

Жизненный цикл системы физической защиты.

Полный жизненный цикл продукции – это срок жизни продукта от момента его создания, до окончания срока эксплуатации.



Цели и задачи

- Обследование объекта и определение приоритетной задачи защиты.
- Обеспечение уровня безопасности, соответствующего бизнес-целям и нормативным документам предприятия.
- Следование экономической целесообразности и выбранной приоритетной задаче при выборе защитных мер.
- Выработка организационных (прямая подчинённость ответственных за ИБ руководству) и технических мер обеспечения ИБ.
- Построение СОИБ.
- Выработка планов восстановления после критических ситуаций и обеспечения непрерывности работы ИС.
- Регулярный аудит СОИБ.

Общие принципы

Стратегия

- Доступность
 - Защититься и продолжить,
- Целостность
 - Восстановить и продолжить
- Конфиденциальность
 - Не допустить
 - Выследить и осудить

Общие принципы

Тактика

- что явно не запрещено, то разрешено;
- что явно не разрешено, то запрещено.

Жизненный цикл

ИС

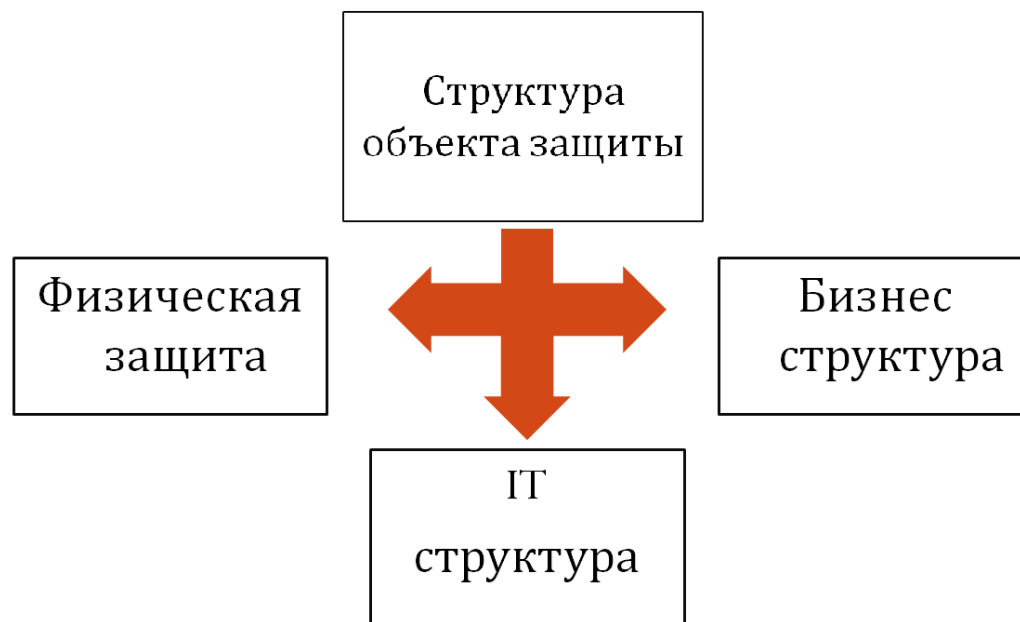
- Формирование требований к ИС
- Разработка концепции ИС
- Техническое задание
- Эскизный проект
- Технический проект
- Реализация
- Ввод в эксплуатацию
- Сопровождение ИС

СЗИ

- Обследование объекта защиты. Выявление приоритетной задачи защиты.
- Построение политики безопасности
- Выбор элементов системы защиты информации.
- Установка.
- Сопровождение.

Обследование объекта защиты

- Определение структуры объекта защиты.

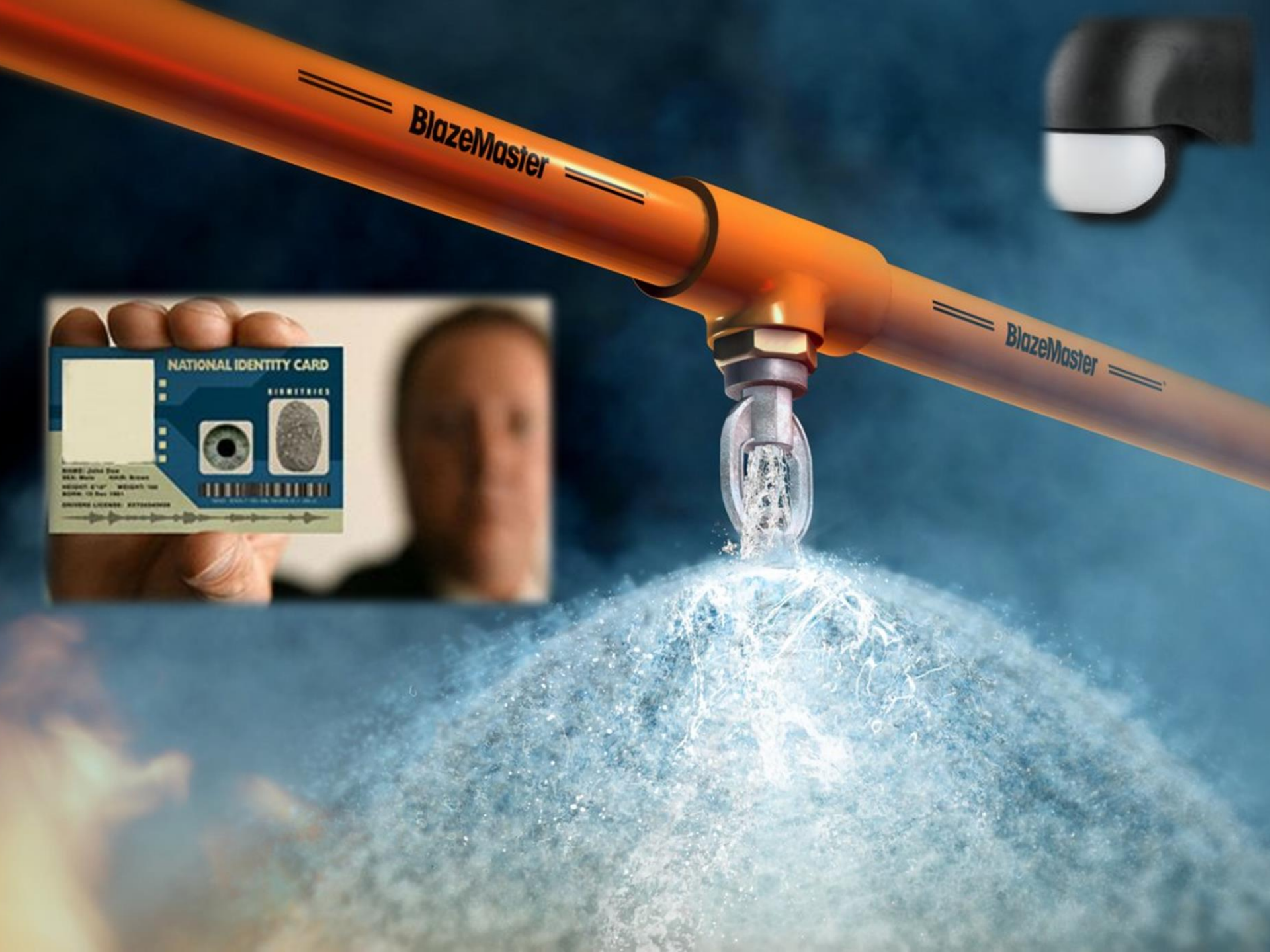


- Выявление приоритетной задачи защиты.



