Лекция 2. Комплексный подход к защите информации

1. Каналы утечки информации.
2. Комплексный подход к защите информации. Организационная защита информации.
3. Правовое обеспечение информационной безопасности.

Каналы утечки информации

Каналы утечки информации (способы несанкционированного ее получения) могут быть разделены на:

- косвенные или общедоступные (не связанные с физическим доступом к элементам КС);
- непосредственные или узкодоступные (связанные с физическим доступом к элементам КС).

Косвенные каналы

- использование подслушивающих (радиозакладных) устройств;
- дистанционное видеонаблюдение;
- перехват побочных электромагнитных излучений и наводок (ПЭМИН).

ПЭМИН

- Побочные электромагнитные излучения создаются техническими средствами КС при обработке информации и могут распространять обрабатываемую информацию. Наиболее опасными с точки зрения ПЭМИ являются дисплеи, кабельные линии связи, накопители на магнитных дисках, матричные принтеры. Для перехвата ПЭМИ используется специальная портативная аппаратура.

ПЭМИН

- Побочные электромагнитные наводки представляют собой сигналы в цепях электропитания и заземления аппаратных средств КС и в находящихся в зоне воздействия ПЭМИ работающих аппаратных средств КС кабелях вспомогательных устройств (звукоусиления, связи, времени, сигнализации), металлических конструкциях зданий, сантехническом оборудовании. Эти наведенные сигналы могут выходить за пределы зоны безопасности КС.

Непосредственные каналы утечки, не требующие изменения элементов КС

- хищение носителей информации;
- сбор производственных отходов с информацией;
- намеренное копирование файлов других пользователей КС;
- чтение остаточной информации после выполнения заданий других пользователей (областей оперативной памяти, удаленных файлов, ошибочно сохраненных временных файлов);
- копирование носителей информации;

Непосредственные каналы утечки, не требующие изменения элементов КС

- намеренное использование для несанкционированного доступа к информации незаблокированных терминалов других пользователей КС;
- маскировка под других пользователей путем похищения их идентифицирующей информации (паролей, карт и т.п.);
- обход средств разграничения доступа к информационным ресурсам вследствие недостатков в их программном обеспечении и др.

Непосредственные каналы утечки, предполагающие изменение элементов КС и ее структуры

- незаконное подключение специальной регистрирующей аппаратуры к устройствам или линиям связи (пассивное для фиксации и сохранения передаваемых данных или активное для их уничтожения, искажения или подмены);
- злоумышленное изменение программ для выполнения ими несанкционированного копирования информации при ее обработке;
- злоумышленный вывод из строя средств защиты информации.

Пассивное и активное подключение

- Пассивное подключение нарушителя к устройствам или линиям связи легко предотвратить (например, с помощью шифрования передаваемой информации), но невозможно обнаружить.
- Активное подключение, напротив, легко обнаружить (например, с помощью механизма электронной цифровой подписи), но невозможно предотвратить.

Необходимость комплексного подхода к защите информации

- Поскольку наиболее опасные угрозы информационной безопасности вызваны преднамеренными действиями нарушителя, которые в общем случае являются неформальными, проблема защиты информации относится к формально не определенным проблемам.

Необходимость комплексного подхода к защите информации

1. Надежная защита информации в КС не может быть обеспечена только формальными методами (например, только программными и аппаратными средствами).
2. Защита информации в КС не может быть абсолютной.

Необходимость комплексного подхода к защите информации

- Обеспечение информационной безопасности КС является непрерывным процессом, целенаправленно проводимым на всех этапах ее жизненного цикла с комплексным применением всех имеющихся методов и средств.

Основные группы методов и средств защиты информации

- методы и средства организационно-правовой защиты информации;
- методы и средства инженерно-технической защиты информации;
- криптографические методы и средства защиты информации;
- программно-аппаратные методы и средства защиты информации.

Организационно-правовое обеспечение информационной безопасности

- Организационно-технические и организационно-правовые мероприятия, проводимые в процессе создания и эксплуатации КС для обеспечения защиты информации.

Основные свойства методов и средств организационной защиты

1. Обеспечивают полное или частичное перекрытие значительной части каналов утечки информации (например, хищения или копирования носителей информации);
2. Объединяют все используемые в КС методы и средства в целостный механизм защиты информации.

Методы организационной защиты информации

- ограничение физического доступа к объектам КС и реализация режимных мер;
- ограничение возможности перехвата ПЭМИН;
- разграничение доступа к информационным ресурсам и процессам КС (установка правил разграничения доступа, шифрование информации при ее хранении и передаче, обнаружение и уничтожение аппаратных и программных закладок);
- резервное копирование наиболее важных с точки зрения утраты массивов документов;
- профилактика заражения компьютерными вирусами.

