Вопрос 3. Виды информационных рисков и угроз. Утечка и перехват информации.

Виды угроз информационным объектам, информационные риски.

Защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России.

Первая составляющая национальных интересов РФ в информационной сфере (соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны) предполагает;

- повышение эффективности использования информационной инфраструктуры в интересах общественного развития, консолидацию российского общества, духовное возрождение многонационального народа РФ;
- совершенствование системы формирования, сохранения и рационального использования информационных ресурсов, составляющих основу научно-технического и духовного потенциала РФ;
- обеспечение конституционных прав и свобод человека и гражданина свободно искать, получать, передавать, производить и распространять информацию любым законным способом, получать достоверную информацию о состоянии окружающей среды;
- обеспечение конституционных прав и свобод человека и гражданина на личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, на защиту своей чести и своего доброго имени;
- укрепление механизмов правового регулирования отношений в области охраны интеллектуальной собственности, создание условий для соблюдения установленных федеральным законодательством ограничений на доступ к конфиденциальной информации;
- обеспечение свободы массовой информации и запрет цензуры;
- недопущение пропаганды и агитации, которые способствуют разжиганию социальной, расовой, национальной или религиозной ненависти и вражды;

запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия и другой информации, доступ к которой ограничен федеральным законодательством.

Вторая составляющая национальных интересов РФ в информационной сфере (информационное обеспечение государственной политики РФ) предполагает:

- укрепление государственных СМИ, расширение их возможности по своевременному доведению достоверной информации до российских и иностранных граждан;
- ускоренное формирование открытых государственных информационных ресурсов, повышение эффективности их использования.

Третья составляющая национальных интересов РФ в информационной сфере (развитие современных информационных технологий, отечественной индустрии информации) предполагает:

развитие и совершенствование инфраструктуры единого информационного пространства РФ;

- развитие отечественной индустрии информационных услуг и повышение эффективности использования государственных информационных ресурсов;
- развитие производства в РФ конкурентоспособных средств и систем информатизации, телекоммуникации и связи, расширение участия России в международной кооперации производителей этих средств и систем;
- обеспечение государственной поддержки отечественных фундаментальных и прикладных исследований, разработок в сферах информатизации, телекоммуникации и

связи.

Четвертая составляющая национальных интересов РФ в информационной сфере (защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем) предполагает:

- повышение безопасности информационных систем, включая сети связи, прежде всего безопасность первичных сетей связи и ИС федеральных органов государственной власти, органов государственной власти субъектов РФ, финансово-кредитной и банковской сфер, сферы хозяйственной деятельности, а также систем и средств информатизации вооружения и военной техники, систем управления войсками и оружием, экологически опасными и экономически важными производствами;
- ускоренное развитие отечественного производства аппаратных и программных средств защиты информации и методов контроля за их эффективностью;
- обеспечение защиты сведений, составляющих государственную тайну;
- расширение международного сотрудничества РФ в области развития и безопасного использования информационных ресурсов, противодействия угрозе развязывания противоборства в информационной сфере.

По своей общей направленности угрозы информационной безопасности Российской Федерации подразделяются на следующие виды:

- угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России;
- угрозы информационному обеспечению государственной политики Российской Федерации;
- угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;
- угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.

Угрозами конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России могут являться:

- принятие федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации нормативных правовых актов, ущемляющих конституционные права и свободы граждан в области духовной жизни и информационной деятельности;
- создание монополий на формирование, получение и распространение информации в Российской Федерации, в том числе с использованием телекоммуникационных систем;
- противодействие, в том числе со стороны криминальных структур, реализации гражданами своих конституционных прав на личную и семейную тайну, тайну переписки, телефонных переговоров и иных сообщений;
- нерациональное, чрезмерное ограничение доступа к общественно необходимой информации;
- противоправное применение специальных средств воздействия на индивидуальное, групповое и общественное сознание;
- неисполнение федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, органами местного самоуправления, организациями и гражданами требований федерального законодательства, регулирующего отношения в информационной сфере;

- неправомерное ограничение доступа граждан к открытым информационным ресурсам федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, к открытым архивным материалам, к другой открытой социально значимой информации;

- дезорганизация и разрушение системы накопления и сохранения культурных ценностей, включая архивы;

- нарушение конституционных прав и свобод человека и гражданина в области массовой информации;

- вытеснение российских информационных агентств, средств массовой информации с внутреннего информационного рынка и усиление зависимости духовной, экономической и политической сфер общественной жизни России от зарубежных информационных структур;

- девальвация духовных ценностей, пропаганда образцов массовой культуры, основанных на культе насилия, на духовных и нравственных ценностях, противоречащих ценностям, принятым в российском обществе;

- снижение духовного, нравственного и творческого потенциала населения России, что существенно осложнит подготовку трудовых ресурсов для внедрения и использования новейших технологий, в том числе информационных;

- манипулирование информацией (дезинформация, сокрытие или искажение информации).

Угрозами информационному обеспечению государственной политики Российской Федерации могут являться:

- монополизация информационного рынка России, его отдельных секторов отечественными и зарубежными информационными структурами;

- блокирование деятельности государственных средств массовой информации по информированию российской и зарубежной аудитории;

- низкая эффективность информационного обеспечения государственной политики Российской Федерации вследствие дефицита квалифицированных кадров, отсутствия системы формирования и реализации государственной информационной политики.

