Тема 2.1. Понятие организационной защиты информации

1 Направления, принципы и условия организационной защиты информации

Задача защиты информации успешно реализуется только при системном подходе к ее решению. С этой целью предложена следующая классификация методов защиты информации.

По классу решаемых задач: технические, программные, организационные, криптографические.

По виду решаемых задач: резервирование, введение избыточности, регулирование доступа, регулирование использования, защитные преобразования, контроль, регистрация, уничтожение, сигнализация, реагирование.

По функциональному назначению: самостоятельное решение средств защиты, решение задач защиты в комплексе с другими средствами, управление средствами защиты, обеспечение функционирования механизмов защиты.

Организационные методы позволяют решать задачи защиты информации как самостоятельно, так и «подкрепляют» и дополняют другие методы защиты. К организационным методам защиты информации относятся организационно-технические и организационно-правовые мероприятия. Вместе с тем в общем комплексе методов и средств защиты информации, организационные методы играют особую роль по следующим причинам:

- повышенное влияние случайных факторов,
- неформальный характер,
- наличие «человеческого фактора».

Из существующих средств и методов защиты информации организационные методы следует выделить особо.

Для наиболее полного и глубокого анализа процессов, происходящих в сфере защиты информации; понимания сущности планируемых и проводимых в этих целях мероприятий, прежде всего, необходимо рассмотреть одно из

важнейших направлений защиты информации – организационную защиту информации.

Организационная защита информации является организационным началом, так называемым «ядром» в общей системе защиты конфиденциальной информации предприятия. От полноты и качества решения руководством и должностными лицами предприятий организационных задач зависит эффективность функционирования системы защиты информации в целом. Роль и место организационной защиты информации в общей системе мер, направленных на защиту информации, определяются исключительной важностью принятия руководством своевременных и верных управленческих решений с учетом имеющихся в его распоряжении сил, средств, методов и способов защиты информации и на основе действующей законодательной и нормативно-правовой базы.

Среди основных направлений защиты информации наряду с организационной выделяют правовую и инженерно-техническую защиту информации.

Однако организационной защите информации среди этих направлений отводится особое место.

Организационная защита информации призвана посредством выбора конкретных сил и средств (включающие в себя правовые, инженерно-технические и инженерно-геологические) реализовать на практике спланированные руководством предприятия меры по защите информации. Эти меры принимаются в зависимости от конкретной обстановки на предприятии, связанной с наличием возможных угроз, воздействующих на защищаемую информацию и ведущих к ее утечке.

Основными направлениями деятельности, осуществляемой руководством предприятия в решении задач по защите информации являются:

– планирование мероприятий по защите информации и персональный контроль за их выполнением,

– принятие решений о непосредственном доступе к конфиденциальной информации своих сотрудников и представителей других организаций,

– распределение обязанностей и задач между должностными лицами и структурными подразделениями, аналитическая работа и т.д.

Цель принимаемых руководством предприятия и должностными лицами организационных мер – исключение утечки информации и, таким образом, уменьшение или полное исключение возможности нанесения предприятию ущерба, к которому эта утечка может привести.

Система мер по защите информации в широком смысле слова должна – строиться исходя из тех начальных условий и факторов, которые, в свою очередь, определяются состоянием устремленности разведок противника либо действиями конкурента на рынке товаров и услуг, направленными на овладение информацией, подлежащей защите. Это правило действует как на государственном уровне, так и на уровне конкретного предприятия.

Используются два равнозначных определения организационной зашиты информации:

1) Организационная защита информации – составная часть системы защиты информации, определяющая и вырабатывающая порядок и правила функционирования объектов защиты и деятельности должностных лиц в целях обеспечения защиты информации.

2) Организационная защита информации на предприятии – регламентация производственной деятельности и взаимоотношений субъектов (сотрудников предприятия) на нормативно-правовой основе, исключающая или ослабляющая нанесение ущерба данному предприятию.

Первое из приведенных определений в большей степени показывает сущность организационной защиты информации. Второе – раскрывает ее структуру на уровне предприятия. Вместе с тем, оба определения подчеркивают важность нормативно-правового регулирования вопросов защиты информации наряду с комплексным подходом к использованию в этих целях имеющихся сил и средств.

Основные направления организационной защиты информации:

1) Организация работы с персоналом.
2) Организация внутри-объектового и пропускного режимов и охраны.
3) Организация работы с носителями сведений.
4) Комплексное планирование мероприятий по защите информации.
5) Организация аналитической работы и контроля.

Основные принципы организационной защиты информации:

– принцип комплексного подхода – эффективное использование сил, средств, способов и методов защиты информации для решения поставленных задач в зависимости от конкретной складывающейся ситуации и наличия факторов, ослабляющих или усиливающих угрозу защищаемой информации;

– принцип оперативности принятия управленческих решений (существенно влияет на эффективность функционирования и гибкость системы защиты информации и отражает нацеленность руководства и персонала предприятия на решение задач защиты информации);

– принцип персональной ответственности – наиболее эффективное распределение задач по защите информации между руководством и персоналом предприятия и определение ответственности за полноту и качество их выполнения.

Основные условия организационной защиты информации:

– непрерывность всестороннего анализа функционирования системы защиты информации в целях принятия своевременных мер по повышению ее эффективности;

– неукоснительное соблюдение руководством и персоналом предприятия установленных норм и правил защиты конфиденциальной информации.

Соблюдении перечисленных условий обеспечивает наиболее полное и качественное решение задач по защите конфиденциальной информации на предприятии.

2 Подходы и требования к организации системы защиты информации

Успешное решение комплекса задач по защите информации не может быть достигнуто без создания единой основы, так называемого «активного кулака» предприятия, способного концентрировать все усилия и имеющиеся ресурсы для исключения утечки конфиденциальной информации и недопущения возможности нанесения ущерба предприятию. Таким «кулаком» призвана стать система защиты информации на предприятии, создаваемая на соответствующей законодательной и нормативно-правовой базе и отражающая все направления и специфику деятельности данного предприятия.

Под системой защиты информации понимают совокупность органов защиты информации (структурных подразделений или должностных лиц предприятия), используемых ими средств и методов защиты информации, а также мероприятий, планируемых и проводимых в этих целях.

Для решения организационных задач по созданию и обеспечению функционирования системы защиты информации используются несколько основных подходов, которые вырабатываются на основе существующей законодательной и нормативно-правовой базе и с учетом методических разработок по тем или иным направлениям защиты конфиденциальной информации.

Один из основных подходов к созданию системы защиты информации заключается во всестороннем анализе состояния защищенности информационных ресурсов предприятия с учетом устремленности конкурирующих организаций к овладению конфиденциальной информацией и, тем самым, нанесению ущерба предприятию. Важным элементом анализа является работа по определению перечня защищаемых информационных ресурсов с учетом особенностей их расположения (размещения) и доступа к ним различных категорий сотрудников (работников других предприятий).

Работу по проведению такого анализа непосредственно возглавляет руководитель предприятия и его заместители по направлениям деятельности. Изучение защищенности информационных ресурсов основывается на положительном и отрицательном опыте работы предприятия, накопленном в течение последних нескольких лет, а также на деловых связях и контактах предприятия с организациями, осуществляющими аналогичные виды деятельности.

При создании системы защиты информации, в первую очередь, учитываются наиболее важные, приоритетные направления деятельности предприятия, требующие особого внимания. Предпочтение также отдается новым, перспективным направлениям деятельности предприятия, которые связаны с научными исследованиями, новейшими технологиями, формирующими интеллектуальную собственность, а также развивающимся международным связям. В соответствии с названными приоритетами формируется перечень возможных угроз информации, подлежащей защите, и определяются конкретные силы, средства, способы и методы ее защиты.

К организации системы защиты информации с позиции системного подхода выдвигается ряд требований, определяющих ее целостность, стройность и эффективность.

Система защиты информации должна быть:

– централизованной – обеспечивающей эффективное управление системой со стороны руководителя и должностных лиц, отвечающих за различные направления деятельности предприятия;

– плановой – объединяющей усилия различных должностных лиц и структурных подразделений для выполнения стоящих перед предприятием задач в области защиты информации;

– конкретной и целенаправленной – рассчитанной на защиту абсолютно конкретных информационных ресурсов, представляющих интерес для конкурирующих организаций;

– активной – обеспечивающей защиту информации с достаточной степенью настойчивости и возможностью концентрации усилий на наиболее важных направлениях деятельности предприятия;

– надежной и универсальной – охватывающей всю деятельность предприятия, связанную с созданием и обменом информацией.

О режимах защиты информации: в соответствии с «Законом об информации, информатизации и защите информации» от 20.02.1995 г. № 24-ФЗ, режим защиты информации устанавливается (статья 21):

– в отношении сведений, отнесенных к государственной тайне, – уполномоченными органами на основании Закона РФ «О государственной тайне»;

– в отношении конфиденциальной информации – собственником информационных ресурсов или уполномоченным лицом на основании «Закона об информации…»;

– в отношении персональных данных – отдельным федеральным законом.

Принципиальным здесь является положение, что режим защиты конфиденциальной информации определяет ее собственник, то есть соответствующий орган государственной власти или управления, организация, учреждение, предприятие.

3 Методы, силы и средства, используемые для организации защиты информации

Один из важнейших факторов, влияющих на эффективность системы защиты конфиденциальной информации, – совокупность сил и средств предприятия, используемых для организации защиты информации.

Силы и средства различных предприятий отличаются по структуре, характеру и порядку использования. Предприятия, работающие с конфиденциальной информацией и решающие задачи по ее защите в рамках повседневной деятельности на постоянной основе, вынуждены с этой целью создавать самостоятельные структурные подразделения и использовать высокоэффективные средства защиты информации. Если предприятия лишь эпизодически работают с конфиденциальной информацией в силу ее небольших объемов, вместо создания подразделений они могут включать в свои штаты отдельные должности специалистов по защите информации. Данные подразделения и должности являются органами защиты информации.

Предприятия, работающие с незначительными объемами конфиденциальной информации, могут на договорной основе использовать потенциал более крупных предприятий, имеющих необходимое количество квалифицированных сотрудников, высокоэффективные средства защиты информации, а также большой опыт практической работы в данной области.

Ведущую роль в организации защиты информации на предприятии играют руководитель предприятия, а также его заместитель, непосредственно возглавляющий эту работу.

Руководитель предприятия несет персональную ответственность за организацию и проведение необходимых мероприятий, направленных на исключение утечки сведений, отнесенных к конфиденциальной информации, и утрат носителей информации. Он обязан:

– знать фактическое состояние дел в области защиты информации, организовывать постоянную работу по выявлению и закрытию возможных каналов утечки конфиденциальной информации;

– определять обязанности и задачи должностным лицам и структурным подразделениям предприятия в этой области;

– проявлять высокую требовательность к персоналу предприятия в вопросах сохранности конфиденциальной информации;

– оценивать деятельность должностных лиц и эффективность мероприятий по защите информации.

Заместитель руководителя предприятия обязан постоянно изучать все стороны и направления деятельности предприятия для принятия своевременных мер по защите информации; руководить работой службы безопасности (иных структурных подразделений, решающих задачи по защите информации); выполнять другие функции по организации защиты информации в ходе проведения предприятием всех видов работ. Более подробно обязанности руководителя предприятия и его заместителя, отвечающего за защиту информации, рассмотрены в других статьях.

На предприятиях для организации работ по защите информации могут создаваться следующие основные виды структурных подразделений: режимно-секретные; подразделения по технической защите информации и противодействию иностранным техническим разведкам; подразделения криптографической защиты информации; мобилизационные; подразделения охраны и пропускного режима. Функции, возлагаемые на перечисленные подразделения, определяются решением (приказом) руководителя предприятия и отражаются в соответствующих положениях.

По решению руководителя предприятия данные подразделения организационно могут объединяться в службу безопасности, руководитель которой в некоторых случаях может быть наделен статусом заместителя руководителя предприятия и полномочиями должностного лица, осуществляющего руководство работой структурных подразделений предприятия, деятельность которых связана с использованием и защитой информации.

Режимно-секретное подразделение, мобилизационное подразделение и подразделение по технической защите информации и противодействию иностранным техническим разведкам создаются на предприятиях, выполняющих работы с использованием сведений, составляющих государственную тайну (вне зависимости от наличия на предприятии иной информации с ограниченным доступом).

Режимно-секретное подразделение является основным структурным подразделением предприятия и решает задачи организации, координации и контроля деятельности других структурных подразделений (персонала предприятия) по обеспечению защиты сведений, составляющих государственную тайну. На предприятиях, не выполняющих работы со сведениями, составляющими государственную тайну, для решения аналогичных задач в отношении других видов информации с ограниченным доступом создается и функционирует служба безопасности (служба защиты информации).

Подразделение по технической защите информации и противодействию иностранным техническим разведкам решает задачи организации и проведения комплекса технических мероприятий, направленных на исключение или существенное затруднение добывания иностранными разведками с помощью технических средств сведений, отнесенных к конфиденциальной информации и подлежащих защите.

Подразделение криптографической защиты информации создается в целях предотвращения утечки конфиденциальной информации при ее передаче по открытым каналам (линиям) связи с помощью технических средств, а также

при использовании локальных вычислительных сетей, имеющих выход за пределы территории предприятия.

Подразделение охраны и пропускного режима создается в целях предотвращения несанкционированного (бесконтрольного) пребывания на территории и объектах предприятия посторонних лиц и транспорта, нанесения ущерба предприятию путем краж (хищений) с территории предприятия материальных средств и иного имущества. В некоторых случаях для решения задач охраны и пропускного режима на предприятиях могут создаваться отдельные самостоятельные подразделения.

Мобилизационное подразделение решает задачи всесторонней подготовки предприятия к работе в условиях военного времени, призыва и поступления мобилизационных людских и материальных ресурсов.

Кроме перечисленных подразделений предприятия к работе по организации защиты информации могут привлекаться и иные структурные подразделения, для которых выполнение мероприятий по защите информации не является основной функцией. К таким подразделениям относятся кадровый орган, орган юридической службы (юрисконсульт), орган психологической и воспитательной работы, пресс-служба предприятия и пр. Особо необходимо отметить важность участия в организации защиты информации производственных, так называемых «тематических» структурных подразделений (отдельных должностных лиц), которые создают продукцию и товары или оказывают услуги (например, производство стрейч-пленки), и в связи с этим самым непосредственным образом взаимодействуют с другими предприятиями и органами государственной власти.

Для проведения работ по организации защиты информации используются также возможности различных нештатных подразделений предприятия, в том числе коллегиальных органов (комиссий), создаваемых для решения специфических задач в этой области. В их числе – постоянно действующая техни-

ческая комиссия, экспертная комиссия, комиссия по рассекречиванию носителей конфиденциальной информации, комиссия по категорированию объектов информатизации и пр. Функции, возлагаемые на данные комиссии, рассмотрены в других статьях.

Чтобы добиться максимальной эффективности при решении задач защиты информации, наряду с возможностями упомянутых штатных и нештатных подразделений (должностных лиц) необходимо использовать имеющиеся на предприятии средства защиты информации.

Под средствами защиты информации понимают технические, криптографические, программные и другие средства и системы, разработанные и предназначенные для защиты конфиденциальной информации, а также средства, устройства и системы контроля эффективности защиты информации.

Технические средства защиты информации – устройства (приборы), предназначенные для обеспечения защиты информации, исключения ее утечки, создания помех (препятствий) техническим средствам доступа к информации, подлежащей защите.

Криптографические средства защиты информации – средства (устройства), обеспечивающие защиту конфиденциальной информации путем ее криптографического преобразования (шифрования).

Программные средства защиты информации – системы защиты средств автоматизации (персональных электронно-вычислительных машин и их комплексов) от внешнего (постороннего) воздействия или вторжения.

Эффективное решение задач организации защиты информации невозможно без применения комплекса имеющихся в распоряжении руководителя предприятия соответствующих сил и средств. Вместе с тем определяющую роль в вопросах организации защиты информации, применения в этих целях сил и средств предприятия играют методы защиты информации, определяющие порядок, алгоритм и особенности использования данных сил и средств в конкретной ситуации.

