Федеральное государственное образовательное учреждение

высшего профессионального образования

Омский государственный аграрный университет

Кафедра информатики

Факультет МОЕНД

Специальность Профессиональное обучение

Отделение Очное

Реферат

По дисциплине: Информационная безопасность

Тема: Классификация противоправных действий персонала фирмы с конфиденциальной информацией

Студента: Сафронова Ивана

Группа № 301 Курс 3

Омск – 2010

**Введение**

По мере своего развития любая фирма сталкивается с противоправными действиями персонала с конфиденциальной информацией. Необходимо разработать ряд мер по устранению противоправных действий персонала по отношению к конфиденциальной информации в любой фирме. Вспомогательными задачами таких мер могут являться:

прогнозирование, своевременное выявление и устранение угроз безопасности ресурсам и персоналу фирмы, причин и условий, способствующих нанесению финансового, материального и морального ущерба фирмы, нарушению ее нормального функционирования и развития;

отнесение информации к категории ограниченного доступа (служебной, коммерческой тайнам, иной конфиденциальной информации, подлежащей защите от неправомерного использования), других ресурсов – к различным уровням уязвимости (опасности) и подлежащих защите;

создание механизма и условий оперативного реагирования на угрозы безопасности и проявления негативных тенденций в функционировании фирмы;

эффективное пресечение угроз персоналу и посягательств на ресурсы фирмы на основе правовых, организационных и инженерно-технических мер и средств обеспечения безопасности;

создание условий для максимально возможной локализации и возмещения наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния на достижение стратегических целей фирмы последствий нарушения режимов безопасности.

Соблюдая ряд данных мер, любая фирма имеет шанс устранить противоправные действия своего персонала.

# Угрозы безопасности фирмы

* стандартизации и унификации;
* лицензирования деятельности;
* сертификации технических и программных средств объектов информатизации;
* аттестации защищенных объектов.

При этом основными направлениями реализации технической политики обеспечения информационной безопасности должны являться:

защита информационных ресурсов от хищения, утраты, уничтожения, разглашения, утечки, искажения и подделки за счет несанкционированного доступа (НСД) и специальных воздействий;

защита информации от утечки вследствие наличия физических полей за счет акустических и побочных электромагнитных излучений и наводок (ПЭМИН) на электрические цепи, трубопроводы и конструкционные элементы зданий.

В рамках указанных направлений технической политики обеспечения информационной безопасности необходимо:

* реализация разрешительной системы допуска исполнителей (пользователей) к работам, документам и информации конфиденциального характера;
* ограничение доступа исполнителей и посторонних лиц в здания, помещения, где проводятся работы конфиденциального характера, в том числе на объекты информатизации, на которых обрабатывается (хранится) информация конфиденциального характера;
* разграничение доступа пользователей к данным автоматизированным системам различного уровня и назначения;
* учет документов, информационных массивов, регистрация действий пользователей информационных систем, контроль несанкционированного доступа за действиями пользователей;
* криптографическое преобразование информации, обрабатываемой и передаваемой средствами вычислительной техники и связи;
* снижение уровня и информативности ПЭМИН, создаваемых различными элементами технических средств обеспечения производственной деятельности и автоматизированных систем;
* снижение уровня акустических излучений;
* электрическая развязка цепей питания, заземления и других цепей технических средств, выходящих за пределы контролируемой территории;
* активное зашумление в различных диапазонах;
* противодействие оптическим и лазерным средствам наблюдения;
* проверка технических средств и объектов информатизации на предмет выявления включенных в них закладных устройств;
* предотвращение внедрения в автоматизированные информационные системы программ вирусного характера.

В целом для создания и обеспечения функционирования системы комплексной безопасности фирмы должны быть разработаны следующие документы:

1. Положение о подразделении безопасности.

2. Перечень сведений, составляющих конфиденциальную информацию.

3.Организационно-распорядительные документы, регламентирующие порядок и правила: обеспечения безопасности конфиденциальной информации; режима и охраны объектов защиты, включая требования к пропускному и внутриобъектовому режимам; по учету и контролю финансов, обеспечения их сохранности в процессе проведения операций, хранения и транспортировки; обеспечения защиты информации, обрабатываемой и передаваемой в автоматизированных системах и средствах связи.

Для осуществления технической политики в области обеспечения физической и информационной защиты необходимо разработать и реализовать следующий комплекс мероприятий:

* оснащение важнейших объектов и помещений средствами и системами физической защиты и контроля;
* обеспечение технической, программной и криптографической защиты информации в системах информатизации и связи;
* обеспечение защиты речевой информации в помещениях, выделенных для ведения конфиденциальных переговоров.

Программа создания системы безопасности должна предусматривать приоритеты реализации наиболее важных и актуальных направлений обеспечения безопасности, с учетом выделяемых финансовых ресурсов, а также предусмотреть привлечение к ее выполнению специализированных организаций, имеющих практический опыт работы по рассматриваемой проблеме и лицензии на соответствующий вид деятельности.

