Курс: **основы информационной безопасности**

Тема: **Концептуальные основы ИБ**

Преподаватель: Пятков Антон Геннадьевич

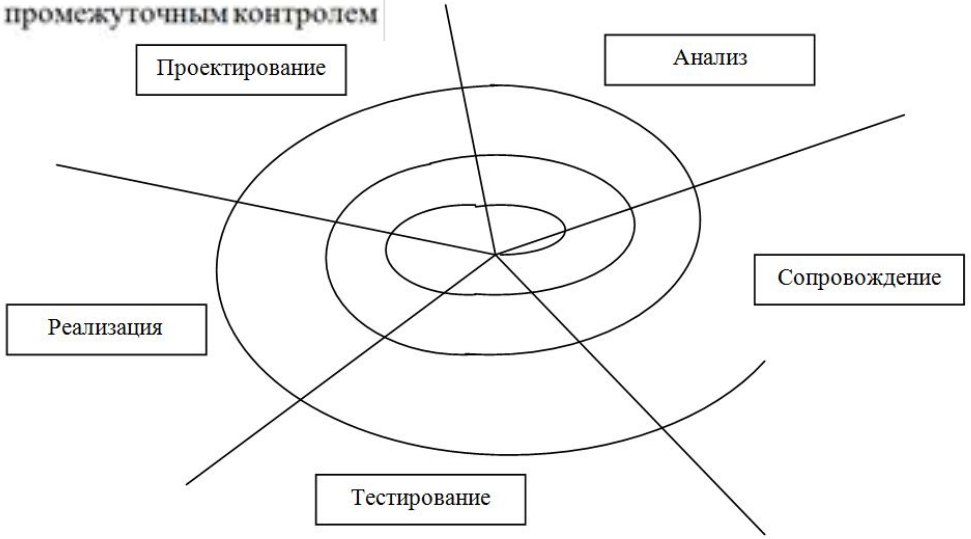
Красноярск

Жизненный цикл

Жизненный цикл – период функционирования изделия (продукции), начиная от его проектирования и изготовления, и заканчивая утилизацией.

Каскадная модель жизненного цикла АС

Поэтапная модель с промежуточным контролем



Спиральная модель жизненного цикла

Принципы построения систем защиты АС

- ✔ принцип системности;
- ✔ принцип комплексности;
- ✔ принцип непрерывности защиты;
- ✔ принцип разумной достаточности;
- ✔ принцип гибкости управления и применения;
- ✔ законность системы обеспечения ИБ (СОИБ);
- ✔ принцип простоты применения защитных мер и средств;
- ✔ принцип экономической целесообразности;
- ✔ принцип открытости алгоритмов и механизмов защиты;
- ✔ преемственность и непрерывность совершенствования СОИБ;
- ✔ персональная ответственность и минимизация полномочий.

Принцип системности:
Для комплексной СОИБ необходим системный подход – учёт всех элементов, условий и факторов, существенно значимых для понимания и решения проблемы ИБ АС, их связи, взаимодействие и изменение во времени.
При создании системы защиты необходимо учитывать все слабые, наиболее уязвимые места системы обработки информации, Ас, а также характер, возможные объекты и направления атак на систему со стороны нарушителей, пути проникновения в распределенные системы и НСД к информации. Система ЗИ должна строиться с учётом не только известных каналов проникновения и НСД к информации, но и с учётом возможности появления принципиально новых.

Принципы построения систем защиты АС

Принцип комплексности:
Комплексное использование мер, методов и средств защиты, их согласованное применение при построении целостной системы защиты, перекрывающей все существенные каналы реализации угроз и не содержащей слабых мест на стыках отдельных её компонентов, эшелонирование ЗИ.

Принцип непрерывности защиты (+контроль)
ЗИ - не разовое мероприятие и не совокупность мер и СЗИ, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла АС, постоянное участие руководства в обеспечении ИБ, конроль.