Методы защиты информации – применяемые в целях исключения утечки информации универсальные и специфические способы использования имеющихся сил и средств (приемы, меры, мероприятия), учитывающие специфику деятельности по защите информации.

Общие методы защиты информации подразделяются на правовые, организационные, технические и экономические.

Методы защиты информации с точки зрения их теоретической основы и практического использования взаимосвязаны. Правовые методы регламентируют и всесторонне нормативно регулируют деятельность по защите информации, выделяя, прежде всего, ее организационные направления. Тесную связь организационных и правовых методов защиты информации можно показать на примере решения задач по исключению утечки конфиденциальной информации, в частности относящейся к коммерческой тайне предприятия, при его взаимодействии с различными государственными и территориальными инспекторскими и надзорными органами. Эти органы в соответствии с предоставленными им законом полномочиями осуществляют деятельность по получению (истребованию), обработке и хранению информации о предприятиях и гражданах (являющихся их сотрудниками).

Передача информации, в установленном порядке, отнесенной к коммерческой тайне или содержащей персональные данные работника предприятия, должна осуществляться на основе договора, предусматривающего взаимные обязательства сторон по нераспространению (неразглашению) этой информации, а также необходимые меры по ее защите.

Организационные механизмы защиты информации определяют порядок и условия комплексного использования имеющихся сил и средств, эффективность которого зависит от применяемых методов технического и экономического характера.

Технические методы защиты информации, используемые в комплексе с организационными методами, играют большую роль в обеспечении защиты

информации при ее хранении, накоплении и обработке с использованием средств автоматизации. Технические методы необходимы для эффективного применения имеющихся в распоряжении предприятия средств защиты информации, основанных на новых информационных технологиях. Среди перечисленных методов защиты информации особо выделяются организационные методы, направленные на решение следующих задач:

– реализация на предприятии эффективного механизма управления, обеспечивающего защиту конфиденциальной информации и недопущение ее утечки;

– осуществление принципа персональной ответственности руководителей подразделений и персонала предприятия за защиту конфиденциальной информации; определение перечней сведений, относимых на предприятии к различным категориям (видам) конфиденциальной информации;

– ограничение круга лиц, имеющих право доступа к различным видам информации в зависимости от степени ее конфиденциальности;

– отбор и изучение лиц, назначаемых на должности, связанные с конфиденциальной информацией, обучение и воспитание персонала предприятия, допущенного к конфиденциальной информации;

– организация и ведение конфиденциального делопроизводства; осуществление систематического контроля за соблюдением установленных требований по защите информации.

Приведенный перечень организационных методов не является исчерпывающим и, в зависимости от специфики деятельности предприятия, степени конфиденциальности используемой информации, объема выполняемых работ, а также опыта работы в области защиты информации, может быть дополнен иными методами

Тема 2.2. Методы обеспечения физической безопасности

1 Средства и методы физической защиты объекта

Организационное обеспечение информационной безопасности. Организационная защита – это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающей или существенно затрудняющей неправомерное овладение конфиденциальной информацией и проявления внутренних и внешних угроз. Организационная защита обеспечивает:

– организацию охраны, режима, работу с кадрами, с документами;

– использование технических средств безопасности и информационно-аналитическую деятельность по выявлению внутренних и внешних угроз безопасности.

Организационные мероприятия играют существенную роль в создании надежного механизма защиты информации, так как возможности несанкционированного использования конфиденциальных сведений в значительной мере обусловливаются не техническими аспектами, а злоумышленными действиями, нерадивостью, небрежностью и халатностью пользователей или персонала защиты. Влияния этих аспектов практически невозможно избежать с помощью технических средств. Для этого необходима совокупность организационно-правовых и организационно-технических мероприятий, которые исключали бы (или, по крайней мере, сводили бы к минимуму) возможность возникновения опасности конфиденциальной информации.

Организационные мероприятия – это мероприятия ограничительного характера, сводящиеся в основном, к регламентации доступа и использования технических средств обработки информации. Они, как правило, проводятся силами самой организации путем использования простейших организационных мер.

К основным организационным мероприятиям можно отнести:

– организацию режима и охраны. Их цель - исключение возможности тайного проникновения на территорию и в помещения посторонних лиц; обеспечение удобства контроля прохода и перемещения сотрудников и посетителей;

– создание отдельных производственных зон по типу конфиденциальных работ с самостоятельными системами доступа;

– контроль и соблюдение временного режима труда и пребывания на территории персонала фирмы;

– организация и поддержание надежного пропускного режима и контроля сотрудников и посетителей и пр.;

– организацию работы с сотрудниками, которая предусматривает подбор и расстановку персонала, включая ознакомление с сотрудниками, их изучение, обучение правилам работы с конфиденциальной информацией, ознакомление с мерами ответственности за нарушение правил защиты информации и пр.;

– организацию работы с документами и документированной информацией, включая организацию разработки и использования документов и носителей конфиденциальной информации, их учет, исполнение, возврат, хранение и уничтожение;

– организацию использования технических средств сбора, обработки, накопления и хранения конфиденциальной информации;

– организацию работы по анализу внутренних и внешних угроз конфиденциальной информации и выработке мер по обеспечению ее защиты;

– организацию работы по проведению систематического контроля за работой персонала с конфиденциальной информацией, порядком учета, хранения и уничтожения документов и технических носителей.

В каждом конкретном случае организационные мероприятия носят специфическую для данной организации форму и содержание, направленные на:

– обеспечение безопасности информации в конкретных условиях.

– определение границ охраняемой зоны (территории);

– определение технических средств, используемых для обработки конфиденциальной информации в пределах контролируемой территории;

– определение «опасных», с точки зрения возможности образования каналов утечки информации, технических средств и конструктивных особенностей зданий и сооружений;

– выявление возможных путей проникновения к источникам конфиденциальной информации со стороны злоумышленников;

– реализация мер по обнаружению, выявлению и контролю за обеспечением защиты информации всеми доступными средствами.

Организационные мероприятия выражаются в тех или иных ограничительных мерах.

Можно выделить такие ограничительные меры, как территориальные, пространственные и временные.

Территориальные ограничения сводятся к умелому расположению источников на местности или в зданиях и помещениях, исключающих подслушивание переговоров или перехват сигналов радиоэлектронных средств.

Пространственные ограничения выражаются в выборе направлений излучения тех или иных сигналов в сторону наименьшей возможности их перехвата злоумышленниками.

Временные ограничения проявляются в сокращении до минимума времени работы технических средств, использовании скрытых методов связи, шифровании и других мерах защиты.

Одной из важнейших задач организационной деятельности является определение состояния технической безопасности объекта, его помещений, подготовка и выполнение организационных мер, исключающих возможность неправомерного овладения конфиденциальной информацией, воспрещение ее

разглашения, утечки и несанкционированного доступа к охраняемым секретам.

Специфической областью организационных мер является организация защиты ПЭВМ, информационных систем и сетей.

Одной из эффективных превентивных мер по обеспечению безопасности важных промышленных объектов является создание системы охраны от несанкционированного проникновения физических лиц – системы физической защиты.

Средства и методы физической защиты объекта. Физическая защита объекта, как правило, предполагает усиление конструкций ограждений, элементов зданий, сооружений и отдельных помещений. К таким средствам относятся защита оконных проемов металлическими решетками и ставнями, специальное остекление окон, использование бронированных дверей, запирающих устройств, сейфов для хранения средств вычислительной техники и носителей информации. В соответствии с особенностями используемых помещений и территорий политика безопасности предприятия также может предусматривать расположение мест хранения и обработки информации (например, архивов или серверных комнат) в помещениях, наименее доступных для проникновения, наиболее удаленных от мест хранения взрывоопасных и легковоспламеняющихся веществ, наименее подверженных затоплению (для объектов расположенных в долинах рек и на побережье), наиболее защищенных от ударов молнии и пр. Принципы и порядок создания системы физической защиты (СФЗ). Учитывая сложность решаемых задач, создание СФЗ важных объектов не может базироваться на довольно часто применяемом на практике принципе «разумной достаточности», а требует комплексного и научного подхода.

Такой подход подразумевает проектирование СФЗ важных объектов в две стадии:

– концептуальное (системное) проектирование;

– рабочее проектирование.

Основными этапами стадии концептуального проекта являются:

1) Анализ уязвимости объекта и существующей СФЗ.

2) Разработка принципов физической защиты объекта.

3) Разработка технико-экономического обоснования создания СФЗ и комплекса инженерно-технических средств охраны (ИТСО).

Основной задачей первых двух этапов стадии концептуального проекта является разработка руководства к действию по созданию СФЗ - «Концепции физической безопасности объекта».

Концепция безопасности определяет пути и методы решения основных задач по обеспечению безопасности объекта и должна отвечать на вопросы: «что защищать?», «от кого защищать?», «как защищать?».

Одной из главных задач начальной стадии концептуального проектирования является проведение Анализа уязвимости объекта и существующей СФЗ.

Целями и задачами проведения анализа уязвимости являются:

– определение важных для жизнедеятельности объекта предметов защиты (наиболее вероятных целей злоумышленных акций нарушителей);

– определение возможных угроз и моделей вероятных исполнителей угроз (нарушителей);

– оценка возможного ущерба от реализации прогнозируемых угроз безопасности;

– оценка уязвимости объекта и существующей системы безопасности;

– разработка общих рекомендаций по обеспечению безопасности объекта.

Работы по анализу проводятся комиссией, в состав которой могут входить специалисты внешних организаций (исполнителей), оказывающих услуги подобного рода и специалисты соответствующих служб защищаемой организации (заказчика): безопасности, главного технолога, главного инженера, пожарной охраны, либо проводятся силами только защищаемой организации при наличии в штате соответствующих подразделений.

Результаты анализа могут оформляться отдельным отчетом. Гриф конфиденциальности определяется заказчиком. К материалам отчета допускается строго ограниченный круг лиц (только непосредственных исполнителей) по существующей на предприятии разрешительной системе. При необходимости, отчет выполняется в одном экземпляре (только для Заказчика).

Реализацию жизненно-важных интересов любого предприятия обеспечивают его корпоративные ресурсы. Эти ресурсы должны быть надежно защищены от прогнозируемых угроз безопасности. Для промышленного предприятия такими важными для жизнедеятельности ресурсами, а, следовательно, предметами защиты являются:

1) Люди (персонал предприятия).

2) Имущество:

– важное или дефицитное технологическое оборудование; секретная и конфиденциальная документация; материальные и финансовые ценности; готовая продукция;

– интеллектуальная собственность (ноу-хау); средства вычислительной техники (СВТ); контрольно-измерительные приборы (КИП) и пр.; информация конфиденциальная: на материальных носителях, а также циркулирующая во внутренних коммуникационных каналах связи и информации, в кабинетах руководства предприятия, на совещаниях и заседаниях; финансово-экономические ресурсы, обеспечивающие эффективное и устойчивое развитие предприятия (капитал, коммерческие интересы, бизнес-планы, договорные документы и обязательства и пр.).

Утрата перечисленных ресурсов может привести: к большому материальному ущербу; созданию угрозы для жизни и здоровья людей; разглашению конфиденциальной информации или сведений, содержащих Государственную тайну; банкротству предприятия. Перечисленные предметы защиты размещаются на соответствующих производственных объектах (подобъектах) предприятия в зданиях и помещениях. Эти подобъекты и являются наиболее уязвимыми местами, выявление которых производится при обследовании объекта. Таким образом, формулируется ответ на вопрос «что защищать?».

По результатам обследования оформляется специальный типовой «Протокол обследования...», который подписывается заинтересованными сторонами.

Основными угрозами безопасности, которые могут привести к утрате корпоративных ресурсов предприятия, являются:

– чрезвычайная ситуация (пожар, разрушение, затопление, авария, хищение опасных веществ и пр.);

– хищение или порча имущества;

– несанкционированный съем конфиденциальной информации;

– ухудшение эффективности функционирования, устойчивости развития.

Самой опасной угрозой безопасности промышленного предприятия являются чрезвычайная ситуации (ЧС), которая может привести к большому материальному ущербу, вызвать угрозу для жизни и здоровья людей, а на потенциально опасных объектах – катастрофические последствия для окружающей среды и населения.

В современных условиях несанкционированные действия физических лиц: диверсантов, террористов, преступников, экстремистов представляют особую опасность, т. к. могут привести к возникновению большинства прогнозируемых угроз.

На этапе анализа угроз совместно со службой безопасности заказчика при предварительном обследовании объекта формируется модель вероятных исполнителей угроз (нарушителей), т. е. их количественные и качественные характеристики (оснащенность, тактика действий и пр.).

В результате проведенной работы формулируется ответ на вопрос: от кого защищать?

Оценка уязвимости, существующей СФЗ производится в два этапа:

На первом этапе (при обследовании объекта) методом экспертных оценок производится оценка уязвимости составных частей СФЗ:

– комплекса организационных мероприятий, проводимых администрацией и службой безопасности объекта;

– комплекса инженерно-технических средств охраны (по основным тактико-техническим характеристикам и степени оснащенности объекта); сил охраны (по организации, качеству, эффективности действий и пр.)

На последующем этапе производится количественная оценка уязвимости, существующей СФЗ.

Оценка возможного ущерба от реализации прогнозируемых угроз безопасности производится методом экспертных оценок совместно с представителями компетентных служб заказчика.

Оценка производится для каждого защищаемого подобъекта предприятия. При этом учитываются варианты прогнозируемых акций нарушителей и сценарии их реализации.

Количественная оценка уязвимости объекта и эффективности СФЗ, производится по имеющимся методикам анализа уязвимости и оценки эффективности систем охраны особо важных объектов.

При анализе учитываются прогнозируемые угрозы и модель исполнителей угроз (нарушителей), вероятности обнаружения нарушителя с помощью

технических средств, варианты тактики ответных действий сил охраны, временные параметры (времена задержки преодоления нарушителем физических барьеров, время ответных действий сил охраны и пр.).

По этой методике в наглядной форме, путем моделирования на ПЭВМ процесса действий нарушителей и сил охраны, производится оценка основного показателя эффективности СФЗ объекта: вероятности перехвата нарушителя силами охраны, действующими по сигналу срабатывания комплекса ИТСО.

По результатам анализа уязвимости разрабатываются общие рекомендации по обеспечению безопасности объекта, с ориентировочной оценкой стоимости создания, предлагаемой СФЗ. При этом сравнивается ориентировочная стоимость предотвращаемого ущерба (Спу) и затрат на создание предлагаемой СФЗ (Ссфз).

Обязательным критерием целесообразности внедрения СФЗ в систему охраны объекта является выполнение условия неравенства: Спу > Ссфз

С целью достижения оптимального уровня защиты, защищаемые предметы и подобъекты классифицируются по важности (значимости) на категории безопасности. В качестве критерия классификации обычно используется характер или масштаб возможного ущерба в случае реализации основных угроз безопасности данному объекту.

Для подобъектов высшей категории безопасности должен быть установлен максимальный уровень защищенности. Основными последующими задачами концептуального проектирования являются:

Разработка структуры СФЗ и вариантов построения комплекса ИТСО объекта с оценкой стоимости их реализации.

Количественная оценка уязвимости предлагаемой СФЗ с различными вариантами структуры комплекса ИТСО и выбор оптимального варианта комплекса по критерию «эффективность – стоимость» (максимум эффективности при минимуме затрат).

От успешного проведения работ на стадии «Концептуального проекта» зависит оптимальность будущих проектно-технических решений. Именно на этой стадии с использованием методов системного анализа и моделирования происходит обоснование и выбор оптимальной структуры и состава СФЗ и комплекса ИТСО по критерию «эффективность – стоимость».

Сравнительная количественная оценка эффективности вариантов комплекса ИТСО позволяет на начальной (допроектной) стадии выбрать оптимальный вариант комплекса, обладающий достаточно высокой эффективностью при минимальных затратах на его создание и внедрение в систему охраны объекта.

Такой подход позволяет избежать серьезных ошибок в рабочем проекте, а, следовательно, и излишних затрат на возможную доработку системы при ее эксплуатации.

Результаты работы этой стадии являются основной составной частью «Концепции...» или технико-экономического обоснование (ТЭО) создания комплекса ИТСО объекта (или группы объектов) и используются в качестве исходных данных для разработки технического задания на рабочее проектирование оборудования объектов комплексами ИТСО.

