов и использованию аутентифицирующих устройств.

7. Политика разграничения доступа, определяющая права доступа и привилегии для пользователей, администраторов, руководства.

8. Правила приобретения информационных технологий, которые отвечают требованиям ИБ.

9. Политику конфиденциальности, связанную с такими сервисами как ЭП, Интернет, VPN, доступ к пользовательским файлам и др.

10. Обучение персонала по вопросам ИБ.

11. Обнаружение и блокирование вирусов и других вредоносных программ, защита от недекларированных возможностей.

12. Последствия нарушения политики безопасности и ответственность нарушителей.

13. Ссылки на более детальные документы по ИБ (положения, инструкции).

14. Периодический анализ и обновление политики безопасности - устаревшая политика ИБ бесполезна. Она должна пересматриваться 1 раз в полгода.

5.2. Процесс реконфигурации аппаратно-программных средств, разработки и внедрения программного обеспечения

В разрешительной системе допуска (система авторизации) устанавливается:

- *кто, кому, при каких условиях, к каким ресурсам ИС и на какие виды доступа может давать разрешения;*
- *система санкционирования и разграничения доступа, которая предполагает определение для всех пользователей конкретных перечней информационных и программных ресурсов, доступных им для чтения, модификации, удаления, выполнения и т.п.* Процесс реконфигурации аппаратно-программных средств устанавливается *Инструкцией по внесению изменений в списки пользователей и наделению их полномочиями доступа к ресурсам ИС организации*. Разрешение на доступ дает руководитель подразделения в документируемом виде. Руководитель несет персональную ответственность за обоснованность предоставления прав.

Процедура регистрации (создания учетной записи) пользователя для сотрудника и предоставления ему (или изменения его) прав доступа к ресурсам

ИС инициируется заявкой начальника подразделения (отдела, сектора), в котором работает данный сотрудник.

Если полномочий непосредственного начальника недостаточно, заявку может визировать вышестоящий руководитель, утверждая тем самым производственную необходимость допуска (изменения прав доступа) конкретного сотрудника к необходимым для решения им указанных задач ресурсам ИС.В заявке должно указываться: содержание запрашиваемых изменений:

- регистрация нового пользователя ИС;
- удаление учетной записи пользователя;
- расширение или сужение полномочий и прав доступа к ресурсам ИС ранее зарегистрированного пользователя; должность (с полным наименованием подразделения), фамилия, имя и отчество сотрудника; имя пользователя (учетной записи) данного сотрудника; полномочия, которых необходимо лишить пользователя или которые необходимо добавить пользователю (путем указания решаемых пользователем задач на конкретных рабочих станциях ИС).Правила именования пользователей, задач, ролей и компьютеров:

Правила именования пользователей

1. С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику ОРГАНИЗАЦИИ, допущенному к работе с конкретной подсистемой ИС ОРГАНИЗАЦИИ, должно быть сопоставлено персональное уникальное имя (бюджет или учетная запись пользователя), под которым он будет регистрироваться и работать в системе. Некоторым сотрудникам в случае производственной необходимости могут быть сопоставлены несколько уникальных имен (учетных записей).

2. Использование несколькими сотрудниками при работе в ИС одного и того же имени пользователя (“группового имени”) ЗАПРЕЩЕНО.

3. Идентификаторы не должны являться источником информации об организации, ее структуре и функциях их владельцев (admin).

4. В ИС должны быть разработаны стандартные профили доступа для всех типовых категорий пользователей (пользователи, операторы, администраторы, привилегированные пользователи, аудиторы).

5.3. Регламентация процесса разработки, испытания, внедрения и сопровождения задач

Стандарт ISO 17799 рекомендует разделить области разработки, тестирования и эксплуатации, чтобы снизить риск случайного изменения или несанкционированного доступа к рабочему программному обеспечению и данным организации.

Рекомендуется предусмотреть следующие меры:

• По возможности средства разработки и программы, используемые в основной работе организации, должны работать на отдельных компьютерных процессорах или в разных доменах или каталогах.

• Действия, связанные с разработкой и тестированием, должны быть как можно больше отделены друг от друга.

• Компиляторы, редакторы и другие системные средства не должны быть доступны из рабочих систем без необходимости.

Планирование действий по ОНРВ

Планирование действий по обеспечению непрерывной работы и восстановления (ОНРВ) нормального функционирования ИТ систем – это процесс разработки планов и принятия организационно-технических мер по подготовке к их реализации, позволяющий после серьезных нарушений и повреждений ИТ систем:

- обеспечить выполнение наиболее важных функций по временным схемам;
- быстро и эффективно восстановить их нормальное функционирование.

Планирование ОНРВ является необходимой составляющей обеспечения безопасности организации (то есть процесса управления рисками, приводящими к нарушению работоспособности системы и доступности ее функций).

Основные положения политики ОНРВ

Для обеспечения эффективности плана и для проверки однозначного понимания его требований персоналом, он должен базироваться на четко определенной политике. Ключевыми положениями политики ОНРВ являются:

- Определение общих целей ОНРВ.
- Определение областей действия различных планов ОНРВ (по типам платформ, функциям организации и т.п.).
- Распределение обязанностей (ролей) и ответственности.
- Определение требований к необходимым ресурсам.
- Определение требований к тестированию планов.
- Определение требований к обучению и подготовке персонала.
- Определение порядка сопровождения плана.

Анализ влияния работы ИТ системы.

Цель такого анализа – выявление зависимости критически важных функций от конкретных компонентов ИТ системы на основе информации, характеризующей последствия нарушений их работы.

Этапы анализа:

А) Выявление критичных ИТ ресурсов.

Б) Определение негативного влияния и допустимого времени простоя.

В) Определение приоритетов восстановления.

Выявление критичных ИТ ресурсов. *На первой стадии анализа определяются критичные функции (процессы) и выявляются конкретные системные ресурсы и компоненты, необходимые для их реализации.*

Критичные бизнес функции и процессы:

- Управление технологическим оборудованием
- Обработка платежей
- Бухгалтерский учет
- Управление персоналом
- Информирование клиентов

Критичные ресурсы:

- Межсетевой экран
- Сервер приложения
- Сервер E-mail
- N сетевых рабочих станций

Определение негативного влияния и допустимого времени простоя. Оценивается степень влияния выявленных критичных компонентов на основные операции (функции системы), в случае повреждения или полного выхода из строя данных компонентов. На основе компромисса между стоимостью потерь от неработоспособности системы и стоимостью ее восстановления определяется оптимальное время восстановления критичных компонентов системы.