Угрозами развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов могут являться:

- противодействие доступу Российской Федерации к новейшим информационным технологиям, взаимовыгодному и равноправному участию российских производителей в мировом разделении труда в индустрии информационных услуг, средств информатизации, телекоммуникации и связи, информационных продуктов, а также создание условий для усиления технологической зависимости России в области современных информационных технологий;

- закупка органами государственной власти импортных средств информатизации, телекоммуникации и связи при наличии отечественных аналогов, не уступающих по своим характеристикам зарубежным образцам;

- вытеснение с отечественного рынка российских производителей средств информатизации, телекоммуникации и связи;

- увеличение оттока за рубеж специалистов и правообладателей интеллектуальной собственности.

Угрозами безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России, могут являться:

- противоправные сбор и использование информации;

- нарушения технологии обработки информации;

- внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;
- разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;
- уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;
- воздействие на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации;
- компрометация ключей и средств криптографической защиты информации;
- утечка информации по техническим каналам;
- внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов государственной власти, предприятий, учреждений и организаций независимо от формы собственности;
- уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;
- перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации;
- использование несертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при создании и развитии российской информационной инфраструктуры;
- несанкционированный доступ к информации, находящейся в банках и базах данных;
- нарушение законных ограничений на распространение информации.

Источники угроз информационной безопасности Российской Федерации подразделяются на внешние и внутренние. К внешним источникам относятся:

- деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов Российской Федерации в информационной сфере;
- стремление ряда стран к доминированию и ущемлению интересов России в мировом информационном пространстве, вытеснению ее с внешнего и внутреннего информационных рынков;
- обострение международной конкуренции за обладание информационными технологиями и ресурсами;
- деятельность международных террористических организаций;
- увеличение технологического отрыва ведущих держав мира и наращивание их возможностей по противодействию созданию конкурентоспособных российских информационных технологий;
- деятельность космических, воздушных, морских и наземных технических и иных средств (видов) разведки иностранных государств;
- разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним.

К внутренним источникам относятся:

- критическое состояние отечественных отраслей промышленности;
- неблагоприятная криминогенная обстановка, сопровождающаяся тенденциями сращивания государственных и криминальных структур в информационной сфере, получения криминальными структурами доступа к конфиденциальной информации,

усиления влияния организованной преступности на жизнь общества, снижения степени защищенности законных интересов граждан, общества и государства в информационной сфере;

- недостаточная координация деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации по формированию и реализации единой государственной политики в области обеспечения информационной безопасности Российской Федерации;

- недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика;

- неразвитость институтов гражданского общества и недостаточный государственный контроль за развитием информационного рынка России;

- недостаточное финансирование мероприятий по обеспечению информационной безопасности Российской Федерации;

- недостаточная экономическая мощь государства;

- снижение эффективности системы образования и воспитания, недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности;

- недостаточная активность федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации в информировании общества о своей деятельности, в разъяснении принимаемых решений, в формировании открытых государственных ресурсов и развитии системы доступа к ним граждан;

- отставание России от ведущих стран мира по уровню информатизации федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления, кредитно-финансовой сферы, промышленности, сельского хозяйства, образования, здравоохранения, сферы услуг и быта граждан.

Последствия совершенных противоправных действий могут быть различными:

а) копирование информации (оригинал при этом сохраняется);

б) изменение содержания информации по сравнению с той, которая была раньше;

в) блокирование информации - невозможность ее использования при сохранении информации;

г) уничтожение информации без возможности ее восстановления;

д) нарушение работы компьютерной техники, системы или их сети.

Курушин В.Д. Компьютерные преступления и информационная безопасность / В.Д. Курушин, В.А. Минаев. М.: Новый юрист, 2012. 256 с.

В мире средняя величина ущерба от одной банковской кражи с применением электронных средств оценивается в 10 тыс. долл. Ежегодные потери от компьютерных преступлений в развитых странах превышают 150 млрд. долл. По мнению американских специалистов, снятие систем защиты информации с компьютерных сетей приведет к разорению каждой пятой организации в течение нескольких часов, 40 % средних и 16% крупных компаний потерпят крах через несколько дней, каждый третий банк «лопнет» за несколько часов, половина банков - через 2-3 дня.

Донцов Г.Ю. Экономическая безопасность: Учебное пособие. – Томск: кафедра ТУ, ТУСУР, 2012. – 112 с.

Угрозы информационным системам и информационным ресурсам можно условно разделить на четыре основные группы:

- программные - внедрение «вирусов», аппаратных и программных закладок; уничтожение и модификация данных в информационных системах;

- технические, в т.ч. радиоэлектронные, - перехват информации в линиях связи; радиоэлектронное подавление сигнала в линиях связи и системах управления;

- физические - уничтожение средств обработки и носителей информации; хищение носителей, а также аппаратных или программных парольных ключей;

- информационные - нарушение регламентов информационного обмена; незаконные сбор и использование информации; несанкционированный доступ к информационным ресурсам; незаконное копирование данных в информационных системах; дезинформация, сокрытие или искажение информации; хищение информации из баз данных.