В целях обеспечения нормальной работы подразделения безопасности в повседневных условиях рекомендуется разработать «Оперативный план подразделения безопасности по обеспечению защиты фирмы». Данным планом предусматриваются конкретные и четкие действия сотрудников фирмы и подразделения безопасности при возникновении критических ситуаций. Должны быть предусмотрены действия, как в момент наступления ситуации, так и в ходе ее развития и по завершению. Главная цель – предупредить наступления ситуации, уменьшить ущерб, сохранить следы (улики) для последующей работы по ликвидации ущерба

# Действия, приводящие к неправомерному овладению

# конфиденциальной информацией

Наиболее надежным средством обеспечения конфиденциальности информации является шифрование. Шифрование - это процесс преобразования открытых данных в закрытые по определенному криптографическому алгоритму с использованием секретного ключевого элемента – ключа шифрования (Рис.1)



рис. 1. Шифрование документов-файлов

Секретный элемент криптографического преобразования – ключ шифрования – может храниться, например, в файле на дискете, или на каком-либо другом ключевом носителе, что рассмотрено в данной статье ниже. Необходимо, чтобы все пользователи, предполагающие обмениваться зашифрованными документами, получили определенный набор ключей шифрования, что позволило бы получателям расшифровывать документы, предварительно зашифрованные отправителями.

Простейший случай – все абоненты компьютерной сети организации получают один и тот же секретный ключ шифрования. Как и все простое, такая схема имеет ряд недостатков:

* + Все абоненты сети имеют один и тот же ключ шифрования. Таким образом, любые зашифрованные этим ключом документы могут быть расшифрованы любым абонентом сети, т. е., невозможно отправить некий документ какому-либо абоненту лично.
  + При компрометации ключа шифрования (утере, хищении и т. д.) под угрозой нарушения конфиденциальности окажется весь документооборот, ключи шифрования придется срочно менять. Если же, например, факт компрометации ключа шифрования обнаружен не сразу, останется только догадываться, сколько документов (и какой важности) успел прочитать злоумышленник.
  + Такие ключи необходимо передавать «из рук в руки», т. е., невозможно, например, переслать по электронной почте, что неудобно.

Проблема передачи ключей решается путем применения схемы открытого распределения ключей. Это означает, что с помощью определенного алгоритма ключ шифрования «делится» на секретную и открытую части. Секретная часть, называемая «секретным ключом», хранится у его владельца, а открытая часть («открытый ключ») передается всем остальным абонентам сети. Таким образом, каждый абонент сети имеет в своем распоряжении свой собственный секретный ключ и набор открытых ключей всех остальных абонентов. С помощью своего секретного ключа и открытого ключа абонента-адресата абонент-отправитель вычисляет ключ парной связи, с помощью которого зашифровывает документы, предназначенные данному получателю. Получатель же, с помощью своего секретного ключа и имеющегося у него открытого ключа отправителя, вычисляет тот же ключ парной связи, с помощью которого может эти документы расшифровать (рис.2)

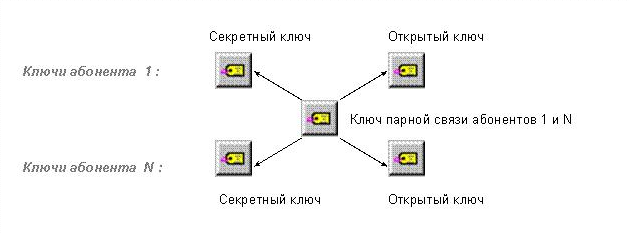


рис. 2. Схема вычисления ключа парной связи

Таким образом, путем использования схемы с открытым распределением ключей достигаются те же положительные моменты, что и при использовании схемы «полная матрица», но также и нейтрализуется недостаток – проблема распределения ключей.

Еще одно существенное достоинство открытого распределения ключей состоит в том, что одни и те же ключи могут быть использованы и для шифрования документов, и для электронной подписи. При использовании других ключевых схем это недостижимо.

# Электронная подпись

Электронная цифровая подпись (ЭЦП) – средство, позволяющее на основе криптографических методов установить авторство и целостность электронного документа.

Схема использования ЭЦП приведена на рис. 3.

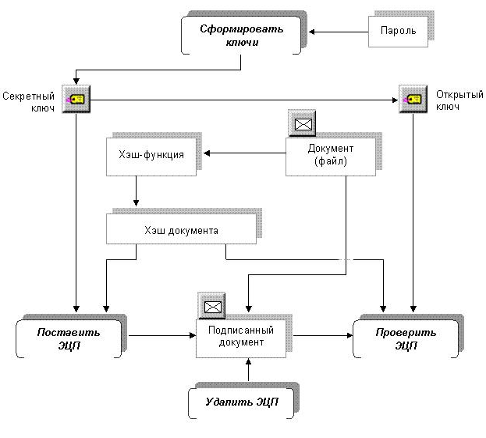


рис. 3. Использование ЭЦП

Секретный ключ (СК) генерируется абонентом сети. ЭЦП формируется на основе СК и вычисленного с помощью хэш-функции значения хэша документа. Хэш представляет собой некоторое значение, однозначно соответствующее содержимому документа-файла. При изменении хотя бы одного символа в документе, хэш документа изменится. Подобрать же изменения в документе таким образом, чтобы хэш документа не изменился, при использовании современных алгоритмов ЭЦП (например, ГОСТ Р 34.10-94 и ГОСТ Р 34.11-94) попросту невозможно.