Дальнейшим развитием в обеспечении безопасности объектов на современном этапе является создание комплексных (интегрированных) систем безопасности и управления системами жизнеобеспечения объектов (КИСБ). В современной терминологии такие системы называют «Автоматизированные системы управления зданиями» или «Автоматизированные системы управления для «интеллектуальных зданий».

Анализ показывает, что «интеллектуальные» системы могут быть созданы на базе автоматизированных СФЗ, а точнее комплексов ИТСО, имеющих в своем составе полный набор основных подсистем (СКУД, СОС, СПС, СОТ).

2 Структура системы физической защиты

Система физической защиты (СФЗ) представляет собой совокупность правовых норм, организационных мер и инженерно-технических решений, направленных на защиту жизненно-важных интересов и ресурсов предприятия (объекта) от угроз, источниками которых являются злоумышленные (несанкционированные) физические воздействия физических лиц - нарушителей (террористов, преступников, экстремистов и пр.).

В этом едином комплексе задействованы и люди (служба безопасности, силы охраны), и техника - комплекс инженерно-технических средств охраны (ИТСО) или комплекс инженерно-технических средств физической защиты (ИТСФЗ). Современные СФЗ строятся на базе широкого применения инженерно-технических и программных средств и содержат следующие основные составные части (подсистемы):

- система контроля и управления доступом персонала (СКУД);
- система охранной сигнализации (СОС);
- система пожарной сигнализации (СПС);
- система охранного телевидения (СОТ);
- система оперативной связи и оповещения;

обеспечивающие системы (освещения, электропитания, охранного освещения и пр.).

Полный перечень основных этапов по созданию и внедрению комплекса ИТСО в эксплуатацию на охраняемом объекте представлен на рис.1.

Методы физической защиты объекта. Типовая структурная схема физической защиты объекта представлена на рис.2.

Обеспечение безопасности объектов представляет собой многогранный процесс реализации охранных мероприятий, по большей части предупреждающего характера.

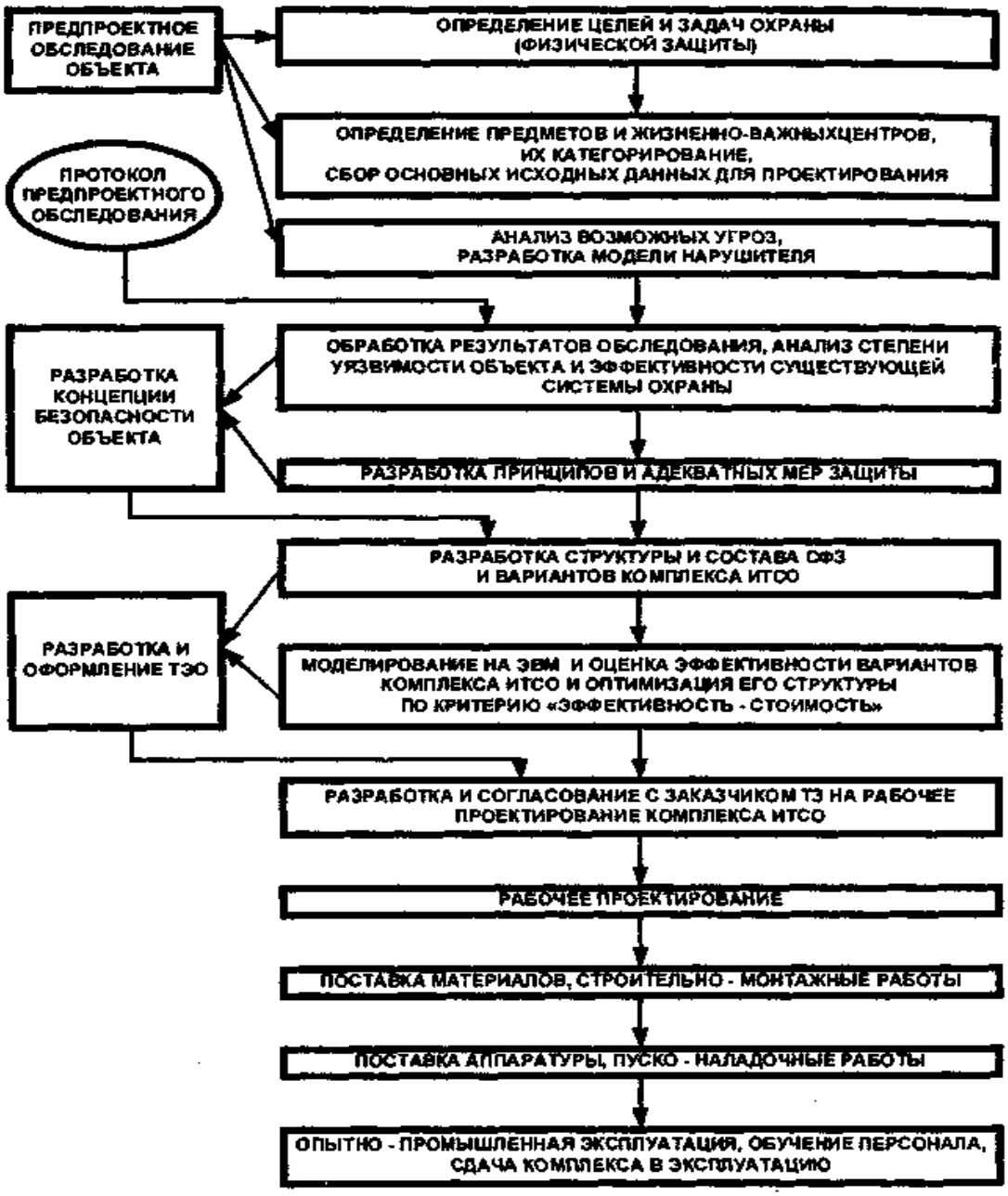

Рис.1 – Полный перечень основных этапов по созданию и внедрению комплекса ИТСО в эксплуатацию на охраняемом объекте

Действительно, эффективной может считаться лишь такая система охраны, которая либо просто не позволяет злоумышленникам найти лазейку в режиме безопасности, либо создает возможность пресечения преступных посягательств на самой ранней стадии.

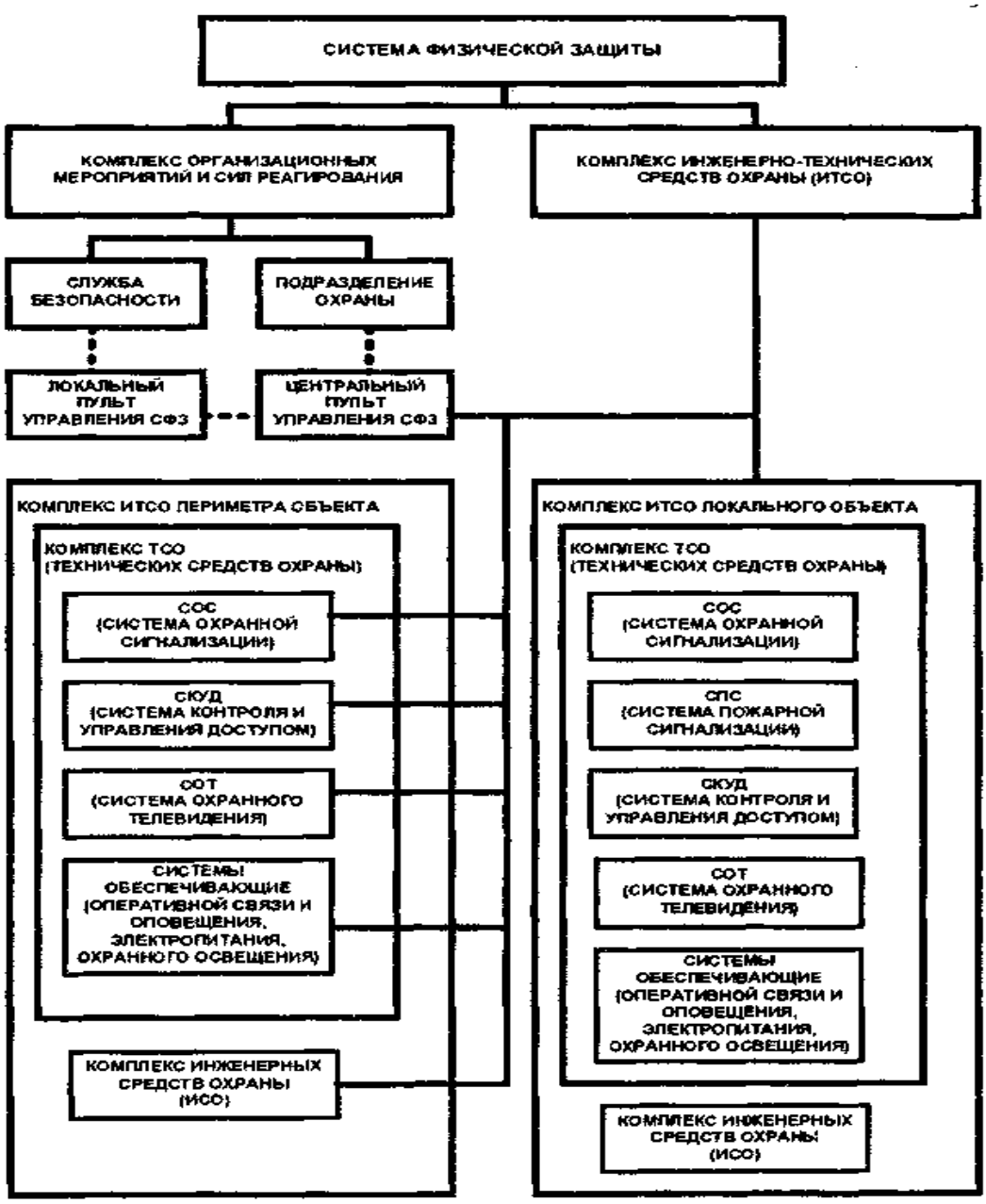

Рис.2 – Типовая структурная схема физической защиты объекта

В основе разработки системы защиты объекта и организации ее функционирования лежит принцип создания последовательных рубежей безопасности, на которых угрозы должны быть своевременно обнаружены. Такие рубежи должны располагаться последовательно, от забора вокруг территории объекта до главного, особо важного помещения.

В качестве примера рассмотрим защиту от несанкционированного проникновения. Злоумышленник проникает на территорию объекта, на котором

располагаются здания и стоянки автомашин посетителей и сотрудников. Возможная угроза для территории – это кража автомобилей, их порча или установка взрывных либо подслушивающих устройств. Защита территории должна состоять из различного рода ограждений ее периметра и специально оборудованных въездов и проходов, охранной сигнализации, охранного оборудованных въездов и проходов, охранной сигнализации, охранного освещения и охранного телевизионного наблюдения. Таким образом, эффективность системы защиты оценивается как время с момента возникновения угрозы до начала ее ликвидации. Чем более сложна и разветвлена система защиты, тем больше времени требуется на ее преодоление и тем больше вероятность того, что угроза будет обнаружена, определена, отражена и ликвидирована.

К числу факторов, влияющих на выбор приемов и средств охраны, относятся:

– возможные способы преступных посягательств на охраняемый объект;

– степень технической укрепленности охраняемого объекта; наличие и качество средств охранно-пожарной сигнализации;

– наличие уязвимых мест в технической укрепленности объекта, которые известны только охране и службе безопасности; условия местности, на которой расположен охраняемый объект, а также его конструктивные особенности.

Таким образом, эффективность системы защиты оценивается как время с момента возникновения угрозы до начала ее ликвидации. Чем более сложна и разветвлена система защиты, тем больше времени требуется на ее преодоление и тем больше вероятность того, что угроза будет обнаружена, определена, отражена и ликвидирована.

К числу факторов, влияющих на выбор приемов и средств охраны, относятся:

– возможные способы преступных посягательств на охраняемый объект;

– степень технической укрепленности охраняемого объекта; наличие и качество средств охранно-пожарной сигнализации;

– наличие уязвимых мест в технической укрепленности объекта, которые известны только охране и службе безопасности; условия местности, на которой расположен охраняемый объект, а также его конструктивные особенности;

– режим и характер работы охраняемого объекта, его технологические характеристики, имеющиеся на объекте материальные и финансовые ценности; режим охраны объекта;

– количественные и качественные характеристики сил охраны; вооруженность и техническая оснащенность охранников, наличие у них автотранспорта, средств связи, сигнализации и специальных средств.

Режим охраны объекта по времени может иметь круглосуточный, частичный (определенные часы суток) или выборочный характер. В зависимости от количества используемых сил и средств, плотности контроля территории и объекта режим охраны может быть простои или усиленный.

На значительной части охраняемых объектов охранники присутствуют круглосуточно. В дневное время они контролируют посетителей, прибывающих на объект, осуществляют контрольно-пропускной режим, а в ночное время несут закрытую охрану объекта, принимая на себя полную ответственность за его сохранность. Некоторые объекты охраняются лишь эпизодически, т.е. выборочно по времени. К таким объектам относятся квартиры, охраняемые на период отсутствия хозяина, временные хранилища или территории в период завоза товарно-материальных ценностей и пр.

Существует несколько методов охраны, в том числе:

– охрана с помощью технических средств с подключением на пульт централизованного наблюдения и с установкой автоматической сигнализации;

– охрана путем выставления постов (силами отдела охраны или милиции);

– комбинированная охрана.

Контрольно-пропускной режим – это комплекс организационно-правовых ограничений и правил, устанавливающих порядок пропуска через контрольно-пропускные пункты в отдельные здания (помещения) сотрудников объекта, посетителей, транспорта и материальных средств. Контрольно-пропускной режим является одним из ключевых моментов в организации системы безопасности на предприятии. С этих позиций контрольно-пропускной режим представляет собой комплекс организационных мероприятий (административно-ограничительных), инженерно-технических решений и действий службы безопасности. Организация контрольно-пропускного режима отличается определенной сложностью. Дело в том, что механизм осуществления контрольно-пропускного режима основывается на применении «запретов» и «ограничений» в отношении субъектов, пересекающих границы охраняемых объектов, для обеспечения интересов предприятия. Такой механизм должен быть безупречным с точки зрения соответствия требованиям действующего законодательства.

Контрольно-пропускной режим (как часть системы безопасности) должен соответствовать действующему законодательству, уставу предприятия, а также иным нормативно-правовым актам, регулирующим деятельность предприятия.

Тема 2.3. Технологические меры поддержания безопасности

1 Процедурные меры обеспечения информационной безопасности

В российских компаниях накоплен богатый опыт регламентирования и реализации процедурных (организационных) мер, однако они пришли из «докомпьютерного» прошлого, поэтому требуют переоценки. Акцент следует делать на аспектах, связанных с поддержанием нормального функционирования аппаратного и программного обеспечения, то есть концентрироваться на вопросах доступности и целостности данных.

Основные процедурные меры обеспечения информационной безопасности:

- управление персоналом;
- физическая защита;
- поддержание работоспособности;
- реагирование на нарушения режима безопасности;
- планирование восстановительных работ.

Управление персоналом начинается с приема нового сотрудника на работу и даже раньше – с составления описания должности. Уже на данном этапе желательно подключить к работе специалиста по информационной безопасности для определения компьютерных привилегий, ассоциируемых с должностью. Существует два общих принципа, которые следует иметь в виду:

- разделение обязанностей;
- минимизация привилегий.

Принцип разделения обязанностей предписывает, как распределять роли и ответственность, чтобы один человек не мог нарушить критически важный для организации процесс.

Принцип минимизации привилегий предписывает выделять пользователям только те права доступа, которые необходимы им для выполнения служебных обязанностей. Назначение этого принципа, очевидно, – уменьшить ущерб от случайных или умышленных некорректных действий.

Физическая защита. Безопасность информационной системы зависит от окружения, в котором она функционирует. Необходимо принять меры для защиты зданий и прилегающей территории, поддерживающей инфраструктуры, вычислительной техники, носителей данных. Основной принцип физической защиты, соблюдение которого следует постоянно контролировать, формулируется как «непрерывность защиты в пространстве и времени».

Направления физической защиты:

- физическое управление доступом;
- противопожарные меры;
- защита поддерживающей инфраструктуры;
- защита от перехвата данных;
- защита мобильных систем.

