Содержательная характеристика этапов разработки КСЗИ

- Выполнил: студент группы 20501
Яшин М.А.

Этап №1. Подготовка организационно-распорядительной документации

Содержание работ:

1. Анализ организационно-распорядительных документов, нормативно-правовых документов в обл. ЗИ, влияющих на деятельность.

2. Установление границ, в которых предполагается поддерживать режим ИБ.

Результат I этапа:

1. Проект документов, определяющие организационную составляющую КСЗИ(проект приказа о создании КСЗИ).

2. Документы, в которых определены границы системы (КСЗИ).

Этап №2. Определение объектов защиты.

Содержание работ:

1. Составление перечня КИ.
2. Структурирование КИ по направлениям, структурирование на ключевые элементы. Ключевой элемент информации - это элемент, удовлетворяющий трем требованиям: принадлежит конкретному источнику (человек, документ, образец и т.д.); содержится на отдельном носителе; имеет конкретную цену.
3. Составление перечня носителей, содержащих КИ
4. Анализ архитектуры существующей системы ЗИ (выявление слабых и сильных сторон системы).

Результат II этапа:

1. Перечень объектов, подлежащих защите (перечень структурированной к.и., носителей, определение места их положения).

2. Акт обследования СЗИ (существующей) (содержит описание, принципы построения и архитектуру).

Этап №3. Анализ угроз

Содержание работ:

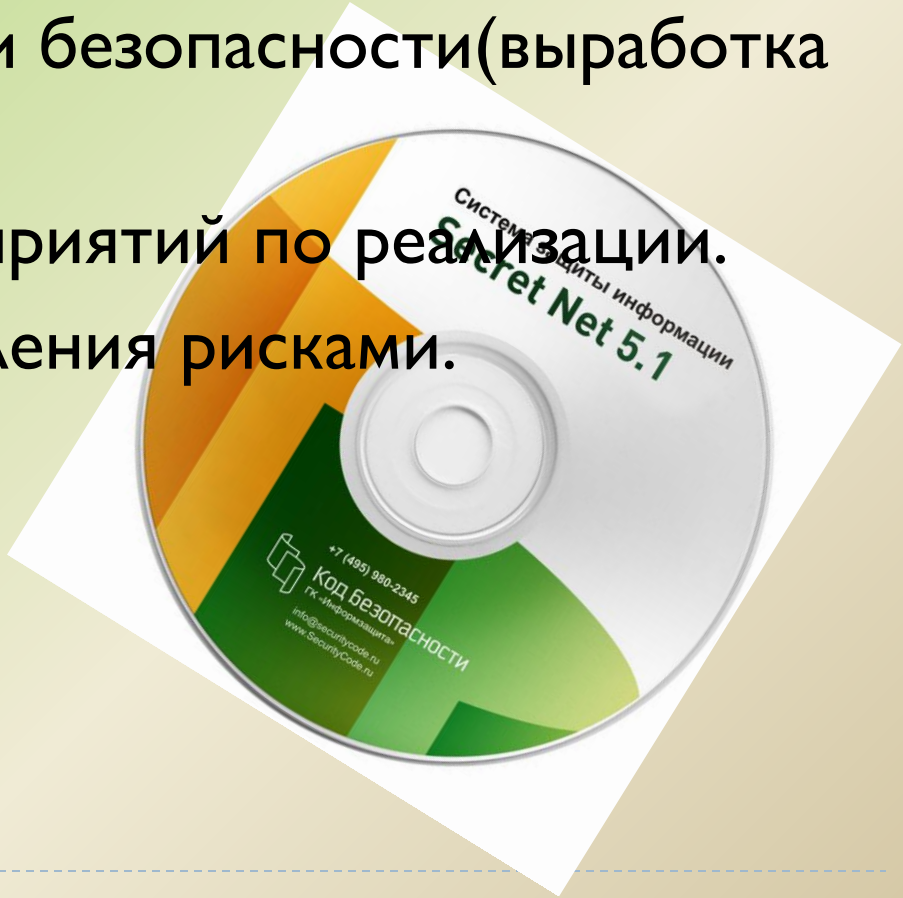
1. Анализ(учет) каналов т.к.у. и НСД.
2. Анализ потенциальных угроз и выявление главных.
3. Ранжирование угроз..
4. Определение круга лиц, которых может интересовать защищаемая И.
5. Построение моделей нарушителя.
6. Определяется вероятность реализации угроз. Проводится соотношение угроз с моделью нарушителя для определения соответствующей категории нарушителя и последующей оценки вероятности реализации данной угрозы. Например, если модель нарушителя не описывает категорию удаленных пользователей (в компании не предусмотрен удаленный доступ), то вероятность утечки информации в результате доступа к ней извне ничтожно мала, и ею можно пренебречь при расчете рисков.
7. Анализ рисков: - выбор и обоснование метода анализа рисков; -подготовка к проведению анализа; - проведение аналитических процедур;- обработка полученных результатов и ранжирование рисков по степени значимости.
8. Выбор политики управления рисками, в частности избегание, принятие, снижение, перенос или разделение риска.