Принцип разумной достаточности
Создать абсолютно непреодолимую систему защиты принципиально невозможно. При достаточном количестве времени и средств можно преодолеть любую защиту. Имеет смысл говорить только о некотором **приемлемом** уровне безопасности. Высокоэффективная система ЗИ стоит дорого, использует существенную часть мощности и ресурсов и может создавать ощутимые дополнительные неудобства пользователям и бизнес-процессу. Выбор достаточного уровня защиты – это выбор, при котором затраты, риск и размер возможного ущерба приемлемы. Необходимо найти баланс защищённости и функциональности.

Принципы построения систем защиты АС

Гибкость системы защиты:
Всегда имеют место неопределённости. Средства ЗИ в начальный период их эксплуатации могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для варьирования уровнем защищённости, а также чтобы оперативно соответствовать меняющимся внешним факторам (угрозам, требованиям и пр.), СЗИ должны обладать гибкостью.
! особенно при установке средств ЗИ на работающую систему

Законность СОИБ:
Обеспечение ИБ в соответствии с действующим законодательством и др. НПА по ИБ, утвержденными органами гос. власти и управления в пределах их компетенции (в частности требования регуляторов), с применением ими всех дозволенных методов обнаружения и пресечения правонарушений. Все пользователи АС должны иметь представление об ответственности за правонарушения в области ИБ.

Принцип простоты применения средств защиты:
Механизмы защиты должны быть интуитивно понятны и просты в использовании. НЕТ непонятным действиям, значительным трудозатратам, большому числу рутинных малопонятных операций.

Принцип экономической целесообразности:
Стоимость системы ЗИ не должна превышать стоимость защищаемой информации (исключение – ГТ). Меры защиты обоснованы и технически реализуемы.

Принципы построения систем защиты АС

Открытость алгоритмов и механизмов защиты:
Защита не должна обеспечиваться только за счёт секретности структуры системы ЗИ и алгоритмов функционирования. Знание алгоритмов работы не должно давать возможности преодоления защиты даже автору этой защиты.

Своевременность СОИБ:
Упреждающий характер мер обеспечения ИБ, превентивные СЗИ, постановка и реализация мер обеспечения ИБ на ранних стадиях разработки АС и системы ЗИ.

Преемственность и непрерывность совершенствования СОИБ:
Постоянное совершенствование мер и средств ЗИ на основе преемственности орг. и тех. решений, кадрового состава, анализа функционирования АС и системы её защиты с учётом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

Персональная ответственность
Возложение ответственности за обеспечение ИБ на каждого сотрудника в пределах его полномочий. Распределение прав и обязанностей строится так, чтобы при любом нарушении круг виновников был чётко известен или сведён к минимуму. Пользователям предоставлены минимальные прав доступа в соответствии со служебной необходимостью (только в случае и в том объеме, который необходим для выполнения должностных обязанностей).

Формирование режима ИБ

С учётом выявленных угроз ИБ режим защиты должен формироваться как **совокупность** способов и мер защиты циркулирующей в АС информации и поддерживающей её инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, влекущих за собой нанесение ущерба владельцам или пользователям информации.

Комплекс мер по формированию режима обеспечения ИБ включает:

- ✔ установление организационно-правового режима обеспечения ИБ (режим КТ, разработка нормативных документов, работа с персоналом, делопроизводство);
- ✔ организационные и программно-технические
- ✔ мероприятия по предупреждению НСД к информационным ресурсам;
- ✔ комплекс мероприятий по контролю функционирования средств и систем защиты информационных ресурсов ограниченного пользования;
- ✔ комплекс оперативных мероприятий подразделений безопасности по предотвращению (выявлению) проникновения в Банк лиц, имеющих отношение к криминальным структурам.