Меры физического управления доступом позволяют контролировать и при необходимости ограничивать вход и выход сотрудников и посетителей. Контролироваться может все здание организации, а также отдельные помещения, например, те, где расположены серверы, коммуникационная аппаратура и пр. Средства физического управления доступом известны давно. Это охрана, двери с замками, перегородки, телекамеры, датчики движения и многое другое, есть смысл периодически отслеживать появление технических новинок в данной области, стараясь максимально автоматизировать физическую защиту.

Противопожарные меры необходимы, т.к. пожары по-прежнему случаются и наносят большой ущерб. Отметим необходимость установки противопожарной сигнализации и автоматических средств пожаротушения.

К поддерживающей инфраструктуре можно отнести системы электро-, водо- и теплоснабжения, кондиционеры и средства коммуникаций. В принципе, к ним применимы те же требования целостности и доступности, что и к информационным системам. Для обеспечения целостности нужно защищать оборудование от краж и повреждений. Для поддержания доступности следует

выбирать оборудование с максимальным временем наработки на отказ, дублировать ответственные узлы и всегда иметь под рукой запчасти. При размещении компьютеров необходимо принять во внимание расположение водопроводных и канализационных труб и постараться держаться от них подальше. Сотрудники должны знать, куда следует обращаться при обнаружении протечек.

Перехват данных может осуществляться самыми разными способами. Злоумышленник может подсматривать за экраном монитора, читать пакеты, передаваемые по сети, производить анализ побочных электромагнитных излучений и наводок и т.д. Следует использовать криптографию (что, сопряжено с техническими и законодательными проблемами); стараться максимально расширить контролируемую территорию, пытаться держать под контролем линии связи

Мобильные и портативные компьютеры – заманчивый объект кражи. Их часто оставляют без присмотра, в автомобиле или на работе, и похитить такой компьютер совсем несложно. Следует шифровать данные на жестких дисках таких компьютеров.

Поддержание работоспособности. Выделяются следующие направления повседневной деятельности, направленные на поддержание работоспособности информационных систем:

- поддержка пользователей;
- поддержка программного обеспечения;
- конфигурационное управление;
- резервное копирование;
- управление носителями;
- документирование;
- регламентные работы.

Поддержка пользователей подразумевает, прежде всего, консультирование и оказание помощи при решении разного рода проблем.

Поддержка программного обеспечения – одно из важнейших средств обеспечения целостности информации. Прежде всего, необходимо следить за тем, какое программное обеспечение установлено на компьютерах. Второй аспект поддержки программного обеспечения – контроль за отсутствием неавторизованного изменения программ и прав доступа к ним. Сюда же можно отнести поддержку эталонных копий программных систем.

Конфигурационное управление позволяет контролировать и фиксировать изменения, вносимые в программную конфигурацию. Прежде всего, необходимо застраховаться от случайных или непродуманных модификаций, уметь, как минимум возвращаться к прошлой, работающей, версии.

Резервное копирование необходимо для восстановления программ и данных после аварий. Здесь целесообразно автоматизировать работу, как минимум, сформировав компьютерное расписание создания полных и инкрементальных копий, а как максимум – воспользовавшись соответствующими программными продуктами.

Управление носителями необходимо для обеспечения физической защиты и учета дискет, лент, печатных выдач и пр. Управление носителями должно обеспечивать конфиденциальность, целостность и доступность информации, хранящейся вне компьютерных систем. Под физической защитой здесь понимается не только отражение попыток несанкционированного доступа, но и предохранение от вредных влияний окружающей среды (жары, холода, влаги, магнетизма).

Документирование – неотъемлемая часть информационной безопасности. Важно, чтобы документация была актуальной, отражала именно текущее состояние дел, причем в непротиворечивом виде. К хранению одних документов (содержащих, например, анализ уязвимых мест системы и угроз) применимы требования обеспечения конфиденциальности, к другим, таким как план восстановления после аварий - требования целостности и доступности (в критической ситуации план необходимо найти и прочитать).

Регламентные работы – серьезная угроза безопасности. Сотрудник, осуществляющий регламентные работы, получает исключительный доступ к системе, и на практике очень трудно проконтролировать, какие именно действия он совершает. Здесь на первый план выходит степень доверия к тем, кто выполняет работу

Реагирование на нарушения режима безопасности. Программа безопасности, принятая организацией, должна предусматривать набор оперативных мероприятий, направленных на обнаружение и нейтрализацию нарушений режима информационной безопасности. Важно, чтобы в подобных случаях последовательность действий была спланирована заранее, поскольку меры нужно принимать срочные и скоординированные. Реакция на нарушения режима безопасности преследует три главные цели:

- локализация инцидента и уменьшение наносимого вреда;
- выявление нарушителя;
- предупреждение повторных нарушений.

Планирование восстановительных работ. Процесс планирования восстановительных работ можно разделить на следующие этапы:

1) Выявление критически важных функций организации, установление приоритетов.
2) Идентификация ресурсов, необходимых для выполнения критически важных функций.
3) Определение перечня возможных аварий.
4) Разработка стратегии восстановительных работ.
5) Подготовка к реализации выбранной стратегии.
6) Проверка стратегии.

2 Программно-технические методы обеспечения информационной безопасности

1) Идентификация и аутентификация.

Идентификация – процесс, позволяющий установить имя пользователя. Хорошим примером здесь, в частности, может служить вручение визитной карточки, где указаны имя, должность и другие атрибуты конкретного лица. Но как убедиться, что визитная карточка принадлежит действительно тому человеку, который называет ее своей? Здесь потребуется уже процедура аутентификации.

Аутентификация предполагает выполнение процесса проверки подлинности введенного в систему имени пользователя. На бытовом уровне аутентификация может, например, осуществляться с помощью фотографии. Еще одним примером аутентификации может служить узнавание голоса при звонках по телефону – вряд ли вы будете продолжать беседу с человеком, назвавшимся по телефону знакомой фамилией, но говорящим незнакомым голосом и с другими интонациями.

Средства идентификации и аутентификации могут и объединяться. Всем известным примером здесь может быть служебное удостоверение, где приведены и данные для идентификации (фамилия, должность и пр.) и данные для аутентификации (фотография). Важно отметить, что и сами средства идентификации и аутентификации могут иметь некоторые признаки, подтверждающие их подлинность. На удостоверении, например, это печати, подписи и, при необходимости, другие признаки защиты от подделок.

Предыдущий пример приведен неслучайно. В информационных технологиях способы идентификации и аутентификации являются своеобразным служебным удостоверением пользователя, обеспечивающим его доступ в информационное пространство организации в целом или отдельные разделы этого пространства.

Весьма значительное число используемых в настоящее время способов идентификации и аутентификации пользователя информационно-вычислительных систем можно разделить на следующие основные группы:

– парольные методы;

– методы с применением специализированных аппаратных средств;

– методы, основанные на анализе биометрических характеристик пользователя.

Наибольшее распространение получили парольные методы, что объясняется относительной простотой их реализации. Смысл этих методов заключается в том, что для входа в систему пользователь вводит два кода: свое условное имя (идентификация) и уникальный, известный только ему одному код-пароль для аутентификации. При правильном использовании парольные схемы могут обеспечить приемлемый для многих организаций уровень безопасности. Тем не менее, по совокупности характеристик они считаются сегодня самым слабым средством аутентификации. Дело в том, что надежность паролей очень сильно зависит от «человеческого фактора». Она изначально основана на способности людей помнить пароль и хранить его в тайне. Однако, чтобы пароль был запоминающимся, его зачастую делают простым, а простой пароль нетрудно угадать, особенно если знать пристрастия данного пользователя. Сложный пароль часто записывают на бумажке, которую не так уж трудно найти злоумышленнику. Кроме того, пароль можно подсмотреть при вводе, подобрать с помощью специальных программ и пр.

Вторая из выделенных схем идентификации и аутентификации предполагает использование специальных устройств – магнитных карт, смарт-карт, так называемых таблеток, токенов и пр., на которых записана уникальная информация. Эти методы отличаются большей устойчивостью, однако потребуют от вас в рабочее время постоянного ношения соответствующего блока. В принципе это необременительно, поскольку сейчас такие устройства по размеру и весу не больше обычного брелка для ключей (да, как правило, они и

носятся таким же образом). Однако существует вполне реальная возможность потери или кражи аппаратного идентификатора, его можно просто забыть дома и пр. Поэтому в ряде организаций практикуется получение аппаратных идентификаторов утром перед началом работы и возврат их на хранение перед уходом с предприятия с соответствующим документированием этой процедуры.

Наиболее перспективным в настоящее время считается использование средств идентификации пользователя по биометрическим признакам – отпечаток пальца, рисунок радужной оболочки глаз, отпечаток ладони и пр. Эти методы обладают достаточно высокой надежностью и в то же время не требуют от пользователя запоминания и хранения в тайне сложных паролей или заботы о сохранности аппаратного идентификатора. Многим из вас, возможно, эти методы знакомы пока лишь по приключенческим кинофильмам, однако развитие информационных технологий ведет к тому, что стоимость этих средств становится доступной для большинства организаций. Правда, и эти средства не лишены недостатков. Не говоря уже о возможности использования «мертвой руки» или «мертвого пальца», здесь можно упомянуть о проблемах с идентификацией, возникающих из-за изменения радужной оболочки под воздействием некоторых лекарств или связанных с изменениями в кожном покрове под воздействием высокой или низкой температуры воздуха. Например, если вы вошли в помещение с замерзшими руками, система аутентификации по отпечаткам пальцев может вас не опознать.

2) Разграничение доступа. Средства логического управления доступом тоже контролируют возможность попадания пользователя в тот или иной раздел информации, хранящейся в системе, только они реализуются программным путем. Логическое управление доступом – это основной механизм многопользовательских систем, призванный обеспечить конфиденциальность и целостность информации.

Нужно сказать, что тема логического управления доступом – одна из сложнейших в области информационной безопасности. Поскольку вам наверняка не придется разбираться в ней «изнутри», отметим следующее: схему управления доступом принято характеризовать так называемой матрицей доступа, в строках которой перечислены субъекты, в столбцах – объекты, а в клетках, расположенных на пересечении строк и столбцов, записаны разрешенные виды доступа и дополнительные условия (например, время и место действия).

Удобной надстройкой над средствами логического управления доступом является ограничивающий интерфейс, когда пользователя лишают самой возможности попытаться совершить несанкционированные действия, включив в число видимых ему объектов только те, к которым он имеет доступ. Подобный подход обычно реализуют в рамках системы меню и пользователю показывают лишь допустимые варианты выбора.

3) Протоколирование и аудит. Под протоколированием понимается сбор и накопление информации о событиях, происходящих в информационно-вычислительной системе. У каждой программы есть свой набор возможных событий, но в любом случае их можно подразделить на внешние – вызванные действиями других программ или оборудования, внутренние – вызванные действиями самой программы, и клиентские – вызванные действиями пользователей и администраторов.

Аудит – это анализ накопленной информации, проводимый оперативно, почти в реальном времени, или периодически.

Реализация протоколирования и аудита преследует следующие главные цели:

– обеспечение подотчетности пользователей и администраторов;

– обеспечение возможности реконструкции последовательности событий;

– обнаружение попыток нарушений информационной безопасности;

– предоставление информации для выявления и анализа проблем.

Пользователь, не в состоянии вмешаться в процесс протоколирования, а в процессе аудита будете участвовать, скорее всего, только тогда, когда по результатам аудита к вам будут претензии. Тем не менее, не стоит забывать, что в хорошо сделанной системе фиксируются все попытки доступа к информации и практически все виды действий, которые над этой информацией производится.

В принципе обеспечение подобной подотчетности считается одним из средств сдерживания попыток нарушения информационной безопасности – в этих условиях труднее замести следы, поэтому злоумышленнику нужно принимать какие-то дополнительные меры, а просто любопытные побоятся предпринимать несанкционированные действия. Если есть основания подозревать какого-то конкретного пользователя, его работу можно рассмотреть «под микроскопом» – регистрировать его действия особенно детально, например, до каждого нажатия клавиши. Последующая реконструкция событий позволяет выявить слабости в защите, найти виновника, определить способ устранения проблемы и вернуться к нормальной работе. Тем самым в определенной степени обеспечивается целостность информации.

Можно, однако, упомянуть – если подобными средствами воспользуется злоумышленник, который тем или иным образом получил соответствующие полномочия, то работа системы будет ему понятна.

4) Криптографическое преобразование данных. Криптография, или шифрование – одна из самых наукоемких и до настоящего времени одна из самых закрытых областей информационной безопасности. Во многих отношениях она занимает центральное место среди программно-технических средств безопасности, являясь основой реализации многих из них и, если можно так выразиться, последним барьером, предотвращающим несанкционированный доступ к информации.

В современной криптографии используются два основных метода шифрования – симметричное и асимметричное. В симметричном шифровании один и тот же ключ используется и для шифровки, и для расшифровки сообщений.

Существуют весьма эффективные методы симметричного шифрования. Имеется и российский стандарт на подобные методы – ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. Основным недостатком симметричного шифрования является то, что секретный ключ должен быть известен и отправителю, и получателю. С одной стороны, это ставит проблему безопасной пересылки ключей при обмене сообщениями. С другой – получатель, имеющий шифрованное и расшифрованное сообщение, не может доказать, что он получил его от конкретного отправителя, поскольку такое же сообщение он мог сгенерировать и сам.

В асимметричных методах применяются два ключа. Один из них, несекретный, используется для шифровки и может без всяких опасений передаваться по открытым каналам, другой – секретный, применяется для расшифровки и известен только получателю.

Асимметричные методы шифрования позволяют реализовать так называемую электронную подпись, или электронное заверение сообщения. Идея состоит в том, что отправитель посылает два экземпляра сообщения – открытое и дешифрованное его секретным ключом (здесь следует учитывать, что дешифровка незашифрованного сообщения на самом деле есть форма шифрования). Получатель может зашифровать с помощью открытого ключа отправителя дешифрованный экземпляр и сравнить с открытым. Если они совпадут, личность и подпись отправителя можно считать установленными.

Существенным недостатком асимметричных методов является их низкое быстродействие, поэтому их приходится сочетать с симметричными. Так,

для решения задачи рассылки ключей сообщение сначала симметрично шифруют случайным ключом, затем этот ключ шифруют открытым асимметричным ключом получателя, после чего сообщение и ключ отправляются по сети.

Обратим внимание на то, что при использовании асимметричных методов необходимо иметь гарантию подлинности пары (имя, открытый ключ) адресата. Для решения этой задачи вводится понятие сертификационного центра, который заверяет справочник имен (ключей) своей подписью.

В любом случае вам нужно иметь в виду, что ахиллесовой пятой любого метода шифрования является секретный ключ. При его случайном или намеренном раскрытии все усилия по шифрованию пропадут даром. Поэтому определенную проблему здесь составляет надежное хранение закрытых ключей.

5) Экранирование. С развитием сетевых технологий все большую актуальность приобретает защита от случайных или намеренных воздействий из внешних сетей (например, Интернет), с которыми взаимодействует сеть предприятия. Для этой цели используются различные разновидности так называемых межсетевых экранов, а сам процесс защиты получил название экранирования. Если опустить технические подробности, то межсетевой экран – это специализированная программная система, ограничивающая возможность передачи информации как из внешней сети в сеть предприятия, так и из сети предприятия во внешнюю среду. Помимо функций разграничения доступа, экраны осуществляют также протоколирование информационных обменов.

Говоря об межсетевых экранах, нельзя не остановиться на одном из общих прагматических аспектов защиты информации. Любое подключение к сети в потенциале предоставляет «лазейку» для несанкционированного доступа к информации. Поэтому для надежного хранения конфиденциальных данных используются автономные, не подключаемые к сети системы. Средства защиты информации в сети имеет смысл использовать, только если эта информация как раз, и предназначена для сетевого применения – например, в электронной коммерции, на информационных серверах Интернет и пр.