Результат III этапа:

1. Реестр угроз(документ «Модель угроз информации»).
2. Документ «Модели нарушителя».
3. Инструкция по анализу рисков; - результаты анализа; - отчет по результатам анализа и реестр рисков по рангам.
4. Документ «Стратегия управления рисками».

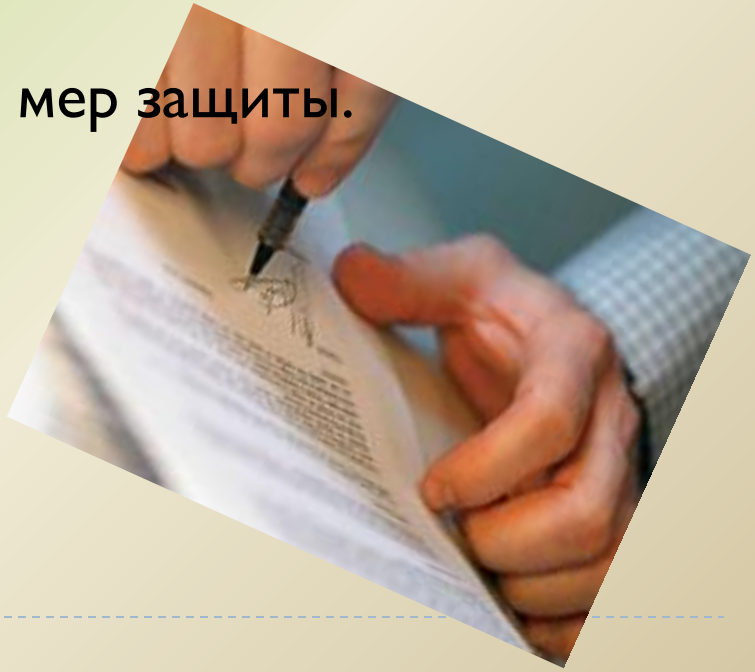
Этап №4. Моделирование способов и средств ЗИ

1. Разработка мер по предотвращению угроз. Оценка вариантов мер
2. Определение политики безопасности(выработка стратегии).
3. Разработка плана мероприятий по реализации.
4. Выбор стратегии управления рисками.



Результат IV этапа

1. Документ «Политика защиты информации».
2. Документы, отражающие расчеты (оценку) эффективности.
3. Документы, отражающие правовые, организационные и инженерно-технические мероприятия по предотвращению угроз.
4. План мероприятий по реализации мер защиты.



Этап №5. Разработка технического задания на систему ЗИ

Содержание работ:

Техническое задание как самостоятельный документ, согласовывается со службой безопасности предприятия и утверждается его руководителем.

Разделы:

- описание объекта защиты, назначение и основные требования к системе защиты,
- технико-экономические характеристики, состав, содержание и организация работ,
- требования по подготовке объекта к монтажу систем, порядок приемки системы в эксплуатацию.

Результат V этапа:

Результатом работы является пакет технических заданий.