Исследование физической защиты объекта





BlazeMaster

BlazeMaster

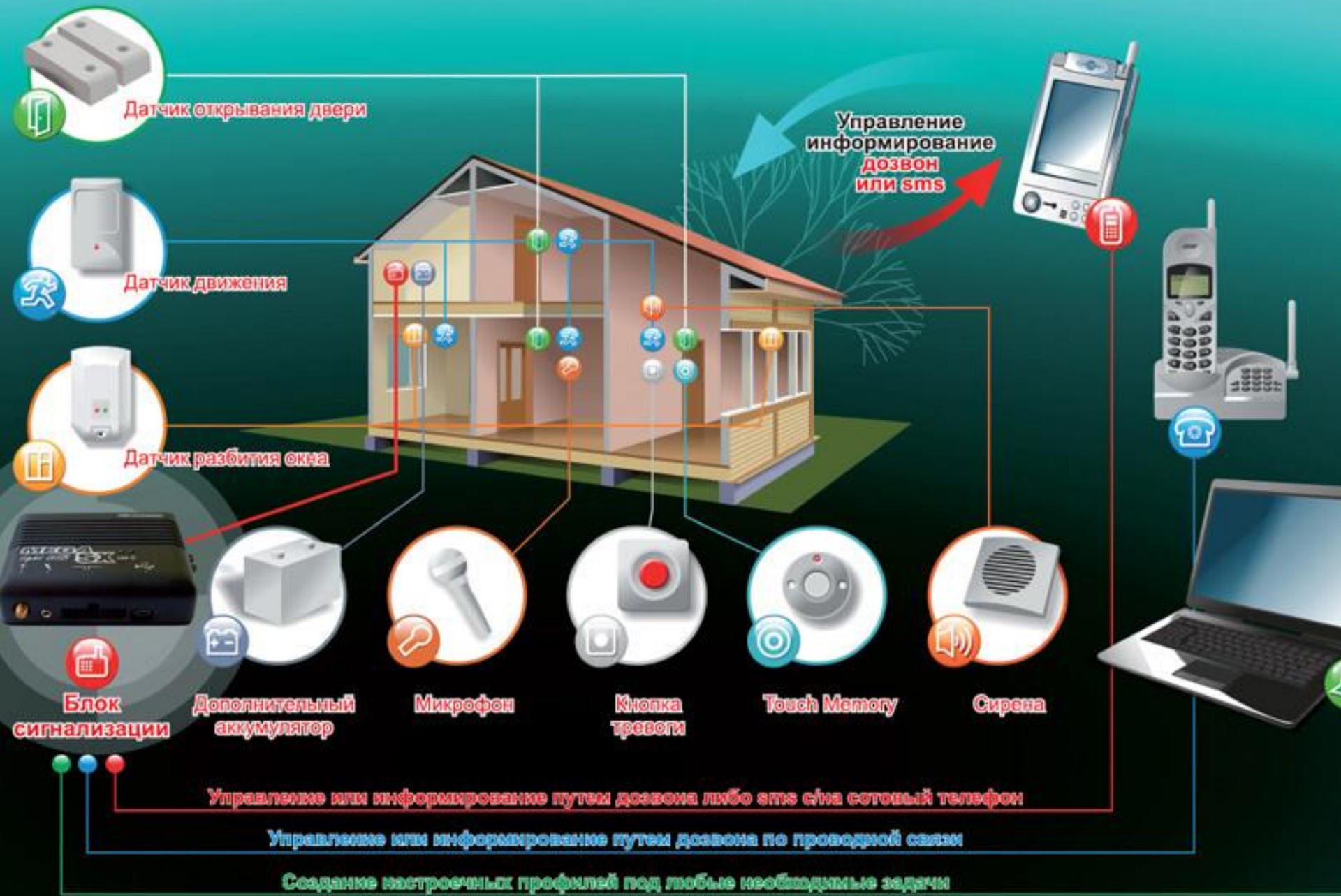
NATIONAL IDENTITY CARD

BIOMETRICS

NAME: John Doe
SEX: Male HAIR: Brown
HEIGHT: 6'10" WEIGHT: 180
DOB: 10 Dec 1981

DRIVING LICENSE: A123456789



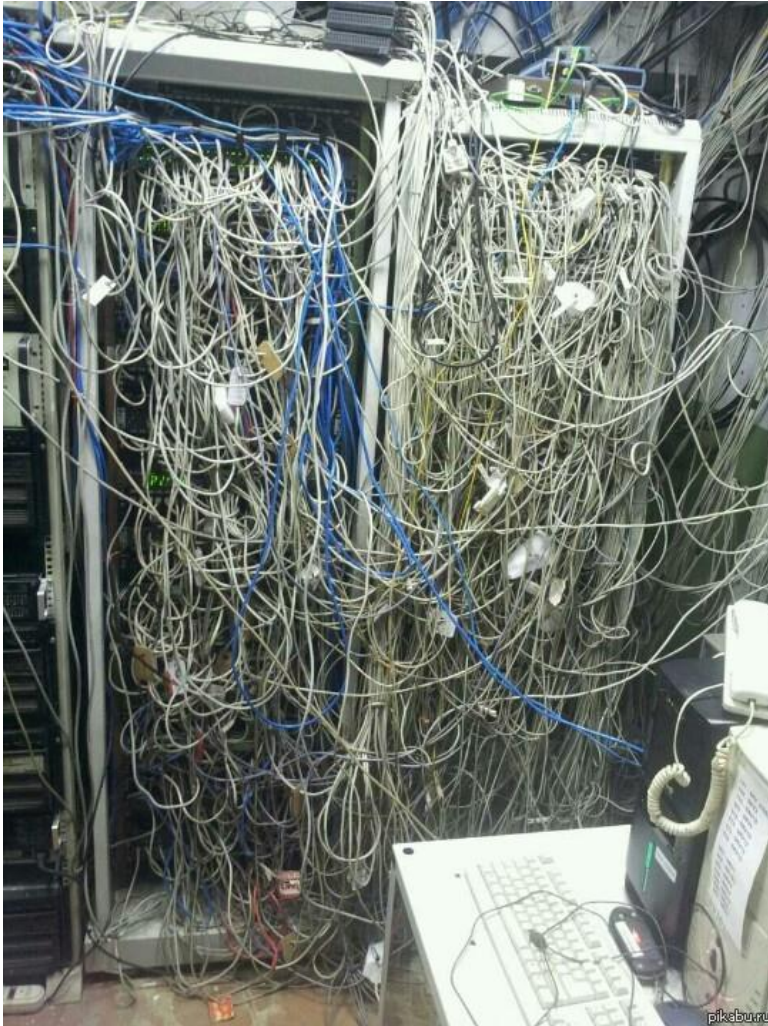


Исследование физической защиты объекта

- Наличие свободного доступа на территорию.
- Наличие видеонаблюдения.
- Наличие записей видеонаблюдения и сроки её хранения.



Исследование физической защиты объекта

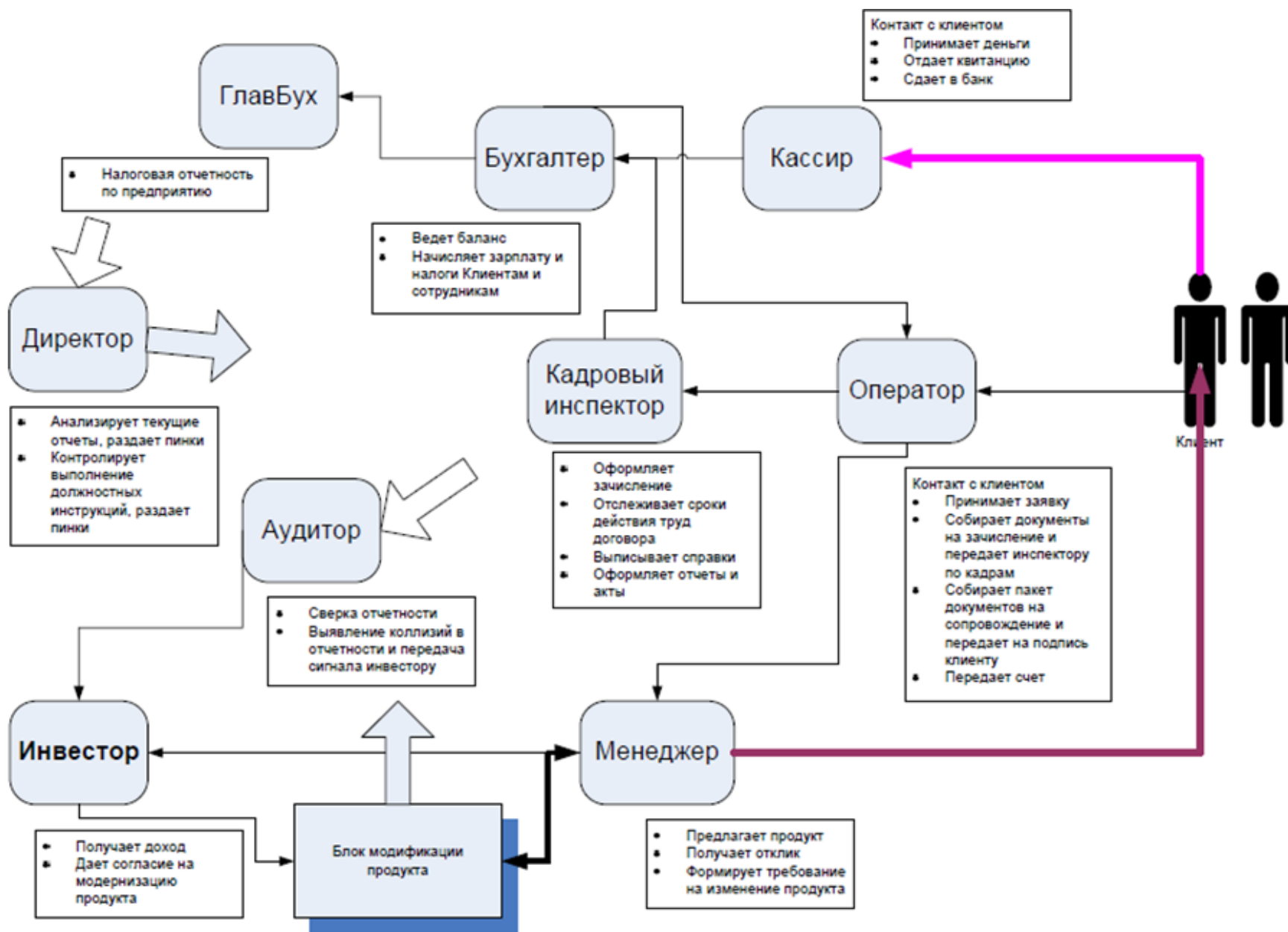


- Наличие свободного доступа к кабельному хозяйству.
- Наличие доступа к серверам и рабочим станциям.

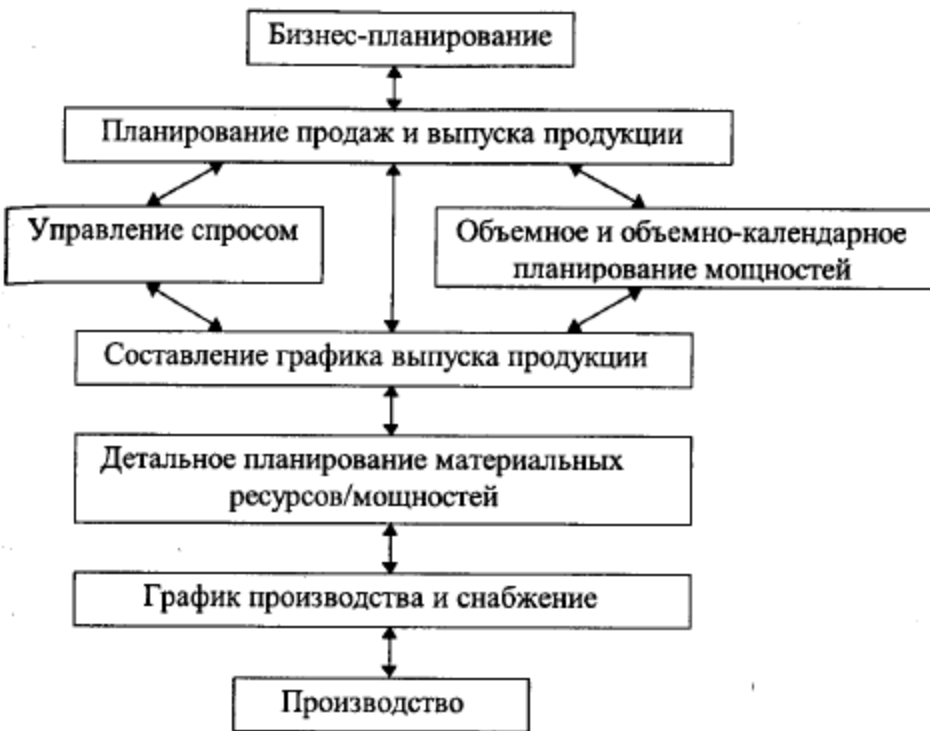
Исследование бизнес-структуры объекта защиты

- Определение и исследование бизнес-модели объекта защиты.
- Определение факторов влияния на бизнес, задание метрик для измеримых факторов.
- Определение целей IT-инфраструктуры (!!!).
- Определение эталонной модели IT-потоков.
- Определение необходимого списка ресурсов общего доступа в зависимости от подразделения.

Исследование бизнес-структуры объекта защиты



структуры объекта защиты



Бизнес-факторы, влияющие на эффективность

- Величина внутренних издержек (конфликт стоимости СЗИ).
- Качество управления собственным активом (конфликт интересов).
- Качество работы коллектива (конфликт с персоналом).
- Скорость реакции на внешние факторы.
- Стратегия и качество ведения самого бизнеса.
- Выбранная стратеги управления рисками.

