Лекция № 15. Методы и приемы обеспечения информационной безопасности.

Цель занятия: знакомство с основными методами и приёмами обеспечения информационной безопасности.

Под безопасностью информации (Information security) **или информационной безопасностью** понимают защищённость информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, способных нанести ущерб владельцам и пользователям информации и поддерживающей её структуре.

При рассмотрении проблем, связанных с обеспечением безопасности, используют понятие «**несанкционированный доступ**» – это неправомочное обращение к информационным ресурсам с целью их использования (чтения, модификации), а также порчи или уничтожения. Данное понятие также связано с распространением разного рода компьютерных вирусов.

В свою очередь «**санкционированный доступ**» – это доступ к объектам, программам и данным пользователей, имеющих право выполнять определённые действия (чтение, копирование и др.), а также полномочия и права пользователей на использование ресурсов и услуг, определённых администратором вычислительной системы.

Вирусы представляют широко распространённое явление, отражающееся на большинстве пользователей компьютеров, особенно работающих в сетях и с нелицензионным программным обеспечением.

Вирусы появились в результате создания самозапускающихся программ.

Вирусы – это класс программ, незаконно проникающих в компьютеры пользователей и наносящих вред их программному обеспечению, информационным файлам и даже техническим устройствам, например, жёсткому магнитному диску. В России вирусы появляются в 1988 году. С развитием сетевых информационных технологий вирусы стали представлять угрозу огромному количеству пользователей сетевых и локальных компьютерных систем.

Современные угрозы информационной безопасности в России

Согласно Закону о безопасности под **угрозой безопасности** понимается *совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства*. Концепция национальной безопасности РФ не дает определения угрозы, но называет некоторые из них в информационной сфере. Так, опасность представляют:

- стремление ряда стран к доминированию в мировом информационном пространстве;
- вытеснение государства с внутреннего и внешнего информационного рынка;
- разработка рядом государств концепции информационных войн;
- нарушение нормального функционирования информационных систем;
- нарушение сохранности информационных ресурсов, получение несанкционированного доступа к ним.

Это так называемые ***внешние угрозы***, которые обусловлены *конкурентным характером развития межгосударственных и международных отношений*. Соответственно существуют и ***внутренние угрозы*** , связанные во многом с *недостаточным проведением экономических, социально-политических и иных преобразований в сфере* ИБ. Концепция национальной безопасности называет их в качестве предпосылок возникновения угроз. С учетом этих предпосылок, по нашему мнению, к источникам внутренних угроз можно отнести:

– отставание России в сфере информатизации органов государственной власти;

– несовершенство системы организации государственной власти по формированию и реализации единой государственной политики обеспечения ИБ;

– криминализацию общественных отношений, рост организованной преступности;

– увеличение масштабов терроризма;

– обострение межнациональных и осложнение внешних отношений.

Для нейтрализации информационных угроз существует исторически сложившаяся система сохранения государственной тайны, включающая подсистемы:

– криптографической сети конфиденциальной связи;

– противодействия иностранным техническим разведкам;

– обеспечения режима секретности на закрытых государственных объектах.

Наряду с традиционными приоритетами иностранных технических разведок в сферу их интересов все в большей мере вовлекаются вопросы технологий, финансов, торговли, ресурсов, доступ к которым открывается в связи с конверсией, развитием международных интеграционных процессов, широким внедрением компьютерных технологий. Из существующих информационных угроз наиболее актуальными являются угрозы экономической безопасности предприятий и фирм, определяемые недобросовестной конкуренцией, экономическим и промышленным шпионажем. Промышленный шпионаж существовал всегда.

Промышленный шпионаж представляет собой *несанкционированную передачу конфиденциальной технологии, материалов, продукции, информации о них.*

Методы и способы ведения шпионажа остаются неизменными на протяжении многих столетий развития общества и государства. При этом меняются только средства и формы его ведения. К таким методам относятся: подкуп, шантаж, деятельность послов-шпионов, перехват сообщений, представленных на различных носителях (магнитные носители, письма и др.).

Что касается ***анализа полученной информации*** , то все осталось без изменений. Им занимается человек или группа людей, осуществляющих аналитико-синтетическую переработку информации, в том числе с использованием новых информационных технологий.

Развитие техники вплоть до начала XX в. не влияло на средства несанкционированного получения информации: сверлили дырки в стенах и потолках, использовали потайные ходы и полупрозрачные зеркала, устраивались у замочных скважин и под окнами. Появление телеграфа и телефона позволило

использовать технические средства получения информации. Гигантское количество сообщений стало перехватываться, влияя на ведение войн и положение на бирже. В 30–40 гг. появились диктофоны, миниатюрные фотоаппараты, различные радиомикрофоны.

Развитие новых информационных технологий позволило осуществлять перехват гигантского количества сообщений, оказывая влияние на все сферы социально-экономического развития общества, в том числе на развитие промышленности.

Анализ результатов исследований угроз информации позволяет утверждать, что одной из основных угроз государственной безопасности Российской Федерации являются попытки западных спецслужб добывать ***конфиденциальные сведения*** , составляющие государственную, промышленную, банковскую и другие виды тайн. Ведущие западные страны продолжают модернизировать и развивать свои разведывательные службы, совершенствовать техническую разведку, наращивать ее возможности.

С учетом рассмотренного содержания понятия угрозы государству, обществу и личности в широком смысле рассмотрим угрозы, непосредственно воздействующие на обрабатываемую конфиденциальную информацию. Система угроз безопасности представляет собой реальные или потенциально возможные действия или условия, приводящие к хищению, искажению, несанкционированному доступу, копированию, модификации, изменению, уничтожению конфиденциальной информации и сведений о самой системе и, соответственно, к прямым материальным убыткам.