Этап №6. Рабочее проектирование

1. **Выбор исполнителя**

Требования:

- требуемые лицензии на выполнение проектных работ;
- опыт работы по проектированию аналогичных систем защиты;
- внедренные системы защиты по выполненным им проектам.

2. **Заключение договора** на выполнение работ. Договор составляется по стандартной форме. Важным вопросом при заключении договора является порядок оплаты работ.

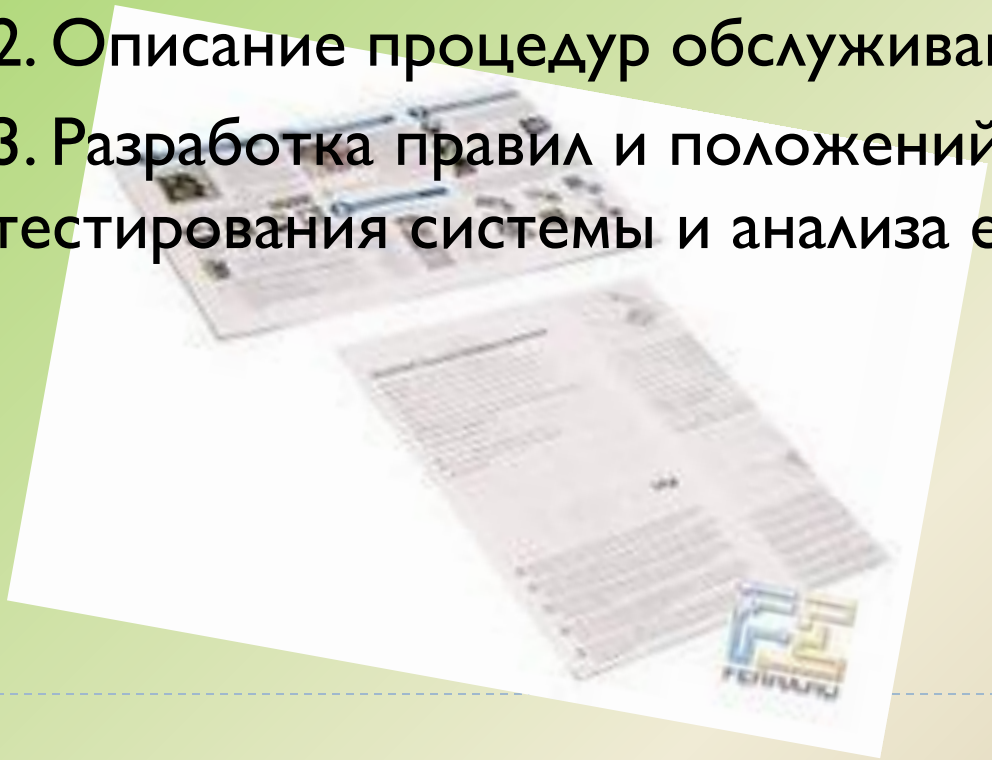
3. **Рабочий проект.** Рабочий проект является документом, на основании которого разрабатывается сметная документация и выполняются строительно-монтажные работы подсистем защиты информации техническими средствами.

4. **Сметная документация.** Расчет затрат на создание КСЗИ

Этап №7. Разработка «Эксплуатационной документации КСЗИ»

Содержание работ:

1. Составление инструкции эксплуатации КСЗИ.
2. Описание процедур обслуживания системы.
3. Разработка правил и положений по проведение тестирования системы и анализа ее работы.



Результат VII этапа:

1. Инструкции эксплуатации КСЗИ и её элементов;
2. Документ, отражающий процедуры регламентного обслуживания КСЗИ;
3. Правила и положения по проведению тестирования и анализа работы КСЗИ.

Этап №8 - №10

Этап 8. **Реализация рабочего проекта – построение системы защиты.**

Этап 9. **Внедрение.**

На этом этапе исполнитель проводит все пусконаладочные работы, обучает и инструктирует персонал предприятия правилам и режимам эксплуатации КСЗИ. После реализации этого этапа внедренная КСЗИ готова к последующему испытанию

Этап 10. **Эксплуатация.**

Спасибо за внимание