Индивидуальное задание по ОИБ

- «Средства телекоммуникации»

- Выполнил студент гр. И-49
  Скворцов Т.М.

- **Телекоммуникация** (греч. tele – вдаль, далеко и лат. communicatio –

общение) – передача данных на большие расстояния.

- **Средства телекоммуникации –** совокупность технических,

программных и организационных средств для передачи данных на большие расстояния.

- **Телекоммуникационная сеть –** множество средств

телекоммуникации, связанных между собой и образующих сеть определённой топологии (конфигурации).

Телекоммуникационными сетями являются :

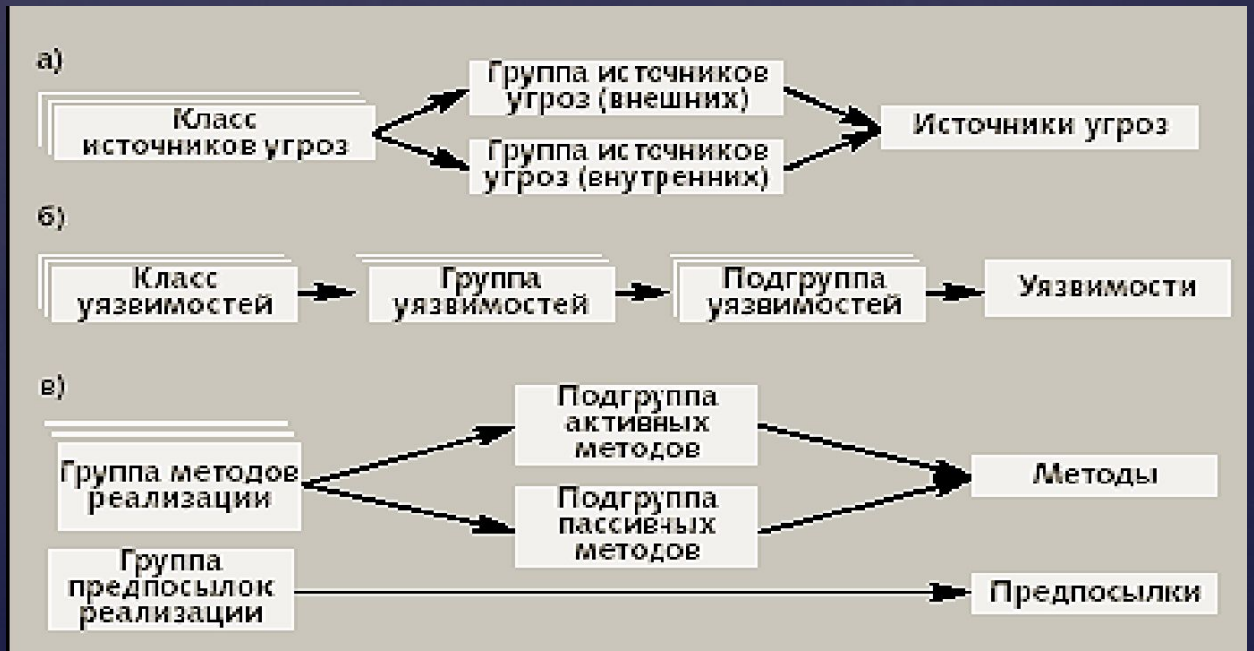
- телефонные сети для передачи телефонных данных (голоса);
- радиосети для передачи аудиоданных;
- телевизионные сети для передачи видеоданных;
- цифровые (компьютерные) сети или сети передачи данных (СПД) для передачи цифровых (компьютерных) данных.

Виды угроз

- Угрозы классифицируются по возможности нанесения ущерба субъекту отношений при нарушении целей безопасности. Ущерб может быть причинен каким-либо субъектом (преступление, вина или небрежность), а также стать следствием, не зависящим от субъекта проявлений. Угроз не так уж и много. При обеспечении конфиденциальности информации это может быть хищение (копирование) информации и средств ее обработки, а также ее утрата (неумышленная потеря, утечка).