При этом угрозы сохранности информации определяются случайными и преднамеренными разрушающими и искажающими воздействиями внешней среды, надежностью функционирования средств обработки информации, а также преднамеренного корыстного воздействия несанкционированных пользователей, целью которых является хищение, уничтожение, разрушение, модификации и использование обрабатываемой информации. Анализ содержания свойств угроз позволяет предложить следующие варианты их классификации (рис. 1).

Проявление угроз характеризуется рядом закономерностей. Во-первых, незаконным овладением конфиденциальной информацией, ее копированием, модификацией, уничтожением в интересах злоумышленников, с целью нанесения ущерба. Кроме этого, непреднамеренные действия обслуживающего персонала и пользователей также приводят к нанесению определенного ущерба. Во-вторых, основными путями реализации угроз информации и безопасности информации выступают:

– агентурные источники в органах управления и защиты информации;

– вербовка должностных лиц органов управления, организаций, предприятий и т. д.;

– перехват и несанкционированный доступ к информации с использованием технических средств разведки;

– использование преднамеренного программно-математического воздействия;

– подслушивание конфиденциальных переговоров в служебных помещениях, транспорте и других местах их ведения.

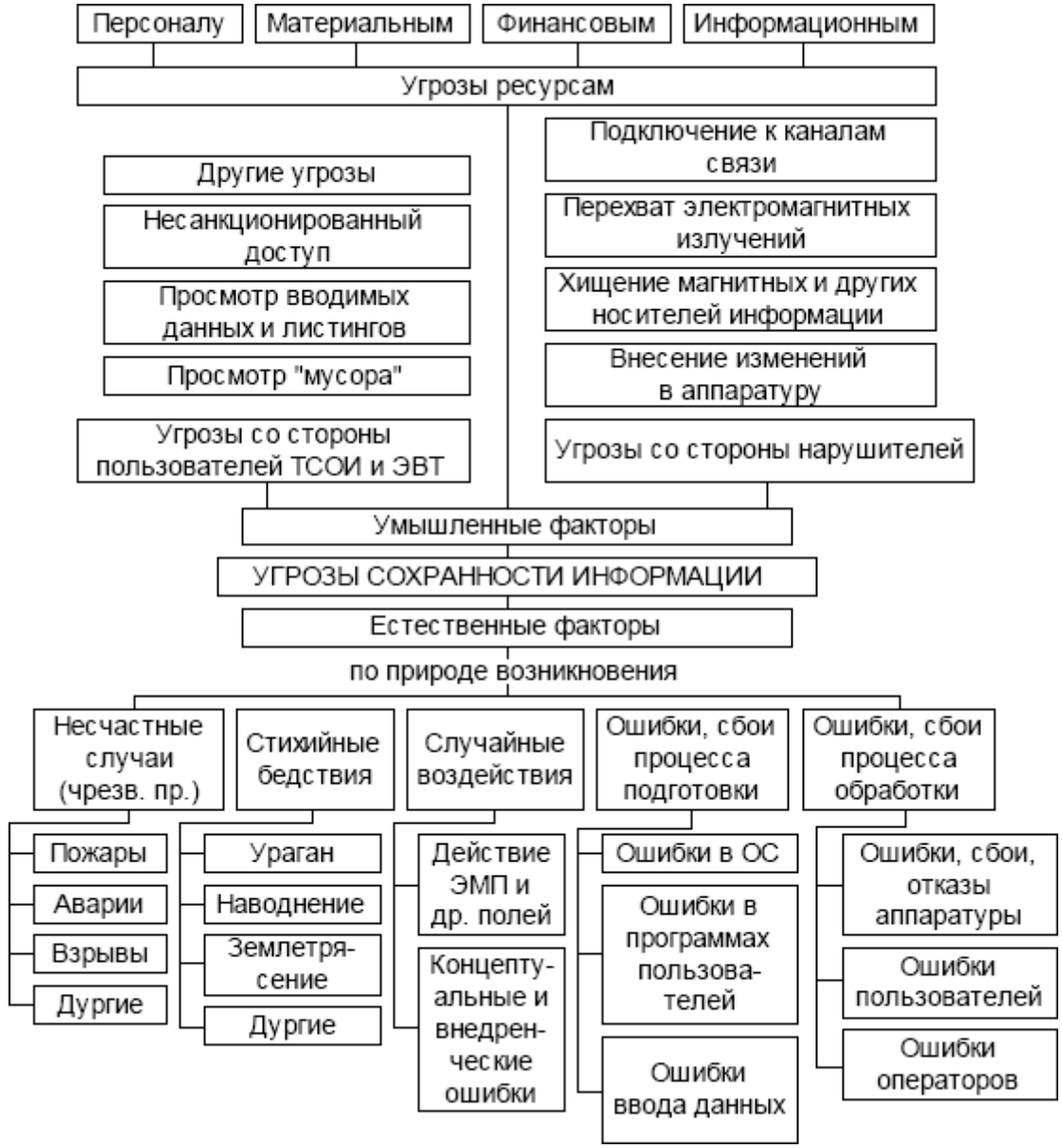

Рис. 1. Классификация угроз безопасности

Основными факторами воздействия угроз, обусловливающими информационные потери и приводящими к различным видам ущерба, возрастание убытков от неправомерных действий, являются:

– несчастные случаи, вызывающие выход из строя оборудования и информационных ресурсов (пожары, взрывы, аварии, удары, столкновения, падения, воздействия химических или физических сред);

– поломки элементов средств обработки информации;

– последствия природных явлений (наводнения, бури, молнии, землетрясения и др.);

– кражи, преднамеренная порча материальных средств;

– аварии и выход из строя аппаратуры, программного обеспечения, баз данных;

– ошибки накопления, хранения, передачи, использования информации;

– ошибки восприятия, чтения, интерпретации содержания информации, соблюдения правил, ошибки как результат неумения, оплошности, наличие помех, сбоев и искажений отдельных элементов и знаков или сообщения;

– ошибки эксплуатации: нарушение защиты, переполнение файлов, ошибки

языка управления данными, ошибки при подготовке и вводе информации, ошибки операционной системы, программирования, аппаратные ошибки, ошибки толкования инструкций, пропуск операций и др.;

– концептуальные ошибки внедрения;

– злонамеренные действия в материальной сфере;

– болтливость, разглашение; – убытки социального характера (уход, увольнение, забастовка и др.).

Информационный ущерб в ряде случаев может быть оценен в зависимости от вида потерь. Это могут быть:

– *потери, связанные с компенсацией или возмещением утраченных, похищенных материальных средств* , которые включают:

- стоимость компенсации возмещения другого косвенно утраченного имущества;
- стоимость ремонтно-восстановительных работ;
- расходы на анализ и исследование причин и величины ущерба;
- другие расходы;

– *дополнительные расходы* на персонал, обслуживающий технические средства обработки конфиденциальной информации, восстановление информации, возобновление работы информационных систем по сбору, хранению, обработке, контролю данных, в том числе расходы:

- на поддержку информационных ресурсов ТСОИ;
- обслуживающий персонал, не связанный с обработкой информации;
- специальные премии, расходы на перевозку и др.;

– *эксплуатационные потери* , связанные с ущербом банковских интересов или финансовыми издержками, потерей клиентов, заказчиков, требующие дополнительных расходов на восстановление: банковского доверия; размеров прибыли; утерянной клиентуры; доходов организации и др.;

- утрата фондов или порча имущества, не подлежащего восстановлению, которые снижают финансовые возможности (деньги, ценные бумаги, денежные переводы и др.);
- расходы и потери, связанные с возмещением морального ущерба, обучением, экспертизой и др.

Анализируя количественные данные потерь, можно сделать вывод о том, что убытки от злонамеренных действий, и особенно от экономического шпионажа, непрерывно возрастают и являются наиболее значимыми. Выводы западных экспертов показывают, что утечка 20 % коммерческой информации в 60 случаях из 100 приводит к банкротству фирмы.

Подводя итоги краткому анализу существующих угроз конфиденциальной информации, можно выделить два направления воздействия угроз, снижающих безопасность информации.

Первое, традиционно сложившееся в рамках защиты конфиденциальных сведений, представляет собой *воздействия*, способствующие несанкционированному доступу к этим сведениям. Второе, сложившееся в рамках широкого понимания проблем ИБ, связано с *использованием* современных технических и организационных систем, а также с участием людей, коллективов людей и общества в целом и их подверженностью внешним, негативным информационным воздействиям.

Так, теоретически доказано, а практикой многократно подтверждено то, что

психика и мышление человека подвержены внешним информационным воздействиям и при их надлежащей организации возникает возможность программирования поведения человека. Более того, в последнее время ведутся разработки методов и средств компьютерного проникновения в подсознание, для того чтобы оказывать на него глубокое воздействие. Поэтому актуальной является проблема не только защиты информации, но и защиты от разрушающего воздействия информации, приобретающей международный масштаб и стратегический характер. В силу изменения концепции развития стратегических вооружений, определяющей, что вооруженное решение мировых проблем становится невозможным, все более прочно входит в обиход понятие ***информационной войны***. Сейчас эффективность наступательных средств информационной войны, информационного оружия превосходит эффективность систем защиты информации.

Представляют интерес угрозы утраты охраняемых сведений в ходе информационных процессов, участники которых представляют противоположные интересы. Анализ этих угроз позволил выявить ряд их характерных признаков. В большинстве случаев активные действия сторон вполне осознанны и целенаправленны. К таким действиям относятся:

– разглашение конфиденциальной информации ее обладателем;

– утечка информации по различным, главным образом техническим, каналам;

– несанкционированный доступ к конфиденциальной информации различными способами.

Разглашение информации – это *умышленные или неосторожные действия должностных лиц и граждан, которым в установленном порядке были доверены соответствующие сведения по работе, приведшие к оглашению охраняемых сведений, а также передача таких сведений по открытым техническим каналам* . Разглашение выражается в сообщении, передаче, предоставлении, пересылке, опубликовании, при обсуждении, утере и оглашении любыми иными способами конфиденциальной информации лицам и организациям, не имеющим права доступа к охраняемым секретам. Разглашение информации может происходить по многим каналам, в том числе через почтовые отправления, радио, телевидение, печать и т. п. Разглашение возможно в ходе деловых встреч, бесед, при обсуждении совместных работ, в договорах, в письмах и документах, деловых встречах и др. В ходе таких мероприятий партнеры ведут интенсивный обмен информацией. Именно при общении между ними устанавливаются «доверительные» отношения, приводящие к оглашению коммерческих секретов.

