Выявление потенциальных угроз и каналов утечки информации

В этой главе

- *Угрозы информационной безопасности в сферах деятельности государства*
- *Анализ характеристик угроз и уязвимых мест для информации в ИС*
- *Угрозы для объектов ИС*
- *Угрозы для процессов, процедур и программ обработки информации*
- *Угрозы для информации в каналах связи*
- *Угрозы информации, возникающие за счет побочных электромагнитных излучений и наводок*
- *Угрозы для механизмов управления системой защиты*
- *Как проводить анализ угроз и каналов утечки информации*

<<< Этапы	Направления >>>	010				020				030				040				050			
		Защита объектов ИС				Защита процессов и программ				Защита каналов связи				ПЭМИН				Управление системой защиты			
	Основы >>>	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства
		011	012	013	014	021	022	023	024	031	032	033	034	041	042	043	044	051	052	053	054
100	Определение информации, подлежащей защите	111	112	113	114	121	122	123	124	131	132	133	134	141	142	143	144	151	152	153	154
200	Выявление угроз и каналов утечки информации	211	212	213	214	221	222	223	224	231	232	233	234	241	242	243	244	251	252	253	254
300	Проведение оценки уязвимости и рисков	311	312	313	314	321	322	323	324	331	332	333	334	341	342	343	344	351	352	353	354
400	Определение требований к СЗИ	411	412	413	414	421	422	423	424	431	432	433	434	441	442	443	444	451	452	453	454
500	Осуществление выбора средств защиты	511	512	513	514	521	522	523	524	531	532	533	534	541	542	543	544	551	552	553	554
600	Внедрение и использование выбранных мер и средств	611	612	613	614	621	622	623	624	631	632	633	634	641	642	643	644	651	652	653	654
700	Контроль целостности и управление защитой	711	712	713	714	721	722	723	724	731	732	733	734	741	742	743	744	751	752	753	754

Угрозы информационной безопасности в сферах деятельности государства (200)

На основе принципов и положений государственной политики обеспечения информационной безопасности должны проводиться все мероприятия по защите информации в политической, экономической, оборонной и других сферах деятельности государства.

В этой связи следует учитывать, что в каждой из этих сфер имеются свои особенности, что в первую очередь связано с характером решения поставленных задач, наличием свойственных каждой области информационной безопасности слабых элементов и уязвимых звеньев.

В каждой сфере деятельности государства требуется специальная организация работ, а также использование форм и способов обеспечения информационной безопасности.

В политической сфере **наиболее серьезной опасности подвергаются:**

- общественное сознание и политическая ориентация различных групп населения страны (регионов), непрерывно формируемые под воздействием отечественных и зарубежных средств массовой информации (печать, радио, телевидение);
- система принятия политических решений, существенно зависящая от качества и своевременности ее информационного обеспечения;
- право политических организаций, партий, объединений и движений на свободное выражение своих программ, социально-политических и экономических ориентацией через средства массовой информации;
- система регулярного информирования населения органами государственной власти и управления о политической и социально-экономической жизни через средства массовой информации, пресс-центры, центры общественных связей и т.п.;
- система формирования общественного мнения, включающая специальные институты, центры и службы выявления, изучения и анализа общественного мнения.

В **сфере экономики** наиболее подвержены воздействию угроз информационной безопасности система государственной статистики, источники, порождающие информацию о коммерческой деятельности хозяйственных субъектов всех форм собственности, о потребительских свойствах товаров и услуг, системы сбора и обработки финансовой, биржевой, налоговой, таможенной информации, информации о внешнеэкономической деятельности государства и коммерческих структур.

В **оборонной сфере** к наиболее уязвимым звеньям относятся:

- информационные ресурсы аппарата Министерства обороны, Генерального штаба, Главных штабов видов Вооруженных сил и родов войск, научно-исследовательских учреждений, содержащие сведения и данные об оперативных и стратегических планах подготовки и ведения боевых действий, о составе и дислокации войск, о мобилизационной готовности, тактико-технических характеристиках вооружения и военной техники;
- информационные ресурсы предприятий оборонного комплекса, содержащие сведения о научно-техническом и производственном потенциале, об объемах поставок и запасах стратегических видов сырья и материалов, об основных направлениях развития вооружения, военной техники, их боевых возможностях и проводимых в интересах обороны фундаментальных и прикладных НИР;
- системы связи и управления войсками и оружием, их информационное обеспечение;
- политико-моральное состояние войск в части, зависящей от информационно-пропагандистского воздействия;
- информационная инфраструктура, в том числе центры обработки и анализа информации Генерального штаба и информационные подразделения штабов видов Вооруженных сил, штабов объединений и соединений видов Вооруженных Сил и родов войск, пунк-

Угрозы в сфере экономики...

ты управления, узлы и линии радиосвязи, радиорелейной, тропосферной и спутниковой, а также линии проводной связи, развертываемые и арендуемые Министерством обороны и другими силовыми структурами.

Разновидности угроз (200)

Все потенциально возможные негативные явления указанного характера могут быть разделены на такие разновидности:

1. Снижение ниже допустимого уровня качества информации, используемой для решения имеющих существенное значение задач;

2. Несанкционированное получение в злоумышленных целях такой информации, на доступ к которой по тем или иным причинам наложены ограничения;

3. Несанкционированное использование информации, являющейся чьей-либо собственностью;

4. Вредное воздействие информации на людей, технические устройства (системы) и технологические процессы.

Угрозы информации по происхождению могут быть случайными (вызываемыми недостаточной надежностью информационных систем, стихийными бедствиями и другими непредвиденными обстоятельствами) или злоумышленными (вызываемыми целенаправленными действиями злоумышленников).

Угрозы безопасности информации (200)

Они могут исходить из внешних и внутренних источников.

К ***внешним*** относятся:

- деятельность разведывательных и специальных служб;
- деятельность различных политических, военных, финансовых и других экономических структур, направленная против интересов государства;
- преступные действия отдельных групп, формирований и физических лиц.

К ***внутренним источникам*** относятся:

- противозаконная деятельность различных структур, группировок и отдельных лиц в области использования информации для сокрытия правонарушений, нанесения убытков законным интересам других юридических и физических лиц;
- нарушение установленных правил сбора, обработки и передачи информации.

Другими формами угроз безопасности информации являются:

- утечка информации по техническим каналам;
- хищение, уничтожение, искажение, подделка, блокирование, задержка, копирование информации в результате несанкционированного доступа к носителям или средствам ее обработки, передачи и хранения;
- хищение или уничтожение (порча) собственно носителей информации.

Основные формы организации работ по защите информации таковы:

- выполнение государственного заказа на проведение соответствующих работ;
- лицензирование деятельности предприятий и организаций по вопросам защиты информации и допуска предприятий к работе со сведениями, составляющими государственную тайну;
- сертификация систем и средств информации и связи в части защищенности информации от утечки по техническим каналам, а также сертификация средств защиты и контроля;
- аттестация объектов по выполнению требований безопасности информации;
- проведение контрольных мероприятий по оценке эффективности защиты информации.

Для проведения работ по защите информации могут быть привлечены на договорной основе специализированные предприятия и организации, имеющие лицензии на проведение работ в области защиты информации.

Значительная роль в государственной системе защиты информации отводится научно-исследовательским,

Противозаконная деятельность группировок...

научно-техническим, проектным и конструкторским организациям, которые призваны внести свой вклад не только в разработку всей совокупности нормативных и методических документов по защите информации, но и на практике реализовать разработку и внедрение методов, способов и средств защиты информации.

Развитие государственной системы защиты информации невозможно без разработки и практического освоения специалистами методического обеспечения, затрагивающего такие вопросы, как комплексная оценка угроз безопасности информации, определение ущерба, нанесенного несанкционированным распространением информации, правовая и материальная ответственность должностных лиц и специалистов за утечку информации по техническим каналам, и других аспектов защиты информации.

Компьютерные терминалы и настольные компьютеры используются везде. Компьютерное оборудование стало дружественным к пользователю, поэтому многие желающие могут быстро и легко освоить его. Число служащих в организации, имеющих доступ к компьютерному оборудованию и информационной технологии, постоянно растет.

Доступ к информации уже не ограничивается узким кругом лиц из руководства организации. Этот процесс привел к "демократизации преступления". Чем больше людей получало доступ к информационной технологии и компьютерному оборудованию, тем больше возникало возможностей для совершения компьютерных преступлений.

Интересно

Типичный компьютерный преступник — это немолодой хакер, использующий телефон и домашний компьютер для получения доступа к большим компьютерам. Типичный компьютерный преступник — это служащий, которому разрешен доступ к системе, пользователем которой он является. В США компьютерные преступления, совершенные служащими, составляют 70—80% ежегодного ущерба, связанного с компьютерами. Остальные 20% дают действия нечестных и недовольных сотрудников.

Следующие признаки могут свидетельствовать о наличии уязвимых мест в системе информационной безопасности.

1. Не разработано положений о защите информации или они не соблюдаются. Не назначен ответственный за информационную безопасность.

2. Пароли пишутся на компьютерных терминалах, помещаются в общедоступные места, ими делятся с другими или они появляются на компьютерном экране при их вводе.

3. Удаленные терминалы и микрокомпьютеры оставляются без присмотра в рабочие и нерабочие часы. Данные отображаются на компьютерных экранах, оставленных без присмотра.

4. Не существует ограничений на доступ к информации или на характер ее использования. Все пользователи имеют доступ ко всей информации и могут использовать все функции системы.

5. Не ведутся системные журналы и не хранится информация о том, кто и для чего использует компьютер.

6. Изменения в программы вносятся без предварительного утверждения руководством.

7. Отсутствует документация или она не позволяет понимать поступающие отчеты и формулы, по которым получаются результаты, модифицировать программы, готовить данные для ввода, исправлять ошибки, производить оценку мер защиты и понимать сами данные — их источники, формат хранения, взаимосвязи.

8. Предпринимаются многочисленные попытки войти в систему с неправильными паролями.

9. Вводимые данные не проверяются на корректность и точность или при их проверке данные отвергаются из-за ошибок в них; требуется внести много исправлений в данные, не ведутся записи в журналах об отвергнутых транзакциях.

10. Имеют место выходы из строя системы, приносящие большие убытки.

11. Не производится анализ информации, обрабатываемой в компьютере, с целью определения необходимого для нее уровня безопасности.

12. Мало внимания уделяется информационной безопасности. Хотя политика безопасности и существует, считается, что практически она не нужна.

Анализ характеристик угроз и уязвимых мест для информации в ИС (200)

Анализ потенциально возможных угроз информации является одним из первых и обязательным этапом разработки любой защищенной ИС. При этом составляется как можно более полная совокупность угроз, анализируется степень риска при реализации той или иной угрозы, после чего определяются направления защиты информации в конкретной ИС.

Разнообразие потенциальных угроз информации в ИС столь велико, что не позволяет предусмотреть каждую из них, поэтому анализируемые характеристики угроз следует выбирать с позиций здравого смысла, одновременно выявляя не только собственно угрозы, вероятность их осуществления, масштаб потенциального ущерба, но и их источники.

