|  |  |  |
| --- | --- | --- |
|  | СОДЕРЖАНИЕ |  |
| 1 | Введение | 3 |
| 2 | Законодательные и административные меры для регулирования вопросов защиты информации | 5 |
| 3 | Технические и программно-математические методы защиты информации | 8 |
| 4 | Методы защиты информации и их главные недостатки: | 10 |
| 5 | Заключение | 13 |
| 6 | Список литературы | 14 |

**Введение**

Данная работа представляет собой сокращенный, актуализированный с учетом ряда происшедших за последний период изменений, вариант учебного пособия книги "Организация безопасности в области защиты информации", опубликованной в 1998 г. в МИФИ. Не проходящий и не снижающийся интерес к этой проблематике, объясняется тем, что происходящие в стране процессы существенно затронули проблему организации системы защиты информации во всех ее сферах - разработки, производства, реализации, эксплуатации средств защиты, подготовки соответствующих кадров. Прежние традиционные подходы в современных условиях уже не в состоянии обеспечить требуемый уровень безопасности государственно значимой и частной конфиденциальной информации, циркулирующей в информационно-телекоммуникационных системах страны.

Существенным фактором, до настоящего времени оказывающим значительное влияние на положение дел в области защиты информации, является то, что до начала 90-х годов нормативное регулирование в данной области оставляло желать лучшего. Система защиты информации в нашей стране в то время определялась существовавшей политической обстановкой и действовала в основном в интересах Специальных служб государства, Министерства обороны и Военно-промышленного комплекса. Цели защиты информации достигались главным образом за счет реализации принципа "максимальной секретности", в соответствии с которым доступ ко многим видам информации был просто ограничен. Никаких законодательных и иных государственных нормативных актов, определяющих защиту информационных прав негосударственных организаций и отдельных граждан, не существовало. Средства криптографической защиты информации использовались только в интересах государственных органов, а их разработка была прерогативой исключительно специальных служб и немногих специализированных государственных предприятий. Указанные предприятия строго отбирались и категорировались по уровню допуска к разработке и производству этих средств. Сами изделия тщательно проверялись компетентными государственными органами и допускались к эксплуатации исключительно на основании специальных заключений этих органов. Любые работы в области криптографической защиты информации проводилась на основании утвержденных Правительством страны специальных секретных нормативных актов, полностью регламентировавших порядок заказа, разработки, производства и эксплуатации шифровальных средств. Сведения о этих средствах, их разработке, производстве, и использовании как в стране, так и за рубежом были строго засекречены, а их распространение предельно ограничено. Даже простое упоминание о криптографических средствах в открытых публикациях было запрещено.

В настоящее время можно отметить, что правовое поле в области защиты информации получило весомое заполнение. Конечно нельзя сказать, что процесс построения цивилизованных правовых отношений успешно завершен и задача правового обеспечения деятельности в этой области уже решена. Важно другое - на мой взгляд, можно констатировать, что уже имеется неплохая законодательная база, вполне позволяющая, с одной стороны, предприятиям осуществлять свою деятельность по защите информации в соответствии требованиями действующих нормативных актов, а с другой - уполномоченным государственным органам на законной основе регулировать рынок соответствующих товаров и услуг, обеспечивая необходимый баланс интересов отдельных граждан, общества в целом и государства.

В последнее время в различных публикациях муссируется вопрос о том, что созданный механизм государственного регулирования в области защиты информации используется государственными органами, уполномоченными на ведение лицензионной деятельности, для зажима конкуренции и не соответствует ни мировому опыту, ни законодательству страны. В этой связи, во-первых, хотели бы отметить, что по состоянию на декабрь месяц 1996 года Федеральным агентством правительственной связи и информации при Президенте Российской Федерации оформлена 71 лицензия на деятельность в области защиты информации. Официально в выдаче лицензии отказано только одной фирме. Еще одному предприятию, кстати, государственному отказано в продлении лицензии за нарушения условий ее действия. Среди лицензиатов - предприятия различных форм собственности и ведомственной принадлежности, включая такие частные фирмы, как: "Авиателеком", "Аргонавт", "Анкей", "КомФАКС", "Инфотекс" и другие. Полный список лицензий, выданных ФАПСИ публикуется в печати, в том числе и в изданиях фирмы "Гротек".

Кроме того, чтобы остудить бушующие вокруг данной проблемы страсти, считаю полезным подробнее ознакомиться с имеющимся опытом зарубежного законодательства и требованиями российских нормативных актов в области защиты информации.