Тема 2.4. Организация режима секретности

1 Понятие режима секретности, его особенности и содержание

Режим секретности – установленный нормами права единый порядок в нашей стране обращения со сведениями, составляющими государственную и служебную тайны. Назначение: предотвращение утечки закрытой информации по агентурным каналам. Режим секретности имеет ряд особенностей:

– единый для всех министерств, ведомств, предприятий, учреждений, организаций порядок обращения с государственными секретами, которые определяются высшими органами государственной власти и управления;

– обязательный для всех государственных органов и должностных лиц порядок обращения с государственными секретами;

– персональная ответственность руководителей всех рангов за организацию режима секретности в их учреждениях, организациях и предприятиях, за проведение необходимого комплекса мероприятий, предотвращающих утечку закрытой информации;

– контроль за деятельностью по обеспечению сохранности государственных секретов, соблюдение требований установленного режима секретности, который осуществляется органами государственной безопасности;

– уголовная ответственность лиц, виновных в разглашении секретных сведений, в утрате секретных документов и изделий.

Режим секретности по содержанию включает в себя:

– порядок установления степени секретности сведений, содержащихся в работах, документах и изделиях;

– порядок допуска граждан к работам, документам и изделиям, которые содержат закрытую информацию;

– порядок выполнения должностными лицами своих должностных обязанностей по сохранению государственных и служебных тайн, по соблюдению режима секретности;

– порядок обеспечения секретности при проведении в учреждениях и на предприятиях работ закрытого характера;

– порядок обеспечения секретности при ведении секретного делопроизводства;

– порядок обеспечения секретности при использовании технических средств, передаче, обработке и хранении информации закрытого характера;

– порядок обеспечения секретности при осуществлении предприятиями, учреждениями и организациями, где ведутся закрытые работы, контактов с зарубежными фирмами;

– порядок проведения служебных расследований по фактам разглашения секретных сведений.

Деятельность по обеспечению сохранности государственных секретов в министерствах, ведомствах, учреждениях, организациях и на предприятиях осуществляется через режимно-секретные органы (РСО), которые состоят из первых отделов и отделов или групп режима. На первые отделы возложена задача ведения секретного делопроизводства. Отделы или группы режима занимаются вопросами организации режима секретности на объекте и режима секретности по проводящимся закрытым работам:

– вопросы допуска сотрудников к закрытым работам и документам;

– организация пропускного режима на объекте;

– вопросы контроля за соблюдением установленных требований режима секретности.

В основу работы РСО положены:

1) Инструкция по обеспечению режима секретности в министерствах, ведомствах, на предприятиях и в организациях» («Инструкция 0126»).

2) «Перечень главнейших сведений, составляющих государственную тайну».

3) «Ведомственный перечень сведений, подлежащих засекречиванию».

4) «Положение о порядке установления степени секретности сведений, содержащихся в работах, документах и изделиях».

Постоянно действующие технические комиссии по защите государственной тайны и конфиденциальной информации (ПДТК) создаются на всех предприятиях, где ведутся закрытые работы. ПДТК является консультативным органом при руководителе предприятия по вопросам режима секретности и противодействия иностранным техническим разведкам.

Основные задачи ПДТК:

– выявление возможных каналов утечки информации, присущих для данного предприятия;

– разработка и реализация мероприятий по своевременному закрытию выявленных каналов утечки закрытой информации;

– планирование всей работы по вопросам режима секретности, защиты от технических разведок на предприятии;

– организация и ведение общей профилактической работы по защите закрытой информации от технических разведок.

При осуществлении своей работы работники РСО имеют право:

– требовать от всех сотрудников, которые допущены к секретным работам и документам, выполнения всех требований установленного режима секретности;

– осуществлять контроль в подразделениях предприятия по обеспечению сохранности государственных и служебных тайн и выполнению требований режима секретности;

– требовать от лиц, виновных в разглашении секретных сведений, в утрате секретных документов и изделий, виновных в грубом нарушении режима секретности, письменных объяснений по факту происшедшего;

– возбуждать ходатайство перед руководством предприятия об отстранении от исполнения служебных обязанностей лиц, виновных в перечисленных выше проступках.

Основные понятия (термины) режима секретности.

Секретный документ – текстовые и графические материалы, выполненные любым способом, кино-, фото- и видеопозитивы и негативы, магнитные ленты звуко- и видеозаписи, перфокарты, перфоленты и другие материалы, которые содержат секретную информацию.

Секретное изделие – засекреченные образцы и комплексы вооружения и военной техники, оборудование, входящее в их состав, комплектующие узлы и элементы, материалы и вещества, которые используются при создании и вооружении военной техники.

Секретная работа – научно-исследовательские и опытно-конструкторские, проектные, диссертационные, дипломные и другие работы, в процессе выполнения которых образуются секретные сведения.

Степени (грифы) секретности сведений:

- особой важности (ОВ);
- совершенно секретные (СС);
- секретные (С).

Государственная, служебная и военная тайны: государственная тайна – сведения научно-технического, экономического, политического и военного характера, разглашение или утрата которых представляет угрозу для безопасности государства; служебная тайна – сведения, утрата и разглашение которых приносит ущерб интересам государства; военная тайна – сведения, охраняемые государством, чисто военного характера (может быть и государственной, и служебной тайной).

2 Порядок работы с секретными документами и изделиями

Порядок обеспечения сохранности государственных и служебных тайн в организациях, учреждениях и на предприятиях.

Утечка секретных сведений – это их бесконтрольное распространение за пределы сферы обращения, ограниченной режимом секретности.

Причинами утечки секретных сведений могут быть:

– нарушение исполнителями установленного режима секретности при выполнении закрытых работ;

– при работе с секретными документами и изделиями;

– разглашение секретных сведений при общении с посторонними лицами;

– утрата секретных документов и изделий;

– недостатки в организации работы по противодействию иностранным техническим разведкам;

– упущения администрации и работников РСО в вопросах организации режима секретности;

– несвоевременное принятие мер по закрытию выявленных каналов утечки информации.

Предотвращение утечки секретных сведений в организациях, учреждениях и на предприятиях обеспечивается:

– установлением специального порядка допуска к секретным работам, документам и изделиям;

– точным выполнением всех правил засекречивания и рассекречивания сведений;

– выполнением всех требований секретного делопроизводства;

– установлением специальных обязанностей для лиц, которые допускаются к секретным документам и изделиям;

– ограничением выезда за рубеж лиц, осведомленных о государственных секретах;

– установлением специальных правил в работе с иностранцами, которые посещают предприятия и организации, где ведутся секретные работы;

– организацией ведения профилактической работы.

Допуск к секретным работам и документам. К секретным работам и документам могут быть допущены только граждане РФ, которые по своим деловым, политическим и моральным качествам способны обеспечить сохранность доверенных им тайн. К секретным работам и документам **не** допускаются лица, имеющие: психические заболевания; лица, которые понесли уголовную ответственность; лица, совершающие поступки, несовместимые с принципами нравственности и морали; лица, имеющие постоянный контакт с лицами (родственниками) за границей.

На каждое лицо, допускаемое к секретным работам и документам, оформляется допуск, то есть официальное разрешение руководителя предприятия на право выполнения закрытых работ, на право ознакомления с секретными работами и документами. Существует три формы допуска к секретным работам и документам:

1) Наивысшая форма допуска (имеют право на ознакомление со сведениями ОВ, СС, С).

2) Вторая форма допуска (имеют право на ознакомление со сведениями СС, С).

3) Третья форма допуска (имеют право на ознакомление со сведениями С).

При командировке сотрудников, имеющих допуск по месту основной работы, на другие предприятия им в первом отделе своего предприятия выдаются справки о допуске к секретным работам и документам, и выписываются командировочные предписания на право выполнения работ.

Засекречивание и рассекречивание сведений. Засекречивание конкретных сведений в связи с наличием в них государственных и служебных тайн осуществляется в соответствии с перечнем главнейших сведений, составляющих государственную тайну, и ведомственными перечнями сведений, подлежащих засекречиванию. Единый порядок засекречивания сведений определен положением о порядке установления степени секретности сведений, содержащихся в работах, документах и изделиях.

При засекречивании сведений руководствуются следующими принципами:

– решение проблемы засекречивания в целом с позиции государственной значимости этих сведений; при этом необходимо учитывать противоречивость и единство двух тенденций: с одной стороны, стремление обеспечить надежность сохранности государственных и служебных тайн, с другой стороны, не допустить необоснованного массового засекречивания;

– объективный характер определения степени секретности сведений, который основывается на точном использовании существующих перечней охраняемых сведений;

– оптимизация объема засекречиваемых сведений;

– периодический просмотр степени секретности сведений на предмет снятия или снижения грифа секретности.

СД - секретный документ. СС - степень секретности.

Рассекречивание СД производится при:

1) Изменении перечней сведений, подлежащих засекречиванию.
2) Окончании срока действия грифа.
3) Изменении международной обстановки.
4) Появлении новых достижений в науке и технике.
5) Продаже или передаче вооружения другим странам.
6) Снятии оружия и боевой техники с вооружения.

Для проведения работ по рассекречиванию создаются специальные комиссии из числа работников РСО и соответствующих специалистов.

Секретное делопроизводство (СДП). СДП – это порядок учета, составления, хранения, размножения, пересылки и уничтожения СД. Ведение СДП возлагается на 1-е отделы РСО предприятия. СДП осуществляется на основании следующих документов:

1) Инструкция 0126.
2) Ведомственные инструкции по СДП.
3) ГОСТ 2904-74 (Правила выполнения, учета и обращения СД).

Условные наименования и обозначения. Условные наименования (шифры) присваиваются закрытым работам. Они представляют из себя явления природы, нарицательные имена существительные. Условные обозначения (индексы) присваиваются секретным изделиям. Они представляют из себя цифробуквенные обозначения. УО и УИ применяются для указания ссылок на СД и секретных изделий (СИ). Само название СД или СИ применяется только в крайних случаях.

Учёт секретных документов. Учет СД – регистрация и контроль за их сохранностью. Существует 2 формы учета СД: журнальная и карточная. При журнальной системе информация о СД хранится в специальных журналах. При карточной – на спец. карточках, отельных для каждого СД. При учете СД присваиваются регистрационные номера и фиксируется информация: гриф, количество листов, количество экземпляров, источник поступления, краткое содержание, дата поступления. Учету подлежат: СД, рабочие тетради, спецблокноты, отдельные листы бумаги.

Хранение секретных документов (ХСД). ХСД – установленный порядок, обеспечивающий содержание в безопасности СД на рабочих местах и в спец. хранилищах; порядок, предотвращающий порчу СД, их утрату и НСК. НСК –

несанкционированное копирование. В рабочее время СД хранятся у исполнителей в личных сейфах или в секретных портфелях (папках). После окончания работы СД сдаются на хранение в 1-е отделы.

Порядок обращения с секретными документами. При обращении с СД следует соблюдать следующие правила:

1) СД выдаются только под личную роспись;

2) Работа с СД осуществляется в спец. помещениях;

3) При работе с СД на рабочем столе должны находиться только необходимые в данный момент документы;

4) Запрещается держать СД вместе с несекретными;

5) Запрещается хранить СД в рабочих столах;

6) При приеме посетителей нельзя оставлять СД в положении, удобном для обозрения;

7) Необходимо убирать СД в сейф при временном выходе из помещения;

8) Запрещается выносить СД за пределы охраняемой территории;

9) При окончании работы с СД необходимо проверить наличие всех СД.

Порядок разработки секретных документов:

1) СД разрабатываются только в спец. блокнотах, рабочих тетрадях;

2) СС документа определяется в соответствии с перечнями;

3) Количество экземпляров СД определяется служебной необходимостью;

4) В СД должен быть представлен минимально возможный объем секретных сведений;

5) В документах для машинописи нельзя указывать ТТХ;

6) Запрещается снимать копии с СД без разрешения;

7) Запрещается самостоятельно уничтожать СД. ТТХ - тактико-технические характеристики.

Оформление секретного документа.

Порядок оформления СД: Гриф; N экземпляра; Адрес; Текст; Приложения; Подпись.

Порядок оформления последнего листа: Исполнители; Гриф; Количество листов и экземпляров; адреса экземпляров; Машинистка; Дата.

Размножение секретных документов. Подготовленный секретный документ подается исполнителями для размножения в 1-й отдел. Сдаются только те листы СД, которые подлежат копированию. После размножения исполнитель получает документы и расписывается за оригинал и каждую копию. Не подлежат копированию СД с грифом ОВ.

Пересылка секретных документов. СД пересылаются только через РСО предприятия. Полностью оформленный и подписанный СД сдается исполнителем в 1-й отдел для пересылки. Перед отправкой СД помещается в спец. упаковку, исключающую несанкционированное изъятие СД. Пересылка СД в другие города осуществляется подразделениями спец. связи Мин. Связи РФ и подразделениями фельдсвязи МО РФ. При пересылке в рамках одного города используются: курьеры, нарочные, работники РСО, исполнители.

Лица, занятые доставкой секретной почты обеспечиваются служебным транспортом и охраной. Передача СД адресатам осуществляется по разносным книгам, распискам, реестрам под личную роспись принимающего, которая скрепляется печатью 1-го отдела с проставлением времени и числа.

Уничтожение секретных документов. СД, потерявшие свою практическую и пр. ценность подлежат уничтожению. Для уничтожения СД приказом руководителя предприятия назначается комиссия в составе не менее 3-х человек. Порядок работы комиссии:

1) Оценка ценности СД.

2) Написание акта на уничтожение СД.

3) Проведение сверки представленных на уничтожение документов с записями в журналах и карточках учета.

4) Проставление росписей в акте и представление его на утверждение руководителю предприятия.

5) Уничтожение в присутствии членов комиссии. Акт на уничтожение хранится в 1-м отделе.

Учёт секретных изделий. Учет делится на предварительный и основной. Предварительный учет ведется при опытном производстве, а основной – при серийном производстве. Начало учета устанавливается:

1) При опытном производстве – с момента начала изготовления изделия по секретным чертежам, или с момента, указанного в их документации.

2) При серийном производстве – с момента, указанного в технических или сопроводительных картах. Если изделие изготовляется из секретных заготовок, то его учет начинается с момента получения этих заготовок. При поступлении изделий извне, их учет начинается с момента поступления. СИ учитываются отдельно от несекретных. При их учете используются только УН и УО. На каждое изделие оформляется тех. паспорт или формуляр, которые учитываются как СД.

Хранение секретных изделий. СИ хранятся в упакованном виде, или под опломбированными чехлами. СИ могут храниться: в спец-хранилищах, на позициях, в местах стоянок, в лабораториях и учебных классах. Места хранения СИ должны быть оборудованы сигнализацией. Малогабаритные СИ могут сдаваться на хранение в 1-е отделы. При хранении СИ на рабочем месте, после окончания работы с ним оно должно быть зачехлено, а помещение - опечатано и сдано под охрану.

Обеспечение режима секретности при транспортировке секретных изделий. Различают внутреннюю и внешнюю транспортировку СИ. Внутренняя транспортировка – это погрузка, выгрузка и перевозка СИ в пределах охраняемой территории предприятия. При внутренней транспортировке необходимо применять меры по маскировке от средств технической разведки. При внеш-

ней транспортировке должны быть применены меры по охране СИ, по его маскировке от технической разведки и по скрытию маршрутов транспортировки и средств доставки.

Обеспечение режима секретности рот испытании секретных изделий. Необходимо соблюдать следующие меры:

1) Ограничивать круг лиц, допущенных к испытаниям.

2) Ознакомление только с теми частями и блоками, которые необходимы для проведения испытаний.

3) Физическая и техническая охрана полигона.

4) Легендирование проводимых испытаний.

5) Маскировка изделий и полигонной аппаратуры.

6) Ликвидация всех следов и последствий сразу же после окончания проведения испытаний.

Уничтожение секретных изделий. Уничтожению подлежат СИ, утратившие практическую и научную ценность, забракованные в процессе производства, пришедшие в негодность в результате испытаний, выработавшие свой ресурс. Для уничтожения СИ назначается комиссия.

Порядок действия комиссии:

1) Оценка СИ на годность.

2) Составление акта на уничтожение.

3) Сверка комплектации СИ с записью в карточках учета.

4) Проставление росписей членов комиссии и представление акта на утверждение руководителю предприятия.

5) Уничтожение. Акт на уничтожение хранится в 1-м отделе.