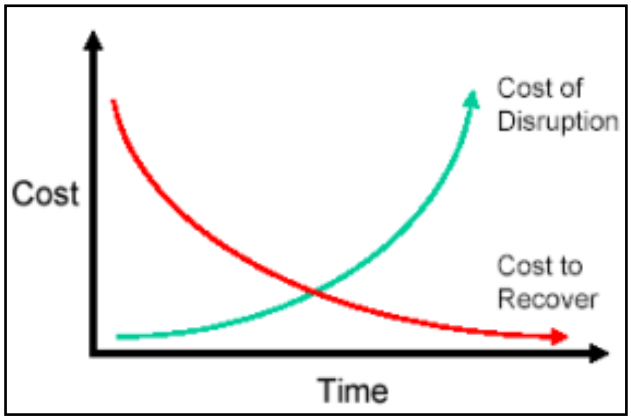

Рис. 3. Время простоя системы

Определение приоритетов восстановления. Размер ущерба, вызванного нарушением в работе, и допустимое время простоя, определенные на предыдущем шаге, позволяют определить приоритетность стратегий восстановления.

Ресурс	Приоритет восстановления
Межсетевой экран	Низкий
Сервер приложения	Высокий
Файловый сервер	Высокий
Сервер E-mail	Средний
Сетевые рабочие станции	Низкий

Подготовка к ОНРВ

Меры повышения готовности компонентов системы к восстановлению:

- Регулярное резервное копирование важных данных.
- Хранение носителей с резервными копиями, с эталонными (лицензионными) копиями программного обеспечения и лицензий для них за пределами офиса.
- Резервирование критичных технических средств.
- Документирование конфигураций компьютеров и сведений о производителях используемых в них компонентов.
- Стандартизация и унификация конфигураций технических средств, программного обеспечения и периферийного оборудования.
- Определение порядка хранения данных на персональных компьютерах пользователей.
- Разработка и согласование процедур восстановления с политиками и процедурами обеспечения безопасности и расследования инцидентов.
- Применение средств сетевого мониторинга.

Глава 6. Основы защиты информации от утечки по техническим каналам

6.1. Модель технического канала утечки информации и порядок определения границы контролируемой зоны

Данное направление как неотъемлемая составная часть комплексной защиты информации достаточно широко и подробно освещено в большом числе закрытых и открытых информационных источников, руководящих и нормативных документов общегосударственного и ведомственного уровня.

Техническими каналами утечки информации принято называть электропроводную цепь или среду, по которой возможна утечка сведений, обрабатываемых ТСПИ или обсуждаемых в выделенных помещениях.

Объект технических средств передачи информации (ТСПИ) – *это отдельное техническое средство или группа технических средств, предназначенных для обработки конфиденциальной информации, вместе с помещением, в котором они размещены.*

Несмотря на объективно обусловленное многообразие видов технических каналов утечки информации, для них характерно наличие ряда общих элементов. Это позволило сформировать, в интересах защиты информации, некоторую обобщенную модель ТКУИ и использовать ее для разработки общих основ и принципов защиты.

Рис. 4. Технический канал утечки информации

Как видно из рис. 4, ключевыми ЭЛЕМЕНТАМИ ТЕХНИЧЕСКОГО КАНАЛА УТЕЧКИ ИНФОРМАЦИИ ЯВЛЯЮТСЯ:

- *одиночное ТСПИ или их совокупность* (Одиночное ТСПИ или их совокупность как источники ОПАСНОГО СИГНАЛА (ОС));

- *опасный сигнал* (ОПАСНЫМ принято называть сигнал любой физической природы, несущий информацию, подлежащую защите). Физически носителями опасного сигнала могут быть:

- акустические колебания, протекающие по любым проводящим коммуникациям токи;

- наводимая на посторонние цепи электродвижущая сила (ЭДС), распространяющиеся в окружающем пространстве электромагнитные поля различных диапазонов. Этим определяется и многообразие вариантов, с физической точки зрения, среды распространения опасных сигналов);

- *среда распространения ОС (*СРЕДА РАСПРОСТРАНЕНИЯ опасного сигнала – это некоторая материальная субстанция между ТСПИ как источником опасного сигнала и местом возможной установки аппаратуры перехвата информации. *В качестве среды распространения ОС могут выступать*: кабели связи, сигнализации и электропитания; шины и провода системы заземления; трубы систем вентиляции, тепло- и водоснабжения; окружающее пространство*)*;

- *аппаратура перехвата информации* (АПИ представлена одиночными или комплексированными средствами разведки ПЭМИН, обеспечивающими прием и регистрацию звуковых сигналов, электромагнитных излучений и наводок ТСПИ (побочные электромагнитные излучения и наводки). Конструктивно АПИ является портативной, исполняемой в возимом, носимом и автоматическом автономном вариантах, аппаратурой. Во всех случаях

основным принципом применения АПИ является ее максимально достижимое приближение к объекту разведки);

- *помехи* (ПОМЕХИ различной физической природы и различного происхождения объективно имеют место в любых условиях функционирования и размещения АПИ и защищаемых ТСПИ. Они воздействуют непосредственно на вход аппаратуры перехвата и существенно влияют на качество приема опасных сигналов. *Реально на входе приемника АПИ существует не чистый опасный сигнал, а некоторое отношение сигнал/помеха*).

Контролируемой зоной (КЗ) называют *территорию, на которой исключено несанкционированное и неконтролируемое пребывание лиц и транспортных средств – потенциальных носителей АППАРАТУРЫ ПЕРЕХВАТА ИНФОРМАЦИИ.*

С изложенных выше позиций контролируемая зона должна иметь определенные размеры, а положение ее границы на местности должно соответствовать условиям, исключающим возможность приема и регистрации опасных сигналов средствами АПИ.

6.2. Источники возникновения опасных сигналов

I. Как видно, первая группа получила общепринятое название ТКУИ за счет АКУСТОЭЛЕКТРИЧЕСКИХ ПРЕОБРАЗОВАНИЙ

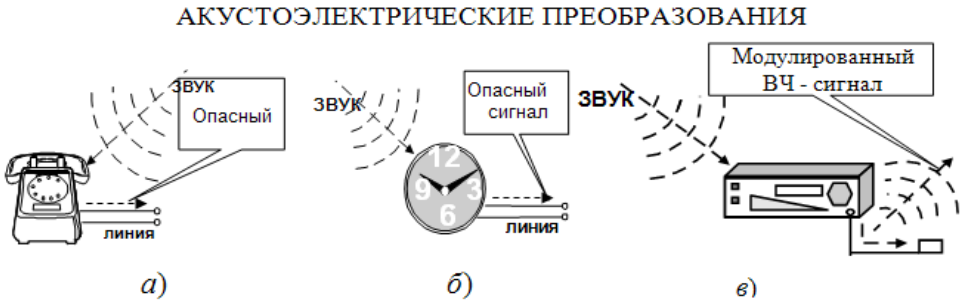

Рис. 5. Акустоэлектрические преобразования

Это обусловлено тем, что первичным в возникновении данных ТКУИ является *акустическое (звуковое) воздействие* на самые обычные в обиходе ТСПИ, приводящее, в конечном итоге, к возникновению ОС в виде протекающих токов или излучаемых модулированных высокочастотных (ВЧ) сигналов.