Как правило, факторами, способствующими разглашению конфиденциальной информации, являются:

– слабое знание (или незнание) требований по защите конфиденциальной информации;

– ошибочность действий персонала из-за низкой производственной квалификации;

– отсутствие системы контроля за оформлением документов, подготовкой выступлений, рекламы и публикаций;

– злостное, преднамеренное невыполнение требований по защите коммерческой тайны.

Разглашение конфиденциальной информации неизбежно приводит к материальному и моральному ущербу.

Утечку информации в общем виде можно рассматривать как *бесконтрольный и неправомерный выход конфиденциальной информации за пределы организации или круга лиц, которым эта информация была доверена* . При этом природа утечки охраняемой информации характеризуется как обстоятельствами происхождения, так и причинами, условиями возникновения утечки.

Неправомерному овладению конфиденциальной информацией вследствие ***неудовлетворительного управления персоналом*** со стороны должностных лиц, организаций и ведомств способствует наличие следующих обстоятельств:

–склонность сотрудников организации к излишней разговорчивости – 32 %;

–стремление сотрудников зарабатывать деньги любыми способами и любой ценой –24 %;

–отсутствие в фирме службы безопасности – 14 %; – привычка сотрудников делится друг с другом информацией о своей служебной деятельности – 12 %;

–бесконтрольное использование в фирме информационных систем – 10 %;

–предпосылки возникновения конфликтных ситуаций в коллективе вследствие отсутствия психологической совместимости сотрудников, случайного подбора кадров, отсутствия работы руководителя по сплочению коллектива и др. – 8 %.

Также утечка охраняемой информации обусловлена наличием соответствующих условий, связанных:

– с ***появлением конкурента*** (злоумышленника), который такой информацией интересуется и затрачивает определенные силы и средства для ее приобретения;

– ***несовершенством норм по сохранению коммерческих секретов, а также нарушением этих норм***, отступлением от правил обращения с соответствующими документами, техническими средствами, образцами продукции и другими материалами, содержащими конфиденциальную информацию;

– разными факторами и обстоятельствами, которые складываются в процессе научной, производственной, рекламной, издательской, информационной и иной деятельности организации и создают предпосылки для ***утечки сведений, составляющих различные виды тайн***.

К таким факторам и обстоятельствам могут, например, относиться:

– недостаточное знание работниками правил защиты соответствующего вида тайны и непонимание необходимости их тщательного соблюдения;

– утрата удостоверений, пропусков, ключей от режимных помещений, хранилищ, сейфов (металлических шкафов), личных печатей – 12 %;

– пронос без разрешения работников службы безопасности (СБ) на территорию организации кино-, звуко-, фото– и видеозаписывающей, радиопередающей, принимающей и множительно-копировальной аппаратуры личного пользования; недонесение о фактах возможной утечки секретных сведений руководству подразделения и СБ; вынос с предприятия секретных документов и изделий без разрешения руководителя организации или начальника СБ – 4 %;

– неправильное определение грифа секретности документа (изделия) – 3 %;

– несвоевременное направление документов для приобщения к делу с

отметками об исполнении и с резолюцией начальника подразделения; оставление открытыми и неопечатанными после окончания работы помещений (спецхранилищ) – 3 %;

– оставление секретных документов на рабочих столах при выходе из помещения, нарушение установленного порядка ознакомления прикомандированных лиц с секретными документами и изделиями, перевозка секретных документов и изделий личным и общественным транспортом и перемещение с ними в места, не связанные с выполнением заданий, – 2 %;

– неправильное оформление секретных документов в печать; несоблюдение порядка отчетности перед СБ за числящиеся за исполнителем документы и изделия при увольнении, перед уходом в отпуск, выездом в командировки; несвоевременное сообщение в кадровую службу об изменениях анкетных и автобиографических данных; ведение переговоров по секретным вопросам по незащищенным линиям связи; выполнение секретных работ на дому; снятие копий с секретных документов или производство выписок из них без письменного разрешения начальника СБ; передача и взятие без расписки секретных документов и изделий

– 1 % по каждому случаю.

Причинами неправомерного овладения конфиденциальной информацией могу быть следующие обстоятельства:

– ***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, составляющими коммерческую тайну;

– ***нарушения, не попадающие в поле зрения администрации и СБ*** , – это могут быть:

• ознакомление лиц с конфиденциальными документами, изделиями, работами, не входящими в круг их служебных обязанностей;

• направление адресатам конфиденциальных документов, к которым они не имеют отношения;

• подготовка конфиденциальных документов на неучтенных носителях;

• нарушение порядка работы с конфиденциальными документами, изделиями, который не допускает обзор их посторонними лицами;

• несвоевременное сообщение в СБ данных о внеслужебных связях с родственниками, проживающими за границей, с родственниками, выезжающими за границу на постоянное место жительства;

• посещение без разрешения руководства организации посольств, консульств, иностранных частных компаний и фирм;

• установление радиосвязи с радиолюбителями иностранных государств;

• использование конфиденциальных сведений в несекретной служебной переписке, технических заданиях, статьях, докладах и выступлениях;

• преждевременная публикация научных и других работ, которые могут расцениваться на уровне изобретений или открытий или опубликование которых запрещено в установленном порядке;

• сообщение устно или письменно кому бы то ни было, в том числе

родственникам, конфиденциальных сведений, если это не вызвано служебной необходимостью;

• сообщение каких-либо сведений о проводимых конфиденциальных работах при обращении по личным вопросам с жалобами, просьбами и предложениями в федеральные государственные органы власти, органы власти субъектов РФ и органы местного самоуправления.

Кроме того, утечке информации способствуют стихийные бедствия, катастрофы, неисправности, отказы, аварии технических средств и оборудования.