**Законодательные и административные меры для регулирования вопросов защиты информации**

Законодательные и административные меры для регулирования вопросов защиты информации на государственном уровне применяются в большинстве научно-технически развитых стран мира. Компьютерные преступления приобрели в странах с развитой информационно-телекоммуникационной инфраструктурой такое широкое распространение, что для борьбы с ними в уголовное законодательство введены специальные статьи.

Первый закон о защите информации был принят в Соединенных Штатах Америки в 1906 году. В настоящее время в США имеется около 500 законодательных актов по защите информации, ответственности за ее разглашение и компьютерные преступления. Проблемы информационной безопасности рассматриваются американской администрацией как один из ключевых элементов национальной безопасности. Национальная политика США в области защиты информации формируется Агентством национальной безопасности (АНБ). При этом наиболее важные стратегические вопросы, определяющие национальную политику в данной сфере, как правило, решаются на уровне Совета национальной безопасности, а решения оформляются в виде директив Президента США. Среди таких директив следует отметить следующие:

директива PD/NSC-24 "Политика в области защиты систем связи" (1977 год, Д. Картер), в которой впервые подчеркивается необходимость защиты важной несекретной информации в обеспечении национальной безопасности;

директива SDD-145 "Национальная политика США в области безопасности систем связи автоматизированных информационных систем" (1984 год, Р. Рейган), которая стала юридической основой для возложения на АНБ функции по защите информации и контролю за безопасностью не только в каналах связи, но и в вычислительных и сложных информационно-телекоммуникацион-ных системах.

В период с 1967 года по настоящее время в США принят целый ряд федеральных законов, создавших правовую основу для формирования и проведения единой государственной политики в области информатизации и защиты информации с учетом интересов национальной безопасности страны. Это законы "О свободе информации" (1967 год), "О секретности" (1974 год), "О праве на финансовую секретность" (1978 год), "О доступе к информации о деятельности ЦРУ" (1984 год), "О компьютерных злоупотреблениях и мошенничестве" (1986 год), "О безопасности компьютерных систем" (1987 год) и некоторые другие.

Во Франции государственному контролю подлежат изготовление, экспорт и использование шифровального оборудования. Экспорт возможен только с разрешения Премьер-министра страны, выдаваемого после консультаций со специальным комитетом по военному оборудованию. Импорт шифровальных средств на территорию Французской республики вообще запрещен. Закон объявляет экспорт и снабжение криптографическими средствами без специального разрешения преступлением, которое наказывается штрафом в размере до 500 000 франков или тюремным заключением на срок от 1 до 3 месяцев.

Нормы и требования российского законодательства включают в себя положения ряда нормативных актов Российской Федерации различного уровня.

19 февраля 1993 года Верховным Советом Российской Федерации был принят закон "О федеральных органах правительственной связи и информации" N 4524-1. Статья 11 данного закона предоставила Федеральному агентству права по определению порядка разработки, производства, реализации, эксплуатации шифровальных средств, предоставления услуг в области шифрования информации, а также порядка проведения работ по выявлению электронных устройств перехвата информации в технических средствах и помещениях государственных структур. Таким образом, закон Российской Федерации "О федеральных органах правительственной связи и информации" является первым собственно российским правовым нормативным актом, который вводит сертификацию в области защиты информации и дата его принятия - 19 февраля 1996г. - является исходной точкой от которой необходимо вести отсчет ограничения прав на занятие предпринимательской деятельностью.

Новым шагом в деле правового обеспечения деятельности в области защиты информации явилось принятие Федеральным собранием России *Федерального закона "Об информации, информатизации и защите информации" от 20.02.95 N 24-ФЗ.* Данный закон впервые официально вводит понятие "конфиденциальной информации", которая рассматривается как документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации, и устанавливает общие правовые требования к организации защиты такой информации в процессе ее обработки, хранения и циркуляции в технических устройствах и информационных и телекоммуникационных системах и комплексах и организации контроля за осуществлением мероприятий по защите конфиденциальной информации. При этом следует подчеркнуть, что Закон не разделяет государственную и частную информацию как объект защиты в том случае, если доступ к ней ограничивается.

Кроме того, закон определяет на государственно-правовом уровне электронную цифровую подпись как средство защиты информации от несанкционированного искажения, подмены (имитозащиты) и подтверждения подлинности отправителя и получателя информации (аутентификации сторон). В соответствии со статьей 5 "юридическая сила документа, хранимого, обрабатываемого и передаваемого с помощью автоматизированных информационных и телекоммуникационных систем, может подтверждаться электронной цифровой подписью". При этом "юридическая сила электронной цифровой подписи признается при наличии в автоматизированной системе программно-технических средств, обеспечивающих идентификацию подписи, и соблюдении установленного режима их использования". Далее закон раскрывает требования, предъявляемые к специализированным программно-техническим средствам, реализующим электронную цифровую подпись, и порядку их использования в информационно-телекомму-никационных системах.