Определение

Угрозой может быть любое лицо, объект или событие, которое, в случае реализации, может потенциально стать причиной нанесения вреда ИС.

Угрозы могут быть злонамеренными (умышленная модификация критической информации), случайными (ошибки в вычислениях или случайное удаление файла) или природными (наводнение, ураган, молния и т.п.)

Непосредственный вред, вызванный угрозой, называется воздействием угрозы.

Уязвимыми являются слабые места СЗИ ИС, которые могут быть использованы для реализации угрозы. Уменьшение уязвимых мест ИС может снизить или устранить риск от угроз ИС.

Идентификация угроз предполагает рассмотрение воздействий и последствий реализации угроз. Проблемы, возникшие после реализации угрозы, приводит к раскрытию, модификации, разрушению или отказу в обслуживании. Более значительные долговременные последствия реализации угрозы приводят к утрате управления войсками, нарушению тайны, потере адекватности данных, к человеческим жертвам или иным долговременным эффектам.

Угрозы безопасности информации, ИС и субъектов информационных отношений

Под угрозой (вообще) понимают потенциально возможное событие, действие (воздействие), процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам. Угрозой интересам субъектов информационных отношений будем называть потенциально возможное событие, процесс или явление, которое посредством воздействия на информацию или другие компоненты ИС может прямо или косвенно привести к нанесению ущерба интересам данных субъектов.

В силу перечисленных особенностей современных ИС, существуют различные виды угроз безопасности субъектов информационных отношений. Нарушением безопасности будем называть реализацию угрозы безопасности.

В настоящей работе предпринята попытка возможно более полного анализа угроз безопасности субъектов информационных отношений. Однако следует учитывать, что научно-технический прогресс может привести к появлению принципиально новых видов угроз и что изощренный ум злоумышленника способен изобрести новые способы преодоления систем безопасности, НСД к данным и дезорганизации работы ИС.

Описываемый подход состоит в классификации типов воздействий, возможных в ИС, которая позволила бы специфические технические угрозы сгруппировать в соответствии с предложенной матрицей безопасности.

Напомним, что элементами матрицы, характеризующими данную тему является:

200 Выявление угроз и каналов утечки информации (общие вопросы)

210 Выявление угроз для объектов информационных систем;

220 Выявление угроз для процессов, процедур и программ обработки информации;

230 Выявление угроз для информации, передаваемой по каналам связи;

240 Выявление угроз, возникающих от побочных электромагнитных излучений и наводок;

250 Выявление угроз для механизмов управление системой защиты.

Откуда исходит угроза (220)

Если первоначально понятие “хакер” ассоциировалось с образом способного молодого человека, который “шарит” по чужим сетям ради любопытства, то сегодня пиратский бизнес поставлен на профессиональную основу и им занимаются вполне взрослые и квалифицированные люди.

Кстати

Понятно, что и интерес у них к чужой информации исключительно коммерческий. Существуют хакерские электронные доски объявлений, где фигурируют расценки на добычу секретной информации, идет обмен известными (хакерам) паролями и кодами доступа к чужим информационным системам.

В наши дни компьютерное пиратство приобрело разнообразные формы и широкий размах. При этом значительный процент преступлений приходится на долю собственных сотрудников организаций (как нынешних, так и бывших).

К сожалению, факты утечки информации изнутри фирмы, как правило, скрываются. Видимо, ущерб от внешнего врага не столь страшен, как недовольство акционеров, готовых обвинить руководство компании в некомпетентности.

Теперь никто не хранит ценную информацию (финансовые документы, деловую переписку, информацию о клиентах) в виде обычных файлов, которые можно легко удалять или копировать.

Секреты удобно помещать в базы данных, доступ к которым гораздо сложнее, чем к обычным файлам, однако, как показывает практика, злоумышленники успешно используют возможности СУБД в личных целях.

Так, инженеры компании Nothern Telecom незаметно модифицировали корпоративную БД, чтобы контролировать реализацию телефонного оборудования своей компанией. Накопленную таким образом информацию они пытались сбыть одной из конкурирующих фирм за очень приличный гонорар.

Факты

В эру развитых компьютерных технологий, когда весь мир превращается в единое кибернетическое пространство, когда информация в электронном формате становится весьма дорогостоящим товаром, а при высоком уровне современных программ хакером может стать каждый, проблема защиты информации выходит на первый план.

Основные виды угроз безопасности субъектов информационных отношений

Основными видами угроз безопасности ИС и информации (угроз интересам субъектов информационных отношений) являются:

- стихийные бедствия и аварии (наводнение, ураган, землетрясение, пожар и т.п.);
- сбои и отказы оборудования (технических средств) ИС;
- последствия ошибок проектирования и разработки компонентов ИС (аппаратных средств, технологии обработки информации, программ, структур данных и т.п.);
- ошибки эксплуатации (пользователей, операторов и другого персонала);
- преднамеренные действия нарушителей и злоумышленников (обиженных лиц из числа персонала, преступников, шпионов, диверсантов и т.п.).

Наиболее распространенные угрозы информации в ИС (220)

Прежде чем переходить к рассмотрению средств обеспечения информационной безопасности, рассмотрим самые распространенные угрозы, которым подвержены современные компьютерные системы. Знание возможных угроз, а также уязвимых мест защиты, которые эти угрозы обычно эксплуатируют, необходимо для выбора наиболее экономичных средств обеспечения безопасности.

Самыми частыми и самыми опасными по размерам 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, а иногда они создают слабости, которыми могут воспользоваться злоумышленники — таковы обычно ошибки администрирования.

Согласно статистике, 65% потерь — следствие непреднамеренных ошибок. ***Пожары и наводнения можно считать пустяками по сравнению с безграмотностью и расхлябанностью.*** Очевидно, радикальный способ борьбы с непреднамеренными ошибками — максимальная автоматизация и строгий контроль за правильностью совершаемых действий.

Весьма опасны так называемые обиженные сотрудники — нынешние и бывшие. Как правило, их действиями движет желание нанести вред организации-обидчику, например:

- повредить оборудование;
- встроить логическую бомбу, которая со временем разрушит программы и/или данные;
- ввести ошибочные данные;
- удалить или;
- изменить их.

Это важно

Обиженные сотрудники, даже бывшие, знакомы с порядками в организации и способны вредить весьма эффективно. Необходимо следить за тем, чтобы при увольнении сотрудника его права доступа к информационным ресурсам аннулировались.

Угрозы, исходящие от окружающей среды, к сожалению, отличаются большим разнообразием. В первую очередь, следует выделить нарушения инфраструктуры — аварии электропитания, временное отсутствие связи, перебои с водоснабжением, гражданские беспорядки и т.п.

Опасны, разумеется, стихийные бедствия и события, воспринимаемые как стихийные бедствия — пожары, наводнения, землетрясения, ураганы. По данным статистики, на долю огня, воды и аналогичных “врагов”, среди которых самый опасный — низкое качество электропитания, приходится 13% потерь, нанесенных информационным системам.

Много говорят и пишут о хакерах, но исходящая от них угроза зачастую преувеличивается. Верно, что почти каждый Internet-сервер по несколько раз в день подвергается попыткам проникновения; верно, что иногда такие попытки оказываются удачными; действительно изредка подобные действия связаны со шпионажем.

Однако в целом ущерб от деятельности хакеров по сравнению с другими угрозами представляется не столь уж значительным. Скорее всего, больше пугает фактор непредсказуемости действий людей такого сорта. Представьте себе, что в любой момент к вам в квартиру могут

забраться посторонние люди. Даже если они не имеют злого умысла, а зашли просто так, посмотреть, нет ли чего интересного, — приятного в этом мало.

Угрозы и каналы утечки информации (200)

Предел степени сохранности данных в любой ИС определяется прежде всего факторами, связанными с участием в ее работе человека. Естественно, что не существует каких-либо причин, по которым в ИС, базирующихся на современных средствах вычислительной техники, невозможно было бы обеспечить большую степень сохранности данных, чем в обычных системах сбора, накопления и обработки информации.

Угрозами информации будем называть потенциально возможные события, которые могут привести к нарушению целостности информации либо оказать негативное воздействие на процессы ее обработки.

Определение

Основными каналами утечки информации считается хищение носителей информации и документов, получаемых в результате работы информационных систем; копирование информации на ПК; несанкционированное подключение к аппаратуре и линиям связи; перехват электромагнитных излучений в процессе обработки информации и многое другое.

Классификация угроз информации (200)

В процессе хранения и обработки информация может быть подвержена воздействию факторов, как случайных, так и умышленных. Все множество потенциальных угроз по природе их возникновения разделяется на два класса: естественные (объективные) и искусственные (субъективные).

Угрозы данным — потенциально существующая опасность случайного или преднамеренного разрушения, несанкционированного получения или модификации данных, обусловленная структурой системы обработки, а также условиями обработки и хранения данных.

Естественные угрозы — это угрозы, вызванные воздействиями на ИС и ее элементы объективных физических процессов или стихийных природных явлений, независящих от человека.

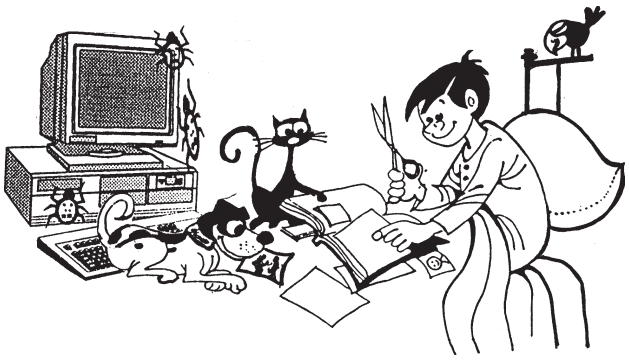
Искусственные угрозы — это угрозы ИС, вызванные деятельностью человека. Среди них, исходя из мотивации действий, можно выделить:

- непреднамеренные (неумышленные, случайные) угрозы, вызванные ошибками в проектировании ИС и ее элементов, ошибками в программном обеспечении, ошибками в действиях персонала и т.п.;
- преднамеренные (умышленные) угрозы, связанные с корыстными устремлениями людей (злоумышленников).

Случайные угрозы информации

К случайным угрозам относятся:

- воздействие сильных магнитных полей на магнитные носители информации или дефекты оборудования, приводящие к разрушению хранимой информации;
- небрежное хранение и учет носителей, а также их нечеткая идентификация;
- программы пользователей, работающие в мультипрограммном режиме и содержащие невыявленные ошибки, представляют угрозу для правильно работающих программ;
- ошибки в программах обработки могут приводить к потере или искажению вводимой и хранящейся информации;
- ошибки ввода данных
- сбои и ошибки в работе аппаратуры, вызванные перепадами напряжения в сети питания, неисправностями энергоснабжения, временными или постоянными ошибками в ее схемах;
- неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы (неумышленная порча оборудования, удаление, искажение файлов с важной информацией или программ, в том числе системных и т.п.);
- неправомерное отключение оборудования или изменение режимов работы устройств и программ;
- неумышленная порча носителей информации;
- запуск технологических программ, способных при некомпетентном использовании привести к потере



Неумышленная порча информации...