Способы **несанкционированного доступа** (НСД) как проблему утечки конфиденциальной информации предлагается рассматривать со следующих позиций. Вопрос обеспечения защиты от НСД связан с проблемой сохранности не только информации как вида интеллектуальной собственности, но физических и юридических лиц, их имущественной собственности и личной безопасности. Известно, что такая деятельность тесно связана с получением, накоплением, хранением, обработкой и использованием разнообразных информационных потоков. Как только информация представляет определенную цену, факт ее получения злоумышленником приносит ему определенный доход, ослабляя тем самым возможности конкурента. Отсюда главная цель противоправных действий – получение информации о составе, состоянии и деятельности объекта конфиденциальной информации для удовлетворения своих информационных потребностей в корыстных целях и внесение изменений в состав информации. Такое действие может привести к дезинформации в определенных сферах деятельности и отражаться, в частности, на учетных данных, результатах решения управленческих задач.

Более опасной угрозой является уничтожение накопленных информационных массивов в документальной или магнитной форме и программных продуктов в среде автоматизированной системы обработки данных.

Уничтожение – это *противоправное действие, направленное на нанесение материального и информационного ущерба конкуренту со стороны злоумышленника* .

Таким образом, рассмотренные угрозы в отношении информации, за исключением последней, как правило, нацелены и ведут к получению злоумышленником конфиденциальной информации. Анализ традиционных приемов и методов получения конфиденциальной информации позволил выделить наиболее характерные источники и методы ее получения, которые в общем виде описывают действия субъектов правовых отношений в сфере обеспечения ИБ:

– сбор информации, содержащейся в средствах массовой информации, включая официальные документы;

– использование сведений, распространяемых служащими конкурирующих организаций;

– документы, отчеты консультантов, финансовые отчеты и документы, выставочные экспонаты и проспекты и др.;

– изучение продукции конкурирующих и других организаций, представляющих интерес для соответствующих видов разведки, использование данных, полученных во время

бесед с обслуживающим персоналом;

– замаскированные опросы и "выуживание" информации у служащих организации на научно-технических конгрессах;

– непосредственное наблюдение, осуществляемое скрытно;

– беседы о найме на работу (без намерений приема их на работу);

– наем на работу служащего конкурирующей фирмы или организации для получения требуемой информации;

– подкуп служащего; – подслушивание переговоров, ведущихся в служебных и иных помещениях, перехват телеграфных сообщений, подслушивание телефонных разговоров;

– кража чертежей, документов и т. д.

– шантаж и вымогательство и др.

Рассмотренные источники и методы не является исчерпывающими, однако они позволяют сгруппировать все ***вероятные источники утечки информации*** следующим образом:

– *персонал, имеющий доступ* к конфиденциальной информации;

– *документы* , содержащие эту информацию; – *технические средства и системы обработки информации* , в том числе линии связи, по которым она передается.

Анализ зарубежных публикаций по источникам утечки информации в коммерческих фирмах позволил выявить, что, несмотря на высокий процент каналов, связанных с использованием для добывания сведений технических средств разведки и различных технологических приемов, персонал остается одним из главных причин и одним из источников утечки конфиденциальной информации, что подтверждается примерными следующих процентных соотношений по каналам утечки информации:

– подкуп, шантаж, переманивание служащих, внедрение агентов – 43;

– подслушивание телефонных переговоров – 5;

– кража документов – 10;

– проникновение в ПЭВМ – 18;

– съем информации с каналов "в темную» – 24.

Для раскрытия характеристик правонарушений, совершаемых в информационной сфере, существенное значение имеют характеристики вероятных каналов утечки информации, которые определяются наличием соответствующих источников конфиденциальной информации. Такую классификацию целесообразно рассматривать с учетом того, что обработка конфиденциальной информации осуществляется в организациях, представляющих собой сложные ***системы организационно-технического типа,*** функционирующие в условиях внешних воздействий и внутренних изменений состояния. При этом независимо от рассматриваемых воздействий на конфиденциальную информации и систему ее обработки возникающие каналы утечки информации проявляются через такие правонарушения. Эти каналы можно сгруппировать в рамках рассмотренных трех основных групп вероятных источников утечки информации. Так, первая группа – **персонал, имеющий доступ к конфиденциальной информации** , – представляет собой *людские потоки* и является важнейшей группой возможных каналов утечки

информации. По распространенности возможные каналы утечки информации этой группы характеризуются следующими примерными показателями:

– приема и увольнения работников предприятия – 32 %;
– посещения предприятия командированными лицами – 28 %;
– проведения совещаний по секретным вопросам – 15 %;
– ведения секретных работ в рабочих помещениях – 15 %;
– допуска, доступа и обращения с секретной (конфиденциальной) информацией – 14 %;
– выезда специалистов за границу – 10 %;
– организации пропускного и внутриобъектового режима – 8 %;
– прохождения практики студентами – 7 %;
– посещения международных выставок – 7 %;
– обучения на курсах повышения квалификации – 5 %;
– подготовки постановлений и решений, приказов и других документов – 4 %.

Типовые нарушения при приеме и увольнении персонала:

– прием на работу лиц без оформления допуска в установленном порядке;
– доступ персонала к конфиденциальной информации в нарушение установленных требований;
– несвоевременное и неполное ознакомление персонала с требованиями нормативных правовых актов по обеспечению ИБ;
– неудовлетворительные знания нормативных правовых актов;
– увольнение персонала, являющегося носителем конфиденциальной информации.