Так Статья 20 определяет основные цели защиты информации. В соответствии с этой статьей таковыми, в частности, являются: предотвращение утечки, хищения, утраты, искажения и подделки информации; предотвращение угроз безопасности личности, общества и государства; предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации; защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных сведений; сохранение государственной тайны и конфиденциальности информации.

Пункт 3 статьи 21 возлагает контроль за соблюдением требований к защите информации, за эксплуатацией специальных средств защиты информации, а также обеспечение организационных мер защиты информационных систем, обрабатывающих информацию с ограниченным доступом, в негосударственных структурах на органы государственной власти.

Статья 23 Закона "Об информации, информатизации и защите информации" посвящена защите прав субъектов в сфере информационных процессов и информатизации. Статья устанавливает, что защита прав субъектов в данной сфере осуществляется судом, арбитражным судом и третейскими судами, которые могут создаваться на постоянной или временной основе.

**Технические и программно-математические методы защиты информации**

Учитывая, что предметом данной работы являются организация безопасности в области защиты информации прежде необходимо дать ряд основных понятий данной сферы деятельности.

*Защита информации* - комплекс мероприятий, проводимых с целью предотвращения утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), несанкционированного копирования, блокирования информации и т.п.

*Средства защиты информации* - технические, криптографические, программные и другие средства, предназначенные для защиты информации, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

*Эффективность защиты информации* - степень соответствия достигнутых результатов действий по защите информации поставленной цели защиты.

*Контроль эффективности защиты информации* - проверка соответствия эффективности мероприятий по защите информации установленным требованиям или нормам эффективности защиты.

*Безопасность информации (информационная безопасность)* - состояние информации, информационных ресурсов и информационных и телекоммуникационных систем, при котором с требуемой вероятностью обеспечивается защита информации.

*Требования по безопасности информации* - руководящие документы ФАПСИ, регламентирующие качественные и количественные критерии безопасности информации и нормы эффективности ее защиты.

*Криптографическая защита* - защита данных при помощи криптографического преобразования преобразования данных.

*Криптографическое преобразование* - преобразование данных при помощи шифрования и (или) выработки имитовставки.

И так *Информацию* достаточно условно можно разделить на сведения, отнесенные к государственной тайне, конфиденциальную информацию, персональную информацию и остальную информацию. Рассматривать первый тип мы не будем. Согласно списку терминов и определений Гостехкомиссии России конфиденциальная информация - это информация, требующая защиты (любая, ее назначение и содержание не оговариваются). Персональные данные - это сведения о гражданах или предприятиях. В соответствии с Федеральным законом № 24 "Об информации, информатизации и защите информации" "защите подлежит любая документированная информация, неправомерное обращение с которой может нанести ущерб собственнику, владельцу или иному лицу". Из описанного следует, что ВЫ обязаны заботиться о сохранности своей информации. Например, никто кроме меня не вправе разглашать мою дату рождения, а ведь она хранится на всех предприятиях, где я работал и работаю.

В данной работе не будут затронуты информация, распространяемая по каналам связи (телефония, WEB, E-mail, локальные сети и т.д.), а также проблемы, связанные с ее перехватом, блокировкой и защитой. Это связано с широтой проблемы и другими методами защиты. Основное внимание мы сосредоточим на информации, хранимой и используемой на предприятии или у граждан. От чего же необходимо защищать информацию? Ответ - в Положении "О государственном лицензировании деятельности в области защиты информации" №60, где говорится, что "защита информации - комплекс мероприятий, проводимых с целью предотвращения утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), несанкционированного копирования, блокирования информации и т.п.". Пример - в одном из РЭУ подмосковного города были похищены компьютеры, и в результате была обнародована информация о прописке граждан. Также в современных российских условиях не следует сбрасывать со счета и попытки предприятий скрыть данные от силовых ведомств. Правомочность этих действий мы не оспариваем, но каждое предприятие само решает, какие данные оно хочет обнародовать, какие - нет (по определению конфиденциальной информации). Кстати, информация, хранимая на компьютерах, не может использоваться как улики в уголовно-гражданских делах, но вполне возможно ее применение для выполнения следственных действий.