работоспособности системы (зависания или зацикливания) или осуществляющих необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т.п.);

- нелегальное внедрение и использование неучтенных программ, не являющихся необходимыми для выполнения служебных обязанностей;
- неосторожные действия, приводящие к разглашению конфиденциальной информации;
- разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);
- проектирование архитектуры системы, технологии обработки данных, разработка прикладных программ с возможностями, представляющими опасность для работоспособности системы и безопасности информации;
- вход в систему в обход средств защиты (загрузка посторонней операционной системы со сменных магнитных носителей и т.п.);
- некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности;
- пересылка данных по ошибочному адресу абонента (устройства);
- неумышленное повреждение каналов связи.

Умышленные угрозы

- использование известного способа доступа к системе или ее части с целью навязывания запрещенных действий, обращения к файлам, содержащим интересующую информацию;
- маскировка под истинного пользователя путем навязывания характеристик авторизации такого пользователя;
- маскировка под истинного пользователя после получения характеристик (авторизации) доступа;
- использование служебного положения, т.е. незапланированного просмотра (ревизии) информации файлов сотрудниками вычислительной установки;
- физическое разрушение системы или вывод из строя наиболее важных компонентов ИС;
- отключение или вывод из строя подсистем обеспечения безопасности ИС;
- изменение режимов работы устройств или программ;
- подкуп или шантаж персонала или отдельных пользователей, имеющих определенные полномочия;
- хищение носителей информации и несанкционированное копирование носителей информации;
- чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
- незаконное получение паролей и других реквизитов разграничения доступа с последующей маскировкой под законного пользователя;
- вскрытие шифров криптозащиты информации;
- внедрение аппаратных и программных закладок и вирусов, позволяющих преодолевать систему защиты, скрытно и незаконно осуществлять доступ к системным ресурсам ИС;
- незаконное подключение к линиям связи с целью работы “между строк”, с использованием пауз в действиях законного пользователя от его имени с последующим вводом ложных сообщений или модификацией передаваемых сообщений;
- незаконное подключение к линиям связи с целью прямой подмены законного пользователя путем его физического отключения после входа в систему и успешной аутентификации с последующим вводом дезинформации и навязыванием ложных сообщений;
- перехват данных, передаваемых по каналам связи, и их анализ с целью выяснения протоколов обмена, правил вхождения в связь и авторизации пользователя и последующих попыток их имитации для проникновения в систему.

Непреднамеренные искусственные угрозы

Основные непреднамеренные искусственные угрозы ИС (действия, совершаемые случайно, по незнанию, невнимательности или халатности, из любопытства, но без злого умысла) таковы:

- неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы (неумышленная порча оборудования, удаление, искажение файлов с важной информацией или программ, в том числе системных и т.п.);
- неправомерное включение оборудования или изменение режимов работы устройств и программ;
- неумышленная порча носителей информации;
- запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания) или осуществляющих необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т.п.);
- нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и других, не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с после-

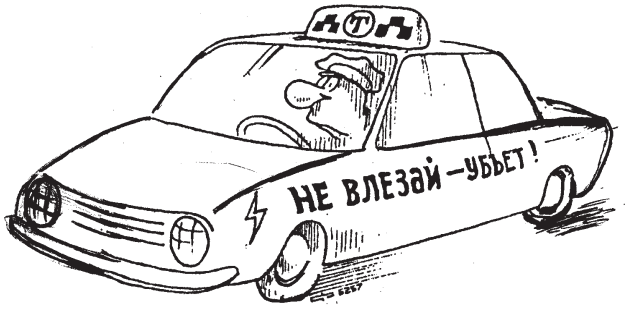
дующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);

- заражение компьютера вирусами;
- неосторожные действия, приводящие к разглашению конфиденциальной информации, или делающие ее общедоступной;
- разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);
- проектирование архитектуры системы, технологии обработки данных, разработка прикладных программ с возможностями, представляющими опасность для работоспособности системы и безопасности информации;
- игнорирование организационных ограничений (установленных правил) при ранге в системе;
- вход в систему в обход средств защиты (загрузка посторонней операционной системы со сменных магнитных носителей и т.п.);
- некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности;
- пересылка данных по ошибочному адресу абонента (устройства);
- ввод ошибочных данных;
- неумышленное повреждение каналов связи.

Преднамеренные искусственные угрозы

Основные пути умышленной дезорганизации работы, вывода системы из строя, проникновения в систему и несанкционированного доступа к информации таковы:

- физическое разрушение системы (взрыв, поджог и т.п.) или вывод из строя наиболее важных компонентов компьютерной системы (устройств, носителей важной системной информации, лиц из числа персонала и т.п.);
- отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т.п.);
- действия по дезорганизации функционирования системы (изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных радиопомех на частотах устройств системы и т.п.);
- внедрение агентов в число персонала системы (в том числе, возможно, и в административную группу, ответственную за безопасность);



Преднамеренные угрозы...

- вербовка (подкуп, шантаж и т.п.) персонала или отдельных пользователей, имеющих определенные полномочия;
- применение подслушивающих устройств, дистанционной фото- и видео съемки и т.п.;
- перехват побочных электромагнитных, акустических и других излучений устройств и линий связи, а также наводок активных излучений на вспомогательные технические средства, непосредственно не участвующие в обработке информации (телефонные линии, сети питания, отопления и т.п.);
- перехват данных по каналам связи, и их анализ с целью выяснения протоколов обмена, правил вхождения в связь и авторизации пользователя и последующих попыток их имитации для проникновения в систему;
- хищение носителей информации (магнитных дисков, лент, микросхем памяти, запоминающих устройств и ПК);
- несанкционированное копирование носителей информации;
- хищение производственных отходов (распечаток, записей, списанных носителей информации и т.п.);
- чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
- чтение информации из областей оперативной памяти, используемых операционной системой (в том числе подсистемой защиты) или другими пользователями, в асинхронном режиме используя недостатки мультизадачных операционных систем и систем программирования;
- незаконное получение паролей и других реквизитов разграничения доступа (агентурным путем, используя халатность пользователей, путем подбора, имитации интерфейса системы и т.д.) с последующей маскиров-

кой под зарегистрированного пользователя (“маскарад”);

- несанкционированное использование терминалов пользователей, имеющих такие уникальные физические характеристики, как номер рабочей станции в сети, физический адрес, адрес в системе связи, аппаратный блок кодирования и т.п.;
- вскрытие шифров криптозащиты информации;
- внедрение аппаратных спецвложений, программных закладок и вирусов (“троянских коней” и “жучков”), т.е. таких участков программ, которые не нужны для осуществления заявленных функций, но позволяющих преодолеть систему защиты, скрытно и незаконно осуществлять доступ к системным ресурсам с целью регистрации и передачи критической информации или дезорганизации функционирования системы;
- незаконное подключение к линиям связи с целью работы “между строк”, с использованием пауз в действиях законного пользователя от его имени с последующим вводом ложных сообщений или модификацией передаваемых сообщений;
- незаконное подключение к линиям связи с целью прямой подмены законного пользователя путем его физического отключения после входа в систему и успешной аутентификации с последующим вводом дезинформации и навязыванием ложных сообщений.

Следует заметить, что чаще всего для достижения цели злоумышленник использует совокупность из перечисленных способов.

Классификация возможных каналов утечки информации (200)

Использование ИС в военной, коммерческой и других областях человеческой деятельности порождает ряд специфических проблем, которые необходимо решить для защиты обрабатываемой информации. Одной из таких проблем является классификация возможных каналов утечки информации. Под возможным каналом утечки будем понимать способ, позволяющий нарушителю получить доступ к обрабатываемой или хранящейся в ПК информации.

Классификацию возможных каналов утечки информации в первом приближении можно провести исходя из типа средства, являющегося основным при получении информации по возможному каналу утечки.

Следует различать три типа средств: человек, аппаратура, программа.

В соответствии с каждым типом средства все возможные каналы утечки также разбиваются на три группы.

Применительно к пользователям ПК возможны следующие каналы утечки:

- хищение носителей информации;
- чтение информации с экрана посторонним лицом (во время отображения информации на экране законным пользователем или в отсутствие его на рабочем месте);
- чтение информации из оставленных без присмотра распечаток программ.

В группе каналов, в которых основное средство — аппаратура, можно выделить такие пути утечки:

- подключение к устройствам ПК специально разработанных аппаратных средств, обеспечивающих доступ к информации;
- использование специальных технических средств для перехвата электромагнитных излучений технических средств ПК.

В группе каналов, в которых основное средство — программа, можно выделить такие основные пути утечки:

- несанкционированный доступ программы к информации;
- расшифровка программой зашифрованной информации;

Утечка информации по каналам ПЭМИН может формироваться за счет:

- побочных электрических и магнитных полей, создаваемых информативными сигналами СВТ, технических средств обработки информации, а также вспомогательных технических средств и систем, на которые могут воздействовать опасные сигналы;
- электрических и магнитных полей, создаваемых гармониками переменного тока электропитания СВТ, модулированными составляющими информативного сигнала;
- наводок информативного сигнала в линиях и каналах систем передачи данных и вспомогательных систем, в цепи электропитания, заземления и других проводящих коммуникациях, имеющих выход за пределы зоны безопасности информации;
- радиоизлучений генераторов, входящих в состав СВТ и других технических средств, а также излучений паразитной генерации, возникающей при неустойчивой работе логических элементов, усилителей, формирователей сигналов, модулируемых информативным сигналом;
- неравномерности потребляемого СВТ тока по сети электропитания.

Все каналы проникновения в систему и утечки информации разделяют на прямые и косвенные. Под косвенными понимают такие каналы, использование которых не требует проникновения в помещения, где расположены компоненты системы. Для использования прямых каналов такое проникновение необходимо. Прямые каналы можно использовать без внесения изменений в компоненты системы или с изменениями компонентов.

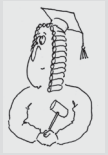
По способу получения информации потенциальные каналы доступа можно разделить на:

- физический;
- электромагнитный (перехват излучений);
- информационный (программно-математический).

При контактном НСД (физическом, программно-математическом) возможные угрозы информации реализуются путем доступа к элементам ИС, носителям информации, к самой вводимой и выводимой информации (и результатам), программному обеспечению (в том числе к операционным системам), а также — путем подключения к линиям связи.

При бесконтактном доступе (например, по электромагнитному каналу) возможные угрозы информации реализуются перехватом излучений аппаратуры ИС, в том числе наводимых в токопроводящих коммуникациях и цепях питания, перехватом информации в линиях связи, вводом в линии связи ложной информации, визуальным наблюдением (фотографирование) устройств отображения информации, прослушиванием переговоров персонала ИС и пользователей.

Преступления, в том числе и компьютерные, совершаются людьми. Пользователи системы и ее персонал, с одной стороны, являются составной частью, необходимым элементом ИС, а с другой стороны, они же являются основной причиной и движущей силой нарушений и преступлений.



Кстати

Угрозы для объектов ИС (210)

Неавторизованный доступ к ИС (210)

Неавторизованный доступ имеет место, когда не уполномоченный пользователь, получает доступ к ИС, действуя обычно как законный пользователь.