Характерные нарушения при посещении предприятий командированными лицами:

–допуск командированных лиц с ведома руководителей подразделений к конфиденциальным работам и документам без соответствующего оформления разрешения;
– невыполнение требований инструкций для внутренних объектов по сопровождению прибывших в подразделения командированных лиц;
– отсутствие в предписаниях отметок о действительно выданной информации представителям других предприятий;
– прием командированных лиц с предписаниями, в которых отсутствуют основания командирования (номер и дата хозяйственного договора, ТЗ совместного плана НИОКР и др.);
– не определена степень конфиденциальности материалов, к которым допускается командированное лицо.

Нарушения, связанные с проведением служебных совещаний :

– проведение совещаний без соответствующего разрешения руководителя предприятия или его заместителей;
– допуск на совещание лиц, не имеющих отношения к обсуждаемым вопросам и участие которых не вызывается служебной необходимостью;
– несоблюдение очередности рассмотрения вопросов конфиденциального характера;
– несоблюдение требований режима внутреннего объекта при проведении

совещаний;

– фотографирование, демонстрация конфиденциальных изделий, фильмов без согласования с СБ;

– звукозапись выступлений участников совещания на носителе, не учтенном в СБ;

– направление тетрадей (записей) секретного характера в учреждения, которых эти сведения непосредственно не касаются;

– недостаточное знание работниками, участвующими в приеме командированных лиц, требований инструкции о порядке приема командированных лиц (об этом заявили около 45 % опрошенных лиц).

Нарушения при ведении конфиденциальных работ в рабочих помещениях

заключаются в отсутствии обеспечения:

– специальных средств защиты конфиденциальной информации, связи, звукозаписи, звукоусиления, переговорных и телевизионных устройств;

– средств изготовления и размножения документов;

– средств пожарной и охранной сигнализации;

– систем электронной часофикации, электрооборудования и других дополнительных технических средств защиты, исключающих утечку информации за счет побочных электромагнитных излучений и наводок.

Такие каналы утечки, как ***доступ и обращение с конфиденциальной информацией*** , образуются за счет расширения круга лиц, имеющих допуск к документам, изделиям, техническим заданиям.

Нарушения в организации пропускного и внутриобъектового режима включают:

- утрату удостоверений, пропусков, ключей от режимных помещений, хранилищ, сейфов (шкафов), личных печатей – 12 %;

– пронос без разрешения СБ на территорию предприятия кино– и фотоаппаратуры, радиопередающей и принимающей, а также множительно-копировальной аппаратуры личного пользования;

– вынос из предприятия секретных документов и изделий без разрешения;

– оставление незакрытыми и не опечатанными после работы помещений (хранилищ).

Каналы утечки конфиденциальных сведений за счет ***неправильной организации прохождения технологической и преддипломной практики студентов*** проявляются в следующем: студенты и учащиеся вузов и средних специальных учебных заведений после прохождения практики не зачисляются на постоянную работу, где они проходили практику и познакомились со сведениями, составляющими государственную или коммерческую тайну, и другие причины.

Характерные нарушения при решении задач отраслевого и межотраслевого характера:

– включение конфиденциальных сведений в открытые документы с целью упрощения порядка доставки и согласования документов;

– ведение секретных записей в личных блокнотах, записных книжках;

– ознакомление с конфиденциальными работами и сведениями лиц, в круг

служебных обязанностей которых они не входят;

– направление адресатам конфиденциальных документов, к которым они не имеют отношения.

Таким образом, проведенный анализ угроз информации позволяет уточнить ее свойства, подлежащие правовой защите. При этом содержание этих свойств будет рассматриваться с учетом положений действующих нормативных актов.

Основные средства и методы защиты информации

Средства и методы защиты информации обычно делят на две большие группы: организационные и технические.

Под организационными подразумеваются законодательные, административные и физические, а **под техническими** – аппаратные, программные и криптографические мероприятия, направленные на обеспечение защиты объектов, людей и информации.

Программные средства защиты – это самый распространённый метод защиты информации в компьютерах и информационных сетях. Обычно они применяются при затруднении использования некоторых других методов и средств. Проверка подлинности пользователя обычно осуществляется операционной системой. Пользователь идентифицируется своим именем, а средством аутентификации служит пароль.

С целью организации защиты объектов используют **системы охраны** и **безопасности объектов** – это совокупность взаимодействующих радиоэлектронных приборов, устройств и электрооборудования, средств технической и инженерной защиты, специально подготовленного персонала, а также транспорта, выполняющих названную функцию. При этом используются различные методы, обеспечивающие санкционированным лицам доступ к объектам и ИР. К ним относят аутентификацию и идентификацию пользователей.

Программные и технические средства защиты.

Программные средства защиты – это самый распространённый метод защиты информации в компьютерах и информационных сетях. Обычно они применяются при затруднении использования некоторых других методов и средств. Проверка подлинности пользователя обычно осуществляется операционной системой. Пользователь идентифицируется своим именем, а средством аутентификации служит пароль.

Программные средства защиты представляют комплекс алгоритмов и программ специального назначения и общего обеспечения работы компьютеров и информационных сетей. Они нацелены на: контроль и разграничение доступа к информации, исключение несанкционированных действий с ней, управление охранными устройствами и т.п. Программные средства защиты обладают универсальностью, простотой реализации, гибкостью, адаптивностью, возможностью настройки системы и др.

Широко применяются программные средства для защиты от компьютерных вирусов.

