Военная кафедра
КазНТУ им. К.Сатпаева

Цикл автоматизированных систем управления войсками и информационной защиты

Тема № 1:

«Сущность, задачи и принципы комплексной системы защиты информации»

ЗАНЯТИЕ 1.

«СУЩНОСТЬ И ЗАДАЧИ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ»

Занятие № 1. «Сущность и задачи комплексной системы защиты информации»

Учебные вопросы.

1. **Основные понятия защиты информации**
2. **Подходы к проектированию систем защиты информации**
3. **Назначение комплексной системы защиты информации**

Вопрос № 1. Основные понятия защиты информации

***Под информацией*, применительно к задаче ее защиты, понимают сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.**

В зависимости от формы представления информация может быть разделена на речевую, телекоммуникационную и документированную.

Вопрос № 1. Основные понятия защиты информации

1. **Речевая информация возникает в ходе ведения в помещениях разговоров, работы систем связи, звукоусиления и звуковоспроизведения.**
2. **Телекоммуникационная информация циркулирует в технических средствах обработки и хранения информации, а также в каналах связи при ее передаче.**
3. **К документированной информации, или документам, относят информацию, представленную на материальных носителях вместе с идентифицирующими ее реквизитами.**

К информационным процессам относят процессы сбора, обработки, накопления, хранения, поиска и распространения информации.

Под информационной системой понимают упорядоченную совокупность документов и массивов документов и информационных технологий,реализующих информационные процессы.

Защитой информации **называют деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.**

Под *утечкой* понимают неконтролируемое распространение защищаемой информации путем ее разглашения, несанкционированного доступа к ней и получения разведками.

Разглашение **— это доведение защищаемой информации до неконтролируемого количества получателей информации.**

Несанкционированный доступ **— получение защищаемой информации заинтересованным субъектом с нарушением правил доступа к ней.**

Под *непреднамеренным воздействием* на защищаемую информацию понимают воздействие на нее из-за ошибок пользователя, сбоя технических или программных средств, природных явлений, иных нецеленаправленных воздействий.

Шифрованием **информации называют процесс ее преобразования, при котором содержание информации становится непонятным для не обладающих соответствующими полномочиями субъектов. Результат шифрования информации называют *шифротекстом*, или *криптограммой.* Обратный процесс восстановления информации из шифротекста называют *расшифрованием* информации.**

Под *угрозой* безопасности информации в компьютерной системе (КС) понимают событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации.

Уязвимость информации **— это возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации.**

Атакой **на КС называют действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости. Иначе говоря, атака на КС является реализацией угрозы безопасности информации в ней.**

Опосредованной угрозой безопасности информации в КС является угроза раскрытия параметров подсистемы защиты информации, входящей в состав КС. Реализация этой угрозы дает возможность реализации перечисленных ранее непосредственных угроз безопасности информации.

Искусственные угрозы исходя из их мотивов разделяются на *непреднамеренные* (случайные) и *преднамеренные* (умышленные).

К непреднамеренным угрозам относятся:

- **ошибки в проектировании КС;**
- **ошибки в разработке программных средств КС;**
- **случайные сбои в работе аппаратных средств КС, линий связи, энергоснабжения;**
- **ошибки пользователей КС;**
- **воздействие на аппаратные средства КС физических полей других электронных устройств (при несоблюдении условий их электромагнитной совместимости) и др.**

К умышленным угрозам относятся:

- несанкционированные действия обслуживающего персонала КС (например, ослабление политики безопасности администратором, отвечающим за безопасность КС);
- несанкционированный доступ к ресурсам КС со стороны пользователей КС и посторонних лиц, ущерб от которого определяется полученными нарушителем полномочиями.

В зависимости от целей преднамеренных угроз безопасности информации в КС угрозы могут быть разделены на три основные группы:

- **угроза нарушения конфиденциальности, т.е. утечки информации ограниченного доступа, хранящейся в КС или передаваемой от одной КС к другой;**

- **угроза нарушения целостности, т. е. преднамеренного воздействия на информацию, хранящуюся в КС или передаваемую между КС (заметим, что целостность информации может быть также нарушена, если к несанкционированному изменению или уничтожению информации приводит случайная ошибка в работе программных или аппаратных средств КС; санкционированным является изменение или уничтожение информации, сделанное уполномоченным лицом с обоснованной целью);**

- **угроза нарушения доступности информации, т. е. отказа в обслуживании, вызванного преднамеренными действиями одного из пользователей КС (нарушителя), при котором блокируется доступ к некоторому ресурсу КС со стороны других пользователей КС (постоянно или на большой период времени).**

Рассмотрим возможные каналы утечки информации в КС. *Косвенными* каналами утечки называют каналы, не связанные с физическим доступом к элементам КС:

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

Побочные электромагнитные наводки представляют собой сигналы в цепях электропитания и заземления аппаратных средств КС и в находящихся в зоне воздействия ПЭМИН 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.

Другим классом каналов утечки информации являются *непосредственные* каналы, связанные с физическим доступом к элементам КС. К непосредственным каналам утечки, не требующим изменения элементов КС, относятся:

- **Хищение носителей информации;**

- сбор производственных отходов с информацией (бумажных и магнитных носителей);
- 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;
- 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.

К непосредственным каналам утечки, предполагающим изменение элементов КС и ее структуры, относятся:

- 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);

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

К методам и средствам *организационной* защиты информации относятся организационно-технические и организационно-правовые мероприятия, проводимые в процессе создания и эксплуатации КС для обеспечения защиты информации. Эти мероприятия должны проводиться при строительстве или ремонте помещений, в которых будет размещаться КС; проектировании системы, монтаже и наладке ее технических и программных средств; испытаниях и проверке работоспособности КС.

Основные свойства методов и средств организационной защиты:

- **обеспечение полного или частичного перекрытия значительной части каналов утечки информации (например, хищения или копирования носителей информации);**
- **объединение всех используемых в КС средств в целостный механизм защиты информации**

Методы и средства организационной защиты информации включают в себя:

- **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;**
- **профилактику заражения компьютерными вирусами.**