Обеспечение режима секретности при использовании технических средств передачи, обработки и хранения информации. К ТСПИ относятся средства ЭВТ, информационные системы, средства радиопередачи, звукозаписи и видеозаписи и воспроизведения, охранной сигнализации, электриче-

ские часы, множительная техника. ЭВТ – электронно-вычислительная техника. При работе ТСПИ возникает ряд технических каналов, по которым возможна утечка секретной информации. К таким каналам относятся электромагнитные поля, возникающие при работе ТСПИ, Электромагнитные наводки на соседние провода, которые уходят за пределы охраняемой территории, токи заземления, сети питания, паразитная генерация, возникающая при самовозбуждении усилителей различных систем, акустические информационные поля, воздействующие на электродинамические системы различных устройств. Для предотвращения утечки закрытой информации по этим каналам реализуется комплекс организационных мероприятий и технических мер.

К организационным мероприятиям относятся: отключение телефонов и динамиков от линии, изъятие электрических и кварцевых часов, отключение систем селекторной и диспетчерской связи.

К техническим мероприятиям относятся: экранирование устройств, излучающих электромагнитную энергию, контуры заземления в пределах охраняемой территории, установка спец-устройств в телефонах, питание ЭВТ от мотор-генераторов.

Обеспечение режима секретности при выполнении диссертационных и дипломных работ. С точки зрения режима секретности процесс выполнения состоит из этапов:

1) Подготовка к выполнению, утверждение темы и плана работ. – Исполнитель вместе с научным руководителем, определяет степень секретности работы, которая должна быть согласована с РСО предприятия, по тематике которого эта работа выполняется;

2) Непосредственно выполнение работы. – РСО предприятия обязаны установить РС по данной работе, который действует до полного завершения работы, включая этап защиты

3) Защита работы и опубликование результата. – Должны быть согласованы и утверждены официальные оппоненты и организации, которые дают

отзыв на работу. Определяется и утверждается список лиц, которые допускаются на защиту. Приказом руководителя предприятия выделяется спец. аудитория, в которой устанавливается пропускной режим. С целью опубликования результатов работы в открытой печати исполнитель работы обязан представить материалы, предназначенные для опубликования, в экспертную комиссию предприятия, которая определяет возможность опубликования. Если решение положительно, то диссертант (дипломант) должен подготовить документы к опубликованию на основе 2-х документов:

– положение о порядке подготовки материалов, предназначенных для опубликования в открытой печати и в изданиях с грифом «Для служебного пользования»;

– перечень сведений, запрещенных к публикации в открытой печати, передаче по радио и ТВ.

Порядок проведения служебных расследования по фактам разглашения секретных сведений, а также по фактам утраты секретных документов и изделий. Каждый исполнитель, обнаруживший недостачу СД или СИ или узнавший о разглашении секретных сведений, обязан немедленно доложить о случившемся своему непосредственному начальнику и в РСО предприятия.

Администрация предприятия в свою очередь должна: сообщить о происшедшем в вышестоящую организацию и в местный орган ФСБ; принять меры к немедленному розыску утраченных СД и СИ; провести служебное расследование.

Для проведения служебного расследования приказом руководителя предприятия назначается комиссия, в которую входят работники РСО и представители подразделений предприятия. Комиссия должна: взять письменное объяснение у лиц, виновных и причастных к случившемуся; тщательно разобраться в обстоятельствах происшедшего; в заключение своей работы представить акт с соответствующими выводами.

Для определения степени секретности утраченных сведений назначается другая комиссия, работа которой заканчивается предварительным заключением о степени секретности утраченных сведений. Акт 1-ой и заключение 2-ой комиссии, а также письменные объяснения виновных и причастных лиц утверждаются руководителем предприятия и направляются в прокуратуру, органы ФСБ и вышестоящие инстанции.

Правовая ответственность граждан за посягательство на государственные секреты и нарушения требований режима секретности. Правовая ответственность граждан за нарушение требований РС и за посягательство на государственные секреты определяется Уголовным и Административным кодексами.

Уголовная ответственность: за измену Родине в форме шпионажа и выдачу государственной тайны противнику; за разглашение государственной тайны без признаков измены Родине; за утрату СД и СИ, содержащих государственную тайну:

1) Ст. 64а УК РФ (измена Родине в форме шпионажа и выдача государственной тайны противнику): высшая мера; лишение свободы (от 10 до 15 лет); ссылка (5 лет); конфискация имущества.

2) Ст. 64б: гражданин, завербованный и получивший шпионское задание, но не предпринявший никаких шагов во исполнение этого задания и добровольно заявивший о своих связях с иностранной разведкой, уголовной ответственности не подлежит.

3) Иностранные граждане, виновные в шпионаже: Ст. 65 УК РФ (от 7 до 15 лет).

4) Граждане, виновные в разглашении государственной тайны без признаков измены Родине: Ст. 75 УК РФ (от 2 до 5 лет, при существенном ущербе – от 5 до 8 лет).

5) Граждане, виновные в утрате СД и СИ: Ст. 76 УК РФ (от 1 до 3 лет, при существенном ущербе – от 3 до 8 лет).

Тема 2.5. Допуск к государственной тайне

1 Допуск и доступ к информации, составляющей государственную тайну

Допуск – это официальное разрешение руководителя предприятия на право выполнения закрытых работ, на право ознакомления с секретными работами и документами.

К секретным работам и документам могут быть допущены только граждане России, которые по своим деловым, политическим и моральным качествам способны обеспечить сохранность доверенных им тайн.

Допуск лиц, имеющих двойное гражданство, лиц без гражданства, а также лиц из числа иностранных граждан, эмигрантов и реэмигрантов к государственной тайне осуществляется в порядке, устанавливаемом Правительством РФ (Постановление Правительства РФ от 06.02.2010 № 63 «Об утверждении инструкции о порядке допуска должностных лиц и граждан РФ к государственной тайне»).

Допуск должностных лиц и граждан РФ к государственной тайне осуществляется в добровольном порядке.

Допуск граждан к государственной тайне на территории РФ и за ее пределами осуществляется руководителями соответствующих организаций.

Граждане, которым по характеру занимаемой ими должности необходим доступ к государственной тайне, могут быть назначены на эти должности только после оформления допуска по соответствующей форме в установленном порядке.

Допуск должностных лиц и граждан к государственной тайне предусматривает:

– принятие на себя обязательств перед государством по нераспространению доверенных им сведений, составляющих государственную тайну;

– согласие на частичные, временные ограничения их прав;

– письменное согласие на проведение в отношении их полномочными органами проверочных мероприятий;

– определение видов, размеров и порядка предоставления льгот, предусмотренных Законом;

– ознакомление с нормами законодательства РФ о государственной тайне, предусматривающими ответственность за его нарушение;

– принятие решения руководителем органа государственной власти, предприятия, учреждения или организации о допуске оформляемого лица к сведениям, составляющим государственную тайну.

Объем проверочных мероприятий зависит от степени секретности сведений, к которым будет допускаться оформляемое лицо.

Решение об отказе должностному лицу или гражданину в допуске к государственной тайне принимается руководителем органа государственной власти, предприятия, учреждения или организации в индивидуальном порядке с учетом результатов проверочных мероприятий.

Основания для отказа должностному лицу или гражданину в допуске к государственной тайне:

– признание его судом недееспособным, ограниченно дееспособным или рецидивистом, нахождение его под судом или следствием за государственные и иные тяжкие преступления, наличие у него неснятой судимости за эти преступления;

– наличие медицинских противопоказаний для работы с использованием сведений, составляющих государственную тайну, согласно перечню, утверждаемому Министерством здравоохранения РФ;

– постоянное проживание его самого или его близких родственников за границей или оформление указанными лицами документов для выезда на постоянное жительство в другие государства; постоянный контакт с лицами (родственниками) за границей;

– выявление в результате проверочных мероприятий действий оформляемого лица, создающих угрозу безопасности РФ;

– уклонение его от проверочных мероприятий или сообщение заведомо ложных анкетных данных.

Решение об отказе гражданину в допуске к государственной тайне принимается руководителем организации в индивидуальном порядке с учетом результатов проверочных мероприятий.

На каждое лицо, допускаемое к секретным работам и документам, оформляется допуск - официальное разрешение руководителя предприятия на право выполнения закрытых работ, на право ознакомления с секретными работами и документами.

В соответствии со степенями секретности сведений, составляющих государственную тайну, устанавливаются следующие формы допуска:

– первая форма – для граждан, допускаемых к сведениям особой важности;

– вторая форма – для граждан, допускаемых к совершенно секретным сведениям;

– третья форма – для граждан, допускаемых к секретным сведениям.

Наличие у должностных лиц и граждан допуска к сведениям более высокой степени секретности является основанием для доступа их к сведениям более низкой степени секретности.

Проверочные мероприятия, связанные с допуском граждан по первой и второй формам, осуществляются Федеральной службой безопасности РФ и ее территориальными органами (далее именуются – органы безопасности) во взаимодействии с органами, осуществляющими оперативно-розыскную деятельность.

Допуск граждан по третьей форме осуществляется руководителем организации без проведения проверочных мероприятий органами безопасности.

Органы безопасности во взаимодействии с заинтересованными организациями имеют право определять те организации, на которых допуск к секретным сведениям осуществляется только после проведения проверочных мероприятий органами безопасности.

Руководители организаций допускаются к секретным сведениям (по третьей форме) только после проведения проверочных мероприятий органами безопасности.

Граждане, принимаемые на временную работу или не достигшие 18-летнего возраста, как правило, не подлежат оформлению на допуск к особой важности и совершенно секретным сведениям.

Граждане, принимаемые на работу в подразделения по защите государственной тайны, а также для ведения секретного делопроизводства в организациях, где штатным расписанием не предусмотрено наличие таких подразделений, оформляются на допуск по второй форме, если по характеру выполняемой работы им не требуется допуск по первой форме.

Перечень должностей, при назначении на которые граждане обязаны оформлять допуск к сведениям, составляющим государственную тайну, определяется номенклатурой должностей, утверждаемой руководителем организации или его заместителем, занимающимся вопросами защиты государственной тайны, после согласования ее с органом безопасности. В номенклатуру включаются только те должности, по которым допуск граждан к указанным сведениям действительно необходим для выполнения ими должностных (функциональных) обязанностей. Изменения и дополнения в номенклатуру должностей вносятся по мере необходимости, согласовываются и утверждаются в установленном порядке. Номенклатура должностей пересматривается не реже одного раза в 5 лет.

При несоответствии формы допуска гражданина степени секретности сведений, к которым он фактически имеет доступ, форма допуска должна быть изменена.

Снижение формы допуска с первой на вторую (третью) или со второй на третью оформляется распоряжением руководителя организации.

В случае производственной необходимости руководитель, ранее снизивший форму допуска работнику, может восстановить ее без проведения проверочных мероприятий органами безопасности.

О фактах снижения и восстановления ранее имевшейся формы допуска информируется территориальный орган государственной безопасности.

Повышение в случае необходимости формы допуска производится в установленном порядке.

Для должностных лиц и граждан, допущенных к государственной тайне на постоянной основе, устанавливаются льготы:

– процентные надбавки к заработной плате в зависимости от степени секретности сведений, к которым они имеют доступ;

– преимущественное право при прочих равных условиях на оставление на работе при проведении органами государственной власти, предприятиями, учреждениями и организациями организационных и (или) штатных мероприятий.

Взаимные обязательства администрации и оформляемого лица отражаются в трудовом договоре (контракте). Заключение трудового договора (контракта) до окончания проверки компетентными органами не допускается.

Допуск должностного лица или гражданина к государственной тайне может быть прекращен по решению руководителя органа государственной власти, предприятия, учреждения или организации в случаях:

– расторжения с ним трудового договора (контракта) в связи с проведением организационных или штатных мероприятий;

– однократного нарушения им взятых на себя предусмотренных трудовым договором (контрактом) обязательств, связанных с защитой государственной тайны;

– возникновения обстоятельств, являющихся основанием для отказа должностному лицу или гражданину в допуске к государственной тайне.

В случае отстранения гражданина от работы со сведениями, составляющими государственную тайну, оформляется письменное заключение, подготовленное подразделением по защите государственной тайны и структурным подразделением, в котором указанный гражданин работает.

Заключение утверждается руководителем организации. Об этом факте письменно сообщается в орган безопасности.

Прекращение допуска должностного лица или гражданина к государственной тайне является дополнительным основанием для расторжения с ним трудового договора (контракта), если такие условия предусмотрены в трудовом договоре (контракте).

Прекращение допуска к государственной тайне не освобождает должностное лицо или гражданина от взятых ими обязательств по неразглашению сведений, составляющих государственную тайну.

Подразделение по защите государственной тайны организации ведет учет фактической степени осведомленности граждан, работающих в данной организации и допущенных к особой важности, совершенно секретным и секретным сведениям.

Должностное лицо или гражданин, допущенные или ранее допускавшиеся к государственной тайне, могут быть временно ограничены в своих правах. Ограничения могут касаться:

– права выезда за границу на срок, оговоренный в трудовом договоре (контракте) при оформлении допуска гражданина к государственной тайне;

– права на распространение сведений, составляющих государственную тайну, и на использование открытий и изобретений, содержащих такие сведения;

– права на неприкосновенность частной жизни при проведении проверочных мероприятий в период оформления допуска к государственной тайне.

Подготовка материалов на граждан, оформляемых (переоформляемых) на допуск к особой важности, совершенно секретным и секретным сведениям, осуществляется управлениями (отделами) кадров, а в случае их отсутствия – работниками, ведущими кадровую работу в организации (кадровый аппарат). Направлять граждан в подразделения по защите государственной тайны и органы безопасности по вопросам оформления допуска запрещается.

Граждане, оформляемые на допуск к государственной тайне, заполняют анкету, в которой обязаны указывать достоверные данные.

Работники кадрового аппарата в ходе беседы с оформляемым на работу (службу) гражданином сверяют указанные в анкете данные с его личными документами (паспорт, военный билет, трудовая книжка, диплом об образовании, свидетельство о рождении и т. д.), уточняют отдельные вопросы анкеты, выявляют представляющие интерес сведения, не предусмотренные вопросами анкеты, выясняют у гражданина, имел ли он за последний год отношение к секретным работам, документам и изделиям, давал ли он обязательство по неразглашению сведений, составляющих государственную тайну, работал ли (служил) на режимных объектах, запрашивают необходимые справки и документы, знакомят гражданина с содержанием договора (контракта) об оформлении допуска к государственной тайне.

Если в ходе беседы или в анкетных данных выявлены обстоятельства, влияющие на принятие решения о допуске гражданина к государственной тайне, или установлено, что он ранее работал с особой важности или совершенно секретными сведениями, то о результатах беседы работники кадрового аппарата обязаны информировать в устной или письменной форме руководителя подразделения по защите государственной тайны соответствующей организации.

Подразделения по защите государственной тайны:

– разрабатывают рекомендации для кадровых аппаратов по оформлению на работу граждан, подлежащих допуску;

– запрашивают при необходимости из подразделений по защите государственной тайны организаций, где оформляемый гражданин в течение последнего года работал;

– дают оценку первичным материалам, представляемым кадровыми аппаратами на оформляемых (переоформляемых) граждан или получаемым из подразделений по защите государственной тайны с прежних мест работы указанных граждан, в целях определения целесообразности проведения проверочных мероприятий органами безопасности;

– оформляют и хранят учетные материалы по допуску,

– осуществляют контроль за исполнением требований по допуску.

Данные положения Закона описывают одну из основных форм отношений – отношения между государством в лице органов государственной власти, предприятий, учреждений и организаций и должностными лицами, и гражданами, допускаемыми к государственной тайне. Статьи Закона и напрямую затрагивают права и свободы граждан.

Основой допуска является его добровольность на условиях, оговариваемых в трудовом договоре (контракте). Выделение из, безусловно, более широкой категории «граждан» категории «должностных лиц» связано с положениями статьи 1 Закона, в соответствии с которой принцип добровольности рассматривается как бы с двух позиций: для граждан - в качестве условия при поступлении на работу или при привлечении их к работам, связанным с использованием сведений, составляющих государственную тайну, а для должностных лиц – в качестве условия для занятия определенных должностей, статус которых, предполагает ознакомление со сведениями, составляющими государственную тайну.