Для получения неавторизованного доступа используются:

- общие пароли;
- угадывание пароля;
- перехват пароля.

Общие пароли позволяют неавторизованному пользователю получить доступ к ИС и привилегии законного пользователя; это происходит с одобрения кого-либо из законных пользователей, под чьим именем осуществляется доступ.

Угадывание пароля является традиционным способом неавторизованного доступа.

Перехват пароля является процессом, в ходе которого законный пользователь раскрывает учетный идентификатор и пароль другого пользователя.

Неавторизованный доступ к ИС может происходить с использованием следующих уязвимых мест:

- отсутствие или недостаточность схемы идентификации и аутентификации,
- совместно используемые пароли,
- плохое управление паролями или простые для угадывания пароли,
- использование известных системных брешей и уязвимых мест, которые не были исправлены,
- однопользовательские ПК, не имеющие парольной защиты во время загрузки,
- неполное использование механизмов блокировки ПК,
- хранимые в пакетных файлах на дисках ПК пароли доступа к ИС,
- слабый физический контроль за сетевыми устройствами,
- незащищенные модемы,
- отсутствие тайм-аута при установлении сеанса и регистрации ошибочных попыток,
- отсутствие отключения терминала при многочисленных неудачных попытках установления сеанса и регистрации таких попыток,
- отсутствие сообщений “дата/время последнего удачного сеанса” и “неуспешная попытка установления сеанса” в начале сеанса,
- отсутствие верификации пользователя в реальном времени (для выявления маскарада).

Несоответствующий доступ к ресурсам ИС (210)

Несоответствующий доступ происходит, когда пользователь получает доступ к ресурсу, который не разрешено использовать. Это может происходить тогда, когда права пользователей на доступ к ресурсу не обозначены должным образом. Однако несоответствующий доступ может также происходить потому, что механизм управления доступом или механизм назначения привилегий недостаточно детализированы. В этих случаях единственный способ предоставить пользователю необходимые права доступа или привилегии со-

стоит в том, чтобы предоставлять пользователю больше доступа или привилегий, чем необходимо.

Несоответствующий доступ к ресурсам ИС может происходить при использовании следующих типов уязвимых мест:

- использование при назначении прав пользователям по умолчанию таких системных установок, которые являются слишком разрешающими для пользователей,
- неправильное использование привилегий администратора или менеджера ИС,
- данные, хранящиеся с неадекватным уровнем защиты или вообще без защиты,
- недостаточное или неправильное использование механизма назначения привилегий для пользователей, ПК, на которых отсутствует контроль доступа на уровне файлов.

Угроза доступа (210)

Неуполномоченный человек может получить логический доступ к ИС.

Термин “неуполномоченный человек” определяет тех, кто имеет или может попытаться получить физический доступ к системе и ее терминалам, но не имеет полномочий на получение логического доступа к ее ресурсам.

Предполагается, что такие неуполномоченные люди могут обладать широким диапазоном навыков, способов и побуждений в пределах от любознательного дилетанта с ограниченными техническими знаниями до тех, кто понимает значение информации, хранимой в системе, подготовлен, чтобы сосредоточить значительные усилия для входа в систему и имеет некоторую техническую осведомленность о ее устройстве.

Предполагается, что значение охраняемых ресурсов не обязывает к применению строгих средств управления безопасностью ИТ, а средства физического контроля оповестят ответственных лиц системы о физическом присутствии нападающих внутри контролируемого пространства.

Неправильное использование привилегий администратора...

Угроза автора (210)

Пользователь может получить доступ к ресурсам, право доступа к которым ему не предоставлено.

Термин “пользователь” определяет людей, которым предоставлена некоторая форма законного доступа к системе, но не обязательно ко всем объектам данных.

Относительно этой угрозы идентифицированы две категории пользователей. Первая — может быть принята как имеющая ограниченные технические навыки и доступ к системе только через средства прикладного уровня. Вторая — как имеющая соответствующие технические навыки и доступ к средствам программирования и способная обходить средства управления системы.

Угроза физическая (210)

Критические к безопасности объекты ИС могут быть подвергнуты физической атаке, которая может поставить под угрозу безопасность ИС.

Угроза дефекта (210)

Нарушения безопасности могут происходить вследствие дефектов в ИС.

Пользователи или внешние агенты угрозы могут случайно или путем направленного поиска обнаруживать дефекты в конструкции или применении ИС, что может привести к использованию уязвимости.

Угроза следу (210)

Относящиеся к безопасности события не могут быть зарегистрированы или различимы пользователем.

Управление и контроль безопасности ИС зависят от способности системы обнаружить и сообщить местонахождение относящихся к безопасности событий, произвести идентификацию ответственных за такие события и их результаты и защитить записи событий от несанкционированного доступа, изменения или разрушения.

Угрозы несанкционированного доступа к информации в ИС (210)

- наблюдение за информацией с целью ее запоминания в процессе ее обработки;
- хищение носителей информации;
- сбор производственных отходов, содержащих обрабатываемую информацию;

- преднамеренное считывание данных из файлов других пользователей;
- чтение остаточной информации, т.е. данных, остающихся на магнитных носителях после выполнения задания;
- копирование носителей информации;
- преднамеренное использование для доступа к информации терминалов зарегистрированных пользователей;
- маскировка под зарегистрированного пользователя путем похищения паролей и других реквизитов разграничения доступа к информации;
- использование для доступа к информации возможностей обхода механизма разграничения доступа, возникающих вследствие несовершенства общесистемных компонентов программного обеспечения (операционных систем, систем управления базами данных и др.) и неоднозначностями языков программирования применяемых в ИС;
- незаконное подключение специальной регистрирующей аппаратуры к устройствам системы или линиям связи;
- злоумышленное изменение программ таким образом, чтобы они наряду с основными функциями обработки информации осуществляли также несанкционированный сбор и регистрацию защищаемой информации;
- злоумышленный вывод из строя механизмов защиты;
- утечка обрабатываемой в ИС информации путем несанкционированного приема сигналов из линий связи. (Местами несанкционированного подключения к линиям передачи данных может быть передающее и приемное оборудование, расположенное в помещениях, а также внешние участки линий связи, кроссы и другие места коммутации линий связи);
- утечка обрабатываемой информации в время приема акустических сигналов, создаваемых работающими принтерами, подслушивание разговоров персонала ИС и пользователей с помощью направленных микрофонов, встроенных пьезодатчиков и других технических средств, а также приема электромагнитных сигналов, модулированных акустическими сигналами в результате паразитных акустоэлектрических преобразований в различных технических средствах.
- утечка обрабатываемой информации также в время визуального наблюдения за экранами устройств отображения информации коллективного или индивидуального пользования через открытые окна и двери, а также путем фотографирования и применения различных оптико-электронных устройств.

Особенности НСД (210)

Более непредсказуемыми в деле защиты информации являются меры по блокированию каналов несанкционированного доступа, связанных со злоумышленными действиями и побочными явлениями.

Злоумышленные действия могут предприниматься по отношению к обработке информации или в процессе ее обработки, с доступом или без доступа к элементам ИС, активно или пассивно (т.е. с изменением состояния системы или без).

В зависимости от этого основные типы злоумышленных угроз информации в ИС можно классифицировать следующим образом.

По отношению к обработке информации и без доступа злоумышленника к элементам ИС:

- подслушивание, использование оптических, визуальных или акустических средств;
- хищение носителей информации на заводах, где производится их ремонт;
- провоцирование на разговоры лиц, имеющих отношение к ИС.

В процессе обработки без доступа злоумышленника к объектам ИС:

- ПЭМИН устройств отображения, процессоров, внешних ЗУ, устройств и линий связи, вспомогательных устройств, устройств ввода/вывода и др.;
- паразитные наводки в сетях электропитания, в цепях часофикации, радиофикации, телефонизации, в системах канализации, вентиляции и теплоснабжения;
- подключение регистрирующей аппаратуры, генераторов помех; осмотр отходов производства за пределами контролируемой зоны.

По отношению к обработке информации с доступом злоумышленника к элементам ИС, но без изменения последних:

- копирование магнитных и других носителей, выходных и других документов;
- хищение производственных отходов, копирование с устройств отображения.

В процессе обработки с доступом злоумышленника к элементам ИС, но без изменения последних:

- копирование или запоминание информации в процессе обработки и при ее выводе;
- использование программных ловушек;
- маскировка под зарегистрированного пользователя;
- использование недостатков языков программирования;

- использование недостатков операционных систем, использование вирусов.

По отношению к обработке информации с доступом злоумышленника к элементам ИС с изменением последних:

- подмена машинных носителей, выходных документов, аппаратуры, элементов программ, элементов баз данных, хищение носителей и документов;
- включение в программы паразитных блоков ("троянских коней", "бомб" и т.п.); чтение остаточной информации в ЗУ после выполнения санкционированных запросов.

В процессе обработки с доступом злоумышленника к элементам ИС с изменением последних:

- незаконное подключение к аппаратуре и линиям связи, снятие информации на шинах питания.

Особенности НСД к информации в ИС определяются, в частности, следующими факторами:

- электронным характером представления данных, который часто усложняет или исключает обнаружение злоумышленных действий с ними (например, несанкционированное копирование данных из ЗУ и с машинных носителей);
- необходимостью обеспечения юридической значимости электронных документов;
- коллективным доступом к ресурсам ИС, создающим предпосылки к НСД;
- наличием совокупности потенциально возможных и дублирующих друг друга каналов НСД; при этом недооценка опасности одного из каналов может сделать бесполезной всю остальную защиту.

Специальные методы и технические средства съема информации (210)

- специально внедренные электронные средства (закладки), разрушающие или искажающие информацию;
- закладки, передающие обрабатываемую в ИС информацию или речевую информацию — переговоры в помещениях, где развернуты технические средства;
- облучение технических средств информационной системы зондирующими сигналами (так называемое навязывание);
- разрушение (искажение) технических средств автоматизированных систем путем подключения их элементов к посторонним источникам напряжения и др.

Акустические каналы утечки информации

Наиболее информативными методами получения конфиденциальных сведений из перечисленных являются акустический контроль и перехват переговоров в линиях связи, причем оба метода предусматривают использование специальных технических средств несанкционированного съема информации.

Акустический контроль

Для перехвата и регистрации акустической информации существует огромный набор средств разведки: микрофоны, электронные стетоскопы, акустические закладки, направленные и лазерные микрофоны, аппаратура магнитной записи. Набор акустических средств разведки, используемых для решения конкретной задачи, существенно зависит от возможности доступа агента в контролируемое помещение или к интересующим лицам.

В том случае, если имеется постоянный доступ к объекту контроля, могут быть использованы простейшие миниатюрные микрофоны, соединительные линии которых выводят в соседние помещения для регистрации и дальнейшего прослушивания акустической информации. Такие микрофоны диаметром 2.5 мм могут улавливать нормальный человеческий голос с расстояния до 20 м.

Если агенты не имеют постоянного доступа к объекту, но имеется возможность его кратковременного посещения под различными предлогами, то для акустической разведки используются миниатюрные диктофоны и магнитофоны закамуфлированные под предметы повседневного обихода: книгу, письменный прибор, пачку сигарет. Кроме этого, диктофон может находиться у кого-либо из присутствующих на закрытом совещании. В этом случае часто используют выносной микрофон, спрятанный под одеждой или закамуфлированный под часы, авторучку, пуговицу.