Все воздействующие на информационную систему рискообразующие факторы на различных предприятиях можно разделить:

1. По направленности на:

- внешние, осуществляются из-за пределов информационной системы предприятия в процессе её обычного функционирования;

- внутренние, возникают в самой информационной системе в связи с появлением нарушений взаимосвязей отдельных подсистем;

2. По целенаправленности на:

- умышленное воздействие самих работников, занятых в обслуживании информационной системы, а также третьих лиц на отдельные подсистемы;

- случайное воздействие, возникающее не зависимо от времени и места, а также воли участников процесса;

3. По источнику воздействия на:

- антропогенное, обусловленное различными видами действий человека или группы лиц;

- техногенное, обусловленное техническими сбоями, авариями и катастрофами;

- природно-климатическое, обусловленное климатическими отрицательными воздействиями;

4. По силе воздействия на:

- сильные, наносящие значительный объем ущерба отдельным подсистемам и всей информационной системе;

- средние, наносящие средний объем ущерба отдельным подсистемам и всей информационной системе;

- слабые, не наносящие или наносящие незначительный объем ущерба отдельным подсистемам и всей информационной системе;

5. По длительности воздействия на:

- краткосрочные в пределах нескольких секунд или часов;

- длительные в течении дней, месяцев и лет (постоянные);

6. По частоте воздействия на:

- однократные и в дальнейшем не повторяющиеся;

- периодические повторяются через какой-то промежуток времени;

7. По объему нанесенного ущерба;

- частичное уничтожение;

- полное уничтожение.

8. По виду воздействия на:

- ресурсное, когда нарушается материально-техническое обеспечение, технические дефекты, моральное устаревание и несовместимость используемой в информационной системы техники и другое;

- технологическое, обусловлено несоблюдением производственной технологии и не настроенностью технологии информационной системы;

- программно-сетевое, вызывается дефектами сети и программного обеспечения, проникновением вирусов и другими.

На подсистемы информационной системы воздействуют различные дестабилизирующие факторы, которые можно разделить на внутренние, присущие самим

объектам уязвимости, и внешние, обусловленные средой, в которой эти объекты функционируют.

Рассматривая внешние воздействия на информационную систему предприятия, следует указать на отнесение к ним всех форм и видов различных факторов внешней среды предприятия, возникающие в процессе производственно-хозяйственной деятельности: поставщики, потребители органы местной власти, налоговые органы и иные. Внешние воздействия необходимо учитывать и максимально регламентировать для предупреждения негативных последствий.

Внешними дестабилизирующими факторами, создающими угрозу безопасности функционирования перечисленных объектов, уязвимости информационной системы являются:

ошибки оперативного и обслуживающего персонала в процессе эксплуатации информационной системы;

искажения в каналах телекоммуникации информации, поступающей от внешних источников и передаваемой потребителям, а также недопустимые изменения характеристик потоков информации;

сбои и отказы аппаратуры на всех этапах ее использования;

изменения состава и конфигурации информационной системы за пределы, проверенные при испытаниях или сертификации.

Внутренними источниками угроз безопасности функционирования сложных информационных систем являются:

системные ошибки при постановке целей и задач проектирования информационной системы, формулировке требований к функциям и характеристикам решения задач, определении условий и параметров внешней среды, в которой предстоит применять информационную систему;

алгоритмические ошибки проектирования при непосредственной алгоритмизации функций программных средств и баз данных, при определении структуры и взаимодействия компонент комплексов программ, а также при использовании информации баз данных;

ошибки программирования в текстах программ и описаниях данных, а также в исходной и результирующей документации на компоненты информационной системы;

недостаточная эффективность используемых методов и средств оперативной защиты программ и данных и обеспечения безопасности функционирования информационной системы в условиях случайных негативных воздействий.

Бодров О.А., Медведев Р.Е. Предметно-ориентированные экономические информационные системы. - М.: Горячая линия - Телеком, 2013. - 244 с.

Рассмотрим наиболее распространенные угрозы, которым подвержены организации. Знание возможных угроз, а также уязвимых мест защиты, которые эти угрозы обычно эксплуатируют, необходимо для того, чтобы выбирать наиболее экономичные средства обеспечения безопасности.

Таблица 1. Системная классификация угроз безопасности информации

Параметры классификации	Значение параметров	Содержание параметров
1. Виды угроз безопасности	1.1. физическая целостность 1.2. конфиденциальность 1.3. отношение к праву собственности 1.4. логическая структура	1.1. уничтожение, хищение, искажение 1.2. несанкционированное получение информации 1.3. присваивание, отчуждение по праву собственности 1.4. искажение логической структуры
2. Природа	2.1. случайные характер	2.1. сбои, ошибки

происхождения угроз безопасности	2.2. преднамеренный характер	2.2. действия злоумышленника
3. Предпосылки появления угроз безопасности	3.1. объективные 3.2. субъективные	3.1. количество и качество недостающих элементов в системе защиты 3.2.действия промышленного шпионажа, конкурентов, разведки
4. Источники угроз	4.1. люди (человеческий фактор) 4.2. технические устройства 4.3. модели, алгоритмы, программы 4.4. технологические сферы обработки информации 4.5. состояние внешней среды	4.1. пользователи информацией, собственный персонал и сторонний злоумышленник 4.2. все виды технических систем связи с приемом, обработкой, хранением, передачей, выдачей информации 4.3. общего пользования, прикладные, специальные, вспомогательные 4.4. ручная, внутримашинная, сетевая, интерактивная схема обработки информации 4.5. всегда присуще и может оказать негативное влияние

Критичные ресурсы обычно относятся к одной из следующих категорий:
- персонал,
- информационная инфраструктура,
- физическая инфраструктура.

Информационная инфраструктура включает в себя следующие элементы:
- компьютеры,
- программы и данные,
- информационные сервисы внешних организаций,
- документацию.

Угрозы, исходящие от окружающей среды, к сожалению, отличаются большим разнообразием.[1]

Целостность информации - свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).

Уязвимость информации - подверженность информации воздействию различных дестабилизирующих факторов, которые могут привести к нарушению ее конфиденциальности, целостности, доступности, или неправомерному ее тиражированию.

Угрозы информационной безопасности делятся на два основных типа - это естественные и искусственные угрозы.