Положения, касающиеся проведения проверочных мероприятий, согласуются с положениями Закона РФ» Об оперативно-розыскной деятельности». В законе есть существующее положение о том, что до окончания проверочных

мероприятий администрация не имеет права вступать с допускаемым лицом в договорные отношения.

Для должностных лиц и граждан, допускаемых к государственной тайне на постоянной основе, Законом предусмотрены льготы, направленные на стабилизацию контингента допущенных лиц. Для работников структурных подразделений по защите государственной тайны предусмотрены дополнительные льготы, увязанные со стажем их работы в указанных подразделениях. Такая мера способствует уменьшению текучести кадров в режимно-секретных и других органах, непосредственно связанных с защитой государственной тайны. Данная норма реализована постановлением Правительства РФ от 18 сентября 2006 г. № 573 «О предоставлении социальных гарантий гражданам, допущенным к государственной тайне на постоянной основе, и сотрудникам структурных подразделений по защите государственной тайны» (в ред. Постановлений Правительства РФ от 06.06.2008 № 440, от 31.01.2012 № 60.

2 Допуск предприятий, учреждений и организаций к государственной тайне

Допуск предприятий, учреждений и организаций (далее – предприятия) к проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны, регламентируется Положением о лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны (утв. постановлением Правительства РФ от 15 апреля 1995 г. № 333 с изменениями и дополнениями от 23 апреля 1996 г., 30 апреля 1997 г., 29 июля 1998 г., 3 октября 2002 г., 17 декабря 2004 г., 26 января 2007 г., 22 мая 2008 г., 31 марта, 24 сентября 2010 г., 3 ноября 2011 г., 5 мая 2012 г)

Лицензии выдаются на конкретный вид деятельности:

– на допуск предприятий к проведению работ, связанных с использованием сведений, составляющих государственную тайну;

– на право проведения работ, связанных с созданием средств защиты информации;

– на право-осуществление мероприятий и (или) оказания услуг в области защиты государственной тайны.

Лицензия является официальным документом, который разрешает осуществление на определенных условиях конкретного вида деятельности в течение установленного срока, в зависимости от специфики вида деятельности, но не более чем на 5 лет. Действует на всей территории РФ.

Лицензии выдаются на основании результатов специальной экспертизы предприятия, учреждения и организации и государственной аттестации их руководителей, ответственных за защиту сведений, составляющих государственную тайну, расходы, по проведению которых относятся на счет предприятия, учреждения, организации, получающих лицензию.

Органами, уполномоченными на ведение лицензионной деятельности, являются:

– по допуску предприятий к проведению работ, связанных с использованием сведений, составляющих государственную тайну, – Федеральная служба безопасности РФ и ее территориальные органы (на территории РФ), Служба внешней разведки РФ (за рубежом);

– на право проведения работ, связанных с созданием средств защиты информации, – Федеральная служба по техническому и экспортному контролю, Служба внешней разведки РФ, Министерство обороны РФ, Федеральная служба безопасности РФ (в пределах их компетенции);

– на право осуществления мероприятий и (или) оказания услуг в области защиты государственной тайны – Федеральная служба безопасности РФ и

ее территориальные органы, Федеральная служба по техническому и экспортному контролю, Служба внешней разведки РФ (в пределах их компетенции).

Работа органов, уполномоченных на ведение лицензионной деятельности, координируется Межведомственной комиссией по защите государственной тайны.

Для получения лицензии заявитель представляет в соответствующий орган, уполномоченный на ведение лицензионной деятельности, следующие документы:

1) Заявление о выдаче лицензии с указанием: наименования, организационно-правовой формы и местонахождения предприятия; идентификационного номера налогоплательщика; даты уплаты предприятием государственной пошлины за предоставление лицензии; сведений о наличии допуска к государственной тайне у руководителя предприятия; адресов мест осуществления лицензируемого вида деятельности; реквизитов правоустанавливающих документов на объекты недвижимости, необходимые для осуществления заявленного вида деятельности на срок действия лицензии, права на которые зарегистрированы в Едином государственном реестре прав на недвижимое имущество и сделок с ним; вида деятельности, на осуществление которого должна быть выдана лицензия; срока действия лицензии; степени секретности сведений, составляющих государственную тайну, с которыми заявитель предполагает осуществлять работы, подтвержденной органом государственной власти или организацией, наделенными полномочиями по распоряжению указанными сведениями; формы предоставления лицензии (на бумажном носителе или в электронной форме (в форме электронного документа, подписанного электронной подписью)).

2) Копии учредительных документов юридического лица.

3) Копии правоустанавливающих документов на объекты недвижимости, необходимые для осуществления заявленного вида деятельности на срок

действия лицензии, права на которые не зарегистрированы в Едином государственном реестре прав на недвижимое имущество и сделок с ним.

4) Копия договора об оказании услуг (в случае использования заявителем услуг структурного подразделения по защите государственной тайны другой организации).

Орган, уполномоченный на ведение лицензионной деятельности, принимает решение о выдаче или об отказе в выдаче лицензии в течение 30 дней со дня получения заявления со всеми необходимыми документами.

В случае необходимости проведения дополнительной экспертизы предприятия решение принимается в 15-дневный срок после получения заключения экспертизы, но не позднее чем через 60 дней со дня подачи заявления о выдаче лицензии и необходимых для этого документов.

В зависимости от сложности и объема, подлежащих специальной экспертизе материалов руководитель органа, уполномоченного на ведение лицензионной деятельности, может продлить срок принятия решения о выдаче или об отказе в выдаче лицензии до 30 дней.

Лицензии выдаются на основании результатов специальных экспертиз предприятий и государственной аттестации их руководителей, ответственных за защиту сведений, составляющих государственную тайну (руководители предприятий), и при выполнении следующих условий:

1) Соблюдение требований законодательных и иных нормативных актов РФ по обеспечению защиты сведений, составляющих государственную тайну, в процессе выполнения работ, связанных с использованием указанных сведений.

2) Наличие в структуре предприятия подразделения по защите государственной тайны и необходимого числа специально подготовленных сотрудников для работы по защите информации, уровень квалификации которых достаточен для обеспечения защиты государственной тайны.

3) Наличие на предприятии средств защиты информации, имеющих сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности.

В лицензии указываются: наименование органа, выдавшего лицензию; наименование, место нахождения предприятия, адреса мест осуществления лицензируемого вида деятельности (при необходимости), в том числе адреса мест осуществления лицензируемого вида деятельности подразделениями предприятия; идентификационный номер налогоплательщика; вид деятельности, на осуществление которого выдана лицензия; условия осуществления вида деятельности, на который выдана лицензия; степень секретности разрешенных к использованию сведений, составляющих государственную тайну, для лицензии на проведение работ, связанных с использованием сведений, составляющих государственную тайну; срок действия лицензии; регистрационный номер и дата выдачи лицензии.

Срок действия лицензии устанавливается в зависимости от специфики вида деятельности, но не более чем на 5 лет. По просьбе заявителя лицензия может выдаваться на срок менее 5 лет. Срок действия лицензии, выданной предприятию, не может превышать срока действия лицензии предприятия, структурное подразделение, по защите государственной тайны которого оказывает услуги по защите государственной тайны.

Продление срока действия лицензии производится в порядке, установленном для ее получения.

Предприятие может иметь несколько лицензий.

Лицензия подписывается руководителем органа, уполномоченного на ведение лицензионной деятельности, либо лицом, им уполномоченным, и заверяется печатью этого органа. Копия лицензии хранится в органе, уполномоченном на ведение лицензионной деятельности.

В случае изменений условий ведения лицензируемого вида деятельности, изменения степени секретности сведений, с которыми осуществляется

(предполагается осуществлять) деятельность, а также в отношении, которых лицензиат предполагает проводить мероприятия и (или) оказывать услуги, смены организационно-правовой формы или реорганизации лицензиата, изменения его наименования, места нахождения, адресов мест осуществления лицензируемого вида деятельности лицензиат или его правопреемник обязаны в 15-дневный срок подать в орган, уполномоченный на ведение лицензионной деятельности, заявление о переоформлении лицензии в связи с изменением условий деятельности с приложением документов, подтверждающих соответствующие изменения. В указанных случаях орган, уполномоченный на ведение лицензионной деятельности, по результатам рассмотрения заявления и проведения проверки соответствия предприятия лицензионным требованиям и условиям принимает решение о необходимости проведения специальной экспертизы и уведомляет о своем решении заявителя. В случае принятия решения о необходимости проведения специальной экспертизы выдача лицензии производится с учетом ее результатов.

Орган, уполномоченный на ведение лицензионной деятельности, вправе отказать в выдаче лицензии. Письменное уведомление об отказе в выдаче лицензии с указанием причин отказа направляется заявителю в 3-дневный срок после принятия соответствующего решения.

Основанием для отказа в выдаче лицензии является: наличие в документах, представленных заявителем, недостоверной или искаженной информации; отрицательное заключение экспертизы, установившей несоответствие необходимым для осуществления заявленного вида деятельности условиям, отрицательное заключение по результатам государственной аттестации руководителя предприятия.

Специальная экспертиза предприятия проводится путем проверки выполнения требований нормативно-методических документов по режиму секретности, противодействию иностранным техническим разведкам и защите

информации от утечки по техническим каналам, а также соблюдения других условий, необходимых для получения лицензии.

Организация и порядок проведения специальных экспертиз предприятий определяются инструкциями, которые разрабатываются уполномоченными государственными органами и согласовываются с Межведомственной комиссией.

Государственная аттестация руководителей предприятий организуется органами, уполномоченными на ведение лицензионной деятельности, а также министерствами и ведомствами РФ, руководители которых наделены полномочиями по отнесению к государственной тайне сведений в отношении подведомственных им предприятий. Методические рекомендации по организации и проведению государственной аттестации руководителей предприятий разрабатываются межведомственной комиссией.

Органы, уполномоченные на ведение лицензионной деятельности, приостанавливают действие лицензии или аннулируют ее в случае: предоставления лицензиатом соответствующего заявления; обнаружения недостоверных данных в документах, представленных для получения лицензии; нарушения лицензиатом условий действия лицензии; невыполнения лицензиатом предписаний или распоряжений государственных органов или приостановления этими государственными органами деятельности предприятия в соответствии с законодательством РФ; ликвидации предприятия.

Тема 2.6 Защита компьютерной информации

1 Технические каналы утечки компьютерной информации

Защита информации от утечки по техническим каналам – это комплекс организационных, организационно-технических и технических мероприятий, исключающих или ослабляющих бесконтрольный выход конфиденциальной информации за пределы контролируемой зоны.

Постулаты:

1) Безопасных технических средств нет.

2) Источниками образования технических каналов утечки информации являются физические преобразователи.

3) Любой электронный элемент при определенных условиях может стать источником образования канала утечки информации.

4) Любой канал утечки информации может быть обнаружен и локализован: «На каждый яд есть противоядие».

5) Канал утечки информации легче локализовать, чем обнаружить.

В основе утечки лежит неконтролируемый перенос конфиденциальной информации посредством акустических, световых, электромагнитных, радиационных и других полей и материальных объектов.

Причины утечки связаны, как правило, с несовершенством норм по сохранению информации, а также нарушением этих норм (в том числе и несовершенных), отступлением от правил обращения с соответствующими документами, техническими средствами, образцами продукции и другими материалами, содержащими конфиденциальную информацию.

Условия включают различные факторы и обстоятельства, которые складываются в процессе научной, производственной, рекламной, издательской, отчетной, информационной и иной деятельности предприятия (организации) и создают предпосылки для утечки информации. К таким факторам и обстоятельствам могут относиться:

– недостаточное знание работниками предприятия правил защиты информации и непонимание (или недопонимание) необходимости их тщательного соблюдения;

– использование не аттестованных технических средств обработки конфиденциальной информации;

– слабый контроль за соблюдением правил защиты информации правовыми, организационными и инженерно-техническими мерами;

– текучесть кадров, в том числе владеющих сведениями конфиденциального характера.

Таким образом, большая часть причин и условий, создающих предпосылки и возможность утечки конфиденциальной информации, возникает из-за недоработок руководителей предприятий и их сотрудников.

Кроме того, утечке информации способствуют: стихийные бедствия (шторм, ураган, смерч, землетрясение, наводнение); неблагоприятная внешняя среда (гроза, дождь, снег); катастрофы (пожар, взрывы); неисправности, отказы, аварии технических средств и оборудования.

Известно, что информация вообще передается полем или веществом. Это акустическая волна (звук), электромагнитное излучение, либо лист бумаги с текстом. Но ни переданная энергия, ни посланное вещество сами по себе никакого значения не имеют, они служат лишь носителями информации. Человек не рассматривается как носитель информации. Он выступает субъектом отношений или источником.

Основываясь на этом, можно утверждать, что по физической природе возможны следующие средства переноса информации: световые лучи; звуковые волны; электромагнитные волны; материалы и вещества.

Иной возможности для переноса информации в природе не существует. Используя в своих интересах те или иные физические поля, человек создаёт определенную систему передачи информации друг другу. Такие системы при-

нято называть системами связи. Любая система связи (система передачи информации) состоит из источника информации, передатчика, канала передачи информации, приемника и получателя сведений. Однако существуют определенные условия, при которых возможно образование системы передачи информации из одной точки в другую независимо от желания объекта и источника. При этом, естественно, такой канал в явном виде не должен себя проявлять. По аналогии с каналом передачи информации такой канал называют каналом утечки информации. Он также состоит из источника сигнала, физической среды его распространения и приемной аппаратуры на стороне злоумышленника. Движение информации в таком канале осуществляется только в одну сторону – от источника к злоумышленнику.

Структура канала утечки информации: Источник информации →

→ Источник сигнала → Среда → Приёмник → Злоумышленник.

Любые технические средства по своей природе потенциально обладают каналами утечки информации.

Под каналом утечки информации будем понимать физический путь от источника конфиденциальной информации к злоумышленнику, по которому возможна утечка охраняемых сведений. Для возникновения (образования, установления) канала утечки информации необходимы определенные пространственные, энергетические и временные условия, а также соответствующие средства восприятия и фиксации информации на стороне злоумышленника.

Применительно к практике с учетом физической природы образования каналы утечки информации можно квалифицировать на следующие группы:

– визуально-оптические;
– акустические (включая и акустико-преобразовательные);
– электромагнитные (включая магнитные и электрические);
– материально-вещественные (бумага, фото, магнитные носители, производственные отходы различного вида).

Таблица 1 – Вариант взаимосвязи

Способы несанкционированного доступа	**Типы технических каналов утечки информации**			
	Визуально-оптические	**Акустические**	**Электромагнитные (магнитные, электрические)**	**Материально-вещественные**
Подслушивание		+	+	
Визуальное наблюдение	+			
Хищение			+	+
Копирование			+	+
Подделка			+	+
Незаконное подключение		+	+	
Перехват		+	+	
Фотографирование	+			
Итого по виду канала	2	3	6	3

Каждому виду каналов утечки информации свойственны свои специфические особенности. Очевидно, что каждый источник конфиденциальной информации может обладать (или может быть доступен) в той или иной степени какой-то совокупностью каналов утечки информации.

Вариант взаимосвязи способов несанкционированного доступа и объектов источников охраняемой информации и каналов утечки конфиденциальной информации приведен в таблице 1.

Визуально-оптические каналы – это, как правило, непосредственное или удаленное (в том числе и телевизионное) наблюдение. Переносчиком информации выступает свет, испускаемый источником конфиденциальной информации или отраженный от него в водимом, инфракрасном и ультрафиолетовом диапазонах.

Классификация визуально-оптических каналов утечки информации:

1) По природе образования:

– за счёт отражения световой энергии;

– за счёт собственного излучения объектов.

2) По диапазону излучения:

– видимая область;

– ИК-область;

– УФ область.

3) По среде распространения:

– свободное пространство;

– направляющие линии.

Акустические каналы. Для человека слух является вторым по информативности после зрения. Поэтому одним из довольно распространенных каналов утечки информации является акустический канал. В акустическом канале переносчиком информации выступает звук, лежащий в полосе ультра (более 20 000 Гц), слышимого и инфразвукового диапазонов. Диапазон звуковых частот, слышимых человеком, лежит в пределах от 16 до 20 000 Гц, и содержащихся в человеческой речи – от 100 до 6000 Гц.