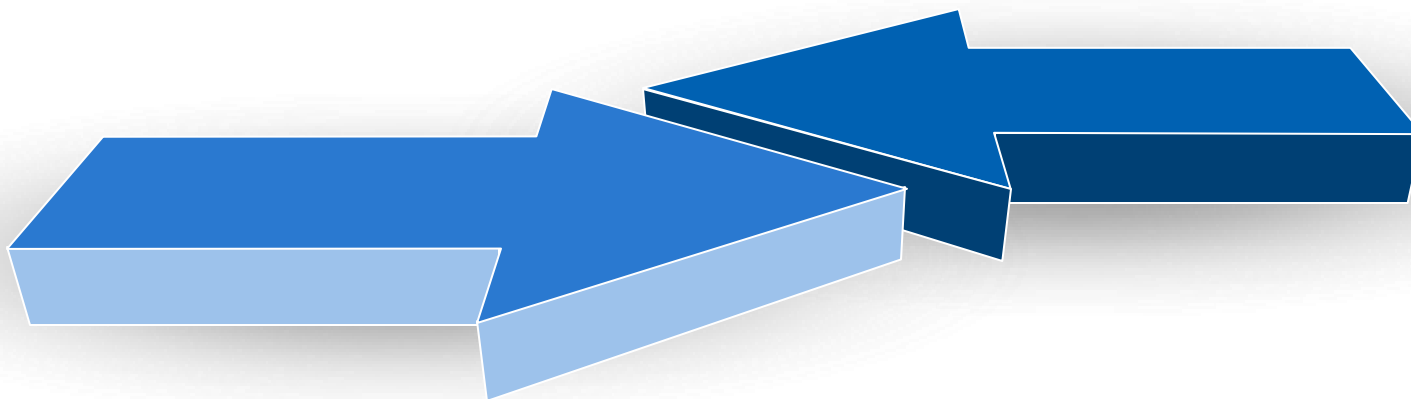
Проблема установления рационального баланса

Безопасность

- Затраты на безопасность
- Внедрение новых элементов СЗИ
- Управление жизненным циклом ИС
- Разграничение доступа

Эффективность

- Увеличение прибыли
- Сокращение расходов
- Накопление знаний
- Повышение осведомленности



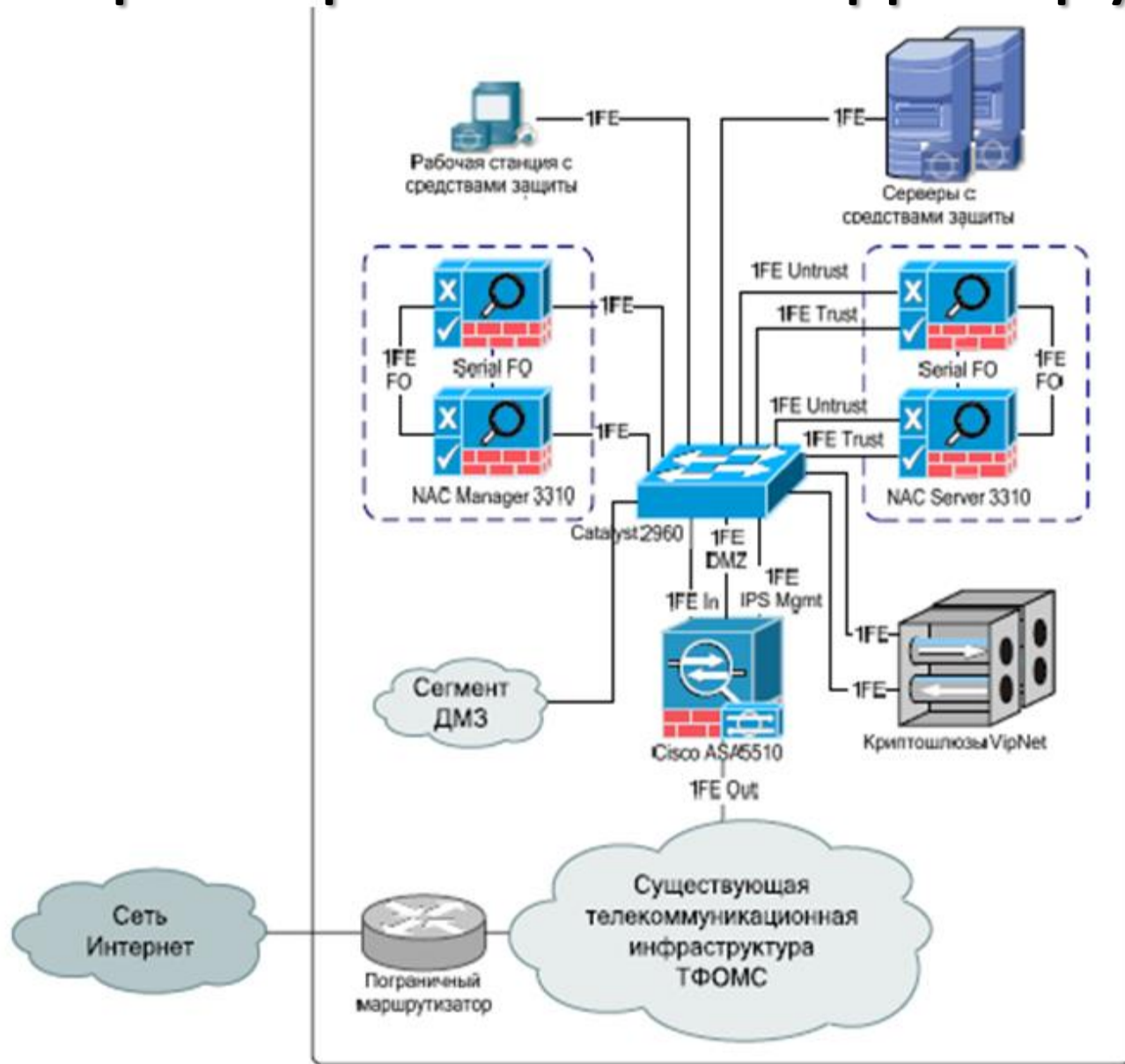
Исследование IT-инфраструктуры объекта защиты

- Обследование аппаратного обеспечения:
 - Маршрутизаторы / точки доступа / фаерволы.
 - Сервера, рабочие станции (рабочие, служебные).
 - Прочее оборудование (ИБП, ...).
- Обследование программного обеспечения:
 - Выявление приложений, работающих с интранетом.
 - Выявление приложений, работающих с Интернетом.
- Обследование кабельного хозяйства.
- Исследование IT-потоков.
- Обследование точек межсетевого взаимодействия:
 - С дружественными (известными) сетями.
 - С недружественными сетями.

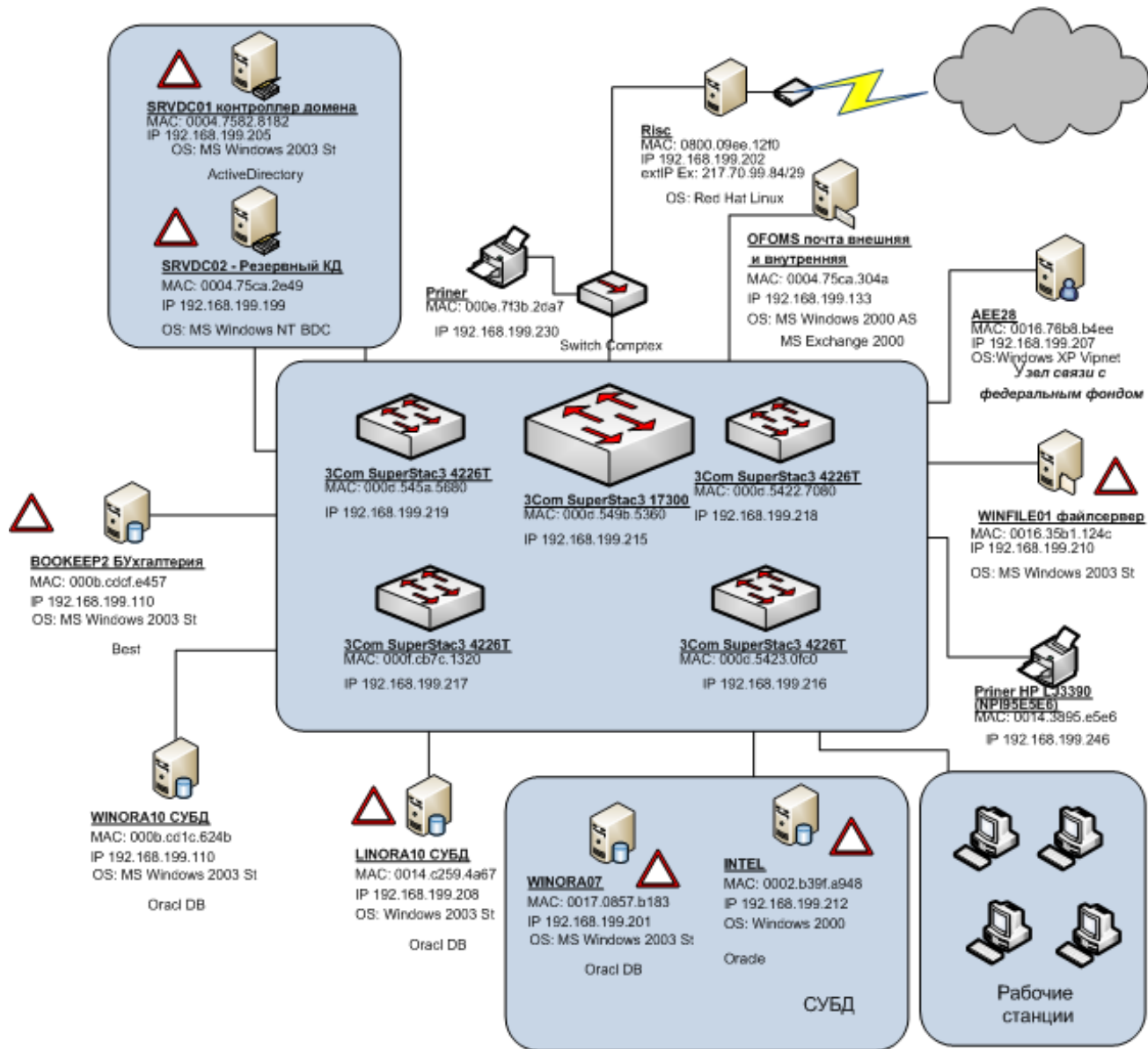
Основные элементы ИС

- Программные средства, применяемые при обработке информации (ОС, СУБД, web-сервера и т.п.).
- Технические средства, осуществляющие обработку данных
 - средства вычислительной техники;
 - информационно-вычислительные комплексы и сети;
 - средства и системы передачи, приема и обработки данных;
 - средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации).
- Совокупность информации и ее носителей, используемых в ИС (данные в БД).
- Средства защиты информации.
- Вспомогательные технические средства и системы.