К естественным угрозам относятся пожары, наводнения, ураганы, удары молний и другие стихийные бедствия и явления, которые не зависят от человека. Наиболее частыми среди этих угроз являются пожары. Для обеспечения безопасности информации, необходимым условием является оборудование помещений, в которых находятся элементы системы (носители цифровых данных, серверы, архивы и пр.), противопожарными датчиками, назначение ответственных за противопожарную безопасность и наличие средств пожаротушения. Соблюдение всех этих правил позволит свести к минимуму угрозу потери

[1] Галатенко В. Информационная безопасность. - М.: Фобос, 2009. - С. 22.

информации от пожара.

Несмотря на относительную устойчивость жестких носителей информации к воздействию окружающей среды, при их хранении необходимо избегать воздействия прямых солнечных лучей, эксплуатации и хранения вблизи отопительных систем и источников влаги.

Причинами потери информации при записи и воспроизведении являются пыль, жировые пятна и царапины на диске-оригинале. Поэтому необходимо хранить диск в чистоте и не касаться руками его поверхности.

Если помещения с носителями ценной информации располагаются в непосредственной близости от водоемов, то они подвержены угрозе потери информации вследствие наводнения. Единственное что можно предпринять в данной ситуации - это исключить хранение носителей информации на первых этажах здания, которые подвержены затоплению.

Преднамеренные угрозы - угрозы, связанные со злым умыслом преднамеренного физического разрушения, впоследствии выхода из строя системы. К преднамеренным угрозам относятся внутренние и внешние атаки. Вопреки распространенному мнению, крупные компании несут многомиллионные потери зачастую не от хакерских атак, а по вине своих же собственных сотрудников. Современная история знает массу примеров преднамеренных внутренних угроз информации - это проделки конкурирующих организаций, которые внедряют или вербуют агентов для последующей дезорганизации конкурента, месть сотрудников, которые недовольны заработной платой или статусом в фирме и прочее. Для того чтобы риск таких случаев был минимален, необходимо, чтобы каждый сотрудник организации соответствовал, так называемому, «статусу благонадежности».

К внешним преднамеренным угрозам можно отнести угрозы хакерских атак. Если информационная система связана с глобальной сетью интернет, то для предотвращения хакерских атак необходимо использовать межсетевой экран (так называемый firewall), который может быть, как встроен в оборудование, так и реализован программно.

К основным искусственным угрозам относятся:

1. Непреднамеренные ошибки пользователей, операторов, системных администраторов и других лиц, обслуживающих информационные системы.
2. Кражи и подлоги.
3. Несанкционированный доступ к информации.
4. Несанкционированное изменение данных.

Рассмотрим подробнее искусственные угрозы информационной безопасности.

1. Самыми частыми и самыми опасными (с точки зрения размера ущерба) являются непреднамеренные ошибки пользователей, операторов, системных администраторов и других лиц, обслуживающих информационные системы. Иногда такие ошибки являются угрозами (неправильно введенные данные, ошибка в программе, вызвавшая крах системы), иногда они создают слабости, которыми могут воспользоваться злоумышленники (таковы обычно ошибки администрирования). 65% потерь - следствие непреднамеренных ошибок. Пожары и наводнения можно считать пустяками по сравнению с безграмотностью и расхлябанностью.

2. На втором месте по размерам ущерба располагаются кражи и подлоги. В результате подобных противоправных действий с использованием персональных компьютеров российским организациям ежегодно наносится суммарный ущерб в размере на десятки миллиардов рублей. Можно предположить, что подлинный ущерб намного больше, поскольку одни организации по понятным причинам скрывают такие инциденты, другим неизвестен подлинный масштаб нанесенного ущерба. Весьма опасны так называемые обиженные сотрудники - нынешние и бывшие.

3. Безопасность любого ресурса - складывается из обеспечения трех его характеристик:

1) конфиденциальность компонента системы заключается в том, что он доступен только тем субъектам доступа (пользователям, программам, процессам), которым предоставлены на то соответствующие полномочия;

2) целостность компонента предполагает, что он может быть модифицирован только субъектом, имеющим для этого соответствующие права. Целостность является гарантией корректности (неизменности, работоспособности) компонента в любой момент времени;

3) доступность компонента означает, что имеющий соответствующие полномочия субъект может в любое время без особых проблем получить доступ к необходимому компоненту системы (ресурсу).

Формы реализации угроз информационной безопасности предприятия разнообразны по своему характеру и содержанию, что объективно затрудняет процесс противодействия им. При этом сотрудники предприятия могут действовать как по собственной инициативе, так и под влиянием сторонних для предприятия третьих лиц. Рассмотрим основные формы реализации угроз информационной безопасности:

1) перехват конфиденциальной информации, в результате которого у субъекта угрозы оказывается ее дубликат. Перехват информации может осуществляться с использованием разнообразных методов - путем простого подслушивания разговоров коллег по работе, использования технических средств (подслушивающих устройств), копирования конфиденциальных документов или электронных баз данных;

2) хищение конфиденциальной информации, в результате которого субъект угрозы одновременно решает две задачи - приобретает соответствующие сведения и лишает их предприятие. Специфика рассматриваемой угрозы заключается в том, что объектом хищения может стать не только конфиденциальная, но и вполне открытая информация, необходимая ее собственнику для нормального функционирования;

3) повреждение или уничтожение информации, в результате которого субъектом угрозы достигается лишь задача нанесения ущерба предприятию. Причиной сознательного уничтожения информации, как правило, являются соображения личной мести работодателю;

4) искажение нелояльным сотрудником конфиденциальной информации, в результате которого специалисты предприятия - объекта угрозы могут принять изначально ошибочное управленческое решение.