СК может быть зашифрован на пароле. Открытый ключ (ОК) вычисляется как значение некоторой функции из СК и используется для проверки ЭЦП. ОК может свободно распространяться по открытым каналам связи, таким образом, ОК должен быть передан всем абонентам сети, с которыми планируется обмен защищенной информацией. При проверке ЭЦП вычисляется значение хэша документа; таким образом, любые изменения документа приведут к другому значению хэша, и вычисленная ЭЦП измененного документа не совпадет с переданной, что явится сигналом нарушения его целостности.

Как уже было сказано, для шифрования и ЭЦП может быть использована одна и та же пара ключей абонента.

# Комплексный метод защиты

Естественно, для защиты и конфиденциальности, и целостности информации следует использовать в комплексе шифрование и ЭЦП, что также можно совместить с каким-либо дополнительным сервисом, например, сжатием информации (архивацией). В качестве примера таких систем следует привести специализированный архиватор электронных документов Crypton ArcMail, предлагаемый фирмой “АНКАД”. Алгоритм создания специализированного архива (архива для передачи по сети) приведен на рис.4.

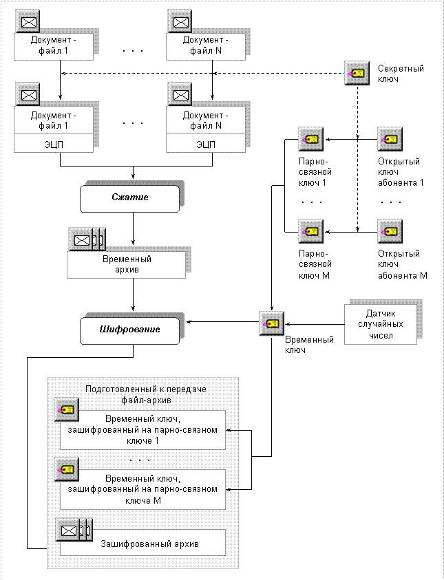


рис. 4. Алгоритм создания архива

Создаваемый таким образом файл-архив можно передавать по сети без каких-либо опасений. При создании архива исходные файлы подписываются на секретном ключе абонента сети, после чего файлы сжимаются и получаемый в результате сжатия архив шифруется на случайном временном ключе. Абоненты, которым предназначается архив, могут расшифровать его с помощью записанного в архив зашифрованного временного ключа. Временный ключ зашифровывается на парно-связном ключе, вычисляемом по алгоритму Диффи-Хеллмана из СК отправителя и открытого ключа ЭЦП (ОК) абонента-адресата. Таким образом, достигаются следующие цели:

* + Передаваемые электронные документы снабжаются кодом подтверждения достоверности – ЭЦП, который защищает их от нарушения целостности или подмены.
  + Документы передаются в защищенном виде, что обеспечивает их конфиденциальность.
  + Абоненты-адресаты могут расшифровать документы, используя свой СК и ОК отправителя.
  + Абоненты сети, которым не предназначается данный архив, не могут прочитать его содержимое, поскольку не имеют временного ключа и не могут его вычислить.
  + Дополнительный сервис – уменьшение объема информации, обусловленное архивацией.

# Заключение

Таким образом, в данном реферате описаны методы защиты передаваемых в глобальных вычислительных сетях (ГВС) электронных документов. Кроме того, изложенные рекомендации будут полезны и для организаций, имеющих единственную ЛВС, поскольку применяемые методы защиты не будут являться избыточными и в этом случае.

Шифрование способно быть центром безопасности всего компьютера, на его базе можно построить полнофункциональную систему криптографической защиты данных, обеспечивающую, например, следующие возможности:

* 1. Защита компьютера от физического доступа.
  2. Защита компьютера от НСД по сети и организация VPN.
  3. Шифрование файлов по требованию.
  4. Автоматическое шифрование логических дисков компьютера.
  5. Вычислени/проверка ЭЦП.
  6. Защита сообщений электронной почты.

Для защиты и конфиденциальности, и целостности информации следует использовать в комплексе шифрование и ЭЦП, что также можно совместить с каким-либо дополнительным сервисом.

**Литература**

1. www.panasenko.ru/Articles/77/77.html // 29/11/2010
2. www.alleng.ru/d/comp/comp96.html // 29/11/2010
3. http://www.intertrust.ru/main/products/protect // 29/11/2010