Формирование режима ИБ

Организационно-правовой режим предусматривает создание и поддержание правовой базы безопасности информации, в частности, разработку (введение в действие) следующих организационно-распорядительных документов:

- ✔ положение о коммерческой тайне (положение регламентирует деятельность организации по ЗИ, порядок работы со сведениями, составляющими КТ, обязанности и ответственность сотрудников, допущенных к этим сведениям, порядок передачи материалов, содержащих сведения, составляющим КТ, государственным (коммерческим) учреждениям и организациям);
- ✔ перечень сведений, составляющих служебную и коммерческую тайну (перечень определяет сведения, отнесенные к категориям конфиденциальных, уровень и сроки обеспечения ограничений по доступу к защищаемой информации);
- ✔ приказы и распоряжения по установлению режима безопасности информации:
  - ✔ допуске сотрудников к работе с информацией ограниченного распространения;
  - ✔ назначении администраторов и лиц, ответственных за работу с информацией ограниченного распространения в корпоративной информационной системе;
- ✔ инструкции и функциональные обязанности сотрудникам:
  - ✔ по организации охранно-пропускного режима;
  - ✔ по организации делопроизводства;
  - ✔ по администрированию информационных ресурсов АС и системы в целом;
  - ✔ другие нормативные документы.

Формирование режима ИБ

Организационно-технические мероприятия по ЗИ ограниченного распространения от утечки по ТКУИ предусматривают:

- ✔ комплекс мер и соответствующих технических средств, ослабляющих утечку речевой и сигнальной информации - пассивная защита (защита);
- ✔ комплекс мер и соответствующих технических средств, создающих помехи при съеме информации - активная защита (противодействие);
- ✔ комплекс мер и соответствующих технических средств, позволяющих выявлять каналы утечки информации - поиск (обнаружение).

Формирование режима ИБ

Физическая охрана объектов информатизации (компонентов ВС) включает:

- ✔ организацию системы охранно-пропускного режима и системы контроля допуска на объект;
- ✔ введение дополнительных ограничений по доступу в помещения, предназначенные для хранения информации ограниченного пользования (кодовые и электронные замки, карточки допуска и т.д.);
- ✔ визуальный и технический контроль контролируемой зоны объекта защиты;
- ✔ применение систем охранной и пожарной сигнализации.

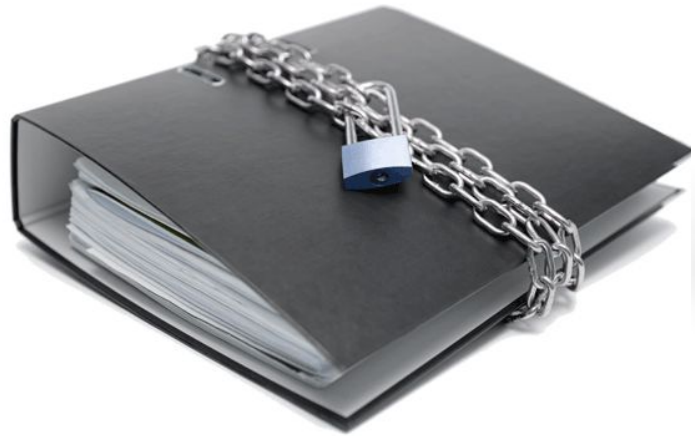





Формирование режима ИБ

Выполнение **режимных требований** при работе с информацией ограниченного пользования предполагает:

- ✔ разграничение допуска к информационным ресурсам ограниченного пользования;
- ✔ разграничение допуска к ресурсам корпоративной информационной системы, АС;
- ✔ ведение учёта ознакомления сотрудников с информацией ограниченного пользования;
- ✔ включение в функциональные обязанности сотрудников обязательства о неразглашении и сохранности сведений ограниченного пользования;
- ✔ организация уничтожения информационных отходов (бумажных, магнитных…);
- ✔ оборудование служебных помещений сейфами, шкафами для хранения бумажных носителей информации и МНИ.



Формирование режима ИБ

Мероприятия **технического контроля** предусматривают:

- ✔ контроль за проведением технического обслуживания, ремонта носителей информации и средств вычислительной техники;
- ✔ проверки определенной части поступающего оборудования, предназначенного для обработки информации ограниченного пользования, на наличие специально внедренных закладных программ и устройств;
- ✔ оборудование компонентов и подсистем корпоративной информационной системы устройствами защиты от сбоев электропитания и помех в линиях связи;
- ✔ защита выделенных помещений при проведении закрытых (секретных) работ (переговоров);
- ✔ постоянное обновление технических и программных средств защиты от НСД к информации в соответствие с меняющейся оперативной обстановкой.