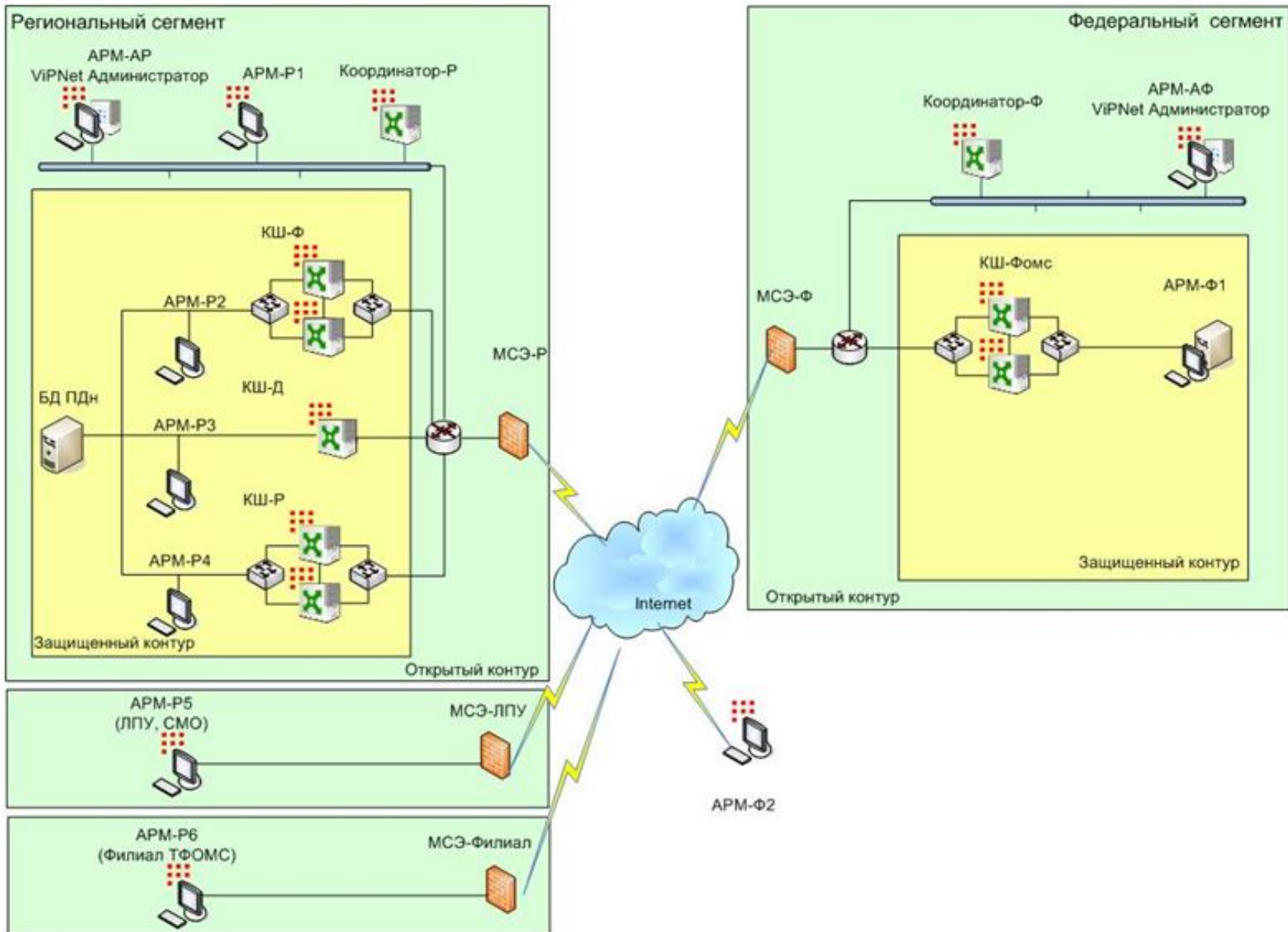
Пример сетевой инфраструктуры



Пример сетевой инфраструктуры



Пример сетевой инфраструктуры

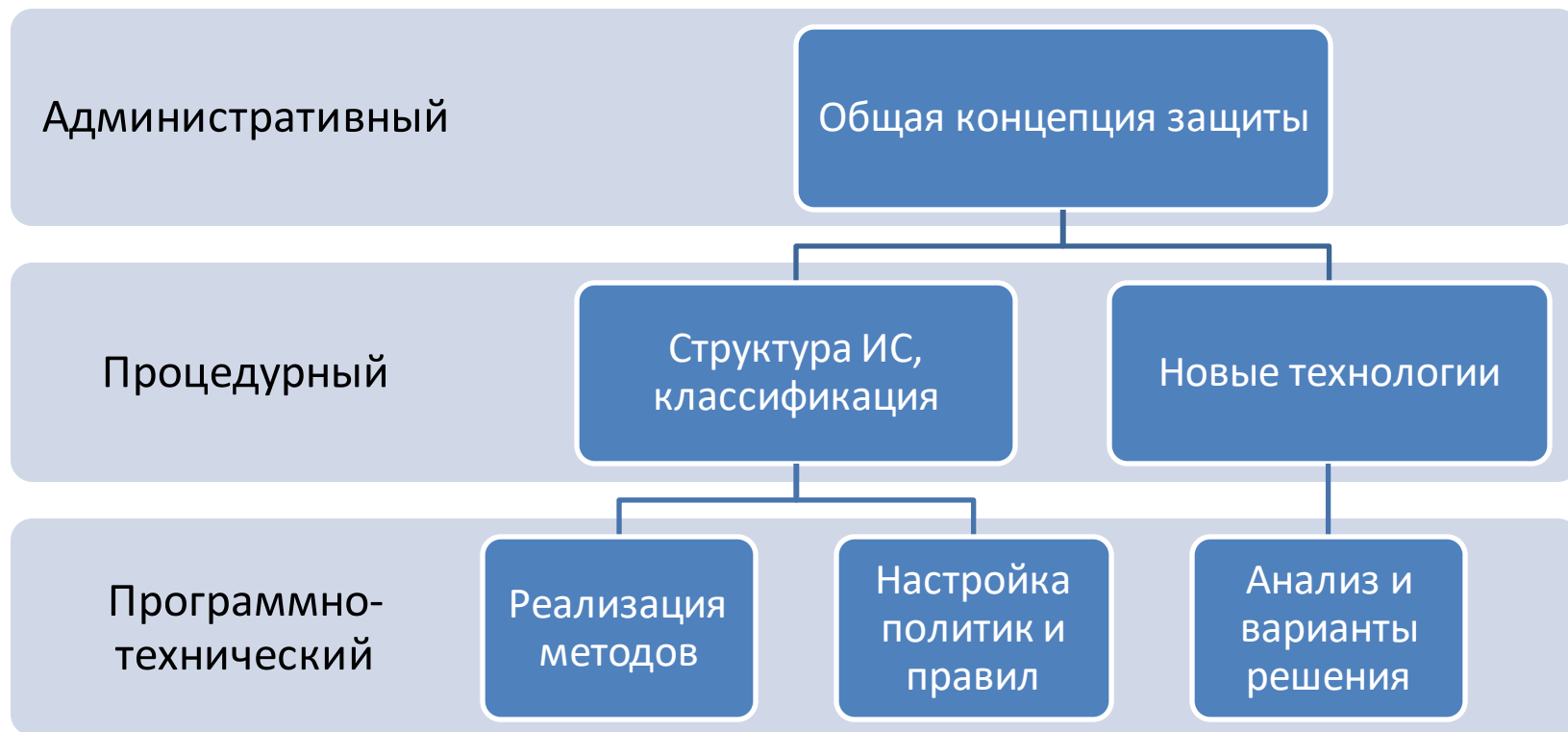


Разработка политики безопасности.

Уровни процессов ИБ.

- Административный уровень защиты информации.
- Базовый уровень безопасности.
- Процедурный уровень защиты информации.
- Стандарты и спецификации в области безопасности информационных технологий.
- Критерии оценки безопасности информационных технологий.

Уровни разработки политики безопасности



Разработка политики безопасности.

Уровни абстракции.

- Законодательный.
- Административный.
- Процедурный.
- Программно-технический.

Политика безопасности

- формальное изложение правил, которым должны подчиняться лица, получающие доступ к корпоративной технологии и информации (RFC 2196).
- совокупность документированных решений, принимаемых руководством организации и направленных на защиту информации и ассоциированных с ней ресурсов
- набор документов описывающих состояние информационной безопасности и определяющий приоритетные задачи СЗИ.

Структура политики безопасности

- Концепция информационной безопасности.
- Организационный уровень: описание отделов и групп, связанных с обеспечением ИБ, их функции.
- Утверждённые модели:
 - Модель актуальных угроз.
 - Модель нарушителя.
 - Анализ и управление рисками.
- Перечень и классификация защищаемых объектов, уровень их защиты.
- Организационные меры:
 - Регламенты доступа, инструкции.
 - Обучение персонала.
 - Порядок реагирования на инциденты.
 - ...



ГАЗПРОМБАНК

(Открытое акционерное общество)

УТВЕРЖДЕНА
решением Правления ГПБ (ОАО)
«24» сентября 2008 г.
(протокол № 35)

С изменениями, утвержденными
решением Правления ГПБ (ОАО)
«30» сентября 2009 г. (протокол № 41),
«10» ноября 2010 г. (протокол № 49),
«22» марта 2012 г. (протокол № 11)

Политика
информационной безопасности
«Газпромбанк»
(Открытое акционерное общество)

| | | |
|-----|--|----|
| 1. | Общие положения..... | 3 |
| 2. | Список терминов и определений..... | 4 |
| 3. | Описание объекта защиты | 5 |
| 4. | Цели и задачи деятельности по обеспечению информационной безопасности | 6 |
| 5. | Угрозы информационной безопасности | 6 |
| 6. | Модель нарушителя информационной безопасности | 7 |
| 7. | Основные положения по обеспечению информационной безопасности | 8 |
| 8. | Организационная основа деятельности по обеспечению информационной безопасности | 10 |
| 9. | Ответственность за соблюдение положений Политики..... | 12 |
| 10. | Контроль за соблюдением положений Политики..... | 13 |
| 11. | Заключительные положения | 13 |

1. Общие положения

1.1. Настоящая Политика разработана в соответствии с законодательством Российской Федерации и нормами права в части обеспечения информационной безопасности, требованиями нормативных актов Центрального банка Российской Федерации, федерального органа исполнительной власти, уполномоченного в области безопасности, федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, и основывается в том числе на:

- Доктрине информационной безопасности Российской Федерации (от 09.09.2000 Пр-1895);
- Стандарте Банка России СТО БР ИББС -1.0 – 2010 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения».

