

ЗАНЯТИЕ 2

«ПРОЦЕДУРЫ РАЗРАБОТКИ И ПРОЕКТИРОВАНИЯ СИСТЕМ БЕЗОПАСНОСТИ»

Учебные вопросы

1. Процедуры разработки систем безопасности.
2. Процедуры проектирования систем безопасности.

1-й учебный вопрос

Процедуры разработки систем безопасности.

Основные принципы построения **системы защиты:**

- 1. Простота механизма защиты.**
- 2. Постоянство защиты.**
- 3. Всеобъемлющий контроль.**
- 4. Несекретность проектирования.**
- 5. Идентификация.**
- 6. Разделение полномочий.**
- 7. Минимальные полномочия.**
- 8. Надежность.**
- 9. Максимальная обособленность**

механизма защиты.

10. Защита памяти.

11. Удобство для пользователей

12. Контроль доступа

13. Авторизация пользователя

14. Отчетность.

15. Доступность к исполнению

16. Наличие механизмов защиты от:

- несанкционированного чтения

информации;

- модификации хранящейся и

циркулирующей в сети информации;

- навязывания информации;

- несанкционированного отказа от

авторства переданной информации.

- 17. Системный подход.**
- 18. Возможность наращивания защиты.**
- 19. Комплексный подход.**
- 20. Адекватность.**
- 21. Минимизация привилегий.**
- 22. Полнота контроля.**
- 23. Наказуемость нарушений.**
- 24. Экономичность механизма.**
- 25. Принцип системности.**
- 26. Специализация.**
- 27. Принцип неформальности.**
- 28. Гибкость системы защиты.**
- 29. Принцип непрерывности.**

Каждой группе объектов должен соответствовать определенный класс защиты конструктивных элементов (ограждающих конструкций и элементов инженерно-технической укреплённости), а также технических средств обеспечения комплексной безопасности.

При этом регламентируется соответствие характеристик элементов **первого класса** минимально необходимой степени защиты, **второго класса** - средней, **третьего класса** - высокой **четвертого класса** - специальной степени защиты объекта от проникновения.

В зависимости от степени потенциальной опасности, а также возможных последствий в случае реализации криминальных угроз объекты подразделяются на три основные группы:

- критически важные и потенциально опасные объекты;
- социально значимые объекты;
- объекты сосредоточения материальных ценностей.

В зависимости от вида и размеров ущерба, который может быть нанесен объекту, находящимся на нём людям и имуществу в случае реализации криминальных угроз принята следующая классификация:

- Класс I (высокая значимость) – ущерб приобретет республиканский или межрегиональный масштаб;

- Класс II (средняя значимость) – ущерб приобретет региональный или межакиматный масштаб;

- Класс III (низкая значимость) – ущерб приобретет акиматный или локальный масштаб.

Угроза безопасности – это совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства.

Угроза криминальная - это совокупность условий и факторов, создающих опасность преднамеренного противоправного нанесения ущерба объекту и имуществу, здоровью и жизни физического лица, хищение материальной и интеллектуальной собственности

К основным угрозам можно отнести:

- угрозы жизни, здоровью, личным правам и свободам человека;
- угрозы материальным и культурным ценностям, физическим носителям информации;
- угрозы экономической деятельности;
- угрозы общественной безопасности;
- угрозы информационной безопасности;
- угрозы юридической деятельности;
- угрозы чрезвычайных ситуаций;
- угрозы отказа оборудования.

В связи с широким спектром угрожающих факторов безопасность защищаемого объекта должна быть **комплексной для решения следующих важных задач:**

- поддержание безопасного состояния объекта,
- предупреждение угроз,
- обнаружение угроз,
- противодействие угрозам,
- ликвидация последствий максимального количества из полного набора возможных угроз для данного объекта.

Существует следующая
классификация нарушителей
(исполнителей угроз) в зависимости от
их подготовленности:

1. Случайный нарушитель.
2. Неподготовленный нарушитель.
3. Подготовленный нарушитель.
4. Осведомленный нарушитель.
5. Сотрудник предприятия или охранник.

2-й учебный вопрос:

**Процедуры проектирования
систем безопасности.**

Комплексный научный подход к созданию СБ важных объектов подразумевает реализацию *трех основных этапов:*

1. Концептуальное (системное)

проектирование.

2. Рабочее проектирование.

3. Внедрение.

Основными разделами

концептуального проекта являются:

1. Анализ уязвимости объекта и существующей СБ.

2. Разработка принципов комплексной защиты объекта.

3. Разработка технико-экономического обоснования (ТЭО) создания СБ и комплекса ТСОБ.

Предпроектное обследование проводится с целью анализа уязвимости существующей на объекте СБ. При этом решаются следующие задачи:

- определение объекта охраны и его категории значимости;
- составление списка и параметров угроз для объекта охраны;
- создание модели нарушителя;
- оценка вероятности реализации угроз;
- оценка потенциального ущерба при реализации угроз;
- оценка эффективности существующей СБ.

Результатом оценки эффективности СБ оформляются в виде ТЭО, которое содержит необходимые сведения по следующим вопросам:

- концепция безопасности;
- структура и состав СБ и комплекса ТСОБ;
- количественная оценка уязвимости объекта и эффективности существующей и предлагаемой СБ;
- ожидаемые тактико-технико-экономические показатели ТСОБ;
- рекомендации по организации оперативных действий сил охраны с применением комплекса ТСОБ;

- ориентировочный расчет необходимой численности технического персонала для обслуживания комплекса;
- ориентировочный расчет необходимой численности сил охраны;
- ориентировочный расчет стоимости всех этапов работ по оборудованию объекта предлагаемым комплексом ТСОБ.

При проектировании СБ создается, согласуется и утверждается рабочая документация, включающая следующие обязательные элементы:

- структурные и функциональные схемы СБ;
- планы объектов с указанием мест размещения оборудования СБ;
- схемы соединений;
- кабельный журнал;
- сметы расходов;
- расчетно-пояснительная записка с описанием схем и расчетами для обоснования предлагаемых технических, организационных и тактических аспектов защиты объекта охраны;
- описание последовательности оснащения объекта элементами СБ.

Осознанный риск означает, что могут быть реализованы угрозы, которые не вошли в отобранный перечень, и СБ не предусматривает защиту от них.

Непредсказуемый риск означает, что угрозы, которые вошли в отобранный перечень, могут быть реализованы в отношении других жизненных приоритетов.

Заданный риск определяет заданный уровень последствий реализации угроз (определение допустимого уровня ущерба).

Технический риск означает, что СБ, как любая техническая система, может не выполнить своей задачи, например из-за отказа, неисправности оборудования.