Когда в воздухе распространяется акустическая волна, частицы воздуха приобретают колебательные движения, передавая колебательную энергию друг другу. Если на пути звука нет препятствия, он распространяется равномерно во все стороны. Если же на пути звуковой волны возникают какие-либо препятствия в виде перегородок, стен, окон, дверей, потолков и т. п., звуковые волны оказывают на них соответствующее давление, приводя их также в колебательный режим. Эти воздействия звуковых волн и являются одной из основных причин образования акустического канала утечки информации.

Различают определенные особенности распространения звуковых волн в зависимости от среды. Это прямое распространение звука в воздушном пространстве, распространение звука в жестких средах (структурный звук). Кроме

того, воздействие звукового давления на элементы конструкции зданий и помещений вызывает их вибрацию.

В свободном воздушном пространстве акустические каналы образуются в помещениях при ведении переговоров в случае открытых дверей, окон, форточек. Кроме того, такие каналы образуются системой воздушной вентиляции помещений. В этом случае образование каналов существенно зависит от геометрических размеров и формы воздуховодов, акустических характеристик фасонных элементов задвижек, воздухораспределителей и подобных элементов.

Под структурным звуком понимают механические колебания в твердых средах. Механические колебания стен, перекрытий или трубопроводов, возникающие в одном месте, передаются на значительные расстояния, почти не затухая. Опасность такого канала утечки состоит в неконтролируемой дальности распространения звука.

Преобразовательный, а точнее, акусто-преобразовательный канал – это изменение тех или иных сигналов электронных схем под воздействием акустических полей. На практике такое явление принято называть микрофонным эффектом.

Электромагнитные каналы. Переносчиком информации являются электромагнитные волны в диапазоне от сверхдлинных с длиной волны 10 000 м. {частоты менее 30 Гц) до субмиллиметровых с длиной волны 1–0,1 мм (частоты от 300 до 3000 ГГц). Каждый из этих видов электромагнитных волн обладает специфическими особенностями распространения, как по дальности, так и в пространстве. Длинные волны, например, распространяются на весьма большие расстояния, миллиметровые – наоборот, на удаление лишь прямой видимости в пределах единиц и десятков километров. Кроме того, различные телефонные и иные провода и кабели связи создают вокруг себя магнитное и электрическое поля, которые также выступают элементами утечки информации за счет наводок на другие провода и элементы аппаратуры в ближней зоне

их расположения.Классификация электромагнитных каналов утечки информации:

1) По природе образования:

– акустопреобразовательные;

– электромагнитные излучения;

– паразитные связи и наводки.

2) По диапазону излучения:

– сверхдлинные волны;

– длинные волны;

– средние волны;

– короткие волны.

– УКВ.

3) По среде распространения:

– безвоздушное пространство;

– воздушное пространство;

– земная среда;

– водная среда;

– направляющие системы.

Материально-вещественными каналами утечки информации выступают самые различные материалы в твердом, жидком и газообразном или корпускулярном (радиоактивные элементы) виде. Очень часто это различные отходы производства, бракованные изделия, черновые материалы и другое.

Классификация материально-вещественных каналов утечки информации:

1) По физическому состоянию:

– твердые массы;

– жидкости;

– газообразные вещества.

2) По физической природе:

– химические;

– биологические;

– радиоактивные.

3) По среде распространения:

– в земле;

– в воде;

– в воздухе.

Очевидно, что каждый источник конфиденциальной информации может обладать в той или иной степени какой-то совокупностью каналов утечки информации.

Защита информации от утечки по техническим каналам в общем плане сводится к следующим действиям:

1) Своевременному определению возможных каналов утечки информации.

2) Определению энергетических характеристик канала утечки на границе контролируемой зоны (территории, кабинета).

3) Оценке возможности средств злоумышленников обеспечить контроль этих каналов.

4) Обеспечению исключения или ослабления энергетики каналов утечки соответствующими организационными, организационно-техническими или техническими мерами и средствами.

2 Защита информации от утечки по техническим каналам

Защита информации от утечки по визуально-оптическому каналу – это комплекс мероприятий, исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет распространения световой энергии.

Человек видит окружающий его мир и предметы за счет отраженного от них света либо за счет их собственного излучения.

Наиболее привычным для человека носителем информации об объектах его интересов является видимое человеческим глазом излучение. С помощью зрительной системы человек получает наибольший (до 90%) объем информации из внешнего мира. Соседние участки видимого спектра – инфракрасный и ультрафиолетовый – также несут существенную информацию об окружающих предметах, но она не может быть воспринята человеческим глазом непосредственно. Для этих целей используются различного рода преобразователи невидимого изображения в видимое – визуализация невидимых изображений.

Окружающий нас мир освещается естественным светом (Солнце, Луна, звезды) и искусственным освещением. Возможность наблюдения объектов определяется величиной падающего потока света (освещенность), отраженного от объекта света (отражающие свойства) и контрастом объекта на фоне окружающих его предметов.

В дневное время, когда освещенность создается светом Солнца, глаз человека обладает наибольшей цветовой и контрастной чувствительностью. В сумерки, когда солнечный диск постепенно уходит за линию горизонта, освещенность падает в зависимости от глубины погружения Солнца. Уменьшение освещенности вызывает ухудшение работы зрения, а, следовательно, сокращение дальности и ухудшение цвето-различия. Эти физические особенности необходимо учитывать при защите информации от утечки по визуально-оптическим каналам.

С целью защиты информации от утечки по визуально-оптическому каналу рекомендуется:

– располагать объекты защиты так, чтобы исключить отражение света в стороны возможного расположения злоумышленника (пространственные ограждения);

– уменьшить отражательные свойства объекта защиты;

– уменьшить освещенность объекта защиты (энергетические ограничения);

– использовать средства преграждения или значительного ослабления отраженного света: ширмы, экраны, шторы, ставни, темные стекла и другие преграждающие среды, преграды;

– применять средства маскирования, имитации и другие с целью защиты и введения в заблуждение злоумышленника;

– использовать средства пассивной и активной защиты источника от неконтролируемого распространения отражательного или излученного света и других излучений;

– осуществлять маскировку объектов защиты, варьируя отражательными свойствами и контрастом фона;

– применять маскирующие средства сокрытия объектов можно в виде аэрозольных завес и маскирующих сеток, красок, укрытий.

В качестве оперативных средств сокрытия находят широкое применение аэрозольные завесы. Это взвешенные в газообразной среде мельчайшие частицы различных веществ, которые в зависимости от размеров и агрегатного сочетания образуют дым, копоть, туман. Они преграждают распространение отраженного от объекта защиты света. Хорошими свето-поглощающими свойствами обладают дымообразующие вещества.

Защита информации от утечки по акустическому каналу – это комплекс мероприятий исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет акустических полей.

Основными мероприятиями в этом виде защиты выступают организационные и организационно-технические меры.

Организационные меры предполагают проведение архитектурно-планировочных пространственных и режимных мероприятий, а организационно-технические – пассивных (звукоизоляция, звукопоглощение) и активных (звукоподавление) мероприятий. Не исключается проведение и технических мероприятий за счет применения специальных защищенных средств ведения конфиденциальных переговоров.

Архитектурно-планировочные меры предусматривают предъявление определенных требований на этапе проектирования зданий и помещений или их реконструкцию и приспособление с целью исключения или ослабления неконтролируемого распространения звуковых полей непосредственно в воздушном пространстве или в строительных конструкциях в виде структурного звука. Эти требования могут предусматривать как выбор расположения помещений в пространственном плане, так и их оборудование необходимыми для акустической безопасности элементами, исключающими прямое или отраженное в сторону возможного расположения злоумышленника распространение звука. В этих целях двери оборудуются тамбурами, окна ориентируются в сторону охраняемой (контролируемой от присутствия посторонних лиц) территории и пр.

Режимные меры предусматривают строгий контроль пребывания в контролируемой зоне сотрудников и посетителей.

Организационно-технические меры предусматривают использование звукопоглощающих средств. Пористые и мягкие материалы типа ваты, ворси-

стые ковры, пенобетон, пориста; сухая штукатурка являются хорошими звукоизолирующими и звукопоглощающими материалами – в них очень много поверхностей раздела между воздухом и твердым телом, что приводит к многократному отражению и поглощению звуковых колебаний.

Для определения эффективности защиты звукоизоляции используются шумомеры. Шумомер –это измерительный прибор, который преобразует колебания звукового давления в показания, соответствующие уровню звукового давления. В сфере акустической защиты речи используются аналоговые шумомеры.

По точности показаний шумомеры подразделяются на четыре класса. Шумомеры нулевого класса служат для лабораторных измерений, первого – для натурных измерений, второго – для общих целей; шумомеры третьего класса используются для ориентированных измерений. На практике для оценки степени защищенности акустических каналов используются шумомеры второго класса, реже – первого.

Измерения акустической защищенности реализуются методом образцового источника звука. Образцовым называется источник с заранее известным уровнем мощности на определенной частоте (частотах).

Выбирается в качестве такого источника магнитофон с записанным на пленку сигналом на частотах 500 Гц и 1000 Гц, модулированным синусоидальным сигналом в 100 – 120 Гц. Имея образцовый источник звука и шумомер, можно определить поглощающие возможности помещения.

Величина акустического давления образцового источника звука известна. Принятый с другой стороны стены сигнал замерен по показаниям шумомера. Разница между показателями и дает коэффициент поглощения.

В зависимости от категории помещения эффективность звукоизоляции должна быть разной. Рекомендуются следующие нормативы поглощения на частотах 500 и 1000 Гц соответственно.

Частота сигнала (Гц)	**Категории помещений (дБ) коэфф. поглощения**		
	1	II	III
500	53	48	43
1000	56	51	46

В тех случаях, когда пассивные меры не обеспечивают необходимого уровня безопасности, используются активные средства. К активным средствам относятся генераторы шума – технические устройства, вырабатывающие шумоподобные электронные сигналы.

Эти сигналы подаются на соответствующие датчики акустического или вибрационного преобразования. Акустические датчики предназначены для создания акустического шума в помещениях, а вибрационные – для маскирующего шума в ограждающих конструкциях. Вибрационные датчики приклеиваются к защищаемым конструкциям, создавая в них звуковые колебания. В качестве примера генераторов шума можно привести систему виброакустического зашумления «Заслон» («Маском»). Система позволяет защитить до 10 условных поверхностей, имеет автоматическое включение вибропреобразователей при появлении акустического сигнала. Эффективная шумовая полоса частот 100–6000 Гц.

Защита информации от утечки по электромагнитным каналам – это комплекс мероприятий, исключающих или ослабляющих возможность неконтролируемого выхода конфиденциальной информации за пределы контролируемой зоны за счет электромагнитных полей побочного характера и наводок.

Известны следующие электромагнитные каналы утечки информации:

– микрофонный эффект элементов электронных схем;

– электромагнитное излучение низкой и высокой частоты;

– возникновение паразитной генерации усилителей различного назначения;

– цепи питания и цепи заземления электронных схем;

– взаимное влияние проводов и линий связи;

- высокочастотное навязывание;
- волоконно-оптические системы.

Для защиты информации от утечки по электромагнитным каналам применяются как общие методы защиты от утечки, так и специфические – именно для этого вида каналов. Кроме того, защитные действия можно классифицировать на конструкторско-технологические решения, ориентированные на исключение возможности возникновения таких каналов, и эксплуатационные, связанные с обеспечением условий использования тех или иных технических средств в условиях производственной и трудовой деятельности.

Конструкторско-технологические мероприятия по локализации возможности образования условий возникновения каналов утечки информации за счет побочных электромагнитных излучений и наводок в технических средствах обработки и передачи информации сводятся к рациональным конструкторско-технологическим решениям, к числу которых относятся: экранирование элементов и узлов аппаратуры; ослабление электромагнитной, емкостной, индуктивной связи между элементами и токонесущими проводами; фильтрация сигналов в цепях питания и заземления и другие меры, связанные с использованием ограничителей, развязывающих цепей, систем взаимной компенсации, ослабителей по ослаблению или уничтожению ПЭМИН.

Экранирование позволяет защитить их от нежелательных воздействий акустических и электромагнитных сигналов и излучений собственных электромагнитных полей, а также ослабить (или исключить) паразитное влияние внешних излучений. Экранирование бывает электростатическое, магнитостатическое и электромагнитное. Электростатическое экранирование заключается в замыкании силовых линий электростатического поля источника на поверхность экрана и отводе наведенных зарядов на массу и на землю. Такое экранирование эффективно для устранения емкостных паразитных связей. Экранирующий эффект максимален на постоянном токе и с повышением частоты снижается. Магнитостатическое экранирование основано на замыкании

силовых линий магнитного поля источника в толще экран, обладающего малым магнитным сопротивлением для постоянного тока и в области низких частот.

С повышением частоты сигнала применяется исключительно электромагнитное экранирование. Действие электромагнитного экрана основано на том, что высокочастотное электромагнитное поле ослабляется им же созданным (благодаря образующимся в толще экран вихревым токам) полем обратного направления.

Если расстояние между экранирующими цепями, проводами, приборами составляет 10% от четверти длины волны, то можно считать, что электромагнитные связи этих цепей осуществляются за счет обычных электрических и магнитных полей, а не в результате переноса энергии в пространстве с помощью электромагнитных волн. Это дает возможность отдельно рассматривать экранирование электрических и магнитных полей, что очень важно, так как на практике преобладает какое-либо одно из полей и подавлять другое нет необходимости.

Заземление и металлизация аппаратуры и ее элементов служат надежным средством отвода наведенных сигналов на землю, ослабления паразитных связей и наводок между отдельными цепями.

Фильтры различного назначения служат для подавления или ослабления сигналов при их возникновении или распространении, а также для защиты систем питания аппаратуры обработки информации. Для этих же целей могут применяться и другие технологические решения.

Эксплуатационные меры ориентированы на выбор мест установки технических средств с учетом особенностей их электромагнитных полей с таким расчетом, чтобы исключить их выход за пределы контролируемой зоны. В этих целях возможно осуществлять экранирование помещений, в которых находятся средства с большим уровнем побочных электромагнитных излучений (ПЭМИ).

Защита информации от утечки по материально-вещественному каналу – это комплекс мероприятий, исключающих или уменьшающих возможность неконтролируемого выхода конфиденциальной информации за пределы контролируемой зоны в виде производственных или промышленных отходов.

В практике производственной и трудовой деятельности отношение к отходам – бросовое. В зависимости от профиля работы предприятия отходы могут быть в виде испорченных накладных, фрагментов исполняемых документов, черновиков, бракованных заготовок деталей, панелей, кожухов и других устройств для разрабатываемых моделей новой техники или изделий.

По виду отходы могут быть твердыми, жидкими и газообразными. И каждый из них может бесконтрольно выходить за пределы охраняемой территории. Жидкости сливаются в канализацию, газы уходят в атмосферу, твердые отходы – просто на свалку. Особенно опасны твердые отходы. Это и документы, и технология, и используемые материалы, и испорченные комплектующие. Все это совершенно достоверные, конкретные данные.

Утечка информации – это ее бесконтрольный выход за пределы организации (территории, здания, помещения) или круга лиц, которым она была доверена. И естественно, что при первом же обнаружении утечки принимаются определенные меры по ее ликвидации.

Для выявления утечки информации необходим систематический контроль возможности образования каналов утечки и оценки их энергетической опасности на границах контролируемой зоны (территории, помещения). Локализация каналов утечки обеспечивается организационными, организационно-техническими и техническими мерами и средствами. Одним из основных направлений противодействия утечке информации по техническим каналам и обеспечения безопасности информационных ресурсов является проведение специальных проверок (СП) по выявлению электронных устройств перехвата

информации и специальных исследований (СИ) на побочные электромагнитные излучения и наводки технических средств обработки информации, аппаратуры и оборудования, в том числе и бытовых приборов.

В заключение следует отметить, что при защите информации от утечки по любому из рассмотренных каналов следует придерживаться следующего порядка действий: выявление возможных каналов утечки; обнаружение реальных каналов; оценка опасности реальных каналов; локализация опасных каналов утечки информации; систематический контроль за наличием каналов и качеством их защиты.