1.2. Настоящая Политика является документом, доступным любому сотруднику Банка и пользователю его ресурсов, и представляет собой официально принятую руководством «Газпромбанк» (Открытое акционерное общество) (далее – Банк) систему взглядов на проблему обеспечения информационной безопасности, и устанавливает принципы построения системы управления информационной безопасностью на основе систематизированного изложения целей, процессов и процедур информационной безопасности Банка.

1.3. Руководство Банка осознает важность и необходимость развития и совершенствования мер и средств обеспечения информационной безопасности в контексте развития законодательства и норм регулирования банковской деятельности, а также развития реализуемых банковских технологий и ожиданий клиентов Банка и других заинтересованных сторон. Соблюдение требований информационной безопасности позволит создать конкурентные преимущества Банку, обеспечить его финансовую стабильность, рентабельность, соответствие правовым, регулятивным и договорным требованиям и повышение имиджа.

2. Список терминов и определений

В настоящей Политике использованы термины с соответствующими определениями согласно СТО БР ИББС–1.0–2010 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения».

2.1. **Бизнес-процесс** – последовательность технологически связанных операций по предоставлению банковских продуктов и/или осуществлению конкретного вида обеспечиваемой деятельности Банка.

2.2. **Информационная безопасность Банка (ИБ)** – в настоящей Политике состояние защищенности технологических и бизнес - процессов Банка, объединяющих в своем составе сотрудников Банка, технические и программные средства обработки информации, информацию в условиях угроз в информационной сфере.

2.3. **Информационная система Банка** – совокупность программно-аппаратных комплексов Банка, применяемых для обеспечения бизнес - процессов Банка. Банкоматы в данной совокупности не рассматриваются как устройства, сильно отличающиеся от остальных компонентов информационной системы Банка и обладающие своими уникальными свойствами с точки зрения информационной безопасности.

2.4. **Инцидент информационной безопасности** – это появление одного или нескольких нежелательных рисков событий информационной безопасности, с которыми связана значительная вероятность нарушения конфиденциальности, целостности или доступности информационных активов и инфраструктуры и создания угрозы информационной безопасности.

2.5. **ИТ-блок** – совокупность самостоятельных структурных подразделений Банка, ответственных за развитие, эксплуатацию и сопровождение информационных банковских систем.

3. Описание объекта защиты

Основными объектами защиты системы информационной безопасности в Банке являются:

- информационные ресурсы, содержащие коммерческую тайну, банковскую тайну, персональные данные физических лиц, сведения ограниченного распространения, а также открыто распространяемая информация, необходимая для работы Банка, независимо от формы и вида ее представления;
- информационные ресурсы, содержащие конфиденциальную информацию, включая персональные данные физических лиц, а также открыто распространяемая информация, необходимая для работы Банка, независимо от формы и вида ее представления;

6. Модель нарушителя информационной безопасности

По отношению к Банку нарушители могут быть разделены на внешних и внутренних нарушителей.

6.1. Внутренние нарушители.

В качестве потенциальных внутренних нарушителей Банком рассматриваются:

- зарегистрированные пользователи информационных систем Банка;
- сотрудники Банка, не являющиеся зарегистрированными пользователями и не допущенные к ресурсам информационных систем Банка, но имеющие доступ в здания и помещения;
- персонал, обслуживающий технические средства корпоративной информационной системы Банка;
- сотрудники самостоятельных структурных подразделений Банка, задействованные в разработке и сопровождении программного обеспечения;
- сотрудники самостоятельных структурных подразделений, обеспечивающие безопасность Банка;
- руководители различных уровней.

6.2. Внешние нарушители.

В качестве потенциальных внешних нарушителей Банком рассматриваются:

- бывшие сотрудники Банка;
- представители организаций, взаимодействующих по вопросам технического обеспечения Банка;
- клиенты Банка;
- посетители зданий и помещений Банка;
- конкурирующие с Банком кредитные организации;
- члены преступных организаций, сотрудники спецслужб или лица, действующие по их заданию;
- лица, случайно или умышленно проникшие в корпоративную информационную систему Банка из внешних телекоммуникационных сетей (хакеры).

6.3. В отношении внутренних и внешних нарушителей принимаются следующие ограничения и предположения о характере их возможных действий:

- нарушитель скрывает свои несанкционированные действия от других сотрудников Банка;
- несанкционированные действия нарушителя могут быть следствием ошибок пользователей, эксплуатирующего и обслуживающего персонала, а также недостатков принятой технологии обработки, хранения и передачи информации;
- в своей деятельности вероятный нарушитель может использовать любое имеющееся средство перехвата информации, воздействия на информацию и информационные

8.2. Оперативная деятельность и планирование деятельности по обеспечению информационной безопасности Банка осуществляются и координируются **Ответственным подразделением**. Задачами **Ответственного подразделения** являются:

- установление потребностей Банка в применении мер обеспечения информационной безопасности, определяемых как внутренними корпоративными требованиями, так и требованиями нормативных актов;
- соблюдение действующего федерального законодательства, нормативных актов федеральных органов исполнительной власти, уполномоченных в области обеспечения безопасности и противодействия техническим разведкам и технической защите информации, нормативных актов Банка России и стандартов Банка России по обеспечению информационной безопасности, нормативных актов по обеспечению информационной безопасности, приватности и неразглашению, принятых регуляторами рынков, на которых представлены интересы и бизнес Банка;
- разработка и пересмотр внутренних нормативных документов по обеспечению информационной безопасности Банка, включая планы, политики, положения, регламенты, инструкции, методики, перечни сведений и иные виды внутренних нормативных документов;
- осуществление контроля актуальности и непротиворечивости внутренних нормативных документов (политик, планов, методик и т.д.), затрагивающих вопросы информационной безопасности Банка;
- обучение, контроль и непосредственная работа с персоналом Банка в области обеспечения информационной безопасности;
- планирование применения, участие в поставке и эксплуатации средств обеспечения информационной безопасности на объекты и системы в Банке;
- выявление и предотвращение реализации угроз информационной безопасности;
- выявление и реагирование на инциденты информационной безопасности;
- информирование в установленном порядке ответственных лиц (Департамент анализа и контроля банковских рисков) об угрозах и рисковом событиях информационной безопасности;
- прогнозирование и предупреждение инцидентов информационной безопасности;
- пресечение несанкционированных действий нарушителей информационной безопасности;
- поддержка базы инцидентов информационной безопасности, анализ, разработка оптимальных процедур реагирования на инциденты и обучение персонала;
- типизация решений по применению мер и средств обеспечения информационной безопасности и распространение типовых решений на филиалы и представительства Банка;
- обеспечение эксплуатации средств и механизмов обеспечения информационной безопасности;
- мониторинг и оценка информационной безопасности, включая оценку полноты и достаточности защитных мер и видов деятельности по обеспечению информационной безопасности Банка;

9. Ответственность за соблюдение положений Политики

Общее руководство обеспечением информационной безопасности Банка осуществляет Куратор.

Ответственность за поддержание положений настоящей Политики в актуальном состоянии, создание, внедрение, координацию и внесение изменений в процессы системы менеджмента информационной безопасности Банка лежит на руководстве **Ответственного подразделения**.

Концепция информационной безопасности



- Цели и задачи СЗИ.
- Определение объекта защиты и приоритетной задачи защиты.
- Подчиненность отдела защиты информации.
- Принципы финансирования.
- Метрики ИБ и схема контроля состояния ИС.
- Создание и схема работы CSIRT-группы.
- ...

Структура политики безопасности

- Вопросы физической защиты.
- Технические вопросы:
 - Перечень лиц, имеющих доступ к защищаемым объектам, и границы сетевых зон.
 - Перечень используемого ПО и его конфигураций.
 - Набор инструкций, корпоративные приказы и распоряжения.
 - Структура и схема активного сетевого оборудования.

Выбор элементов СЗИ. Принципы.

- Производится на этапе построения политики безопасности.
- Основывается на анализе рисков.
- Требует проведения технических тестов и серьёзной аналитической работы.
- Требует наличия технических специалистов.

Выбор элементов СЗИ. Подсистемы.

- Физической защиты
- Криптографической защиты
- Авторизации и аутентификации
- Управления
 - Пользователями
 - Сетью
- Резервирования
- Антивирусная
- Мониторинга событий и обнаружения атак

Подсистема физической защиты

- Физическое управление доступом.
- Противопожарные меры.
- Защита поддерживающей инфраструктуры.
- Защита информации от перехвата по тех. каналам.
- Защита мобильных систем.

Построение модели угроз и нарушителя.

Взаимосвязь элементов



Угроза

Угроза ИБ – совокупность условий и факторов, создающих опасность для информации и/или поддерживающей инфраструктуры.

Классификация:

- Активная угроза безопасности – угроза, связанная с изменением состояния автоматизированной системы.
- Пассивная угроза безопасности – угроза, не связанная с изменением состояния автоматизированной системы.

КЛАССИФИКАЦИЯ УГРОЗ

Классификационные признаки

- По виду нарушаемого свойства информации (виду несанкционированных действий, осуществляемых с данными).
- По видам возможных источников угроз.
- По виду защищаемой от угроз информации.
- По способу реализации угроз.
- По используемой уязвимости.

Зачем нужна классификация

- Позволяет сократить количество рассматриваемых одновременно объектов
- Упорядочить процесс рассмотрения объектов
- Выделить общие характеристики

Виды угроз по нарушаемому свойству

- Угрозы конфиденциальности.
- Угрозы доступности:
техногенные, непреднамеренные ошибки, пользовательская сложность ИС, инсайдеры.
- Угрозы целостности:
фальсификация данных (в т.ч. инсайдеры), нарушение атомарности транзакций.
- Угрозы раскрытия параметров защищенной компьютерной системы: новые угрозы, уязвимости, увеличение рисков.

Классификация по виду носителя

- акустическая (речевая) информация (РИ), содержащаяся непосредственно в произносимой речи пользователя ИС при осуществлении им функции голосового ввода данных в ИС, либо воспроизводимая акустическими средствами ИС, а также содержащаяся в электромагнитных полях и электрических сигналах, которые возникают за счет преобразований акустической информации;
- видовая информация (ВИ), представленная в виде текста и изображений различных устройств отображения информации средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИС;
- информация, обрабатываемая (циркулирующая) в ИС, в виде электрических, электромагнитных, оптических сигналов;
- информация, обрабатываемая в ИС, представленная в виде бит, байт, файлов и других логических структур.