Интересно

Современные диктофоны обеспечивают непрерывную запись речевой информации от 30 минут до 7-8 часов, они оснащены системами акустопуска (VOX, VAS), автореверса, индикации даты и времени записи, дистанционного управления. Примером такого диктофона может выступать модель OLYMPUS L-400, который оборудован всеми перечисленными системами. В качестве носителя информации кроме магнитной ленты используются цифровые микрочипы и минидиски.

В случае если агентам не удается проникнуть на объект даже на короткое время, но есть доступ в соседние помещения, то для ведения разведки использу-

ются электронные стетоскопы, чувствительным элементом которых является пьезоэлемент. Электронные стетоскопы усиливают акустический сигнал, проникающий сквозь стены, пол, потолок в 20-30 тысяч раз и способны улавливать шорохи и тиканье часов через бетонные стены толщиной до 1 м.

Наряду с диктофонами для перехвата акустической информации используются акустические закладки, несанкционированно и скрытно устанавливаемые в помещениях, автомашинах. В качестве канала передачи перехваченной информации используются радио и оптический каналы, силовые, слаботочные и обесточенные коммуникации.

Наибольшее распространение получили радиозакладки, которые можно классифицировать по нескольким критериям:

- по используемому диапазону частот;
- по мощности излучения: маломощные — до 10 мВт, средней мощности — 10 мВт–100 мВт, большой мощности — свыше 100 мВт;
- по виду используемых сигналов: простой (с AM, FM и WFM), сложный (ППРЧ, шумоподобные сигналы);
- по способу модуляции: с модуляцией несущей, с модуляцией промежуточной частоты;
- по способу стабилизации частоты: нестабилизированные, со схемотехнической стабилизацией (мягкий канал), с кварцевой стабилизацией (кварцованные);
- по исполнению: в виде отдельного модуля, закамуфлированные под различные предметы (авторучка, калькулятор, электроудлинитель, деревянный брусок).

Срок службы радиозакладки в значительной степени зависит от типа питания. При использовании аккумуляторных батарей время непрерывной работы — от нескольких часов (авторучка — 2 часа) до нескольких суток (калькулятор — 15 суток). Если используется внешнее питание от телефонной линии, электросети, цепей питания бытовой аппаратуры, то срок службы радиозакладок практически не ограничен.

Радиозакладки обеспечивают дальность передачи от десятков метров (авторучка — 50 м) до 1 км. При использовании ретрансляторов дальность передачи перехваченной информации увеличивается до десятков километров. С целью повышения скрытности работы радиозакладки оборудуются системами акустопуска, дистанционного управления, пакетной передачи, используются шумоподобные, скремблированные, шифрованные сигналы.

Прием информации от радиозакладок обычно осуществляется на широкополосный приемник, например AR-8000 фирмы AOR, Ltd или IC-R10 фирмы Icom, Inc.

Сетевые закладки, использующие в качестве канала передачи информации электросеть, устанавливаются в электророзетки, удлинители, пилоты, бытовую аппаратуру или непосредственно в силовую сеть. Их недостатком является малая дальность передачи (в пределах одного здания до трансформаторной подстанции). Преимущество сетевой закладки — сложность обнаружения. Приемная часть выполнена в виде спецприемника.

Для перехвата акустической информации с передачей по телефонной линии используется "телефонное ухо". После дозвона на абонентский номер по определенной схеме агенту предоставляется возможность прослушивать помещение даже из другого города.

Контроль и прослушивание телефонных переговоров

Прослушивание телефонных каналов связи объекта в настоящее время является одним из основных способов получения конфиденциальной информации. Съем информации с телефонной линии связи может осуществляться либо непосредственным подключением к линии (в разрыв или параллельно), либо бесконтактно при помощи индуктивного датчика. Факт контактного подключения к линии легко обнаружить, в то время как использование индуктивного подключения не нарушает целостности кабеля и не вносит изменения в параметры телефонной линии.

Сигналы с телефонной линии могут записываться на магнитофон (используется специальный адаптер) или передаваться по радиоканалу.

Выполняются телефонные закладки в виде отдельных модулей (брусок) или камуфлируются под элементы телефонного оборудования: адаптеры, розетки, телефонные и микрофонные капсюли, конденсаторы. Телефонные закладки устанавливаются непосредственно в телефонный аппарат, телефонную трубку, розетку, а также непосредственно на телефонную линию. Передача информации от телефонной закладки начинается в момент поднятия трубки абонентом.

Наряду с телефонными и радиозакладками используются комбинированные закладки, которые при ведении телефонных переговоров осуществляют их перехват, а по окончании — автоматически переключаются на перехват акустической информации.

Угрозы для процессов, процедур и программ обработки информации (220)

Раскрытие данных (220)

Раскрытие данных или программного обеспечения ИС происходит, когда к данным или программному обеспечению осуществляется доступ, при котором они читаются и, возможно, разглашаются некоему лицу, не имеющему доступа к данным. Это может осуществляться путем получения доступа к незашифрованной информации, путем просмотра экрана монитора или распечаток информации.

Компрометация данных ИС может происходить при использовании следующих типов уязвимых мест:

- неправильные установки управления доступом,
- данные, которые считаются достаточно критичными, чтобы нужно было использовать шифрование, но хранятся в незашифрованной форме,
- исходные тексты приложений, хранимые в незашифрованной форме,
- мониторы, находящиеся в помещениях, где много посторонних лиц,
- станции печати, находящиеся в помещениях, где много посторонних лиц,
- резервные копии данных и программного обеспечения, хранимые в открытых помещениях.

Неавторизованная модификация данных и программ (220)

Неавторизованная модификация данных или программного обеспечения происходит, когда в файле или программе осуществляются неавторизованные изменения (добавление, удаление или модификации).

Когда незаметная модификация данных происходит в течение длительного времени, измененные данные могут распространиться по ИС, возможно искажая базы данных, электронные таблицы и другие прикладные данные. Это может привести к нарушению целостности почти всей прикладной информации.

Кстати

Если в программном обеспечении были проведены незаметные изменения, то все программное обеспечение ЭВМ может оказаться под подозрением, что приводит к необходимости детального изучения (и, возможно, переустановки) всего соответствующего программного обеспечения и приложений.

Эти неавторизованные изменения могут быть сделаны в простых командных файлах (например, в пакетных файлах ПК), в сервисных программах, используемых в многопользовательских системах, в главных прикладных программах или в любом другом типе программного обеспечения. Они могут быть сделаны неавторизованными посторонними лицами, а также теми, кто уполномочен вносить изменения в программное обеспечение (хотя изменения, которые они делают, не разрешены).

Эти изменения могут привести к передаче информации (или копии информации) другим пользователям, искажению данных при обработке или нанесению вреда доступности системы или служб ИС.

Неавторизованная модификация данных и программного обеспечения может происходить при использовании следующих типов уязвимых мест:

- разрешения на запись, предоставленного пользователям, которым требуется только разрешение на доступ по чтению,
- необнаруженных изменений в программном обеспечении, включая добавление кода для создания программы троянского коня,
- отсутствия криптографической контрольной суммы критических данных,
- механизма привилегий, который позволяет избыточное разрешение записи,
- отсутствия средств выявления и защиты от вирусов.

Угроза функционирования (220)

Нарушения безопасности могут происходить из-за некомпетентности администрации в применении ИС.

Пользователи или внешние агенты угрозы могут случайно или путем направленного поиска обнаруживать несоответствия в управлении безопасностью ИС, кото-

Вирусные угрозы...

рые позволяют им получить логический доступ к ресурсам в нарушение любых разрешений.

Потенциальные нарушители могут пытаться разрабатывать методы, при которых ошибочно управляемые функции безопасности ИС могут быть обойдены.

Вирусные угрозы (220)

- искажение (разрушение) файлов и системных областей DOS;
- снижение скорости работы, неадекватная реакция на команды оператора и т. д.;
- вмешательство в процесс обмена сообщениями по сети путем непрерывной посылки хаотических сообщений;
- блокирование принимаемых (передаваемых) сообщений, их искажение;
- имитация физических сбоев типа “потеря линии” и т. д.;
- имитация пользовательского интерфейса или приглашений ввода пароля (ключа) с целью запоминания этих паролей (ключей);
- накопление обрабатываемой конфиденциальной информации в скрытых областях внешней памяти;
- дампирование оперативной памяти с целью выявления ключевых таблиц или фрагментов ценной информации;
- искажение программ и данных в оперативной памяти АЛ.
- внедрение программных закладок в программное обеспечение рабочих станций или общедоступные ресурсы (во внешней памяти файл-серверов) локальных сегментов сети.

Вирусные угрозы для серверов ИС (220)

- искажение проходящей через сервер информации (при обмене между РС);
- сохранение проходящей информации в скрытых областях внешней памяти;
- искажение или уничтожение собственной информации сервера (в частности, идентификационных таблиц), а значит, нарушение работы локальной сети;
- внедрение вирусов в пересылаемые внутри локальной сети или на удаленные РС файлы.

Программные закладки – угроза ИС (220)

Остановимся на программных закладках и их влиянии на процесс взаимодействия сегментов сети.

По принципу специфицирования действий программной закладки можно выделить две их основные группы:

Закладки вирусного типа (220)

Способны уничтожить или вызвать искажение информации, нарушения сеансов работы. Основную опасность представляют для абонентского пункта (пунктов) сети и рабочих станций ЛВС, поскольку могут распространяться от одного абонентского пункта (РС) к другому с потоком передаваемых файлов или инифицировать программное обеспечение рабочей станции при использовании удаленных ресурсов (запуске инифицированных программ в оперативной памяти рабочей станции, причем без экспорта выполняемого модуля с файл-сервера, т. е. в случае удаленного доступа к ресурсам сети).

Специально написанные закладки (220)

Специально написанные закладки типа:

а) ***троянский конь*** — закладки, проявляющие себя в определенных условиях (по времени, ключевым сообщениям и т. д.); могут разрушать (искажать) информацию, копировать фрагменты конфиденциальной информации или пароли (ключи), засылать сообщения не по адресу или блокировать прием (отправку) сообщений.

Закладки этого типа, как правило, жестко функциональны и учитывают различные нюансы среды, в которой работают. При этом информация для их работы доставляется закладками следующего типа.

б) ***компьютерный червь*** — закладки, нацеленные на проникновение в системы разграничения доступа пользователей к ресурсам сети; могут приводить к утере (компрометации) матриц установления полномочий пользователей, к нарушению работы всей сети в целом и системы разграничения доступа в частности.

Примером закладки этого типа является известный репликатор Морриса. Возможно существование сразу двух этих типов закладок или одной, объединяющей черты обеих.

Программные закладки представляют опасность для РС, программного обеспечения, коммутаторов и серверов локальной сети (СЛС).