Для **защиты машин от компьютерных вирусов**, профилактики и «лечения» используются программы-антивирусы, а также средства диагностики и профилактики, позволяющие не допустить попадания вируса в компьютерную систему, лечить заражённые файлы и диски, обнаруживать и предотвращать подозрительные действия. Антивирусные программы оцениваются по точности обнаружения и эффективному устранение вирусов, простое использование, стоимость, возможности работать в сети.

Наибольшей популярностью пользуются программы, предназначенные для профилактики заражения, обнаружения и уничтожения вирусов. Среди них отечественные антивирусные программы DrWeb (Doctor Web) И. Данилова и AVP (Antiviral Toolkit Pro) Е. Касперского. Они обладают удобным интерфейсом, средствами сканирования программ, проверки системы при загрузке и т.д. В России используются и зарубежные антивирусные программы.

Абсолютно надёжных программ, гарантирующих обнаружение и уничтожение любого вируса, не существует. Только многоуровневая оборона способна обеспечить наиболее полную защиту от вирусов. Важным элементом защиты от компьютерных вирусов является профилактика. Антивирусные программы применяют одновременно с регулярным резервированием данных и профилактическими мероприятиями. Вместе эти меры позволяют значительно снизить вероятность заражения вирусом.

Основными мерами профилактики вирусов являются:

1) применение лицензионного программного обеспечения;

2) регулярное использование нескольких постоянно обновляемых антивирусных программ для проверки не только собственных носителей информации при переносе на них сторонних файлов, но и любых «чужих» дискет и дисков с любой информацией на них, в т.ч. и переформатированных;

3) применение различных защитных средств при работе на компьютере в любой информационной среде (например, в Интернете). Проверка на наличие вирусов файлов, полученных по сети;

4) периодическое резервное копирование наиболее ценных данных и программ.

Одним из наиболее известных способов защиты информации является её кодирование (шифрование, криптография). Оно не спасает от физических воздействий, но в остальных случаях служит надёжным средством.

Код характеризуется: *длиной* – числом знаков, используемых при кодировании и структурой – порядком расположения символов, используемых для обозначения классификационного признака.

Средством кодирования служит таблица соответствия. Примером такой таблицы для перевода алфавитно-цифровой информации в компьютерные коды является кодовая таблица ASCII.

Криптографические методы защиты информации.

Криптография - это тайнопись, система изменения информации с целью её защиты от несанкционированных воздействий, а также обеспечения достоверности передаваемых данных.

Общие методы криптографии существуют давно. Она считается мощным средством обеспечения конфиденциальности и контроля целостности информации. Пока альтернативы методам криптографии нет.

Стойкость криптоалгоритма зависит от сложности методов преобразования. Вопросами разработки, продажи и использования средств шифрования данных и сертификации средств защиты данных занимается Гостехкомиссия РФ.

Одной из важных проблем информационной безопасности является организация защиты электронных данных и электронных документов. Для их кодирования, с целью удовлетворения требованиям обеспечения безопасности данных от несанкционированных воздействий на них, используется электронная цифровая подпись (ЭЦП).

Электронная подпись

Цифровая подпись представляет последовательность символов. Она зависит от самого сообщения и от секретного ключа, известного только подписывающему это сообщение.

Первый отечественный стандарт ЭЦП появился в 1994 году. Вопросами использования ЭЦП в России занимается Федеральное агентство по информационным технологиям (ФАИТ).

Биометрические методы защиты.

Наиболее чётко обеспечивают защиту средства идентификации личности, использующие биометрические системы. Понятие «биометрия» определяет раздел биологии, занимающийся количественными биологическими экспериментами с привлечением методов математической статистики. Это научное направление появилось в конце XIX века.

Биометрия - это совокупность автоматизированных методов и средств идентификации человека, основанных на его физиологических или поведенческих характеристиках.

Биометрические системы позволяют идентифицировать человека по присущим ему специфическим признакам, то есть по его статическим (отпечаткам пальцев, роговице глаза, форме руки и лица, генетическому коду, запаху и др.) и динамическим (голосу, почерку, поведению и др.) характеристикам. Уникальные биологические, физиологические и поведенческие характеристики, индивидуальные для каждого человека. Они называются биологическим кодом человека.

Первые биометрические системы использовали рисунок (отпечаток) пальца. Примерно одну тысячу лет до н.э. в Китае и Вавилоне знали об уникальности отпечатков пальцев. Их ставили под юридическими документами. Однако дактилоскопию стали применять в Англии с 1897 года, а в США – с 1903 года. Пример современного считывающего устройства отпечатки пальцев

С помощью биометрических систем осуществляются:
1) ограничение доступа к информации и обеспечение персональной ответственности за её сохранность;
2) обеспечение допуска сертифицированных специалистов;
3) предотвращение проникновения злоумышленников на охраняемые территории и в помещения вследствие подделки и (или) кражи документов (карт, паролей);
4) организация учёта доступа и посещаемости сотрудников, а также решается ряд других проблем.
Одним из наиболее надёжных способов считается идентификация глаз человека

: идентификация рисунка радужной оболочки глаза или сканирование глазного дна (сетчатки глаза). Это связано с отличным соотношением точности идентификации и простотой использования оборудования. Изображение радужной оболочки оцифровывается и сохраняется в системе в виде кода. Код, полученный в результате считывания биометрических параметров человека, сравнивается с зарегистрированным в системе. При их совпадении система снимает блокировку доступа. Время сканирования не превышает двух секунд.
К новым биометрическим технологиям следует отнести трёхмерную идентификацию личности, использующую трёхмерные сканеры идентификации личности с параллаксным методом регистрации образов объектов и телевизионные системы регистрации изображений со сверхбольшим угловым полем зрения. Предполагается, что подобные системы будут использоваться для идентификации личностей, трёхмерные образы которых войдут в состав удостоверений личности и других документов.