Источник ОС	Данные для ТКУИ	Защита информации
телефонный аппарат с электрическим звонком	*Звуковое воздействие на корпус*	*Запрет установки*
электрочасы, имеющие в конструкции электро-магнит, управляющий передвижением стрелок	*Звуковое воздействие на корпус*	*Запрет установки*
работающий радио- или телевизионный приемник	*Звуковое воздействие на корпус*	*Запрет установки*

Особо опасным источником опасного сигнала этой группы является широко распространенный телефонный аппарат с электрическим звонком сигнализации вызова от абонента.

II. Второй группой ТКУИ являются каналы утечки по цепям электропитания и заземления. И то и другое является обязательным условием выполнения эксплуатационных, экологических и эргономических требований при использовании ТСПИ по целевому предназначению.

Утечку информации по цепям электропитания могут вызвать две основные причины:

1) неравномерность потребления тока в процессе работы ТСПИ;

2) “стекание” тока опасного сигнала в провода системы энергообеспечения каждого средства и объекта в целом.

В обоих случаях защиту рекомендуется обеспечивать за счет реализации двух наиболее радикальных мер. Ими являются: питание каждого ТСПИ через специальные сетевые помехоподавляющие фильтры; размещение (по возможности) понижающей электропитающей подстанции в пределах контролируемой зоны и подключение наиболее важных средств и объектов ТСПИ к отдельным трансформаторам.

Глава 7. Управление целостностью данных, их восстановлением и хранением

7.1. Разработка стратегии хранения данных

Хорошая стратегия хранения данных учитывает множество факторов, влияющих на надежность и производительность сети, включая планирование восстановления после аварий.

Выделяют *семь* этапов разработки стратегии хранения данных.

На практике некоторые этапы будут скорее всего выполняться параллельно, а сам ступенчатый процесс имеет непрерывный характер.

1. *Первым* шагом в разработке стратегии хранения данных является исследование имеющейся среды хранения данных (под управлением какой

серверной операционной системы осуществляется хранение критических данных).

2. Следующим шагом, после того как получена статическая картина среды хранения данных, будет сбор статистики о том, насколько используются ресурсы хранения данных, насколько хорошо работает система хранения и в каком направлении она развивается. Где *наиболее интенсивно* потребляются данные (*производительность*)? Возможно, тысячи файлов, к которым обращаются крайне редко, хранятся на отказоустойчивых высокопроизводительных серверах. В этом случае естественным решением будет перенос таких файлов на оптическую библиотеку, где стоимость хранения ниже, хотя при этом скорость доступа невысока. Данные, к которым никто не обращался в течение последних четырех недель, лучше хранить в оптической библиотеке, а серверам найти более достойное применение.

3. После этапа исследования и сбора статистики составьте *список потенциальных проблем*. Этот список станет хорошей исходной точкой для оценки риска, определение которого составляет третий этап в разработке стратегии управления хранением данных. Составив список потенциальных проблем, вы сможете расставить приоритеты, основываясь на возможных последствиях и потерях в случае наступления каждой из них, а затем поочередно заняться решением всех существующих проблем, начиная, разумеется, с наиболее критических.

4. После того как вы обследовали среду хранения данных, оценили ее производительность и определили вероятные проблемы, можно приступать к *четвертому* этапу - *тестированию* продуктов, отвечающих вашим требованиям к хранению данных.

5. *Пятый* этап планирования хранения данных состоит в выработке мер по восстановлению после аварии. Определите, какие данные непременно должны быть в порядке для поддержания бизнеса. Схема восстановления должна учитывать тот факт, что эти данные нужны в первую очередь.

6. Самого по себе плана недостаточно, вы должны проверить его действенность - этап номер *шесть*. Если у вас есть резервный центр, временно изолируйте его и убедитесь в том, что он может выполнять ключевые функции полностью самостоятельно. *Все ли ваши приложения работают нормально?* Очень часто якобы полные резервные копии на самом деле не содержат таких критически важных компонентов, как файлы .DLL или конфигурационные файлы, находящиеся на рабочих станциях. Убедитесь, что вы на самом деле можете выполнять критические функции, от которых зависит жизнедеятельность компании.

7. *Седьмой*, завершающий этап планирования хранения данных - разработка плана поддержания непрерывности бизнеса. Согласно статистике, после катастрофы бизнес сокращается на 50% только потому, что клиенты предпочитают обратиться к кому-нибудь еще. Планирование непрерывности

может включать в себя меры по удержанию клиентов или страхование на случай потери бизнеса при катастрофе.

Многие из описанных задач, такие как контроль производительности системы и сбор статистики о росте объемов данных, должны производиться на постоянной основе. Кроме того, по мере роста компании и ее реорганизации вы должны регулярно проводить проверку принятых мер, поскольку те, что срабатывали несколько месяцев назад, могут отказать завтра.

7.2. Резервирование, архивирование и управление восстановлением данных

Резервирование позволяет восстанавливать данные в случае их потери. Причиной потери данных может *стать крах диска или сервера, удаление файла, перезапись файла или порча данных из-за возможных проблем в ЦП, оперативной памяти, питании или приложении.* Избыточность резервирования важна для обеспечения восстановимости файлов, которые могут быть утеряны несколько дней, недель или даже месяцев тому назад.

Архивирование позволяет создавать архивы, которые являются постоянными или полупостоянными копиями данных для долгосрочного хранения. Архивы можно создавать во время резервирования или при помощи отдельной процедуры.

7.2.1. Обеспечение целостности данных

Когда дело доходит до резервного копирования и архивирования данных, выбор стратегии определяется двумя факторами: свободное для резервного копирования время ("окно резервирования") и максимально допустимое время восстановления резервных копий файлов.

Самым легким и надежным решением будет резервирование в нерабочие часы, когда сеть не используется и доступ к данным не осуществляется. Причина в том, что резервирование может вызвать замедление работы системы, увеличивая и нагрузку на систему, и сетевой трафик. Так что проведение резервного копирования в рабочее время чревато снижением производительности сети.

Другая причина проведения резервного копирования в нерабочее время в том, что копирование данных, которыми в этот момент пользуются, - дело достаточно рискованное. По соображениям *целостности данных, программы резервного копирования обычно предусматривают, что любые транзакции, записанные в файл во время резервного копирования, либо полностью включаются в резервную копию, либо полностью исключаются.*

Чтобы этого добиться, программа резервного копирования блокирует каждый копируемый файл, так что никакая другая программа не сможет произвести в него запись во время этого процесса. Но программа резервного копирования не способна заблокировать файл, когда другая программа уже имеет разрешение на запись в него. Многие программы резервного

копирования выдают предупредительное сообщение и пропускают этот файл, если они не могут гарантировать его беспроблемного копирования.