При обеспечении целостности информации список угроз таков: модификация (искажение) информации; отрицание подлинности информации; навязывание ложной информации. При обеспечении доступности информации возможно ее блокирование, либо уничтожение самой информации и средств ее обработки.

- Все источники угроз можно разделить на классы, обусловленные типом носителя, а классы на группы по местоположению (рис. 1.2а).
- Уязвимости также можно разделить на классы по принадлежности к источнику уязвимостей, а классы на группы и подгруппы по проявлениям (рис.1.2б). Методы реализации можно разделить на группы по способам реализации (рис.1.2в). При этом необходимо учитывать, что само понятие «метод», применимо только при рассмотрении реализации угроз антропогенными источниками



- Классификация возможностей реализации угроз (атак), представляет собой совокупность возможных вариантов действий источника угроз определенными методами реализации с использованием уязвимостей, которые приводят к реализации целей атаки. Цель атаки может не совпадать с целью реализации угроз и может быть направлена на получение промежуточного результата, необходимого для достижения в дальнейшем реализации угрозы. В случае такого несовпадения атака рассматривается как этап подготовки к совершению действий, направленных на реализацию угрозы, т. е. как «подготовка к совершению» противоправного действия. Результатом атаки являются последствия, которые являются реализацией угрозы и/или способствуют такой реализации.

- Исходными данными для проведения оценки и анализа служат результаты анкетирования субъектов отношений, направленные на уяснение направленности их деятельности, предполагаемых приоритетов целей безопасности, задач, решаемых автоматизированной системой и условий расположения и эксплуатации объекта. Благодаря такому подходу возможно:
- • установить приоритеты целей безопасности для субъекта отношений;
- • определить перечень актуальных источников угроз;
- • определить перечень актуальных уязвимостей;
- • оценить взаимосвязь угроз, источников угроз и уязвимостей;
- • определить перечень возможных атак на объект;
- • описать возможные последствия реализации угроз.

- Источники угроз безопасности информации подразделяются на внешние и внутренние.
- К внешним источникам относятся:
- - недружественная политика иностранных государств в области информационного мониторинга, распространения информации и новых информационных технологий;
- - деятельность иностранных разведывательных и специальных, направленная против интересов Российской Федерации;
- - деятельность иностранных экономических структур, направленная против интересов Российской Федерации;
- - преступные действия международных групп, формирований и отдельных лиц;
- - стихийные бедствия и катастрофы.

- Внутренними источниками являются:
- - противозаконная деятельность политических, экономических и криминальных структур и отдельных лиц в области формирования, распространения и использования информации, направленная в т.ч. и на нанесение экономического ущерба государству;
- - неправомерные действия различных структур и ведомств, приводящие к нарушению законных прав работников в информационной сфере;
- - нарушения установленных регламентов сбора, обработки и передачи информации;
- - преднамеренные действия и непреднамеренные ошибки персонала автоматизированных систем, приводящие к утечке, уничтожению, искажению, подделке, блокированию, задержке, несанкционированному копированию информации;
- - отказы технических средств и сбои программного обеспечения в информационных и телекоммуникационных системах;
- - каналы побочных электромагнитных излучений и наводок технических средств обработки информации.

- Способы воздействия угроз на объекты защиты информации подразделяются на информационные, аппаратно-программные, физические, радиоэлектронные и организационно-правовые.
- К информационным способам относятся:
- - нарушение адресности и своевременности информационного обмена;
- - несанкционированный доступ к информационным ресурсам;
- - незаконное копирование данных в информационных системах;
- - хищение информации из банков и баз данных;
- - нарушение технологии обработки информации.