Виды мероприятий по защите информации

1. На этапе создания КС (при разработке ее общего проекта и проектов отдельных структурных элементов, строительстве или переоборудовании помещений, разработке математического, программного, информационного и лингвистического обеспечения, монтаже и наладке оборудования, испытаниях и приемке в эксплуатацию).

Виды мероприятий по защите информации

2. В процессе эксплуатации КС – организация пропускного режима, определение технологии автоматизированной обработки документов, организация работы обслуживающего персонала, распределение реквизитов разграничения доступа пользователей к элементам КС (паролей, ключей, карт и т.п.), организация ведения протоколов работы КС, контроль выполнения требований служебных инструкций и т.п.

Виды мероприятий по защите информации

3. Мероприятия общего характера – подбор и подготовка кадров, организация плановых и предупреждающих проверок средств защиты информации, планирование мероприятий по защите информации, обучение персонала, участие в семинарах, конференциях и выставках по проблемам безопасности информации и т.п.

Роль правового обеспечения

- Основой проведения организационных мероприятий является использование и подготовка законодательных и нормативных документов в области информационной безопасности, которые на правовом уровне должны регулировать доступ к информации со стороны потребителей.

Уровни правового обеспечения информационной безопасности

Первый уровень образуют международные договора, к которым присоединилась Российская Федерация, и федеральные законы России:

- международные (всемирные) конвенции об охране промышленной собственности, об охране интеллектуальной собственности, об авторском праве;
- Конституция РФ (статья 23 определяет право граждан на тайну переписки, телефонных, телеграфных и иных сообщений);

Первый уровень правового обеспечения информационной безопасности

- Гражданский кодекс РФ (в статье 139 устанавливается право на возмещение убытков от утечки с помощью незаконных методов информации, относящейся к служебной и коммерческой тайне, четвертая часть посвящена вопросам правовой охраны интеллектуальной собственности – прав авторов и изобретателей, создателей баз данных и т. п.);

Первый уровень правового обеспечения информационной безопасности

- Уголовный кодекс РФ (статья 272 устанавливает ответственность за неправомерный доступ к компьютерной информации, статья 273 – за создание, использование и распространение вредоносных программ для ЭВМ, статья 274 – за нарушение правил эксплуатации ЭВМ, систем и сетей);

Первый уровень правового обеспечения информационной безопасности

- федеральный закон «Об информации, информационных технологиях и о защите информации»;
- федеральные законы «О государственной тайне», «О коммерческой тайне», «О персональных данных»;
- федеральные законы «О лицензировании отдельных видов деятельности», «О связи», «Об электронной подписи».

Уровни правового обеспечения информационной безопасности

Второй уровень правового регулирования защиты информации составляют подзаконные акты, к которым относятся указы Президента и постановления Правительства РФ, а также определения Конституционного суда РФ, письма Высшего арбитражного суда РФ и постановления пленумов Верховного суда РФ.

Второй уровень правового регулирования

- Концепция информационной безопасности Российской Федерации. Утверждена Указом Президента РФ №24 от 10 января 2000 г.
- Указ Президента РФ от 20 января 1996 г. № 71 «Вопросы Межведомственной комиссии по защите государственной тайны».
- Постановление Правительства РФ от 4 сентября 1995 г. №870 «Об утверждении правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности».

Уровни правового обеспечения информационной безопасности

Третий уровень правового обеспечения информационной безопасности составляют государственные стандарты (ГОСТы) в области защиты информации, руководящие документы, нормы, методики и классификаторы, разработанные соответствующими государственными органами.

Третий уровень правового обеспечения

- Государственные стандарты РФ «Защита информации. Основные термины и определения», «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования», «Системы обработки информации. Защита криптографическая» и др.
- Руководящие документы, инструкции, методики Федеральной службы по техническому и экспортному контролю (ФСТЭК) и Федеральной службы безопасности (ФСБ).

Уровни правового обеспечения информационной безопасности

Четвертый уровень правового обеспечения информационной безопасности образуют локальные нормативные акты, положения, инструкции, методические рекомендации и другие документы по комплексной защите информации в КС конкретной организации.

Четвертый уровень правового обеспечения

- Приказ об утверждении перечня сведений, составляющих коммерческую тайну предприятия (организации).
- Разделы в трудовых и гражданско-правовых договорах, заключаемых с сотрудниками и контрагентами предприятия (организации) об обязанности возмещения ущерба за разглашение сведений, составляющих коммерческую тайну предприятия.
- Соглашение о конфиденциальности и др.