ТЕМА № 3

«Дестабилизирующее воздействие и несанкционированный доступ к информации»

Цель занятия:

- 1. Изучить методы и средства защиты информации и требования к ним.
- 2. Обучить организационно-правовому обеспечению информационной безопасности.
- 3. Воспитывать высокие морально-психологические и профессиональные качества, твердую и непоколебимую уверенность в своем оружии и военной технике, чувство превосходства своих ВС.

ЗАНЯТИЕ 2/2.

Методы и средства защиты информации и требования к ним.

Учебные вопросы.

1. Организационно-правовое обеспечение информационной безопасности.
2. Инженерно-технические методы и средства защиты информации.
3. Программные и программно-аппаратные методы и средства обеспечения информационной безопасности.
4. Требования к комплексным системам защиты информации.

1-й учебный вопрос

Организационно-правовое обеспечение информационной безопасности.

К методам и средствам организационной защиты информации относятся:

- организационно-технические мероприятия;
- организационно-правовые мероприятия.

Проводятся как в процессе создания, так и в процессе эксплуатации КС для обеспечения защиты информации, а именно:

- при строительстве или ремонте помещений, в которых будет размещаться КС;
- проектировании системы;
- монтаже и наладке технических и программных средств КС;
- 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.

На этапе создания КС:

- при разработке ее общего проекта и проектов отдельных структурных элементов — ***анализ возможных угроз и методов их нейтрализации***;
- при строительстве и переоборудовании помещений — ***приобретение сертифицированного оборудования, выбор лицензированных организаций;***

- при разработке математического, программного, информационного и лингвистического обеспечения — ***использование сертифицированных программных и инструментальных средств***;

- при монтаже и наладке оборудования — ***контроль за работой технического персонала***;

- при испытаниях и приемке в эксплуатацию — ***включение в состав аттестационных комиссий сертифицированных специалистов***;

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.

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.

Первый уровень образуют международные договоры, к которым присоединилась Республика Казахстан, т.е.международные (всемирные) конвенции об охране промышленной собственности, охране интеллектуальной собственности, авторском праве.

Второй уровень правового обеспечения информационной безопасности составляют подзаконные акты, к которым относятся указы Президента РК и постановления Правительства РК, а также письма Высшего Арбитражного Суда РК и постановления пленумов Верховного Суда РК.

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

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.

К таким нормативным документам относятся:

- приказ об утверждении перечня сведений, составляющих коммерческую тайну предприятия;
- трудовые и гражданско-правовые договоры (подряда, поручения, комиссии и т.п.), в которые включены пункты об обязанности возмещения ущерба за разглашение сведений, составляющих коммерческую тайну предприятия.

2-й учебный вопрос

Инженерно-технические методы и средства защиты информации.

Под ***инженерно-техническими средствами защиты информации*** понимают физические объекты, механические, электрические и электронные устройства, элементы конструкции зданий, средства пожаротушения и другие средства, обеспечивающие:

- защиту территории и помещений КС от проникновения нарушителей;

- защиту аппаратных средств КС и носителей информации от хищения;
- предотвращение возможности удаленного (из-за пределов охраняемой территории) видеонаблюдения (подслушивания) за работой персонала и функционированием технических средств КС;

- предотвращение возможности перехвата ПЭМИН, вызванных работающими техническими средствами КС и линиями передачи данных;
- организацию доступа в помещения КС сотрудников;
- контроль над режимом работы персонала КС;
- контроль за перемещением сотрудников КС в различных производственных зонах;

- противопожарную защиту помещений КС;
- минимизацию материального ущерба от потерь информации, возникших в результате стихийных бедствий и техногенных аварий.

Основной задачей ***методов и средств защиты информации от утечки по каналам ПЭМИН*** является уменьшение соотношения сигнал/шум в этих каналах до предела, при котором восстановление информации становится принципиально невозможным.

Возможными методами решения этой задачи могут быть:

- снижение уровня излучений сигналов в аппаратных средствах КС;
- увеличение мощности помех в соответствующих этим сигналам частотных диапазонах.

Методы и средства защиты информации в КС от утечки по каналам ПЭМИН:

- выбор элементной базы технических средств КС с возможно более малым уровнем информационных сигналов;
- замена в информационных каналах КС электрических цепей волоконно-оптическими линиями;

- локальное экранирование узлов технических средств, являющихся первичными источниками информационных сигналов;

- включение в состав информационных каналов КС устройств предварительного шифрования обрабатываемой информации.