Классификация по способу реализации угроз

- Угрозы, связанные с НСД к данным (атаки; внедрение вредоносного ПО; повышение / использование привилегий и т.д.);
- Угрозы утечки данных по техническим каналам (ПЭМИН, ...).
- Угрозы специальных воздействий на ИС.

Классификация по используемой уязвимости

- угрозы, реализуемые с использованием уязвимости системного ПО;
- угрозы, реализуемые с использованием уязвимости прикладного ПО;
- угрозы, реализуемые наличием в ИС аппаратной закладки;
- угрозы, реализуемые с использованием уязвимостей протоколов сетевого взаимодействия и каналов передачи данных;
- угрозы, возникающие в результате использования уязвимости, вызванной недостатками организации ТЗИ от НСД;
- угрозы, реализуемые с использованием уязвимостей, обуславливающих наличие технических каналов утечки информации;
- угрозы, реализуемые с использованием уязвимостей СЗИ.

Примеры угроз

- наблюдение за источниками информации;
- подслушивание конфиденциальных разговоров и акустических сигналов;
- перехват электрических, виброакустических, магнитных и электромагнитных полей и электрических сигналов излучений;
- несанкционированное распространение материальных носителей за пределами организации;
- разглашение информации компетентными людьми;
- Утеря / кража носителей информации;
- несанкционированное распространение информации через поля и электрические сигналы случайно возникшие в аппаратуре;
- воздействие стихийных сил;
- сбои в аппаратуре или ПО;
- воздействие мощных электромагнитных и электрических помех.

Источники угроз

- Внешние атаки.
- Инсайдерские атаки.
- Непреднамеренные ошибки.
- Отказ инфраструктуры.
- Внутренний отказ ИС.
- Юридические проблемы.
- Преднамеренные атаки физического уровня.

Классификация по источникам угроз

- Угрозы обусловленные действиями субъекта (антропогенные угрозы).
- Угрозы, обусловленные техническими средствами (техногенные угрозы).
- Угрозы, обусловленные стихийными источниками (стихийные угрозы).

Антропогенные угрозы

- Внешние:
 1. Криминальные структуры.
 2. Рецидивисты и потенциальные преступники.
 3. Недобросовестные партнёры.
 4. Конкуренты.
 5. Политические противники.
- Внутренние:
 1. Персонал учреждения.
 2. Персонал филиалов.
 3. Специально внедрённые агенты.

Техногенные угрозы

- Внутренние:
 1. Некачественные технические, средства обработки информации - некачественные программное средства.
 2. Некачественные программные средства обработки.
 3. Вспомогательные средства.
 4. Другие технические средства.
- Внешние:
 1. Средства связи.
 2. Близко расположенные опасные производства.
 3. Сети инженерных коммуникаций (канализация, энерго-, тепло и водоснабжение).
 4. Транспорт.

Стихийные угрозы



- Пожары, молнии, включая шаровые.
- Землетрясения.
- Ураганы.
- Наводнения.
- Другие форс-мажорные обстоятельства.
- Различные непредвиденные обстоятельства.
- Необъяснимые явления.

Идентификация угроз

- Необходимо идентифицировать опасности:
 - Известные опасности.
 - Неучтённые ранее опасности.
- Предварительная оценка позволяет:
 - Принять немедленные меры.
 - Прекратить анализ из-за несущественности опасности.
 - Перейти к оценке рисков и угроз.

Условия реализации угрозы

- Угроза безопасности реализуется в результате образования канала реализации угрозы между источником угрозы и носителем (источником) защищаемых данных, что создает условия для нарушения безопасности данных (несанкционированный или случайный доступ).



Источник
угрозы



- источник– субъект, материальный объект или физическое явление, создающие угрозу;
- среда распространения, в которой физическое поле, сигнал, данные или программы могут распространяться и воздействовать на защищаемые свойства;
- Носитель – физическое лицо или материальный объект, в том числе физическое поле, в котором данные находят свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Уровни детализации

- **Угрозы общего уровня.**
Пример: нарушение доступности сайта интернет-магазина.
- **Угрозы общего технического уровня.**
Пример: угроза реализации XSS-атаки (межсайтовый скриптинг); угроза нарушения доступности хостинга.
- **Угрозы детального технического уровня.**
Пример: наличие уязвимости CVE в SharePoint платформе; DDoS-атака на сервер хостинга / ошибки персонала хостинга.

Компьютерная атака

- Целенаправленное несанкционированное воздействие на информацию, на ресурс автоматизированной информационной системы или получение несанкционированного доступа к ним с применением программных или программно-аппаратных средств.

Виды атак

Mailbombing

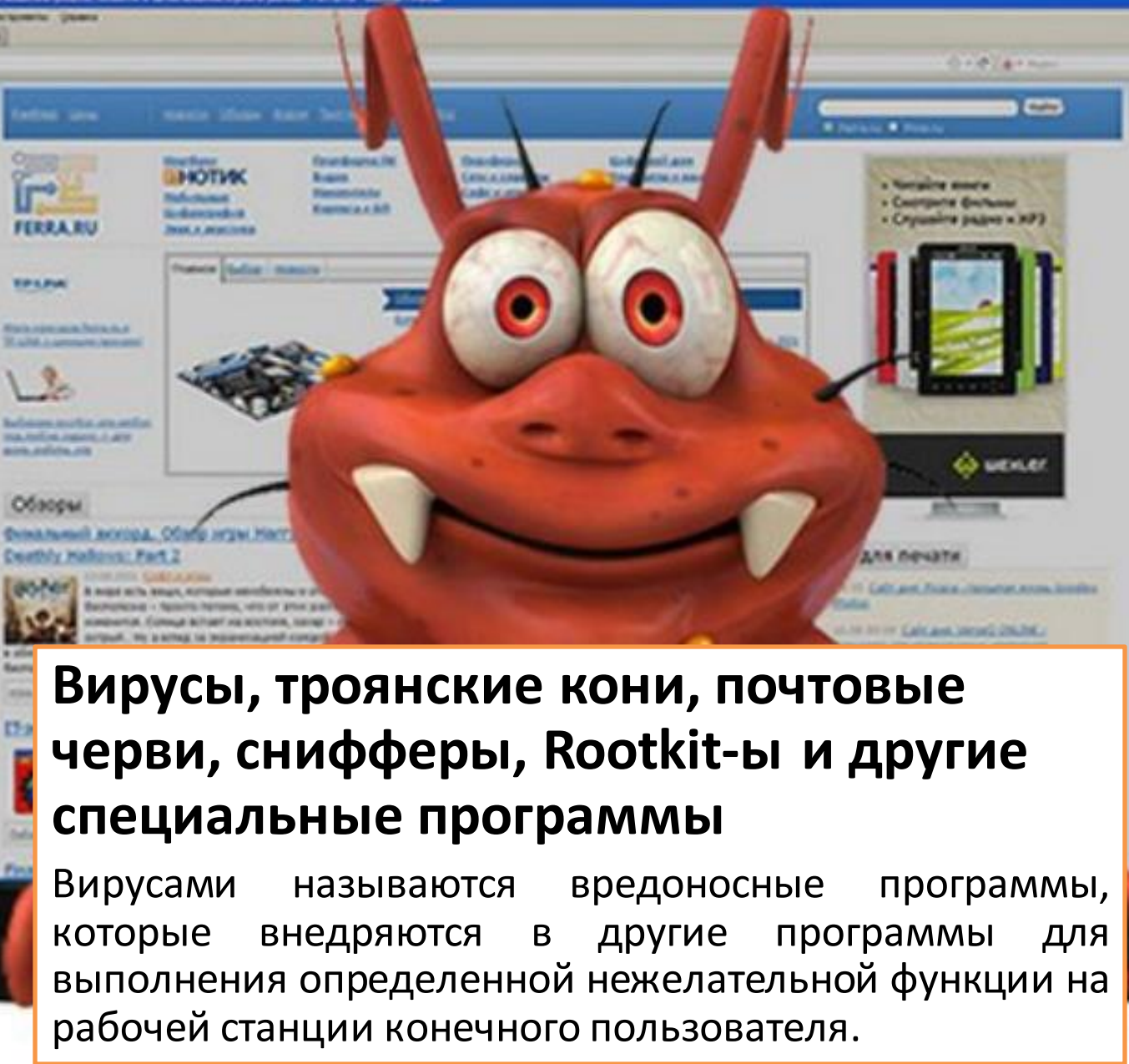
Суть данной атаки заключается в том, что на почтовый ящик посылается огромное количество писем на почтовый ящик пользователя. Эта атака может вызвать отказ работы почтового ящика или даже целого почтового сервера. Данная атака может проводиться любым хотя бы немного подготовленным противником. Простым примером программы, с помощью которой можно осуществить подобную атаку- The Unabomber. Достаточно знать адрес сервера, позволяющего анонимно отправлять почтовые сообщения, и адрес пользователя, которому эти сообщения предназначены. Количество писем, которое можно отослать для этой программы равно 12 разрядному числу.

Переполнение буфера

Атака на переполнение буфера основывается на поиске программных или системных уязвимостей, способных вызвать нарушение границ памяти и аварийно завершить приложение или выполнить произвольный бинарный код от имени пользователя, под которым работала уязвимая программа. Если программа работает под учетной записью администратора, то данная атака может позволить получить полный контроль над компьютером, на котором исполняется данная программа.