Внедрение закладок (220)

Возможны следующие пути их проникновения (внедрения) в сеть:

- заражение ПО вирусами путем нерегламентированных действий пользователей (запуск посторонних программ, игр, иных внешне привлекательных или обещающих некоторый “выигрыш” программных средств и т. д.);

- умышленное внедрение закладок в ПО путем их маскировки под выполняемые модули или программы начальной загрузки, либо использование в виде отдельных модулей;
- передача вирусов с пересылаемыми файлами и заражение данного после пользования зараженными программами;
- распространение вирусов внутри ПК, объединенных в локальную сеть общего доступа;
- внедрение в ПО вирусов при возможности запуска программ с удаленного терминала;
- внедрение вирусов при разрешении записи с удаленного терминала.

Угрозы для информации в каналах связи (230)

Раскрытие трафика ИС (230)

Раскрытие трафика ИС происходит, когда кто-то, кому не разрешено, читает информацию или получает к ней доступ другим способом, в то время как она передается через ИС.

Трафик ИС может быть скомпрометирован при прослушивании и перехвате во время передачи по транспортной среде ИС (при подключении к кабелю сети, прослушивании в эфире, злоупотреблении предоставленным подключением к сети с помощью присоединения сетевого анализатора, и т.д.).

Кстати

Информация, которая может быть скомпрометирована при передаче по каналам связи содержит системные имена и имена пользователей, пароли, сообщения электронной почты, прикладные данные и т.д.

Например, даже если пароли могут быть зашифрованы при хранении в системе, они могут быть перехвачены в открытом виде в то время, когда их посылают от автоматизированного рабочего места или ПК к файловому серверу.

Файлы сообщений электронной почты, к которым обычно доступ очень ограничен при хранении в ЭВМ, часто посылаются в открытом виде по среде передачи ИС, что делает их легкой добычей для перехвата.

Перехват, искажение, навязывание информации со стороны коммуникационных фрагментов сети.

Имитация посылки ложных сообщений на локальные фрагменты сети.

Имитация логического канала (удаленный доступ) к ресурсам локальных сегментов сети.

Внедрение в проходящую информацию различных функционально законченных блоков кода и данных, могущих реализовать разрушающее воздействие на ПО и данные сети.

Перехват, навязывание, искажение информации при передаче по собственным линиям связи локальных сегментов сети.

Компрометация трафика ИС может происходить при использовании следующих типов уязвимых мест:

- неадекватная физическая защита устройств ИС и среды передачи,
- передача открытых данных с использованием широковещательных протоколов передачи,
- передача открытых данных (незашифрованных) по среде ИС.

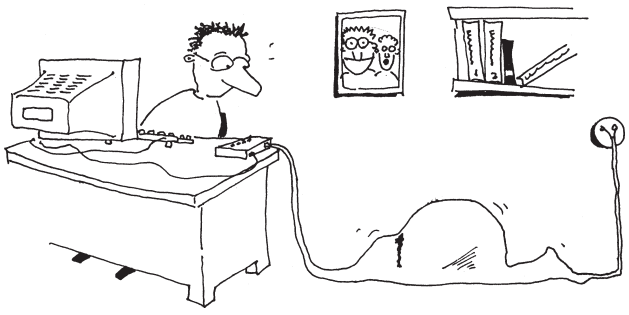
Подмена трафика ИС (230)

Подмена трафика ИС включает 1) способность получать сообщение, маскируясь под легитимное место назначения, и 2) способность маскироваться под отправителя и посылать сообщения. Получение трафика ИС возможно при прослушивании сообщений, поскольку они в широковещательном режиме передаются всем узлам.

Воспроизведение предполагает перехват сеанса между отправителем и получателем и повторную передачу впоследствии этого сеанса (или только заголовков с новым содержанием сообщения).

Подмена трафика ИС или модификации трафика ИС может происходить при использовании следующих типов уязвимых мест:

- передача трафика ИС в открытом виде,
- отсутствие отметки даты / времени, показывающей время посылки и время получения,
- отсутствие механизма кода аутентификации сообщения или цифровой подписи,
- отсутствие механизма аутентификации в реальном масштабе времени (для защиты от воспроизведения).



Подмена трафика...

Вирусные угрозы для коммуникационных узлов ИС (230)

- разрушение собственного ПО КУ и вывод из строя коммутационного узла вместе со всеми присоединенными РС;
- засылка пакетов не по адресу, потеря пакетов, неправильная сборка пакетов, подмена пакетов;
- внедрение вирусов в пакеты, коммутируемые КУ;
- контроль активности абонентов КУ для получения костонной информации о характере информации, которой обмениваются абоненты сети.

Угрозы, связанные с электронной почтой (230) [12]

Основные протоколы передачи почты(SMTP, POP3,IMAP4) обычно не осуществляют надежной аутентификации, что позволяет легко создать письма с фальшивыми адресами. Ни один из этих протоколов не использует криптографию, которая могла бы гарантировать конфиденциальность электронных писем. Хотя существуют расширения этих протоколов, решение использовать их должно быть явно принято как составная часть политики администрации почтового сервера. Некоторые такие расширения используют уже имеющиеся средства аутентификации, а другие позволяют клиенту и серверу согласовать тип аутентификации, который будет использован в данном соединении.

Фальшивые адреса отправителя (230) [12]

Адресу отправителя в электронной почте Internet не следует доверять, так как отправитель может указать фальшивый обратный адрес, или заголовок может быть модифицирован в ходе передачи письма, или отправитель может сам соединиться с SMTP-портом на машине, от имени которой он хочет отправить письмо, и ввести текст письма.

Перехват письма (230) [12]

Заголовки и содержимое электронных писем передаются в чистом виде. В результате содержимое сообщения может быть прочитано или изменено в процессе передачи его по системе Internet. Заголовок может быть модифицирован, чтобы скрыть или изменить отправителя, или для того чтобы перенаправить сообщение.

Почтовые бомбы (230) [12]

Почтовая бомба — это атака с помощью электронной почты. Атакуемая система переполняется письмами до тех пор, пока не выйдет из строя. Как это может случиться, зависит от типа почтового сервера и его конфигурации.

Некоторые провайдеры Internet дают временные логины любому для тестирования подключения к Internet, и эти логины могут быть использованы для начала подобных атак.

Типовые причины выхода почтового сервера из строя:

- Почтовые сообщения принимаются до тех пор, пока диск, на котором они размещаются не переполнится. Следующие письма не принимаются. Если этот диск — основной в системе, то вся система может аварийно завершиться.
- Входная очередь переполняется сообщениями, которые нужно обработать и передать дальше, до тех пор, пока не будет достигнут предельный размер очереди. Последующие сообщения не попадут в очередь.
- У некоторых почтовых систем можно установить максимальное число сообщений или их максимальный общий размер, что пользователь может принять за один раз. Последующие сообщения будут отвергнуты или уничтожены.
- Может быть превышена квота диска для данного пользователя. Это помешает принять последующие письма, и может помешать ему выполнять другие действия. Восстановление может оказаться трудным для пользователя, так как ему может понадобиться дополнительное дисковое пространство для удаления писем.
- Большой размер почтового ящика может затруднить для системного администратора получение системных предупреждений и сообщений об ошибках.
- Посылка почтовых бомб в список рассылки может привести к тому, что его члены могут выйти из списка.

Угрожающие письма (230)

Поскольку любой человек в мире может послать кому-либо письмо, трудно заставить его прекратить это. Можно узнать адрес из списка адресов организации, из списка рассылки или писем в Usenet. Если указан почтовый адрес в каком-нибудь WEB-сайте, от он может быть продан “почтовым мусорщикам”.

Это важно

Многие почтовые системы имеют возможности фильтрации почты, т.е. поиска указанных слов или словосочетаний в заголовке письма или его теле, и последующего помещения его в определенный почтовый ящик или удаления. Но большинство пользователей не знает, как использовать механизм фильтрации.

Кроме того, фильтрация у клиента происходит после того, как письмо уже получено или загружено, поэтому таким образом трудно удалить большие объемы писем.

Для безопасной атаки можно использовать анонимный ремэйлер. Когда хотят послать оскорбительное или угрожающее письмо анонимно, можно воспользоваться анонимным ремэйлером. При нежелании раскрывать домашний адрес можно также использовать анонимный ремэйлер. Кроме того, можно при необходимости отказаться от своего текущего адреса и взять новый.

Одним часто используемым средством защиты, применяемым некоторыми пользователями Usenet, является конфигурирование своих клиентов для чтения новостей таким образом, что в поле Reply-To (обратный адрес) письма, посылаемого ими в группу новостей, помещается фальшивый адрес, а реальный помещается в сигнатуре или в теле сообщения.

Таким образом, программы сбора почтовых адресов, собирающие адреса из поля Reply-To, окажутся бесполезными.

В конгрессе США было подано несколько биллей об ограничениях на работу таких программ-мусорщиков. В одном предлагалось создать списки стоп-слов и помещать слово “реклама” в строку темы письма. В другом предлагалось считать их просто незаконными.

Угрозы информации, возникающие при побочных электромагнитных излучениях и наводках (240)

Побочные электромагнитные излучения и наводки (240)

В зависимости от характера и параметров ПЭМИН могут стать источником сведений о принадлежности данного объекта (средства) к системе управления, о его месте и роли в этой системе и иногда — о характере и содержании информации, циркулирующей в системе управления.

Большую опасность с точки зрения утечки информации представляют побочные (паразитные, непреднамеренные) излучения технических средств, участвующих в процессе передачи, обработки и хранения секретной информации.

Надо знать

На современном уровне развития разведывательной техники ***утечка информации*** вследствие использования в системах управления и связи технических средств передачи, обработки и хранения информации возможна в силу следующих причин:

- излучения электрических и магнитных полей в спектре информационного (первичного) сигнала;
- электромагнитных излучений на частотах подмагничивания магнитофонов и диктофонов;
- электромагнитных излучений, возникающих при самовозбуждении усилителей низкой частоты;
- электромагнитных наводок сигналов, несущих информацию, на посторонние цепи, уходящие за пределы контролируемых зон;
- электромагнитного поля, возникающего в грунте вокруг заземлителей;
- просачивания информационных сигналов в цепи питания технических средств;
- электроакустического преобразования акустических полей сигналов на элементах основных и вспомогательных средств и систем.

Перехват ПЭМИН (240)

Возможность утечки информации в процессе перехвата побочных электромагнитных излучений (ПЭМИ), создаваемых техническими средствами ИС.

ПЭМИ существуют в диапазоне частот от единиц герц до полутора гигагерц и способны переносить (распространять) сообщения, обрабатываемые в ИС. Дальность распространения ПЭМИ исчисляется десятками, сотнями, а иногда и тысячами метров.

Кстати

Наиболее опасными источниками ПЭМИ являются дисплеи, проводные линии связи, накопители на магнитных дисках и печатающие аппараты последовательного типа.

Перехват ПЭМИ может осуществляться с помощью портативной аппаратуры. Такая аппаратура может представлять собой широкополосный автоматизированный супергетеродинный приемник. В качестве уст-

Перехват ПЭМИН может осуществляться с помощью портативной аппаратуры...

ройств регистрации принятых сигналов (сообщений) можно использовать магнитный носитель или дисплей.