Однако в сегодняшней производственной среде резервное копирование данных во внерабочее время - непростая задача. К несчастью, компьютерные системы компаний все чаще продолжают использоваться и по окончании рабочего дня. *Виной тому и пользователи, работающие на дому, и мобильные пользователи, и пользователи, находящиеся в другой временной зоне*. В то же время объем данных, подлежащих резервному копированию, продолжает расти. Соответственно, окно резервирования сузилось до такой степени, что многие устройства резервного копирования не в состоянии справиться со стоящей перед ними задачей.

7.2.2. Резервирование и архивирование - raid и hsm

Резервные диски и серверы

В этом случае диски зеркалируются и дуплексируются, а также применяется технология RAID и зеркалирование серверов.

Зеркалирование дисков означает, что данные записываются на два массива дисков более или менее одновременно.

Дуплексирование является видом зеркалирования, при котором все компоненты дискового "канала", включая адаптеры хоста или контроллеры, дублируются. Сокращение RAID иногда расшифровывают по-*разному (Redundant Arrays of Inexpensive Disks - избыточные массивы недорогих дисков*, либо *Redundant Arrays of Independent Disks - избыточные массивы независимых дисков*), в любом случае наиболее распространенным подходом к организации хранения в локальной сети является запись данных на нескольких дисках таким образом, что если один диск выходит из строя, то дисководы других дисков могут "вычислить" данные, которые хранились на поврежденном диске. *Зеркалирование сервера* означает запись данных на двух серверах одновременно.

7.2.3. Технология теневого копирования данных

Суть данной технологии заключается в создании копий выбранных файлов через определенные промежутки времени.

Реализована технология в виде отдельной службы теневого копирования тома (VSS). Она используется для управления данными на дисках и может взаимодействовать с различными приложениями. Например, в программах резервного копирования эта служба обеспечивает копирование файлов, занятых во время архивации другими приложениями.

Важной практической функцией технологии теневого копирования является возможность восстановления последних версий случайно удаленных или поврежденных файлов. В ОС предоставляется возможность пользователям клиентских компьютеров восстанавливать файлы из теневой копии

самостоятельно без вмешательства системных администраторов, что, безусловно, очень удобно с точки зрения экономии времени.

7.2.4. Архивация данных

Под архивацией принято понимать обычное копирование данных на резервный носитель информации, чтобы в случае отказа или повреждения основного устройства хранения можно было быстро восстановить имеющиеся на нем данные. *Архивация дает наивысшую степень отказоустойчивости по сравнению со всеми другими технологиями хранения данных, обеспечивающих отказоустойчивость, такими как теневое копирование, избыточные массивы независимых дисков, кластерные серверы.*

Эффективность применения архивации в сетевой инфраструктуре зависит от правильного выбора специального ПО и планирования. В состав ОС Microsoft Windows входит служебная программа Backup, обеспечивающая основные функции архивации, включая возможности работы по расписанию и взаимодействие со службой теневого копирования тома.

7.2.5. Создание отказоустойчивых томов для хранения данных

В ОС Windows Server 2007 возможно создание отказоустойчивых томов RAID-1 (зеркальный том) и RAID-5, которые поддерживаются только на динамических дисках. По умолчанию ОС Microsoft Windows используют традиционное базовое хранение. Для эффективности управления хранением данных базовые диски преобразуют в динамические, на которых можно создавать различные типы томов.

RAID (избыточный массив независимых жестких дисков) – массив из нескольких дисков, управляемый контроллером, взаимосвязанных скоростными каналами и воспринимаемых внешней системой как единое целое.

Глава 8. Криптология, основные понятия и определения

8.1. Основные понятия и определения

Криптология - наука, занимающаяся проблемами шифрования и дешифрования.

Криптография - наука о способах преобразования (шифрования) информации с целью ее защиты от незаконных пользователей.

Криптоанализ - наука (и практика ее применения) о методах и способах вскрытия шифров.

Шифр (от франц. chiffre) - совокупность условных знаков (условная азбука из цифр или букв) для секретной переписки.

Шифр замены - шифр, осуществляющий преобразование замены букв или других "частей" открытого текста на аналогичные "части" шифрованного текста.

Шифр перестановки - шифр, осуществляющий преобразование перестановки букв в открытом тексте.

Блочный шифр - шифр, разбивающий исходный текст на блоки и преобразующий каждый блок входных данный в блок шифротекста

Поточный шифр - шифр, преобразующий открытый текст в шифротекст по одному биту за такт.

Абсолютно стойкий шифр - шифр, не поддающийся расшифровке.

Ключ - сменный элемент шифра, который применяется для шифрования конкретного сообщения.

Стойкость шифра (криптостойкость) - способность шифра противостоять всевозможным атакам на него.

Атака на шифр - попытка вскрытия шифра.

Односторонняя функция - функция шифрования F(X)=Y, не имеющая решения уравнения относительно X.

Функция с секретом - функция шифрования, FK: X®Y, зависящая от параметра К и не имеющая обратного решения при неизвестном К.

Цифровая подпись (digital signature) - способ проверки целостности содержимого сообщения и подлинности его отправителя, основанный на формировании небольшого количества цифровой информации и ее передаче вместе с подписываемым текстом.

Разовый ключ (message key) - выработанный случайным образом секретный ключ, зашифрованный другим ключом и посылаемый вместе с зашифрованным им сообщением.

Предметом криптографии является один из классов методов, предназначенных для защиты процессов информационного взаимодействия от отклонений от их нормального течения, вызванных целенаправленными воздействиями со стороны злонамеренных субъектов, называемых злоумышленниками. От прочих методов защиты информации криптографические методы отличаются тем, что основаны на преобразовании информации по секретным алгоритмам. Понятие "секретный алгоритм" трактуется широко - алгоритм, хоть какая-то деталь которого держится в секрете.

8.2. Принципы шифрования. Классификация алгоритмов шифрования

Принципы шифрования

Криптографическое преобразование (шифрование) - взаимно-однозначное математическое преобразование, зависящее от ключа (секретный параметр преобразования), которое ставит в соответствие блоку открытой информации (представленной в некоторой цифровой кодировке) блок шифрованной информации, также представленной в цифровой кодировке. Термин шифрование объединяет в себе два процесса: зашифрование и расшифрование информации.

Криптография делится на два класса: с симметричными ключами и открытыми ключами. В криптографии с симметричными ключами отправитель и получатель используют один и тот же (общий) ключ, как для шифрования, так и для расшифрования.

Классификация алгоритмов шифрования:

1) **Симметричные** (с секретным, единым ключом, одноключевые, single-key).

- Потоковые (шифрование потока данных):

1. с одноразовым или бесконечным ключом (infinite-key cipher);
2. с конечным ключом (система Вернама - Vernam);
3. на основе генератора псевдослучайных чисел (ПСЧ).