Итак, наиболее распространенной причиной реализации угроз информационной безопасности российских работодателей является безответственность их персонала. Она проявляется в нарушении сотрудниками действующих на предприятии требований по обеспечению информационной безопасности, что приводит к утечке конфиденциальных сведений в самых различных формах.

Так, на 65% всех предприятий не контролируется внос и вынос сотрудниками с территории предприятия бумажных документов, дисков, электронных накопителей и других носителей информации, а также видео- и фотосъемочной аппаратуры. В 33,5% всех случаев на предприятиях помещения, где расположены компьютеры, не защищены от несанкционированного доступа. На 55% предприятий у сотрудников при увольнении не берется расписка о неразглашении конфиденциальной информации.

На 55% всех предприятий на предприятии не назначено лицо, ответственное за учет работников, имеющих доступ к сведениям, содержащим информацию, составляющую коммерческую тайну, которое обеспечивает хранение документации, выдачу ее работникам под роспись и контроль над своевременным возвратом указанной документации на хранение.

На 47,5% всех предприятий отсутствуют специально организованные места приема посетителей.

На 3/4 предприятий были зафиксированы случаи разглашения информации, составляющей коммерческую тайну, при движении персонала (приеме, перемещении, увольнении).

Западные специалисты по обеспечению экономической безопасности считают, что сохранность конфиденциальной информации на 80% зависит от правильного подбора, расстановки и воспитания персонала <4>.

См.: Ищейнов В.Я., Мецатунян М.В. Защита конфиденциальной информации: Учеб. пособие. М.: ФОРУМ, 2009. С. 32.

Правонарушения в сфере компьютерной информации могут совершаться в форме:

- махинаций путем компьютерного манипулирования системой обработки данных в целях получения финансовой выгоды;
- компьютерного шпионажа и кражи программного обеспечения;
- компьютерных диверсий;
- кражи услуг (времени), неправомерного использования систем обработки данных;
- неправомерного доступа к системам обработки данных и «взламывания» их;
- традиционных преступлений в сфере бизнеса (экономики), совершаемых с помощью систем обработки данных.

Совершают компьютерные преступления, как правило, высококвалифицированные системные и банковские программисты, специалисты в области телекоммуникационных систем. Нешуточную угрозу информационным ресурсам представляют ***хакеры*** и ***крэкеры,*** проникающие в компьютерные системы и сети путем взлома программного обеспечения защиты. Крэкеры, кроме того, могут стереть или изменить данные в информационном банке в соответствии со своими интересами. За последние десятилетия в странах бывшего СССР появилась мощная генерация высокоподготовленных потенциальных хакеров, работавших в организациях и ведомствах, занимавшихся информационным пиратством на государственном уровне для использования полученной с Запада информации в военных и экономических интересах.

Потенциальным объектом может служить любая информация, заложенная в ЭВМ, проходящая по вычислительным сетям или находящаяся на носителях ЭВМ и способная принести прибыль хакеру или его работодателю. К данной информации относятся практически все сведения, составляющие коммерческую тайну фирм, начиная от разработок и «ноу-хау» и заканчивая платежными ведомостями, по которым легко «вычислить» оборот фирмы, количество сотрудников и т.д. Особо ценной является информация по банковским сделкам и кредитам, проводимая по электронной почте, а также сделки на бирже. Большой интерес представляют для хакеров программные продукты, оценивающиеся на современном рынке в тысячи, а то и в миллионы долларов.

Крэкеры - «компьютерные террористы» – занимаются порчей программ или информации с помощью вирусов - специальных программ, обеспечивающих уничтожение информации или сбои в работе системы. Создание «вирусных» программ - дело весьма прибыльное, так как некоторые фирмы-производители используют вирусы для защиты своих программных продуктов от несанкционированного копирования.

Для многих фирм получение информации с помощью внедрения к конкурентам хакера-программиста - дело наиболее простое и прибыльное. Внедрять соперникам спецтехнику, постоянно контролировать их офис на излучение с помощью специальной аппаратуры - дело дорогостоящее и опасное. К тому же фирма-конкурент при обнаружении технических средств может в ответ затеять игру, давая ложную информацию. Поэтому свой хакер-программист в «стане врага» - наиболее надежный способ борьбы с конкурентами.

Донцов Г.Ю. Экономическая безопасность: Учебное пособие. – Томск: кафедра ТУ, ТУСУР, 2012. – 112 с.

Несанкционированный доступ, утечка и перехват информации по техническим каналам утечки информации и способы противодействия.

Несанкционированный доступ к информации бывает:

1) косвенным - без физического доступа к элементам сети;

2) прямым - с физическим доступом к элементам сети (с изменением их или без изменения).

Таблица 2. Классификация структуры каналов несанкционированного получения информации

Зависимость от доступа к элементам системы	Отношение к обработке информации	
	Проявляющиеся без относительно к обработке	Проявляющиеся в процессе обработки
Не требует доступа к элементам системы	1 класс: общедоступные постоянные данные	2 класс: общедоступные функциональные связи и схемы
Требует доступ к элементам системы без их изменения	3 класс: информация узкодоступного характера, получение информации не оставляет следов	4 класс: узко доступная информация, связанная с функциональными и структурными схемами
Действие связанные с доступом к элементам системы, приводящие к их изменению	5 класс: специальные сведения и данные получение, которых требует оставление следов.	6 класс: специальные сведения и процессы обработки, связанные с функциональными и структурными схемами.