Утечка обрабатываемой в ИС информации при приеме информационных сигналов, наведенных в цепях электропитания и заземления аппаратных средств ИС, выходящих за пределы охраняемой (контролируемой) зоны — зоны безопасности.

Возможность утечки обрабатываемой в ИС информации во время приема сигналов, наведенных в проводах и кабелях вспомогательных технических средств ИС, находящихся в зоне воздействия ПЭМИ работающих технических средств ИС.

Источники утечки информации по каналам ПЭМИН (240)

К техническим средствам, которые могут быть источником утечки информации по каналам ПЭМИН относятся:

- средства и системы телефонной, телеграфной (телетайпной), директорской, громкоговорящей, диспетчерской, внутренней, служебной и технологической связи;
- средства и системы звукоусиления, звукозаписи и звуковоспроизведения;
- устройства, образующие дискретные каналы связи: абонентская аппаратура со средствами отображения и сигнализации, аппаратура повышения достоверности передачи, каналообразующая и т.п.;
- аппаратура преобразования, обработки, передачи и приема видеоканалов, содержащих факсимильную информацию;
- средства и системы специальной охранной сигнализации (на вскрытие дверей, окон и проникновение в помещение посторонних лиц), пожарной сигнализации (с датчиками, реагирующими на дым, свет, тепло, звук);
- система звонковой сигнализации (вызов секретаря, входная сигнализация);
- контрольно-измерительная аппаратура;
- средства и системы кондиционирования (датчики температуры, влажности, кондиционеры);
- средства и системы проводной радиотрансляционной сети и приема программ радиовещания и телевидения (абонентские громкоговорители системы радиовещания и оповещения, радиоприемники и телевизоры);
- средства и системы часофикации (электронные часы, вторичные электрочасы);
- средства и системы электроосвещения и бытового электрооборудования (светильники, люстры, настольные и стационарные вентиляторы, электронагревательные приборы, холодильники, бумагорезательные машины, проводная сеть электроосвещения);
- электронная и электрическая оргтехника.

Перечисленные технические средства (ТС) могут представлять собой ***сосредоточенные случайные антенны (аппаратура и ее блоки) и распределенные случайные антенны (кабельные линии и провода).***

Указанными элементами могут быть:

- технические средства и приборы;
- кабельные сети и разводки, соединяющие устройства и оборудование;
- коммутационные устройства (коммутаторы, кроссы, боксы и т.п.);
- элементы заземления и электропитания.

Краткое описание возможной утечки информации по каналам ПЭМИН

В процессе функционирования средств вычислительной техники в конструктивных элементах и кабельных соединениях циркулируют электрические токи информативных сигналов, в результате чего формируются электромагнитные поля, уровни которых могут быть достаточными для приема сигналов и извлечения информации с помощью специальной аппаратуры.

Каналы утечки информации могут возникать вследствие излучения информативных сигналов при работе ТС и наведения этих сигналов в линиях связи, цепях электропитания и заземления, других коммуникациях, имеющих выход за пределы контролируемой территории (КТ). Информативные сигналы могут распространяться на большие расстояния и регистрироваться средствами технических разведок за пределами КТ.

Частоты, на которых могут излучаться (наводиться) информативные сигналы, зависят от типов и видов аппаратурных средств и могут распространяться в диапазоне от сотен герц до нескольких десятков гигагерц.

Уровень наводок определяется расстоянием между источниками излучения и аппаратурой, подверженной влиянию этих излучений, длиной параллельного пробега и величиной переходного затухания линий, напряжением информативного сигнала в линии и уровнем шумов (помех).

Надо знать

Утечка информации по цепям заземления

Утечка информации по цепям заземления может возникнуть при наличии разнесенных точек заземления информативных цепей в случае образования в разных точках системы заземления разности потенциалов и

возникновения в результате этого токов в цепях заземления, при большом значении сопротивления цепи заземления, а также вследствие несовершенства экранов, приводящего к асимметрии линий относительно экрана и к возникновению в цепи между корпусом экрана и землей информативных токов.

Кроме того, ***возможные каналы утечки информации образуются:***

- низкочастотными электромагнитными полями, возникающими при работе ТС;
- при воздействии на ТС электрических, магнитных и акустических полей;
- при возникновении паразитной высокочастотной (ВЧ) генерации;
- при прохождении информативных (опасных) сигналов в цепи электропитания;
- при взаимном влиянии цепей;
- при прохождении информативных (опасных) сигналов в цепи заземления;
- при паразитной модуляции высокочастотного сигнала;
- вследствие ложных коммутаций и несанкционированных действий.

При передаче информации в элементах схем, конструкций, в подводящих и соединяющих проводах технических средств протекают токи информативных сигналов. Возникающие при этом электромагнитные поля могут воздействовать на случайные антенны. Сигналы, принятые случайными антеннами, могут привести к образованию каналов утечки информации.

Интересно

Источниками возникновения электромагнитных полей в ТС могут быть неэкранированные провода, разомкнутые контуры, элементы контрольно-измерительных приборов, контрольные гнезда на усилительных блоках и пультах, неэкранированные оконечные устройства, усилители мощности и линейные усилители, трансформаторы, дроссели, соединительные провода, разъемы, громкоговорители, кабельные линии.

Информативные (опасные) сигналы могут возникать на элементах технических средств, чувствительных к воздействию:

- электрического поля (неэкранированные провода и элементы технических средств);
- магнитного поля (микрофоны, громкоговорители, головные телефоны, трансформаторы, катушки индуктивности, дроссели, электромагнитные реле);
- акустического поля (микрофоны, громкоговорители, головные телефоны, трансформаторы, катушки индуктивности, дроссели, электромагнитные реле).

При наличии в технических средствах элементов, способных преобразовывать эти поля в электрические сигналы, возможна утечка информации по незащищенным цепям абонентских линий связи, электропитания, заземления, управления и сигнализации.

Паразитная высокочастотная генерация (240)

Паразитная высокочастотная генерация (ПВЧГ) в ТС возникает вследствие самовозбуждения усилительных устройств либо вследствие отражения сигналов от концов линий связи между усилителями при переходных процессах.

Высокочастотные паразитные колебания, модулированные информативным сигналом по амплитуде, частоте и фазе или по амплитуде и частоте, создают канал утечки информации.

ПВЧГ образуется в элементах аппаратуры, охваченных отрицательной обратной связью и не имеющих достаточного запаса устойчивости, в концах линий связи между усилительными устройствами в моменты переключений из-за возникновения переходных процессов.

Утечка информации через источники электропитания (240)

Во время работы ТС возможна утечка информации через источники электропитания:

- в результате прохождения информативного сигнала через технические средства на входном сопротивлении его источника питания может возникнуть напряжение, несущее сигнал, содержащий информативную составляющую. Через выпрямительное устройство и силовой трансформатор этот сигнал распространяется по сетевым линиям за пределы контролируемой территории;
- при прохождении речевого сигнала через оконечное усилительное устройство может наблюдаться неравномерное потребление тока от источника питания. Ток, потребляемый усилителем от сети, может быть модулирован информативным сигналом, проходящим через усилитель.

Трассы кабельных цепей, несущих информацию, могут прокладываться в одной кабельной канализации с незащищенными цепями ТС и проходить через общие протяжные коробки и шкафы.

При передаче информативного сигнала по одной цепи в соседних цепях – при их параллельном пробеге – возникают токи, наведенные вследствие электромагнитного влияния. Переход электромагнитной энергии из одной цепи в другую является возможным каналом утечки информации.

Надо знать

Источниками образования информативных сигналов являются участки, охваченные случайными емкостными и магнитными связями. Такими участками могут быть отрезки параллельного пробега линий, несущих информацию, с незащищенными линиями, уходящими за пределы контролируемой территории; монтажные колодки, разъемы блоков, контакты переключателей и реле, используемые для коммутации выходных линий, и блоки, подверженные влиянию электромагнитного поля.

Источником образования информативных сигналов являются элементы цепей и схем, если эти элементы находятся под потенциалом таких сигналов и выходят из экранов.

При поступлении высокочастотных сигналов в нелинейные (или параметрические) цепи, несущие информативные сигналы, происходит модуляция высокочастотного сигнала. Таким образом, высокочастотные колебания становятся носителями информативных сигналов и создают канал утечки информации.

Линиями, на которые подается или с которых снимается высокочастотный сигнал, могут быть незащищенные линии связи, цепи электропитания, заземления, управления и сигнализации; цепи, образованные паразитными связями, конструктивными элементами зданий, сооружений, оборудования и т.п.

Источниками информативных сигналов являются нелинейные радиоэлементы, на которых происходит модуляция таких сигналов.

При возникновении неисправностей в аппаратуре или несанкционированных действиях обслуживающего персонала в схемах управления может возникнуть нежелательная коммутация информативного сигнала, приводящая к выходу информации в незащищенный канал связи.

Источниками информативного сигнала этого канала являются пульты управления, щиты распределения и коммутации, блоки контроля, реле, трансформаторы, разъемы, переключатели или запоминающие устройства, в которых может возникнуть ложная коммутация в результате неисправностей или несанкционированных действий.

Параметры оценки угроз(240)

Основными параметрами возможной утечки информации по каналам ПЭМИН являются:

- напряженность электрического и магнитного полей информативного сигнала;
- величина звукового давления;
- величина напряжения информативного сигнала;
- величина напряжения наведенного информативного сигнала;
- величина напряжения шумов (помех);
- величина тока информативного сигнала;
- величина чувствительности аппаратуры к воздействию магнитных и электрических полей (собственная емкость аппаратуры) для точечного источника;
- величина чувствительности к воздействию акустических полей;
- отношение “информативный сигнал/шум”;
- отношение напряжения опасного сигнала к напряжению шумов (помех) в диапазоне частот такого сигнала.

Указанные параметры определяются и рассчитываются по результатам измерений в заданных точках. Предельно допустимые значения основных параметров являются нормируемыми величинами и определяются по соответствующим методикам. Отношения расчетных (измеренных) значений основных параметров к предельно допустимым (нормированным) значениям определяют необходимые условия защиты информации.

Угрозы для механизмов управления системой защиты (250)

Разрушение функций СЗИ (250)

Разрушение функциональных возможностей СЗИ происходит, когда она не может своевременно обеспечить необходимые функциональные возможности. Разрушение может охватывать как один тип функциональных возможностей СЗИ, так и группу возможностей.

Разрушение функциональных возможностей СЗИ может происходить при использовании следующих типов уязвимых мест:

- неспособность обнаружить необычный характер трафика (т.е. намеренное переполнение трафика),
- неспособность перенаправить трафик, выявить отказы аппаратных средств ЭВМ, и т.д.,
- конфигурация ИС, допускающая вероятность выхода из строя в случае отказа в одном месте,

- неавторизованные изменения компонентов аппаратных средств ИС (переконфигурирование адресов на автоматизированных рабочих местах, изменение конфигурации маршрутизаторов или хабов, и т.д.),
- неправильное обслуживание аппаратных средств ИС,
- недостаточная физическая защита аппаратных средств ИС

Как проводить анализ угроз и каналов утечки информации (200)

Лучше всего анализировать опасность еще на стадии проектирования локальной сети, рабочего места или системы, чтобы сразу определить потенциальные потери и установить требования к мерам обеспечения безопасности. ***Выбор защитных и контрольных мероприятий на ранней стадии требует гораздо меньших затрат***, чем выполнение подобной работы с эксплуатируемой компьютерной системой. Но и в последнем случае анализ опасностей может выявить уязвимые места, которые можно усилить разумными средствами.