- Блочные (шифрование данных поблочно):

1. Шифры перестановки (permutation, P-блоки);
2. Шифры замены (подстановки, substitution, S-блоки):

- моноалфавитные (код Цезаря);
- полиалфавитные (шифр Видженера, цилиндр Джефферсона, диск Уэтстоуна, Enigma);

- Составные:

1. Lucipher (фирма IBM, США);
2. DES (Data Encryption Standard, США);
3. FEAL-1 (Fast Enciphering Algoritm, Япония);
4. IDEA/IPES (International Data Encryption Algorithm);
5. Improved Proposed Encryption Standard, фирма Ascom-Tech AG, Швейцария);
6. B-Crypt (фирма British Telecom, Великобритания);
7. ГОСТ 28147-89 (СССР); * Skipjack (США).

2) **Асимметричные** (с открытым ключом, public-key):

1. Диффи-Хеллман DH (Diffie, Hellman);
2. Ривест-Шамир-Адлеман RSA (Rivest, Shamir, Adleman);
3. Эль-Гамаль ElGamal.

Кроме того, есть разделение алгоритмов шифрования на собственно шифры (ciphers) и коды (codes). Шифры работают с отдельными битами, буквами, символами. Коды оперируют лингвистическими элементами (слоги, слова, фразы).

Симметричные алгоритмы шифрования

Симметричные алгоритмы шифрования (или криптография с секретными ключами) основаны на том, что отправитель и получатель информации используют один и тот же ключ. Этот ключ должен храниться в тайне и передаваться способом, исключающим его перехват. *Обмен информацией осуществляется в 3 этапа:*

- *отправитель передает получателю ключ (в случае сети с несколькими абонентами у каждой пары абонентов должен быть свой ключ, отличный от ключей других пар);*
- *отправитель, используя ключ, зашифровывает сообщение, которое пересылается получателю;*
- *получатель получает сообщение и расшифровывает его.*

Если для каждого дня и для каждого сеанса связи будет использоваться уникальный ключ, это повысит защищенность системы.

Асимметричные алгоритмы шифрования

В асимметричных алгоритмах шифрования (или криптографии с открытым ключом) для зашифровывания информации используют один ключ (открытый), а для расшифровывания - другой (секретный). Эти ключи различны и не могут быть получены один из другого.

Схема обмена информацией :

- получатель вычисляет открытый и секретный ключи, секретный ключ хранит в тайне, открытый же делает доступным (сообщает отправителю, группе пользователей сети, публикует);
- отправитель, используя открытый ключ получателя, зашифровывает сообщение, которое пересылается получателю;
- получатель получает сообщение и расшифровывает его, используя свой секретный ключ.

Глава 9. Симметричные и асимметричные криптосистемы

9.1. Асимметричные алгоритмы шифрования

Симметричные криптосистемы, рассмотренные нами в предыдущих главах, несмотря на множество преимуществ, обладают одним серьезным недостатком, о котором Вы, наверное, еще не задумывались. Связан он с ситуацией, когда общение между собой производят не три-четыре человека, а сотни и тысячи людей. В этом случае для каждой пары, переписывающейся между собой, необходимо создавать свой секретный симметричный ключ. Это в итоге приводит к существованию в системе из N пользователей $N^2/2$ ключей. А это уже очень "приличное" число. Кроме того, при нарушении конфиденциальности какой-либо рабочей станции злоумышленник получает доступ ко всем ключам этого пользователя и может отправлять, якобы от его имени, сообщения всем абонентам, с которыми "жертва" вела переписку.

Своеобразным решением этой проблемы явилось появление асимметричной криптографии. Эта область криптографии очень молода по сравнению с другими представителями. Первая схема, имевшая прикладную значимость, была предложена всего около 20 лет назад. Но за это время асимметричная криптография превратилась в одно из основных направлений криптологии, и используется в современном мире также часто, как и симметричные схемы.

Асимметричная криптография изначально задумана как средство передачи сообщений от одного объекта к другому (а не для конфиденциального хранения информации, которое обеспечивают только симметричные алгоритмы). Поэтому дальнейшее объяснение мы будем вести в терминах "отправитель" – лицо, шифруюшее, а затем отпраляющее информацию по незащищенному каналу, и "получатель" – лицо, принимающее и восстанавливающее информацию в ее исходном виде. Основная идея асимметричных криптоалгоритмов состоит в том, что для шифрования сообщения используется один ключ, а при дешифровании – другой.

Кроме того, процедура шифрования выбрана так, что она необратима даже по известному ключу шифрования – это второе необходимое условие асимметричной криптографии. То есть, зная ключ шифрования и зашифрованный текст, невозможно восстановить исходное сообщение. Прочесть его можно только с помощью второго ключа – ключа дешифрования. А раз так, то ключ шифрования для отправки писем какому-либо лицу можно вообще не скрывать. Зная его все равно невозможно прочесть зашифрованное сообщение. Поэтому ключ шифрования называют в асимметричных системах "открытым ключом", а ключ дешифрования получателю сообщений необходимо держать в секрете – он называется "закрытым ключом". Алгоритмы шифрования и дешифрования создаются так, чтобы зная открытый ключ, невозможно было вычислить закрытый ключ.

В целом система переписки при использовании асимметричного шифрования выглядит следующим образом. Для каждого из N абонентов, ведущих переписку, выбрана своя пара ключей : "открытый" E_j и "закрытый" D_j, где j – номер абонента. Все открытые ключи известны всем пользователям сети, каждый закрытый ключ, наоборот, хранится только у того абонента, которому он принадлежит. Если абонент, скажем под номером 7, собирается передать информацию абоненту под номером 9, он шифрует данные ключом шифрования E_9 и отправляет ее абоненту 9. Несмотря на то, что все пользователи сети знают ключ E_9 и, возможно, имеют доступ к каналу, по которому идет зашифрованное послание, они не могут прочесть исходный текст, так как процедура шифрования необратима по открытому ключу. И только абонент №9, получив послание, производит над ним преобразование с помощью известного только ему ключа D_9 и восстанавливает текст послания. Заметьте, что если сообщение нужно отправить в противоположном направлении (от абонента 9 к абоненту 7), то нужно будет использовать уже другую пару ключей (для шифрования ключ - E_7, а для дешифрования - ключ D_7).

Как мы видим, во-первых, в асимметричных системах количество существующих ключей связано с количеством абонентов линейно (в системе из N пользователей используются 2*N ключей), а не квадратично, как в симметричных системах. Во-вторых, при нарушении конфиденциальности k-й рабочей станции злоумышленник узнает только ключ D_k : это позволяет ему

читать все сообщения, приходящие абоненту k, но не позволяет выдавать себя за него при отправке писем. Кроме этого, асимметричные криптосистемы обладают еще несколькими очень интересными возможностями, которые мы рассмотрим через несколько разделов.

Алгоритм RSA является классикой асимметричной криптографии. В нем в качестве необратимого преобразования отправки используется возведение целых чисел в большие степени по модулю.

9.2. Функции и классификация криптосистем. Требования к криптосистемам.