В настоящее время существуют следующие пути несанкционированного получения информации (каналы утечки информации):

- применение подслушивающих устройств;
- дистанционное фотографирование;
- перехват электромагнитных излучений;
- хищение носителей информации и производственных отходов;
- считывание данных в массивах других пользователей;
- копирование носителей информации;
- несанкционированное использование терминалов;
- маскировка под зарегистрированного пользователя с помощью хищения паролей и других реквизитов разграничения доступа;
- использование программных ловушек;
- получение защищаемых данных с помощью серии разрешенных запросов;
- использование недостатков языков программирования и операционных систем;
- преднамеренное включение в библиотеки программ специальных блоков типа «троянских коней»;
- незаконное подключение к аппаратуре или линиям связи вычислительной системы;
- злоумышленный вывод из строя механизмов защиты.

Канал утечки информации - это совокупность источников информации, материального носителя или среды распространения несущего эту информацию сигнала и средства выделения информации из сигнала или носителя.

Может быть полезным следующий обобщенный перечень официальных каналов утечки информации, в который входят:

- публичные лекции по научно-технической тематике, чтение лекций на различных курсах;
- течка кадров и прохождение студентами практики на предприятии;

- передача информации в процессе общения и обмена опытом с партнерами;
- демонстрация научно-технических разработок и усовершенствований;
- демонстрация действующих объектов научно-технических достижений (оборудования, изделий, технологий) на предприятиях;
- все виды рекламы продукции в форме печатных произведений - брошюр, пристендовой литературы для выставок и ярмарок;
- обмен научно-технической литературой (книгами, журналами), осуществляемый библиотеками и отдельными научными учреждениями России с библиотеками и другими организациями;
- передача технической документации (в т.ч. товаросопроводительной) фирмам (организациям), включая проектирование и строительство объектов, а также продажу лицензий;
- передача сведений представителям других фирм в процессе переговоров или при заключении соглашений;
- проведение совместных разработок (проектов, экспериментов) в рамках осуществления научно-технических связей.

Каждый из вышеуказанных каналов характеризуется весьма значительными объемами утечки информации. Помимо рассмотренных открытых каналов утечки информации могут существовать еще агентурный и технологический, организация работы по перекрытию которых носит сугубо специфический характер.

Относительно государственных секретов эту работу выполняют специальные органы государства, режимно-секретные подразделения предприятий. Что же касается коммерческой тайны, то организация ее защиты от утечки в комплексе по всем каналам, включая агентурный и технологический, целиком и полностью ложится на предприятие. Как свидетельствует зарубежный опыт, для этого в зависимости от объема и сложности решаемых на данном участке задач может быть эффективным создание специального подразделения, например, службы безопасности.

4. Уничтожение информации называется санацией. Имеется три метода уничтожения: перезапись, размагничивание и разрушение носителя. Если речь идет о данных на магнитных носителях, то для санации вполне достаточно тройной перезаписи случайными последовательностями бит. После этого даже с помощью специальной аппаратуры прочитать первоначальную информацию невозможно.[2]

После определения сведений, составляющих коммерческую или государственную тайну предприятия, предстоит разработать и осуществить мероприятия по обеспечению их сохранности. Сущность защитных мероприятий сводится к перекрытию возможных каналов утечки защищаемой информации, которые появляются в силу объективно складывающихся условий ее распространения и возникающей у конкурентов заинтересованности в ее получении.

При этом особое значение придается НИОКР, результаты которых открывают новые направления в развитии науки и техники и могут быть использованы в создании принципиально новых изделий и технологических процессов в различных отраслях промышленности. Именно они первоисточник радикального обновления и расширения номенклатуры выпускаемой продукции.

Кроме того, возникновение конкуренции между предприятиями внутри государства породит и между ними подобные взаимные устремления. Для построения системы защиты коммерческой тайны предприятия очень важно определить источник и соответствующие им возможные официальные каналы утечки защищаемой информации. На каждом конкретном

[2] Журавленко Н.И., Кадулин В.Е., Борзунов К.К. Основы информационной безопасности: Учебное пособие. - М.: МосУ МВД России, 2011. - С. 31.

предприятии перечень таких каналов носит индивидуальный характер, что определяется спецификой его производственной, научно-технической, коммерческой и иной деятельности и степенью развития связей с деловыми партнерами внутри государства и за рубежом.

Утечка информации - это несанкционированный выход ее за пределы круга лиц, которым эта информация доверена. Иными словами, это неправомерное завладение злоумышленником этой информацией и получение тем самым возможности ее использования в собственных интересах. Основными формами утечки информации являются ее разглашение, раскрытие и распространение.

Источник утечки защищаемой информации - это любой носитель конфиденциальной информации, к которому сумел получить несанкционированный доступ злоумышленник, располагающий необходимыми знаниями и техническими средствами для снятия информации, ее расшифровки и использования в своих целях в ущерб интересам.

Канал утечки защищаемой информации - это социальное явление, отражающее противостояние сотрудника (защитника информации) и злоумышленников.

Наиболее распространенными причинами, факторами и явлениями, приводящими к утечке информации в сфере деятельности, являются:

- несовершенство нормативных актов, регламентирующих защиту информации в этой области;
- недостаточность наличных сил и средств для перекрытия каналов утечки информации;
- нарушение лицами, допущенными к работе с защищаемой информацией, установленных правил ее защиты.

Указанные причины приводят к утечке информации в том случае, если этому способствуют соответствующие субъективные или объективные условия. К субъективным условиям относятся:

- незнание исполнителями нормативных актов по вопросам защиты информации;
- слабая воспитательно-профилактическая работа с сотрудниками;
- недостаточное внимание со стороны руководителей к вопросам обеспечения конфиденциальности информации;
- слабый контроль за состоянием системы обеспечения конфиденциальности информации;
- принятие руководителями решений без учета требований обеспечения конфиденциальности информации.