*Защиту информации* следует рассматривать как неотъемлемую часть хранения. Невозможно обеспечить серьезную защиту, не выполняя резервное копирование информации. К счастью, обеспечить сохранность копий гораздо проще, для этого достаточно административных мер (хранение в несгораемых сейфах). Емкость стриммеров, CD-R, CD-RW, DVD достаточна для составления резервных копий и восстановления из них в кратчайшие сроки. Пренебрежение данными мерами чревато даже по техническим соображениям - надежность технических средств хранения далека от 1 (а вероятность сбоя Windows 95/98 в течение рабочего дня равна 1), и потерять информацию по причине программного сбоя или поломки накопителя очень обидно и дорого. Известны случаи потери бухгалтерской отчетности за три месяца, восстановление заняло два месяца, штрафы за несвоевременное представление отчетности превысили стоимость сломавшегося накопителя более чем в 100 раз, не считая приостановки лицензии и косвенных потерь.

**Методы защиты информации и их главные недостатки:**

# Административные меры

Если территория (помещение) предприятия имеет охрану, персоналу можно доверять, локальная сеть не имеет выходов в глобальные сети, то такую защищенность надо признать очень высокой. Однако это идеальный случай, и в практике такое не всегда выполнимо (пример - персональная база жителей Санкт-Петербурга из ГУВД, обнародованная на CD). Пренебрегать этим методом нельзя, и он, как правило, дополняет или контролирует другие методы.

*Защита средствами операционной системы*

MS-DOS, как наиболее распространенная операционная система, не представляет каких-либо методов защиты. Это наиболее открытая операционная система, и на ее базе разработано много различных аппаратных и программных средств, в частности - виртуальные кодируемые или шифруемые диски, блокираторы загрузки и тд. Однако имеющиеся средства дисассемблирования, отладчики, а также большое количество квалифицированных программистов сводят на нет все программные методы. DR-DOS, как одна из разновидностей MS-DOS, хоть и поддерживает блокировку файлов, но загрузка с дискеты или с другого накопителя делает бесполезной использование встроенных систем защиты. Windows 95/98 основаны на базе MS-DOS, и им присущи все ее недостатки. Парольная система Windows 95/98 не выдерживает никакой критики, и даже установка дополнительных модулей системной политики не решает данную задачу. Windows NT и Novell, хотя и решают задачу защиты, но... вот простейший пример - у Вас похитили, или изъяли в установленном порядке, компьютер. Диск установили вторым - и все ваше администрирование, на которое потрачены тысячи (если не миллионы) человеко-часов,- уже никому не помеха.

Я не хотел упоминать в данной работе защиту информации установкой пароля BIOS, но большое количество наблюдаемых установок данного пароля вынудило затронуть и данный метод. Максимум что надо для блокировки, это - открыть компьютер, установить перемычку и снять ее (самое большее - две минуты). Есть два (известных мне) исключения - системы с часами на базе микросхем DALLAS и переносные компьютеры. Здесь задачка не так просто решается. Помогает снятие накопителя и установка его в другой компьютер (опять же две минуты).

# Блокировка загрузки операционной системы

По этому пути идут многие фирмы. У данного метода опять-таки недостатки всплывают, если к компьютеру или накопителю можно получить доступ. Известные платы перехватывают прерывание по загрузке, однако Setup современных компьютеров позволяет блокировать эту возможность, изъятие этой платы или накопителя сводит на нет кажущуюся мощь данного средства.

# Физическое уничтожение накопителя

Это наиболее древний и действенный метод, вспомните сжигание, съедание бумаг. Конечно, в наше время он становится более изощренным, в частности, к компьютерной безопасности можно приобщить следующие методы:

* выкинуть из окна винчестер или целиком компьютер, сломать дискету;
* электромагнит, пробивающий насквозь накопитель или дискету (московская разработка, последствия очень впечатляющие);
* пиропатрон, установленный под накопителем (за хранение и применение взрывчатых веществ предусмотрена уголовная ответственность).

Данным методам очень тяжело что-то противопоставить, но при ложном срабатывании слишком велика стоимость потерь. Имеются в виду только материальные потери, так как грамотное ведение резервного копирования решает задачу восстановления в кратчайшие сроки. Очень интересно, конечно, кроме последнего пункта, что эти меры не требуют никакого согласования, лицензирования и сертификации, если они выполнены силами самого предприятия. Например, нельзя обвинить изготовителя окна, что он стал виновником уничтожения информации, если компьютер был с него скинут. Очень распространено использование сменных HDD или магнитооптических дисков. Однако опыт их использования, особенно при постоянном изъятии, говорит о значительном сокращении срока их службы (удары по винчестеру) и частых сбоях (характерных для магнитооптики).