Сетевые методы защиты

Для защиты информации в информационных компьютерных сетях используют специальные программные, технические и программно-технические средства. С целью защиты сетей и контроля доступа в них используют:
● фильтры пакетов, запрещающие установление соединений, пересекающих границы защищаемой сети;
● фильтрующие маршрутизаторы, реализующие алгоритмы анализа адресов отправления и назначения пакетов в сети;
● шлюзы прикладных программ, проверяющие права доступа к программам.

В качестве устройства, препятствующего получению злоумышленником доступа к информации, используют **Firewalls** (англ. «огненная стена» или «защитный барьер» – брандмауэр). Такое устройство располагают между внутренней локальной сетью организации и Интернетом. Оно ограничивает трафик, пресекает попытки несанкционированного доступа к внутренним ресурсам организации. Это внешняя защита. Современные брандмауэры могут «отсекать» от пользователей корпоративных сетей незаконную и нежелательную для них корреспонденцию, передаваемую по электронной почте. При этом ограничивается возможность получения избыточной информации и так называемого «мусора» (спама).

Другим техническим устройством эффективной защиты в компьютерных сетях является **маршрутизатор**. Он осуществляет фильтрацию пакетов передаваемых данных. В результате появляется возможность запретить доступ некоторым пользователям к определённому «хосту», программно осуществлять детальный контроль адресов отправителей и получателей. Так же можно ограничить доступ всем или определённым категориям пользователей к различным серверам, например, ведущим распространение противоправной или антисоциальной информации (пропаганда секса, насилия и т.п.).

Защита может осуществляться не только в глобальной сети или локальной сети организации, но и отдельных компьютеров. Для этой цели создаются специальные программно-аппаратные комплексы.

Для комплексной защиты информации, объектов и людей на различных предприятиях рекомендуется разрабатывать и внедрять соответствующие мероприятия.

Общие выводы

Важно знать, что характерной особенностью электронных данных является возможность легко и незаметно искажать, копировать или уничтожать их. Поэтому необходимо организовать безопасное функционирование данных в любых информационных системах, т.е. защищать информацию.

Защищённой называют информацию, не изменившую в процессе передачи, хранения и сохранения достоверность, полноту и целостность данных.

Несанкционированные воздействия на информацию, здания, помещения и людей могут быть вызваны различными причинами и осуществляться с помощью разных методов воздействия. Подобные действия могут быть обусловлены стихийными бедствиями (ураганы, ливни, наводнения, пожары, взрывы и др.), техногенными катастрофами, террористическими актами и т.п. Борьба с ними обычно весьма затруднена из-за в значительной степени непредсказуемости таких воздействий.

Наибольший ущерб информации и информационным системам наносят неправомерные действия сотрудников и компьютерные вирусы. Для защиты информации в компьютерах и информационных сетях широко используются разнообразные программные и программно-технические средства защиты. Они включают различные системы ограничения доступа на объект, сигнализации и видеонаблюдения.

Для защиты информации от утечки в компьютерных сетях используют специальное техническое средство – **Firewall**s, располагаемое между внутренней локальной сетью организации и Интернетом.

Другим устройством эффективной защиты в компьютерных сетях является **маршрутизатор.** Он осуществляет фильтрацию пакетов передаваемых данных и, тем самым, появляется возможность запретить доступ некоторым пользователям к определённому «хосту», программно осуществлять детальный контроль адресов отправителей и получателей и др.

Охрана и безопасность объектов, людей и информации достигается взаимодействием специальных радиоэлектронных приборов, устройств и электрооборудования, в т.ч. пожарной и охранной сигнализации, средств технической и инженерной защиты, специально подготовленного персонала и транспорта. В качестве технических средств используются решётки на окна, ограждения, металлические двери, турникеты, металодетекторы и др.

К наиболее практикуемым способам защиты информации относится её кодирование, предполагающее использование криптографических методов защиты информации. Оно не спасает от физических воздействий, но в остальных случаях служит надёжным средством. Другой метод предполагает использование устройств, ограничивающих доступ к объектам и данным. Ведущее место среди них занимают биометрические системы. Они позволяют идентифицировать человека по присущим ему специфическим статическим и динамическим признакам (отпечаткам пальцев, роговице глаза, форме руки, лицу, генетическому коду, запаху, голосу, почерку, поведению и др.).

Комплексно мероприятия по обеспечению сохранности и защиты информации, объектов и людей включают организационные, физические, социально-психологические мероприятия и инженерно-технические средства защиты.

Контрольные вопросы.

1. Что такое компьютерный вирус?
2. Назначение компьютерного вируса?
3. Типы вирусов.
4. Программные средства защиты – антивирусные программы (характеристика).
5. Безопасность программно-технических средств и информационных ресурсов (характеристика).
6. Программная защита от несанкционированных воздействий.
7. Криптография, криптографическая защита от несанкционированных воздействий (характеристика).
8. Что такое электронная подпись?
9. Физическая и техническая защита от несанкционированных воздействий (характеристика).
10. Воздействия на здания, помещения, личную безопасность пользователя и обслуживающий персонал.
11. Технические возможности и мероприятия по обеспечению сохранности людей, зданий, помещений, программно-технических средств и информации (характеристика).
12. Охрана объектов с целью ограничения свободного доступа, смарткарты и др. (характеристика).