К объективным условиям относятся:

- несовершенство или отсутствие нормативных актов, регламентирующих правила защиты информации по отдельным вопросам деятельности;
- несовершенство перечня сведений, подлежащих защите;
- текучесть кадров;
- несоответствие условий работы требованиям, необходимым для осуществления защищенной информационной деятельности.

Указанные причины и условия создают предпосылки и возможности для образования канала утечки защищаемой информации.

По отношению к информационной деятельности методы добывания защищаемой информации достаточно условно можно разделить на агентурные и технические. Условность состоит в том, что добывание информации агентурными методами осуществляется с использованием технических средств, а технические средства применяются людьми. Поэтому отличия заключаются только в преобладании человеческого или технического фактора.

Наиболее эффективным способом добывания защищаемой информации в сфере деятельности, используемым злоумышленниками, является агентурный способ, который базируется на использовании тайных агентов.

Опасность агентурного способа добывания информации заключается в том, что агент имеет непосредственный доступ к конфиденциальной информации. Он находится среди тех, кто работает с секретными сведениями и осуществляет их защиту.

Для добывания защищаемой информации через агентуру используются следующие методы: доступ к конфиденциальной информации, выведывание, наблюдение.

Используя доступ по роду деятельности к работам и документам, носящим конфиденциальный характер, агент в целях сбора интересующей его информации может ее запомнить, делать выписки из документов, копировать документы от руки или на ксероксе, сфотографировать и т.д.

При выведывании информации расчет делается на людскую болтливость, жажду известности или утрату.

Наблюдение может быть физическим, электронным или комплексным, т.е. сочетающим в себе элементы того и другого. Физическое наблюдение осуществляется непосредственно агентом или иным лицом, заинтересованным в получении защищаемой информации. Электронное наблюдение основано на применении специальных технических средств, оно может сопровождаться фиксацией полученной аудио- и видеоинформации.

Технические способы добывания информации направлены на выявление и фиксирование данных с помощью технических средств. Многообразие видов носителей информации породило множество технических способов добывания информации. При классификации по физической природе носителя информации технические способы добывания информации подразделяются на следующие виды: оптические, радиоэлектронные, акустические, химические, радиационные, магнитометрические, компьютерные.

Под техническим каналом утечки информации понимают совокупность источника информации, линий связи (физической среды), по которой распространяется информационный сигнал, шумов, препятствующих передаче сигнала в линиях связи, и технических и программных средств перехвата информации. Источниками информации могут быть технические и программные средства информационно - коммуникационных технологий (ИКТ), непосредственно голосовой аппарат человека, излучатели систем звукоусиления, печатающие устройства, радиосистемы различного назначения и т.п.

Наиболее распространенные из технических каналов утечки информации можно условно разделить на три основные группы:

- 1 группа - акустический (распространение звука в воздухе) и виброакустический (распространение звука в твёрдой среде) каналы утечки акустической (чаще всего речевой) информации;

- 2 группа - каналы утечки акустической (речевой) информации за счёт акустоэлектрических преобразований;

- 3 группа - каналы утечки информации (акустической, в форме текстовых и цифровых данных и т.п) за счёт побочных электромагнитных излучений и наводок (ПЭМИН). Рассмотрим первую группу каналов утечки - акустический и виброакустический (рис. 7.4.1).

Рис. 7.4.1. Акустический и виброакустический каналы утечки

Звук, распространяясь от источника в помещении, достигает ограждающих конструкций. При взаимодействии с ними часть звуковой волны отражается (сиреневые стрелки), часть поглощается (желтые стрелки), а часть звуковой волны, показанная красными стрелками, во-первых, «проходит сквозь» ограждающую конструкцию (переизлучается), во-вторых, возбуждает в ней вибрацию и, соответственно, становится доступна для ведения речевой разведки. На рис. 7.4.2 показана степень опасности различных конструкций с точки зрения утечки речевой информации (чем больше стрелок - тем опаснее).

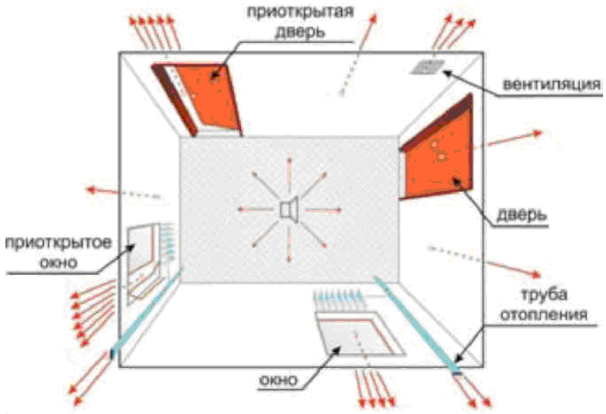

Рис. 7.4.2. Степень опасности различных конструкций с точки зрения утечки речевой информации

Наиболее опасным конструктивным элементом являются окна. На поверхности лежит возможность подслушивания, если окно открыто. Но и в случае, когда оно закрыто, проблема не снимается. Перехватить информацию в таких случаях можно, например, с помощью бесконтактного акустооптического («лазерного») микрофона (рис. 7.4.3).