3-й учебный вопрос

Программные и программно-аппаратные методы и средства обеспечения информационной безопасности

К ***аппаратным средствам защиты информации*** относятся электронные и электронно-механические устройства, включаемые в состав технических средств КС и выполняющие (самостоятельно или в едином комплексе с программными средствами) некоторые функции обеспечения информационной безопасности.

К основным ***аппаратным средствам защиты информации*** относятся:

- устройства для ввода идентифицирующей пользователя информации (магнитных и пластиковых карт, отпечатков пальцев и т.п.);
- устройства для шифрования информации;
- устройства для воспрепятствования несанкционированному включению рабочих станций и серверов (электронные замки и блокираторы).

Примеры вспомогательных аппаратных средств защиты информации:

- устройства уничтожения информации на магнитных носителях;
- устройства сигнализации о попытках несанкционированных действий пользователей КС и др.

Под ***программными средствами защиты информации*** понимают специальные программы, включаемые в состав программного обеспечения КС исключительно для выполнения защитных функций.

К основным ***программным средствам защиты информации*** относятся:

- программы идентификации и аутентификации пользователей КС;
- программы разграничения доступа пользователей к ресурсам КС;

- программы шифрования информации;
- программы защиты информационных ресурсов (системного и прикладного программного обеспечения, баз данных, компьютерных средств обучения и т. п.) от несанкционированного изменения, использования и копирования.

Примеры ***вспомогательных программных*** средств защиты информации:

- программы уничтожения остаточной информации (в блоках оперативной памяти, временных файлах и т. п.);
- программы аудита (ведения регистрационных журналов) событий, связанных с безопасностью КС, для обеспечения возможности восстановления и доказательства факта происшествия этих событий;

- программы имитации работы с нарушителем (отвлечения его на получение якобы конфиденциальной информации);
- программы тестового контроля защищенности КС и др. формации.

К преимуществам ***программных средств защиты информации*** относятся:

- простота тиражирования;
- гибкость (возможность настройки на различные условия применения, учитывающие специфику угроз информационной безопасности конкретных КС);

- простота применения — одни программные средства, например шифрования, работают в «прозрачном» (незаметном для пользователя) режиме, а другие не требуют от пользователя никаких новых (по сравнению с другими программами) навыков;
- практически неограниченные возможности их развития путем внесения изменений для учета новых угроз безопасности информации.

К недостаткам ***программных средств защиты информации*** относятся:

- снижение эффективности КС за счет потребления ее ресурсов, требуемых для функционирование программ защиты;
- более низкая производительность (по сравнению с выполняющими аналогичные функции аппаратными средствами защиты, например шифрования);

- пристыкованность многих программных средств защиты (а не их встроенность в программное обеспечение КС), что создает для нарушителя принципиальную возможность их обхода;
- возможность злоумышленного изменения программных средств защиты в процессе эксплуатации КС.

4-й учебный вопрос

Требования к комплексным системам защиты информации

Под ***комплексной системы защиты информации (КСЗИ)*** понимается совокупность методов и средств, объединенных единым целевым назначением и обеспечивающих необходимую эффективность защиты информации в КС.

Основные ***требования*** к комплексной системе защиты информации:

- разработка на основе положений и требований существующих законов, стандартов и нормативно-методических документов по обеспечению информационной безопасности;
- использование комплекса программно-технических средств и организационных мер для защиты КС;

- надежность, производительность, конфигурируемость;
- экономическая целесообразность (поскольку стоимость КСЗИ включается в стоимость КС, стоимость средств защиты не должна быть выше возможного ущерба от потери информации);
- выполнение на всех этапах жизненного цикла обработки информации в КС (в том числе при проведении ремонтных и регламентных работ);
- возможность совершенствования;

- обеспечение разграничения доступа к конфиденциальной информации с отвлечением нарушителя на ложную информацию (обеспечение не только пассивной, но и активной защиты);
- взаимодействие с незащищенными КС по установленным для этого правилам разграничения доступа;

- обеспечение проведения учета и расследования случаев нарушения безопасности информации в КС;
- не сложная для пользователя (не должна вызывать у него психологического противодействия и стремления обойтись без применения ее средств);
- возможность оценки эффективности ее применения.

три основные категории требований «Оранжевой книги»

1. Политика:

- наличие явной и хорошо определенной политики обеспечения безопасности;
- использование маркировки объектов КС для управления доступом к ним.

2. Подотчетность:

- индивидуальная идентификация субъектов КС;
- сохранение и защита информации аудита.

3. Гарантии:

- включение в состав КС программно-аппаратных средств для получения гарантий выполнения требований категорий 1 и 2;
- постоянная защищенность средств обеспечения безопасности информации в КС от их преодоления и (или) несанкционированного изменения.