В большинстве случаев даже проведение анализа возможных опасностей позволяет персоналу лучше осознать проблемы, которые могут проявиться во время работы, что позволяет усилить программу управления риском. Что касается последней, то прежде за разработку таких мероприятий обычно отвечал менеджер системы информации и управления или автоматизированной обработки данных. Теперь применяется другой подход, при котором в каждой организации ответственность за выполнение анализа опасностей и разработку методики их исключения возлагается на несколько групп служащих.

В рабочую группу, призванную проанализировать возможные опасные ситуации, рекомендуется включать таких специалистов:

Аналитика по опасным ситуациям (лицо, назначенное для проведения анализа), ответственного за сбор исходных данных и за представление руководству информации, способствующей лучшему выбору защитных мероприятий;

Пользователей, ответственных за предоставление аналитику точной информации о применяемых приложениях.

Служащих, занимающихся эксплуатацией здания, работников отдела кадров, охрану и других сотрудников, которые могут предоставить информацию о внешних опасностях и проблемах, связанных с окружающей средой;

Персонал сопровождения сети. На них возлагается ответственность за предоставление информации об аппаратном и программном обеспечении, а также применяемых процедурах;

Типичная модель нарушителя...

Представителей руководства, ответственных за обеспечение защиты ценностей организации.

Представители руководства должны:

- представлять и поддерживать на всех уровнях организации задачу по разработке и сопровождению программы управления при возникновении опасных ситуаций. Такая задача часто выполняется путем выработки и утверждения в организации единой политики в данной области;
- обеспечивать рабочую группу необходимыми ресурсами и управлять ходом разработки программы;
- требовать периодической проверки принимаемых мер и подтверждать их действенность.

Неформальная модель нарушителя (200)

Нарушитель — это лицо, предпринявшее попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осочзнанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т.п.) и использующее для этого различные возможности, методы и средства.

Злоумышленником будем называть нарушителя, намеренно идущего на нарушение из корыстных побуждений.

Неформальная модель нарушителя отражает его практические и теоретические возможности, априорные знания, время и место действия и т.п. Для достижения своих целей нарушитель должен приложить усилия, затратить определенные ресурсы. Исследовав причины

нарушений, можно либо повлиять на эти причины (если возможно), либо точнее определить требования к системе защиты от данного вида нарушений или преступлений.

В каждом конкретном случае, исходя из конкретной технологии обработки информации, может быть определена модель нарушителя, которая должна быть адекватна реальному нарушителю для данной ИС.

При разработке модели нарушителя определяются:

- предположения о категориях лиц, к которым может принадлежать нарушитель;
- предположения о мотивах (целях) нарушителя;
- предположения о квалификации нарушителя и его технической оснащенности;
- ограничения и предположения о характере возможных действий нарушителей.

По отношению к ИС нарушители могут быть внутренними (из числа персонала) или внешними (посторонние лица).

Внутренним нарушителем могут быть:

- пользователи (операторы) системы;
- персонал, обслуживающий технические средства (инженеры, техники);
- сотрудники отделов разработки и сопровождения ПО (прикладные и системные программисты);
- технический персонал, обслуживающий здания (уборщики, электрики, сантехники и другие сотрудники, имеющие доступ в здания и помещения, где расположены компоненты ИС);
- сотрудники службы безопасности ИС;
- руководители различных уровней должностной иерархии.

Посторонние лица, которые могут быть нарушителями:

- клиенты;
- посетители;
- представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации (энерго-, водо-, теплоснабжения и т.п.);
- представители конкурирующих организаций (иностранных спецслужб) или лица, действующие по их заданию;
- лица, случайно или умышленно нарушившие пропускной режим (без цели нарушить безопасность ИС);
- любые лица за пределами контролируемой территории.

Можно выделить ***три основных мотива нарушений:*** безответственность, самоутверждение и корыстный интерес.

При нарушениях, вызванных ***безответственностью***, пользователь целенаправленно или случайно производит какие-либо разрушающие действия, не связанные тем не менее со злым умыслом. В большинстве случаев это следствие некомпетентности или небрежности.

Некоторые пользователи считают получение доступа к системным наборам данных крупным успехом, затевая своего рода игру “пользователь — против системы” ***ради самоутверждения*** либо в собственных глазах, либо в глазах коллег.

Нарушение безопасности ИС может быть вызвано и ***корыстным интересом*** пользователя системы. В этом случае он будет целенаправленно пытаться преодолеть систему защиты для доступа к хранимой, передаваемой и обрабатываемой в ИС информации. Даже если ИС имеет средства, чрезвычайно усложняющие проникновение, полностью защитить ее от этого практически невозможно.

Классификация нарушителей

Всех нарушителей можно классифицировать следующим образом.

По уровню знаний об ИС:

- знает функциональные особенности ИС, основные закономерности формирования в ней массивов данных и потоков запросов к ним, умеет пользоваться штатными средствами;
- обладает высоким уровнем знаний и опытом работы с техническими средствами системы и их обслуживания;
- обладает высоким уровнем знаний в области программирования и вычислительной техники, проектирования и эксплуатации автоматизированных информационных систем;
- знает структуру, функции и механизм действия средств защиты, их сильные и слабые стороны.

По уровню возможностей (используемым методам и средствам):

- применяющий чисто агентурные методы получения сведений;
- применяющий пассивные средства (технические средства перехвата без модификации компонентов системы);
- использующий только штатные средства и недостатки систем защиты для ее преодоления (несанкционированные действия с использованием разрешенных

средств), а также компактные магнитные носители информации, которые могут быть скрытно пронесены через посты охраны;

- применяющий методы и средства активного воздействия (модификация и подключение дополнительных технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ).

По времени действия:

- в процессе функционирования ИС (во время работы компонентов системы);
- в период пассивности компонентов системы (нерабочее время, плановые перерывы в работе, перерывы для обслуживания и ремонта и т.п.);
- как в процессе функционирования ИС, так и в период пассивности компонентов системы.

По месту действия:

- без доступа на контролируемую территорию организации;
- с контролируемой территории без доступа в здания и сооружения;
- внутри помещений, но без доступа к техническим средствам ИС;
- с рабочих мест конечных пользователей (операторов) ИС;
- с доступом в зону данных (баз данных, архивов и т.п.);
- с доступом в зону управления средствами обеспечения безопасности ИС.

Необходимо учитывать следующие ограничения и предположения о характере действий возможных нарушителей:

- работа по подбору кадров и специальные мероприятия затрудняют возможность создания коалиций нарушителей, т.е. объединения (сговора) и целенаправленных действий по преодолению подсистемы защиты двух и более нарушителей;
- нарушитель, планируя попытки НСД, скрывает свои несанкционированные действия от других сотрудников;

НСД может быть следствием ошибок пользователей, администраторов, эксплуатирующего и обслуживающего персонала, а также недостатков принятой технологии обработки информации и т.д.

Совет

Определение конкретных значений характеристик возможных нарушителей в значительной степени субъективно. Модель нарушителя, построенная с учетом особенностей конкретной предметной области и технологии обработки информации, может быть представлена перечислением нескольких вариантов его облика. Каждый вид нарушителя должен быть охарактеризован приведенными выше признаками.

Резюме

На основе принципов и положений государственной политики обеспечения информационной безопасности должны проводиться все мероприятия по защите информации в политической, экономической, оборонной и других сферах деятельности государства.

В этой связи следует иметь ввиду, что в каждой из этих сфер имеются свои особенности, что в первую очередь связано с характером решения поставленных задач, наличием свойственных каждой области информационной безопасности слабых элементов и уязвимых звеньев.

Разнообразие потенциальных угроз информации в ИС столь велико, что не позволяет предусмотреть каждую из них, поэтому анализируемые характеристики угроз следует выбирать с позиций здравого смысла, одновременно выявляя не только сами угрозы, вероятность их осуществления, размер потенциального ущерба, но и их источники.

Угрозой может быть любое лицо, объект или событие, которое, в случае реализации, может потенциально стать причиной нанесения вреда ИС.

Угрозы могут быть злонамеренными (умышленная модификация критической информации), случайными (ошибки в вычислениях или случайное удаление файла) или природными (наводнение, ураган, молния и т.п.)

Непосредственный вред, вызванный угрозой, называется воздействием угрозы.

Уязвимыми местами являются слабые места СЗИ ИС, которые могут использоваться угрозой для своей реализации. Уменьшение или ограничение уязвимых мест ИС может снизить или вообще устранить риск от угроз ИС.

Более непредсказуемыми с точки зрения защиты информации являются меры по блокированию каналов несанкционированного доступа, связанных со злоумышленными действиями и побочными явлениями.

Злоумышленные действия могут осуществляться по отношению к обработке информации или в процессе ее обработки, с доступом или без доступа к элементам ИС, активно или пассивно (т.е. с изменением состояния системы или без).

Раскрытие данных или программного обеспечения ИС происходит, когда к данным или программному обеспечению осуществляется доступ, при котором они читаются и, возможно, разглашаются некоторому лицу, которое не имеет доступа к данным. Это может производиться кем-либо путем получения доступа к информации, которая не зашифрована, или путем просмотра экрана монитора или распечаток информации.

Компрометация данных ИС может происходить при использовании следующих типов уязвимых мест:

- неправильные установки управления доступом,
- данные, которые считаются достаточно критичными, чтобы нужно было использовать шифрование, но хранятся в незашифрованной форме,
- исходные тексты приложений, хранимые в незашифрованной форме,
- мониторы, находящиеся в помещениях, где много посторонних людей
- станции печати, находящиеся в помещениях, где много посторонних людей
- резервные копии данных и программного обеспечения, хранимые в открытых помещениях.

В процессе функционирования средств вычислительной техники в конструктивных элементах и кабельных соединениях циркулируют электрические токи информативных сигналов, в результате чего формируются электромагнитные поля, уровни которых могут быть достаточными для приема сигналов и извлечения информации с помощью специальной аппаратуры.

Разрушение функциональных возможностей СЗИ происходит, когда она не может своевременно обеспечить необходимые функциональные возможности. Разрушение может охватывать как один тип функциональных возможностей СЗИ, так и группу возможностей.

Разрушение функциональных возможностей СЗИ может происходить при использовании следующих типов уязвимых мест:

- неспособность обнаружить необычный характер трафика (то есть намеренное переполнение трафика),
- неспособность перенаправить трафик, выявить отказы аппаратных средств ЭВМ, и т.д.,
- конфигурация ИС, допускающая возможность выхода из строя из-за отказа в одном месте,
- неавторизованные изменения компонентов аппаратных средств ИС (переконфигурирование адресов на автоматизированных рабочих местах, изменение конфигурации маршрутизаторов или хабов, и т.д.),
- неправильное обслуживание аппаратных средств ИС,
- недостаточная физическая защита аппаратных средств ИС