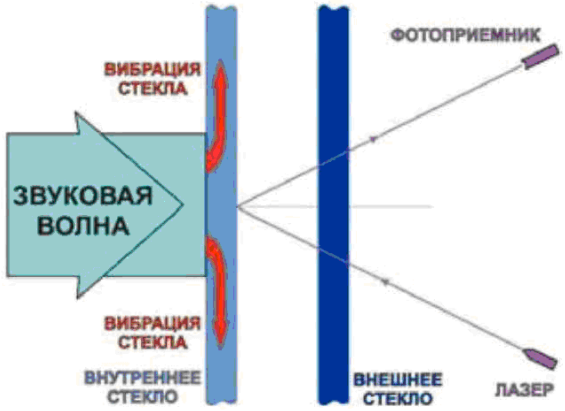

Рис. 7.4.3. Перехват информации с помощью бесконтактного акустооптического («лазерного») микрофона

Луч лазера направляют на стекло, которое в такт механическим колебаниям модулирует его параметры. Отраженный луч принимают и соответствующим образом обрабатывают, восстанавливая речь. Съём информации производится с внутреннего стекла, и теоретически существует возможность «снимать» акустическую информацию с предметов внутри помещения.

Со стен и перекрытий «снять» акустическую информацию можно с помощью стетоскопа (рис. 7.4.4). Это устройство, которое не работает как обычный микрофон, т. е. не воспринимает колебаний воздуха и чувствительно к колебаниям твердых конструкций.

Факт использования стетоскопа в смежном помещения практически невозможно установить.

С помощью стетоскопа можно перехватить акустическую информацию не только через стену, но и с труб отопления, вентиляционных каналов, а значит не только из соседнего помещения.

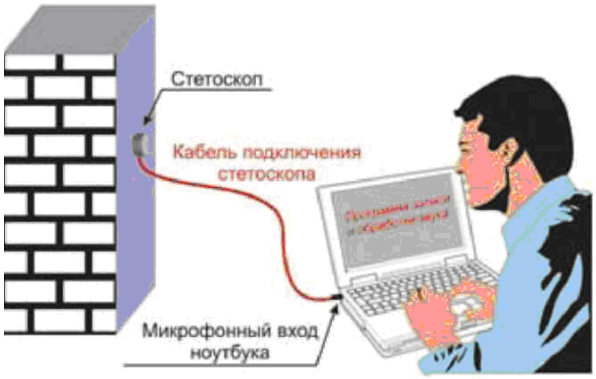

Рис. 7.4.4. Перехват акустической информации со стен и перекрытий можно с помощью стетоскопа

Перейдем ко второй группе каналов утечки: акустоэлектрическим преобразованиям. Уже из названия понятно, что речь пойдет о преобразовании акустического сигнала (наша речь) в электрический - как же это возможно?

Звуковая волна вызывает вибрацию этого молоточка, а он возбуждает электрический ток в звонковой цепи телефона.

Снять такой сигнал с телефонной линии достаточно просто.

Аналогичные эффекты, сопровождающиеся преобразованием звука в электрический сигнал, наблюдаются и в современных устройствах связи и информатизации, оснащенных

пьезоэлектрическими приборами, микрофонами, динамиками и т. д.

В результате такой канал утечки информации могут создавать практически все электрические и электронные устройства, используемые в офисных и жилых помещениях.

Третья группа - каналы утечки информации за счет побочных электромагнитных излучений и наводок.

Дело в том, что все современные системы связи и обработки данных строятся на базе электронных устройств, при работе которых возникает электромагнитное излучение. Часть этого излучения информативна по происхождению. Это излучение распространяется подобно радиосигналу вещательных станций за пределы помещения (здания). Кроме того, в качестве среды распространения могут выступать любые токопроводящие элементы здания (сеть 220 В, линии сигнализации, телефонные линии, трубы отопления и т. д.). При этом за пределами контролируемой зоны эти сигналы становятся доступными для перехвата с использованием специальной радиоприемной аппаратуры.

Наиболее показательным примером является перехват изображения с монитора компьютера.

Наряду с информацией, обрабатываемой в ТСПИ, и речевой информацией важную роль играет видовая информация, получаемая техническими средствами перехвата информации в виде изображений.

В зависимости от характера информации можно классифицировать следующие способы её получения:

- наблюдение за объектами;
- съёмка объектов;
- снятие копии документов.

В зависимости от условий наблюдения и освещения для наблюдения за объектами могут использоваться различные технические средства. Для наблюдения днём - оптические приборы (монокуляры, оптические трубы, бинокли, телескопы и т. д.), телевизионные камеры, для наблюдения ночью - приборы ночного видения, телевизионные камеры, тепловизоры.

Для наблюдения с большого расстояния используются средства аэро - и космической кино - фото съёмки, длиннофокусные оптические системы, а для наблюдения с близкого расстояния - камуфлированные скрытно установленные телевизионные камеры. При этом изображение с телевизионных камер может передаваться на мониторы как по кабелю, так и по радиоканалу.

Съёмка объектов проводится для документирования результатов наблюдения и более подробного изучения объектов. Для съёмки объектов используются телевизионные и фотографические средства, включая аэро -космические.

Съёмка документов осуществляется, как правило, с использованием портативных фотоаппаратов.

Представленные способы добывания информации обеспечивают съем, перехват и копирование информации с любых известных носителей.

Опасность рассмотренных способов добывания информации как источника угроз безопасности информационной деятельности обусловливает необходимость совершенствования способов противодействия добыванию злоумышленниками информации в этой области.

Для предотвращения утечки информации существует большое количество самых разнообразных средств защиты информации. Это в первую очередь технические средства обнаружения средств несанкционированного съема информации (детекторы поля, сканирующие приемники, нелинейные локаторы для обнаружения внедренных электронных средств перехвата акустической информации и др.), технические средства противодействия

средствам несанкционированного съема информации (различные генераторы шума и т.п.), а также средства защиты линий связи (скремблеры, маскираторы речи и др.).