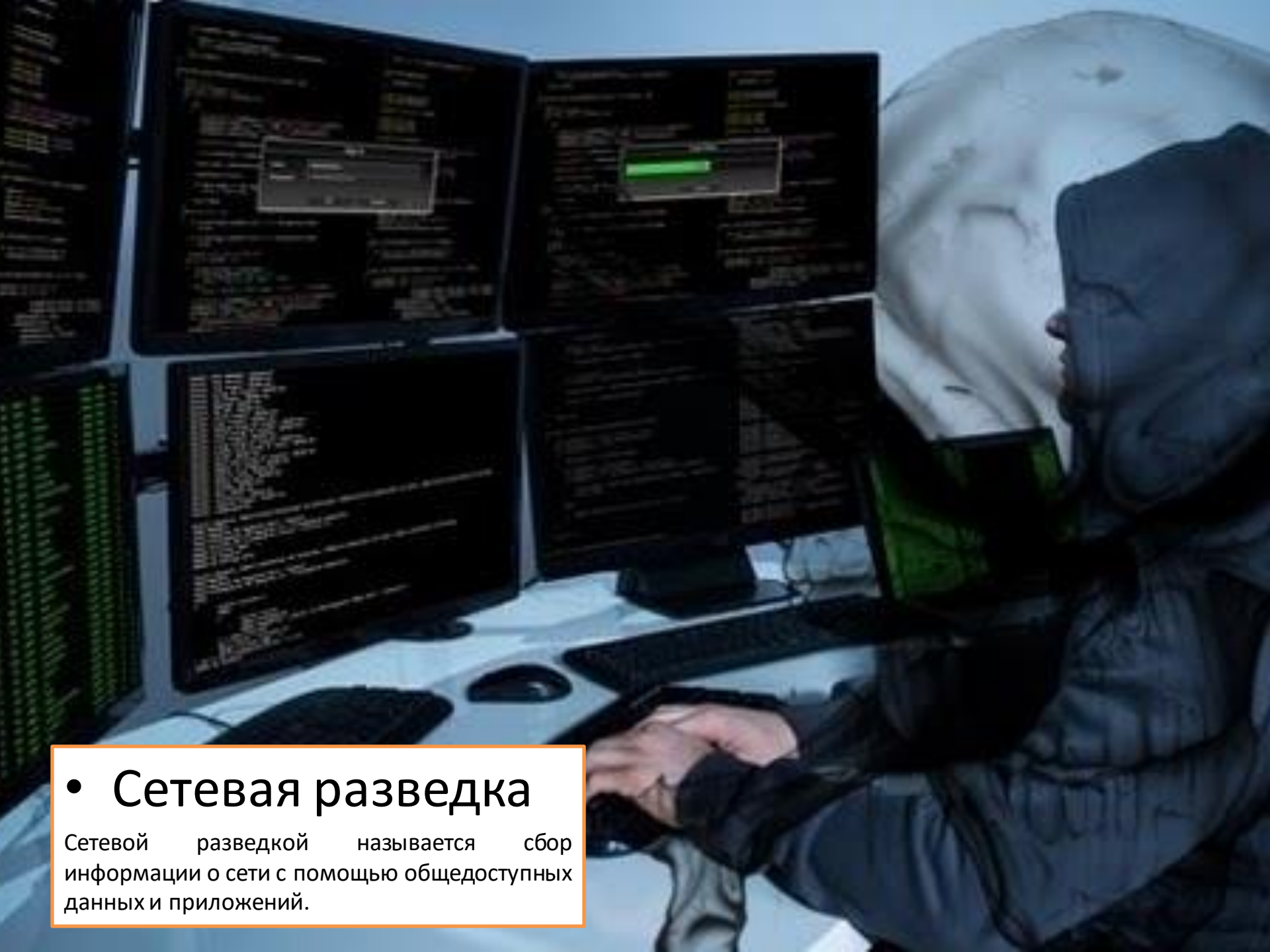


fffer Overfl



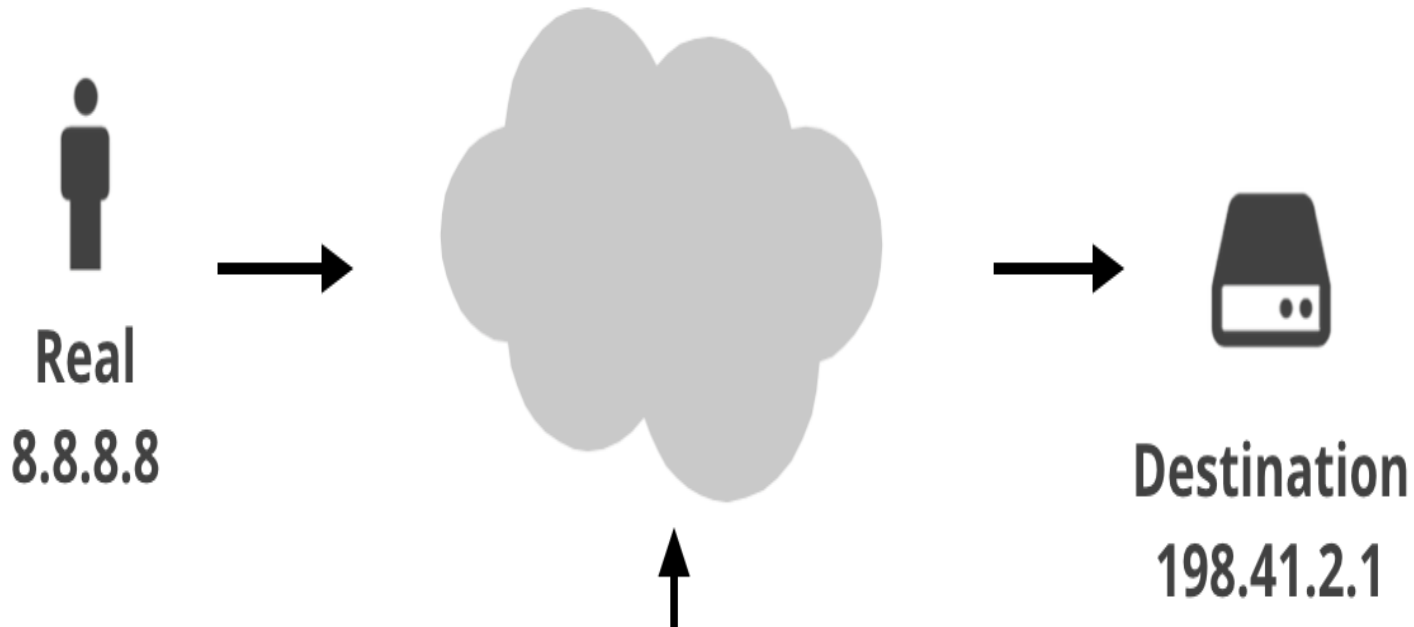
Вирусы, троянские кони, почтовые черви, снифферы, Rootkit-ы и другие специальные программы

Вирусами называются вредоносные программы, которые внедряются в другие программы для выполнения определенной нежелательной функции на рабочей станции конечного пользователя.



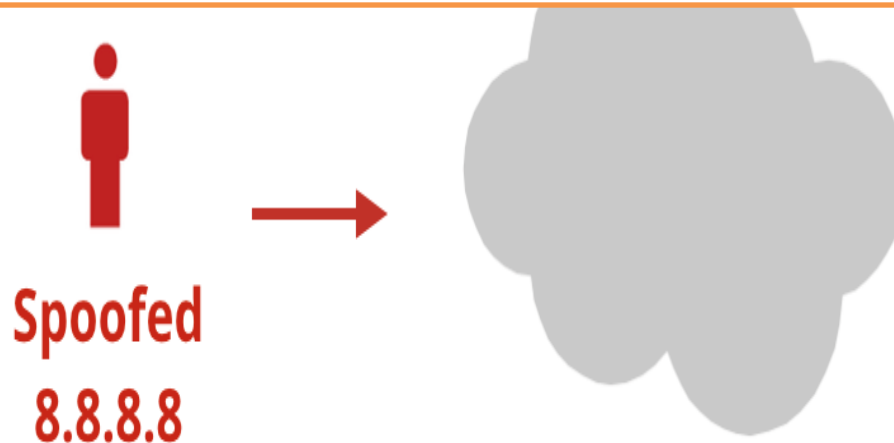
- **Сетевая разведка**

Сетевой разведкой называется сбор информации о сети с помощью общедоступных данных и приложений.



IP-спуфинг

IP-спуфинг происходит, когда злоумышленник, находящийся внутри корпорации или вне ее выдает себя за санкционированного пользователя.



Man-in-the-Middle

Для атаки типа Man-in-the-Middle злоумышленнику нужен доступ к пакетам, передаваемым по сети. Такой доступ ко всем пакетам, передаваемым от провайдера в любую другую сеть, может, к примеру, получить сотрудник этого провайдера.



- **Инъекция**

SQL-инъекция. SQL-инъекция – это атака, в ходе которой изменяются параметры SQL-запросов к базе данных.

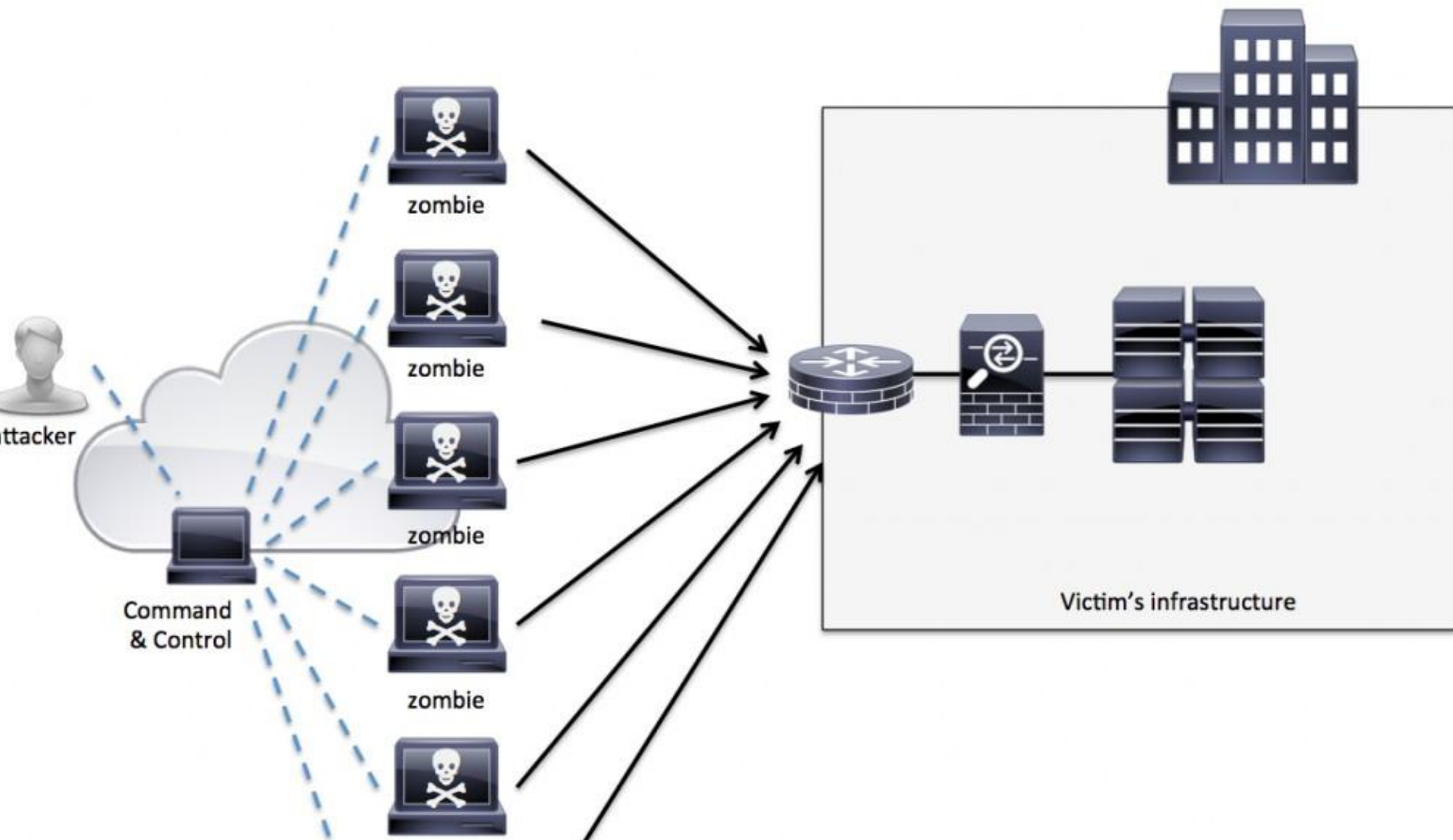


SQL Injection



Социальная инженерия

Социальная инженерия – метод получения необходимого доступа к информации, основанный на особенностях психологии людей.