Все предыдущие исследования касались только криптоалгоритмов, то есть методов преобразования небольшого блока данных (от 4 до 32 байт) в закодированный вид в зависимости от заданного двоичного ключа. Криптоалгоритмы несомненно являются "сердцем" криптографических систем, но, как мы сейчас увидим, их непосредственное применение без каких-либо модификаций для кодирования больших *объемов данных на самом деле не очень приемлемо.*

Все недостатки непосредственного применения криптоалгоритмов устраняются в криптосистемах.

Криптосистема - это завершенная комплексная модель, способна производить двусторонние криптопреобразования над данными произвольного объема и подтверждать время отправки сообщения, обладающая механизмом преобразования паролей и ключей и системой транспортного кодирования.

Функции криптосистемы:

- усиление защищенности данных;
- облегчение работы с криптоалгоритмом со стороны человека.

9.3. Архивация

Существуют две большие группы алгоритмов архивации: сжатие без потерь объективно перекодирует информацию по другим законам, то есть возможно абсолютно идентичное ее восстановление; сжатие с потерями необратимо удаляет из информации некоторые сведения, оказывающие наименьшее влияние на смысл сообщения.

Общие принципы архивации. Классификация методов

Подавляющее большинство современных форматов записи данных содержат их в виде, удобном для быстрого манипулирования, для удобного прочтения пользователями. При этом данные занимают объем больший, чем это действительно требуется для их хранения. Алгоритмы, которые устраняют избыточность записи данных, называются алгоритмами сжатия данных, или алгоритмами архивации. В настоящее время существует огромное множество программ для сжатия данных, основанных на нескольких основных способах.

Существует два основных метода архивации без потерь:

- алгоритм Хаффмана (англ. Huffman) ориентирован на неосмысленные последовательности символов какого-либо алфавита. Необходимым условием для сжатия является различная вероятность появления этих символов (и чем различие в вероятности ощутимее, тем больше степень сжатия);
- алгоритм Лемпеля-Зива (англ. Lempel, Ziv), ориентированный на сжатие любых видов текстов, то есть использующий факт неоднократного повторения "слов" – последовательностей байт (основан на корреляциях между расположенными рядом символами алфавита - словами, управляющими последовательностями, заголовками файлов фиксированной структуры).
-

9.4. Алгоритмы Хаффмана и Лемпеля-Зива

Алгоритмы Хаффмана и Лемпеля-Зива занимают объем больший, чем это действительно требуется для их хранения. Алгоритм Хаффмана основан на том факте, что некоторые символы из стандартного 256-символьного набора в произвольном тексте могут встречаться чаще среднего периода повтора, а другие соответственно – реже. Следовательно, если для записи распространенных символов использовать короткие последовательности бит, длиной меньше 8, а для записи редких символов – длинные, то суммарный объем файла уменьшится.

В теории кодирования информации показывается, что код Хаффмана является префиксным, то есть код никакого символа не является началом кода какого-либо другого символа. Проверьте это на нашем примере. А из этого следует, что код Хаффмана однозначно восстановим получателем, даже если не сообщается длина кода каждого переданного символа. Получателю пересылают только дерево Хаффмана в компактном виде, а затем входная последовательность кодов символов декодируется им самостоятельно без какой-либо дополнительной информации. Например, при приеме "0100010100001" им сначала отделяется первый символ "Б" : "01-00010100001", затем снова, начиная с вершины дерева – "А" "01-000-10100001", затем аналогично декодируется вся запись "01-000-1-01-000-01" "БАОБАБ".

Классический алгоритм Лемпеля-Зива, названный так по году своего опубликования, предельно прост. Он формулируется следующим образом: "если в прошедшем ранее выходном потоке уже встречалась подобная последовательность байт, причем запись о ее длине и смещении от текущей позиции короче чем сама эта последовательность, то в выходной файл записывается ссылка (смещение, длина), а не сама последовательность". Так фраза "КОЛОКОЛ_ОКОЛО_КОЛОКОЛЬНИ" закодируется как "КОЛО(-4,3)_(-5,4)О_(-14,7)ЬНИ".

9.5. Хеширование паролей

От методов, повышающих криптостойкость системы в целом, перейдем к блоку хеширования паролей – методу, позволяющему пользователям

запоминать не 128 байт, то есть 256 шестнадцатеричных цифр ключа, а некоторое осмысленное выражение, слово или последовательность символов, называющуюся паролем. Действительно, при разработке любого криптоалгоритма следует учитывать, что в половине случаев конечным пользователем системы является человек, а не автоматическая система. Это ставит вопрос о том, удобно и вообще реально ли человеку запомнить 128-битный ключ (32 шестнадцатеричные цифры). На самом деле предел запоминаемости лежит на границе 8-12 подобных символов, а следовательно, если мы будем заставлять пользователя оперировать именно ключом, тем самым мы практически вынудим его к записи ключа на каком-либо листке бумаги или электронном носителе, например, в текстовом файле. Это, естественно, резко снижает защищенность системы.

Для решения этой проблемы были разработаны методы, преобразующие произносимую, осмысленную строку произвольной длины – пароль, в указанный ключ заранее заданной длины.

В подавляющем большинстве случаев для этой операции используются так называемые хеш-функции (от англ. hashing – мелкая нарезка и перемешивание). Хеш-функцией называется такое математическое или алгоритмическое преобразование заданного блока данных, которое обладает следующими свойствами:

1. хеш-функция имеет бесконечную область определения;
2. хеш-функция имеет конечную область значений;
3. она необратима;
4. изменение входного потока информации на один бит меняет около половины всех бит выходного потока, то есть результата хеш-функции.

Эти свойства позволяют подавать на вход хеш-функции пароли, то есть текстовые строки произвольной длины на любом национальном языке и, ограничив область значений функции диапазоном $0..2^N-1$, где N – длина ключа в битах, получать на выходе достаточно равномерно распределенные по области значения блоки информации – ключи.

9.6. Транспортное кодирование

Поскольку системы шифрования данных часто используются для кодирования текстовой информации: переписки, счетов, платежей электронной коммерции, и при этом криптосистема должна быть абсолютно прозрачной для пользователя, то над выходным потоком криптосистемы часто производится транспортное кодирование, то есть дополнительное кодирование (не шифрование!) информации исключительно для обеспечения совместимости с протоколами передачи данных.

Все дело в том, что на выходе криптосистемы байт может принимать все 256 возможных значений, независимо от того был ли входной поток текстовой информацией или нет. А при передаче почтовых сообщений многие системы ориентированы на то, что допустимые значения байтов текста лежат в более

узком диапазоне: все цифры, знаки препинания, алфавит латиницы плюс, алфавит национального языка. Первые 32 символа набора ASCII служат для специальных целей. Для того, чтобы они и некоторые другие служебные символы никогда не появились в выходном потоке, используется транспортное кодирование.