- Аппаратно-программные способы включают:
- - внедрение компьютерных вирусов;
- - установку программных и аппаратных закладных устройств;
- - уничтожение или модификацию данных в информационных системах.
- Физические способы включают:
- - уничтожение или разрушение средств обработки информации и связи;
- - уничтожение, разрушение или хищение машинных или других оригиналов носителей информации;
- - хищение аппаратных или программных ключей и средств криптографической защиты информации;
- - воздействие на персонал;
- - поставку "зараженных" компонентов информационных систем.

- Радиоэлектронными способами являются:
- - перехват информации в технических каналах ее утечки;
- - внедрение электронных устройств перехвата информации в технические средства передачи информации и помещения;
- - перехват, дешифрование и внедрение ложной информации в сетях передачи данных и линиях связи;
- - воздействие на парольно-ключевые системы;
- - радиоэлектронное подавление линий связи и систем управления.
- Организационно-правовые способы включают:
- - закупки несовершенных или устаревших информационных технологий и компьютерных средств;
- - невыполнение требований законодательства Российской Федерации в информационной сфере;
- - неправомерное ограничение доступа к документам, содержащим важную для граждан и органов информацию.

- Таким образом, надежная защита телекоммуникационных сетей от различного вида угроз возможна только на основе построения комплексной системы безопасности информации на всех этапах разработки, ввода в действие, модернизации аппаратно-программных средств телекоммуникаций, а также при обработке, хранении и передаче по каналам связи информации с широким применением современных средств криптографической защиты, которая бы включала в себя взаимоувязанные меры различных уровней: нормативно-правового; организационного (административного); программно-аппаратного; технического.

Этап II

Анализ увеличения защищенности объекта защиты информации

Методы защита информации в телекоммуникационных сетях предприятия

Отраслевой стандарт по информационной безопасности определяет защиту информации как деятельность, направленную на предотвращение утечки информации, несанкционированных и непреднамеренных воздействий на информацию. И если первое направление (предотвращение утечки) должно предупреждать разглашение конфиденциальных сведений, несанкционированный доступ к ним и/или их получение разведками (например, коммерческой разведкой фирм-конкурентов), то два других направления защищают от одинаковых угроз (искажение конфиденциальной информации, ее уничтожение, блокирование доступа и аналогичные действия с носителем информации). Вся разница заключается в наличии или отсутствии умысла в действиях с информацией (рис. 3.1.).


Направление
В чем заключается
От чего защищает
защита информации
от утечки
предотвращение неконтролируемого распространения защищаемой информации
разглашение защищаемой информации
несанкционированный доступ к защищаемой информации
получение защищаемой информации разведками
от несанкционированного воздействия
предотвращение воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на ее изменение
искажение информации
уничтожение информации
копирование информации
блокирование доступа к информации
от непреднамеренного воздействия
предотвращение воздействия на защищаемую информацию ошибок ее пользователей, сбоя технических и программных средств, природных явлений, иных не направленных на изменение информации мероприятий
утрата, уничтожение, сбой функционирования носителя информации

- Больше всего угроз по-прежнему создают компьютерные вирусы (в число которых помимо традиционных файловых, загрузочных, макровирусов и т. п. вредоносных программ входят также «трояны», «вандалы», перехватчики паролей и т. д.) и атаки распространителей спама.
- Внутри локальной сети актуальна задача надежной аутентификации пользователей: хрестоматийный пример прикрепления к монитору бумажки с записанным логином и паролем. В качестве еще одного канала вероятной утечки можно назвать, к примеру, сервис-центры, в которые поступают диски с не уничтоженной должным образом информацией.
- Наконец, не стоит забывать, что в значительном числе случаев пользователи оперируют информацией не только в электронном, но и в бумажном виде, и регулярное обследование содержимого мусорных ведер, куда отправляются черновики и наброски, может дать вашим конкурентам больше, чем хитроумные атаки и попытки взлома.