*Стирание информации*

Метод имеет много общего с предыдущим и в тоже время лишен ряда его недостатков, так как теряется только информация, а не накопитель (яркий пример - стирание пленки в фильме "Гений"). Информацию восстанавливаем с резервной копии - и нет проблем. Программное стирание и комплексы, использующие данную функцию, требуют нахождения компьютера исключительно под напряжением. Это трудно выполнимо, даже мощные UPS не могут обеспечить работу компьютеров более часа. Пример: один комплекс дал сбой, так как удаляемый файл был открыт программой и блокировка операционной системы остановила дальнейшее удаление. Аппаратное стирание, выполняющее свои функции без участия компьютера, особенно при наличии резервного источника питания, устраняет эти проблемы. Скорость уничтожения, как правило, соизмерима со скоростью работы самого накопителя. Хотя для магнитной ленты возможно и мгновенное стирание. Данные устройства могут применятся не только в помещении офиса, но, например, и в кейсе, при перевозке информации.

*Шифрование данных*

Это одно из мощнейших методов. Начнем его рассмотрение с определения по ГОСТ 19781: Шифрование - это процесс преобразования открытых данных в зашифрованные при помощи шифра или зашифрованных данных в открытые при помощи шифра - совокупность обратимых преобразований множества возможных открытых данных на множество возможных зашифрованных данных, осуществляемых по определенным правилам с применением ключей (конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного преобразования). Стойкость современных шифровальных систем достаточно высока, и будем считать ее достаточной. Но - !!! Вот тут-то мы и получаем мощное сопротивление со стороны законодательства. Во-первых, разработчик, продавец и установщик должны иметь лицензию. Но и этого мало! ДАЖЕ ПОЛЬЗОВАТЕЛЬ обязан иметь лицензию ФАПСИ. В России разрешено использование только одного алгоритма и принципиально невозможно получить, а значит и использовать, импортные разработки! Например, появившаяся в печати реклама комплекса "Secret Disk" о продаже его в магазинах просто непонятна (одно из двух - или это не шифрование или это уголовно наказуемо). Статья 4 Указа № 334 прямо гласит: "В интересах информационной безопасности РФ и усиления борьбы с организованной преступностью запретить деятельность юридических и физических лиц, связанную с разработкой, производством, реализацией и эксплуатацией шифровальных средств, а также защищенных технических средств хранения, обработки и передачи информации, предоставлением услуг в области шифрования информации, без лицензий, выданных ФАПСИ". Сможете ли вы применить данный метод после этих разъяснений?

Приобретаемые технические устройства защиты информации могут не иметь сертификации, при условии, что они не будут использованы в государственных и банковских учреждениях. Однако предприятие-продавец должно иметь лицензию на право занятия данной деятельностью. Ответственность за использование несертифицированных средств, как ни странно, лежит на самом потребителе, хотя он может (или должен? и куда?) обратиться для проверки на соответствие данной системы.

**Заключение**

Итак, подведем итоги. Эту работу ни в коем случае не следует рассматривать как полную (есть о чем поговорить !?) и , не содержащий ошибок или противоречий. Но однако известно множество случаев, когда фирмы (не только зарубежные !!!) ведут между собой настоящие "шпионские войны", вербуя сотрудников конкурента с целью получения через них доступа к информации, составляющую коммерческую тайну. Регулирование вопросов, связанных с коммерческой тайной, еще не получило в России достаточного развития. Принятый еще в 1971 году КЗоТ несмотря на многочисленные изменения безнадежно устарел и не обеспечивает соответствующего современным реалиям регулирования многих вопросов, в том числе и о коммерческой тайне. Наличие норм об ответственности, в том числе уголовной, может послужить работникам предостережением от нарушений в данной области, поэтому целесообразно подробно проинформировать всех сотрудников о последствиях нарушений. В то же время надо отдавать себе отчет, что ущерб, причиненный разглашением коммерческой тайны, зачастую имеет весьма значительные размеры (если их вообще можно оценить). Компенсировать убытки, потребовав их возмещения с виновного работника, скорее всего не удастся, отчасти из-за несовершенного порядка обращения имущественных взысканий на физических лиц, отчасти - просто из-за отсутствия у физического лица соответствующих средств. Хотелось бы надеяться что создающееся в стране система защиты информации и формирование комплекса мер по ее реализации не приведет к необратимым последствиям на пути зарождающегося в России информационно - интеллектуального объединения со всем миром.

**Список литературы**

1. Статья «Правовые средства защиты конфиденциальной информации» журнал «Банковское дело в Москве» № 15 1998г
2. по материалам “Компьютер Price”, №31 2000г
3. "Организация безопасности в области защиты информации", 1998 г. МИФИ.
4. Законы и нормативные акты правительства РФ