Наиболее простой метод состоит в записи каждого байта двумя шестнадцатиричными цифрами-символами. Так байт 252 будет записан двумя символами 'FC'; байт с кодом 26, попадающий на специальный символ CTRL-Z, будет записан двумя допустимыми символами '1A'. Но эта схема очень избыточна: в одном байте передается только 4 бита информации.

На самом деле практически в любой системе коммуникации без проблем можно передавать около 68 символов (латинский алфавит строчный и прописной, цифры и знаки препинания). Из этого следует, что вполне реально создать систему с передачей 6 бит в одном байте (2^6<68), то есть кодировать 3 байта произвольного содержания 4-мя байтами из исключительно разрешенных (так называемых печатных) символов. Подобная система была разработана и стандартизирована на уровне протоколов сети Интернет – это система Base64 (стандарт RFC1251).

9.7. Общие схемы криптосистем

Общая схема симметричной криптосистемы с учетом всех рассмотренных пунктов изображена на рис. 6.

Общая схема асимметричной криптосистемы изображена на рис. 7. По структуре она практически идентична симметричной криптосистеме с ключом сеанса.

Глава 10. Windows-хуки

10.1. Обработка операционной системой сообщений от клавиатуры

Как правило, у каждого компьютера есть только одна клавиатура, поэтому все запущенные Windows программы должны разделять ее между всеми. Windows ответственна за то, чтобы отсылать информацию о нажатых клавишах активному в данный момент окну.

Хотя на экране может быть сразу несколько окон, только одно из них имеет фокус ввода, и только оно может получать сообщения от клавиатуры. Вы можете отличить окно, которое имеет фокус ввода от окна, которое его не имеет, посмотрев на его "title bar" - он будет подсвечен, в отличии от других.

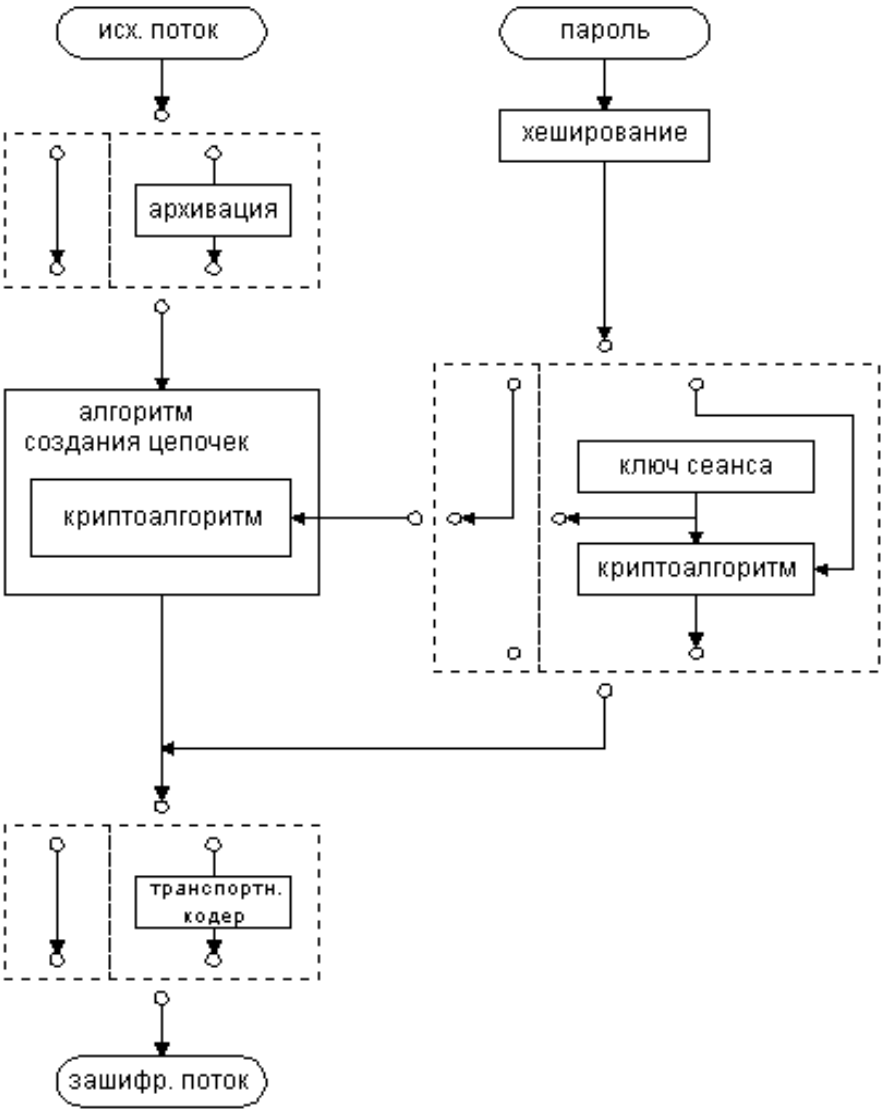

Рис. 6. Симметричная криптосистема

Рис. 7. Асимметричная криптосистема

В действительности есть два типа сообщений от клавиатуры, зависящих от того, чем вы считаете клавиатуру. Вы можете считать ее набором кнопок.

В этом случае, если вы нажмете кнопку, Windows пошлет сообщение WM_KEYDOWN активному окну, уведомляя о нажатии клавиши.

Когда вы отпустите клавишу, Windows пошлет сообщение WM_KEYUP. Вы думаете о клавише как о кнопке, но другой взгляд на клавиатуру предполагает, что это устройство ввода символов. Тогда Windows шлет сообщения WM_KEYDOWN или WM_KEYUP окну, в котором есть фокус ввода, и эти сообщения будут транслированы в сообщение WM_CHAR функцией TranslateMessage. Процедура окна может обрабатывать все три сообщения или только то, в котором оно заинтересовано. Большую часть времени вы можете игнорировать WM_KEYDOWN и WM_KEYUP, так как вызов функции TranslateMessage в цикле обработки сообщений транслирует

сообщения WM_KEYDOWN и WM_KEYUP в WM_CHAR. Мы будем опираться именно на это сообщение в данном уроке.

Char WPARAM 20h; символ, который программа получает от клавиатуры Это переменная, в которой будет сохраняться символ, получаемый от клавиатуры. Так как символ шлется в WPARAM процедуры окна, мы для простоты определяем эту переменную как обладающую типом WPARAM. Начальное значение - 20h или "пробел", так как когда наше окно обновляет свою клиентскую область в первое время, символ еще не введен, поэтому мы делаем так, чтобы отображался пробел.

```
ELSEIF uMsg==WM_CHAR
push wParam
pop  char
invoke InvalidateRect, hWnd,NULL,TRUE
```

Это было добавлено в процедуру окна для обработк сообщения WM_CHAR. Она всего лишь помещает символ в переменную char и затем вызывает InvalidateRect, что вынуждает Windows послать сообщение WM_PAINT процедуре окна. Синтаксис этой функции следующий:

```
InvalidateRect proto hWnd:HWND,\
lpRect:DWORD,\
bErase:DWORD
```

- lpRect - указатель на прямоугольник в клиентской области, который мы хотим объявить требующим перерисовки. Если этот параметр равен NULL'у, тогда вся клиентская область объявляется такой.
- bErase - флаг, говорящий Windows об уничтожении бэкграунд. Если он равен TRUE, тогда она делает это при вызове функции BeginPaint.