- Таким образом, можно сделать вывод: защита информации — одно из ключевых направлений деятельности любой успешной фирмы. Перед специально отобранным для этого сотрудником (или подразделением) стоят следующие задачи:
- • анализ угроз конфиденциальной информации, а также уязвимых мест автоматизированной системы и их устранение;
- • формирование системы защиты информации - закупка и установка необходимых средств, их профилактика и обслуживание;
- • обучение пользователей работе со средствами защиты, контроль за соблюдением регламента их применения;
- • разработка алгоритма действий в экстремальных ситуациях и проведение регулярных "учений";
- • разработка и реализация программы непрерывной деятельности автоматизированной системы и плана восстановительных мероприятий (в случае вирусной атаки, сбоя/ошибки/отказа технических средств и т. д.).

- С какими же проблемами приходится сталкиваться при построении системы защиты информации?
- Метод заплаток. «Кусочное» обеспечение информационной безопасности лишь на отдельных направлениях. Следствие — невозможность отразить атаки на незащищенных участках и дискредитация идеи информационной безопасности в целом.
- Синдром амебы. Фрагментарное реагирование на каждый новый раздражитель; часто сочетается с применением «метода заплаток». Следствие — запаздывание с отражением новых угроз, усталость от бесконечной гонки по кругу.
- Лекарство от всего. Попытки возложить на одно средство защиты информации все функции обеспечения информационной безопасности (например, стремление отождествить аутентификацию и полный комплекс задач защиты от несанкционированного доступа).
- Следствие — непрерывный переход, миграция от одного средства защиты к другому, «более комплексному», последующее разочарование и паралич дальнейших действий.
- Волшебная палочка. Вторая ипостась поисков «универсального лекарства», искреннее непонимание необходимости дополнения технических мер защиты организационными. Следствие — предъявление завышенных требований к системе или средству защиты.
- Стремление к экономии. Желание построить систему защиты на беззатратной основе. Следствие — применение непроверенных и/или нелицензионных средств защиты, отсутствие поддержки со стороны производителей, постоянные попытки разобраться во всем самостоятельно, неэффективные и разорительные, как и любая самодеятельность.
- Таким образом, на предприятии должен быть создан следующий набор средств и методов для защиты информации в сети (табл.3.1)
- Мельников В. Защита информации в компьютерных системах. - М.: Финансы и статистика, Электронинформ, 1997.С.79-81.

Минимальный пакет	Оптимальный пакет (в дополнение к минимуму)
Средства антивирусной защиты рабочих станций, файловых и почтовых серверов	Антивирусные средства в программно-аппаратном исполнении; средства контроля содержимого (Content Inspector) и борьбы со спамом
Программный межсетевой экран (МЭ)	Программно-аппаратный МЭ, система обнаружения атак (Intrusion Detection System)
Программные средства формирования защищенных корпоративных сетей (VPN - Virtual Private Network)	То же в программно-аппаратном исполнении и интеграции с межсетевым экраном
Аппаратные средства аутентификации пользователей (токены, смарт-карты, биометрия и т. п.)	То же в интеграции со средствами защиты от несанкционированного доступа (НСД) и криптографическими средствами
Разграничение доступа пользователей к конфиденциальной информации штатными механизмами защиты информации и разграничение доступа операционных систем, прикладных программ, маршрутизаторов и т. п.	Программно-аппаратные средства защиты от НСД и разграничения доступа
Программные средства шифрования и электронной цифровой подписи (ЭЦП) для обмена конфиденциальной информацией по открытым каналам связи	Аппаратные шифраторы для выработки качественных ключей шифрования и ЭЦП; интеграция со средствами защиты от НСД и аутентификации
Средства "прозрачного" шифрования логических дисков пользователей, используемых для хранения конфиденциальной информации	Средства "прозрачного" шифрования конфиденциальной информации, хранимой и обрабатываемой на серверах
Средства уничтожения неиспользуемой конфиденциальной информации (например, с помощью соответствующих функций шифраторов)	Аппаратные уничтожители носителей информации
Средства резервного копирования, источники бесперебойного питания, уничтожители бумажных документов	