Таким образом, мы будем использовать следующую стратегию: мы сохраним всю необходимую информацию, относящуюся к отрисовке клиентской области и генерирующую сообщение WM_PAINT, чтобы перерисовать ее. Конечно, код в секции WM_PAINT должен знать заранее, что от него ожидают. Это кажется обходным путем делать дела, но это путь Windows.

На самом деле, мы можем отрисовать клиентскую область в ходе обработки сообщения WM_CHAR между вызовами функций GetDC и ReleaseDC. Так как код, рисующий символ находится в секции WM_CHAR, программа не сможет перерисовать символ в клиентской части. Поэтому необходимо поместить все данные и код, отвечающий за рисование в WM_PAINT. Можно послать это сообщение из любого места кода, где нужно перерисовать клиентскую область.

Когда InvalidateRect вызвана, она шлет сообщение WM_PAINT обратно процедуре окна, вызывается код в секции WM_PAINT. Далее вызывает BeginPaint, чтобы получить хэндл контекста устройства, и затем вызывается TextOut, рисующая наш символ в клиентской области в x=0, y=0. Когда

запускается программа и нажимается любая клавиша, можно увидеть символьное эхо в верхнем левом углу клиентского окна.

10.2. Обработка операционной системой сообщений от "мыши"

Так же, как и при вводе с клавиатуры, Windows определяет и шлет уведомления об активности мыши относительно какого-либо окна. Эта активность включает в себя нажатие на правую и левую клавишу, передвижение курсора через окно, двойные нажатия. В отличие от клавиатуры, сообщения передаются окну, над которым находится мышь, независимо от того, активно оно или нет. Кроме этого, есть сообщения от мыши, связанные с неклиентской частью окна, но их, как правило, можно игнорировать.

Есть два сообщения для каждой из кнопок мыши:

WM_LBUTTONDOWN, WM_RBUTTONDOWN и WM_LBUTTONUP, WM_RBUTTONUP.

Если мышь трехкнопочная, то есть еще WM_MBUTTONDOWN и WM_MBUTTONUP. Когда курсор мыши двигается над клиентской областью, Windows шлет WM_MOUSEMOVE окну, над которым он находится.

Окно может получать сообщения о двойных нажатиях, WM_LBUTTONDBCLK или WM_RBUTTONDBCLK, тогда и только тогда, когда окно имеет стиль CS_DBLCLKS, или же оно будет получать только серию сообщений об одинарных нажатиях.

Во всех этих сообщениях значение lParam содержит позицию мыши. Нижнее слово - это x-координата, верхнее слово - y-координата верхнего левого угла клиентской области окна.

wParam содержит информацию о состоянии кнопок мыши, Shift'a и Ctrl'a.

10.3. Программирование Windows-хуков

С их помощью вы сможете вмешиваться в другие процессы и иногда менять их поведение.

Хуки Windows можно считать одной из самых мощных техник. С их помощью вы можете перехватывать события, которые случатся внутри созданного вами или кем-то другим процесса. Перехватывая что-либо, вы сообщайте Windows о фильтрующей функции, также называющейся функцией перехвата, которая будет вызываться каждый раз, когда будет происходить интересующее вас событие.

Есть два вида хуков: локальные и удаленные.

- Локальные хуки перехватывают события, которые случаются в процессе, созданном вам.
- Удаленные хуки перехватывают события, которые случаются в других процессах. Есть два вида удаленных хуков:
- тредоспециализированные перехватывают события, которые случатся в определенном треде другого процесса. То есть, такой хук нужен вам,

когда необходимо наблюдать за процессами, происходящими в определенном треде какого-то процесса.

- системные перехватывают все события, предназначенные для всех тредов всех процессов в системе.

При установке хуков помните, что они оказывают отрицательное воздействие на быстродействие системы. Особенно в этом отличаются системные. Так как все требуемые события будут проходить через вашу функцию, ваша система может значительно потерять в быстродействии.

Поэтому, если вы используете системный хук, вам следует использовать их только тогда, когда вам это действительно нужно. Также существует высокая вероятность того, что другие процессы могут зависнуть, если что-нибудь неправильно в вашей функции. Помните: вместе с силой приходит ответственность.

Вы должны понимать, как работают хуки, чтобы использовать их эффективно. Когда вы создадаете хук, Windows создает в памяти структуры данных, которая содержит информацию о хуке, и добавляет ее в связанный список уже существующих хуков.

Вопросы для самопроверки

1. Цели и задачи обеспечения информационной безопасности в информационной системе.
2. Угрозы информационной безопасности в информационной системе.
3. Основные принципы, требования и способы обеспечения информационной безопасности в информационной системе.
4. Государственные стандарты и руководящие документы в области информационной безопасности.
5. Международное право в сфере защиты информации.
6. Виды информации, защищаемой законодательством РФ.
7. Классификация информации по категориям доступа.
8. Информационное оружие и его классификация.
9. Информационная война.
10. Способы несанкционированного доступа в информационные системы.
11. Способы несанкционированного доступа к программам.
12. Способы несанкционированного доступа в операционные системы.
13. Способы несанкционированного доступа в базы данных.
14. Система защиты информации.
15. Идентификация и аутентификация в информационной системе.
16. Разграничение доступа к ресурсам информационной системы.
17. Механизм контроля целостности информационной системы. Другие методы защиты.
18. Регламентация процесса функционирования информационной системы.

19. Процесс реконфигурации аппаратно-программных средств, разработки и внедрения программного обеспечения.

20. Регламентация процесса разработки, испытания, внедрения и сопровождения задач.

21. Модель технического канала утечки информации и порядок определения границы контролируемой зоны.

22. Источники возникновения опасных сигналов.

23. Разработка стратегии хранения данных. Составление плана восстановительных работ.

24. Резервирование и архивирование данных. Управление восстановлением данных.

25. Основные понятия и определения криптологии.

26. Принципы шифрования. Классификация алгоритмов шифрования.

27. Области применения скремблирующих алгоритмов.

28. Асимметричные алгоритмы шифрования.

29. Технологии цифровых подписей.

30. Функции и классификация криптосистем. Требования к криптосистемам.

Литература

1. Белов Е.Б., Лось В.П. Основы информационной безопасности. - М.: Горячая линия-Телеком, 2006.

2. Расторгуев С.П. Основы информационной безопасности. - М.: Издательский центр "Академия", 2007.

3. Безбогов А.А. Безопасность операционных систем. - М.: Гелиос АРВ, 2008.

4. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства. - М.: ДМК Пресс. www.iqlib.ru.