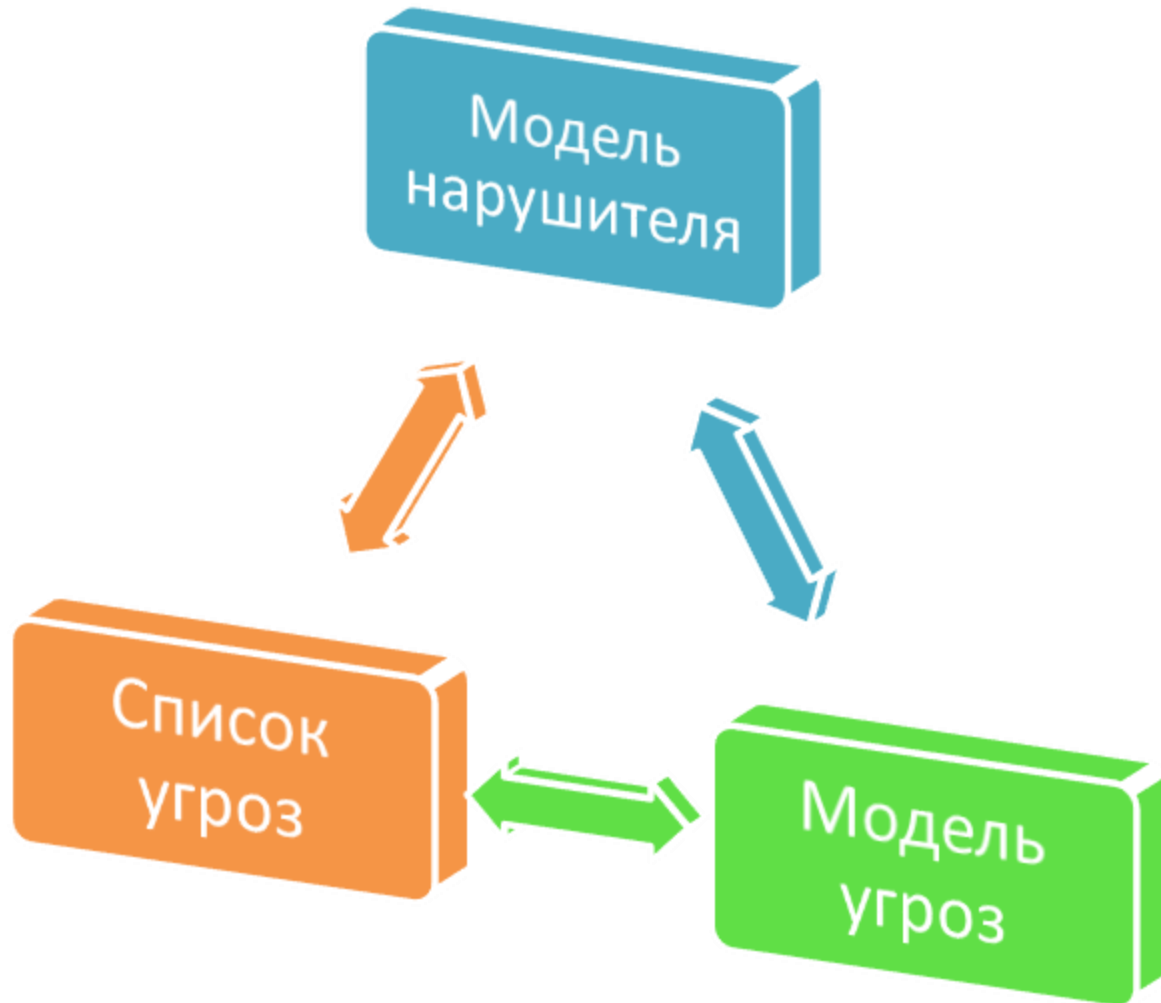
Отказ в обслуживании

Атаки DoS отличаются от атак других типов. Они не нацелены на получение доступа к вашей сети или на получение из этой сети какой-либо информации.

Модель угроз

МОДЕЛИРОВАНИЕ ОКРУЖЕНИЯ

Модели ИБ



Модель угроз

Систематизированный перечень угроз безопасности при обработке информации в информационных системах. Эти угрозы обусловлены преднамеренными или непреднамеренными действиями физических лиц, действиями зарубежных спецслужб или организаций (в том числе террористических), а также криминальных группировок, создающих условия для нарушения безопасности, которое ведет к ущербу жизненно важных интересов личности, общества и государства.

(ФСТЭК России)

Зачем нужно моделирование угроз

- Систематическая идентификация потенциальных опасностей.
- Систематическая идентификация возможных видов отказов.
- Количественные оценки или ранжирование рисков.
- Выявление факторов, обуславливающих риск, и слабых звеньев в системе.
- Более глубокое понимание устройства и функционирования системы.

РАСЧЕТ СТЕПЕНИ ОПАСНОСТИ

$$K(O) = (K_D * K_{\Phi} * K_K) / 125$$

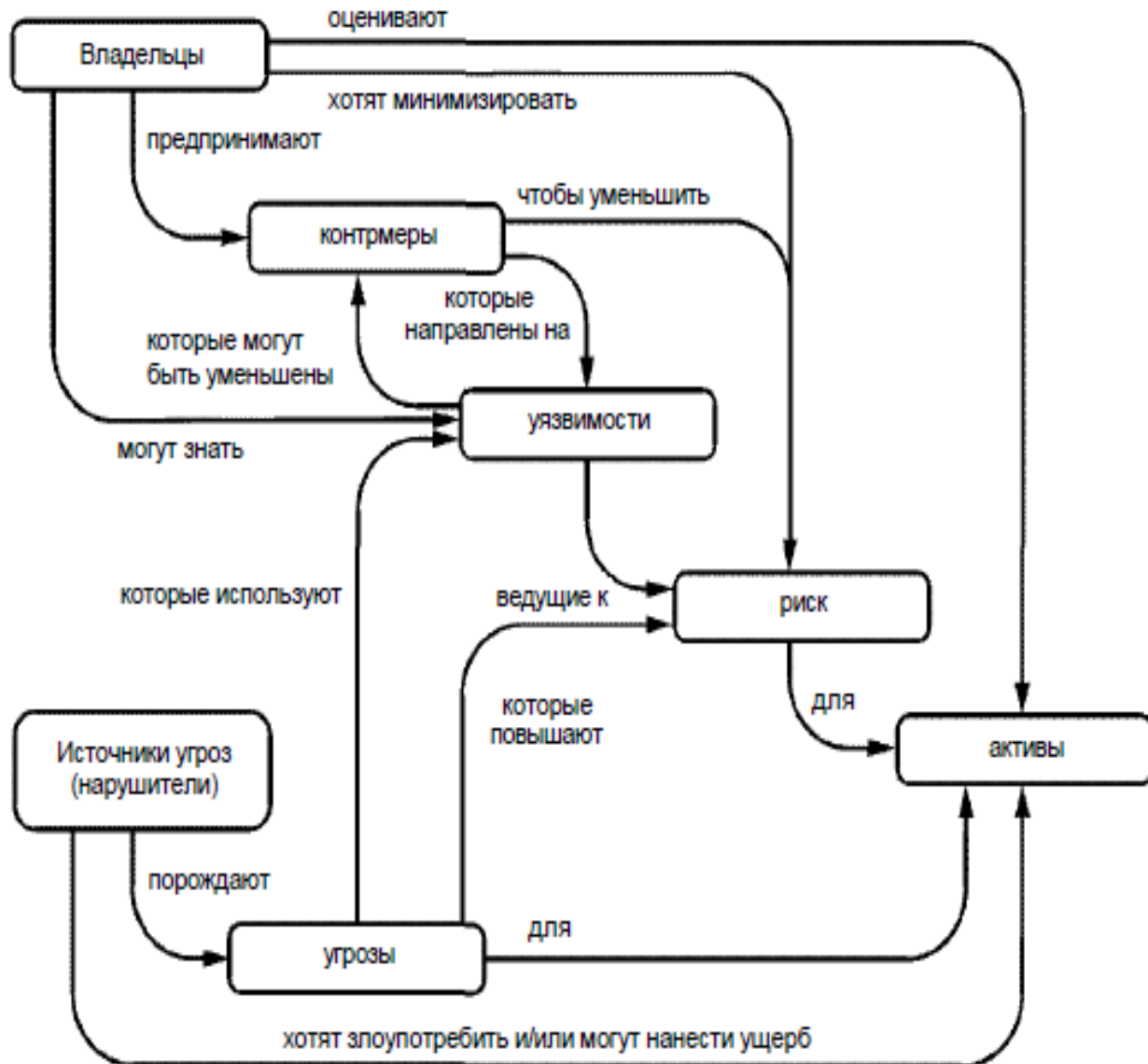
Зачем нужно моделирование угроз

- Сопоставление риска исследуемой системы с рисками альтернативных систем или технологий.
- Идентификация и сопоставление рисков и неопределенностей.
- Возможность выбора мер и приемов по обеспечению снижения риска.
- Основная задача моделирования окружения – обоснование решений, касающихся рисков.

Вопросы для модели

- Какие угрозы могут быть реализованы?
- Как могут быть реализованы эти угрозы?
- С какой вероятностью могут быть реализованы эти угрозы?
- Каков потенциальный ущерб от этих угроз?
- Каким образом могут быть реализованы эти угрозы?
- Почему эти угрозы могут быть реализованы?
- На что могут быть направлены эти угрозы?
- Как можно отразить эти угрозы?

Как все устроено



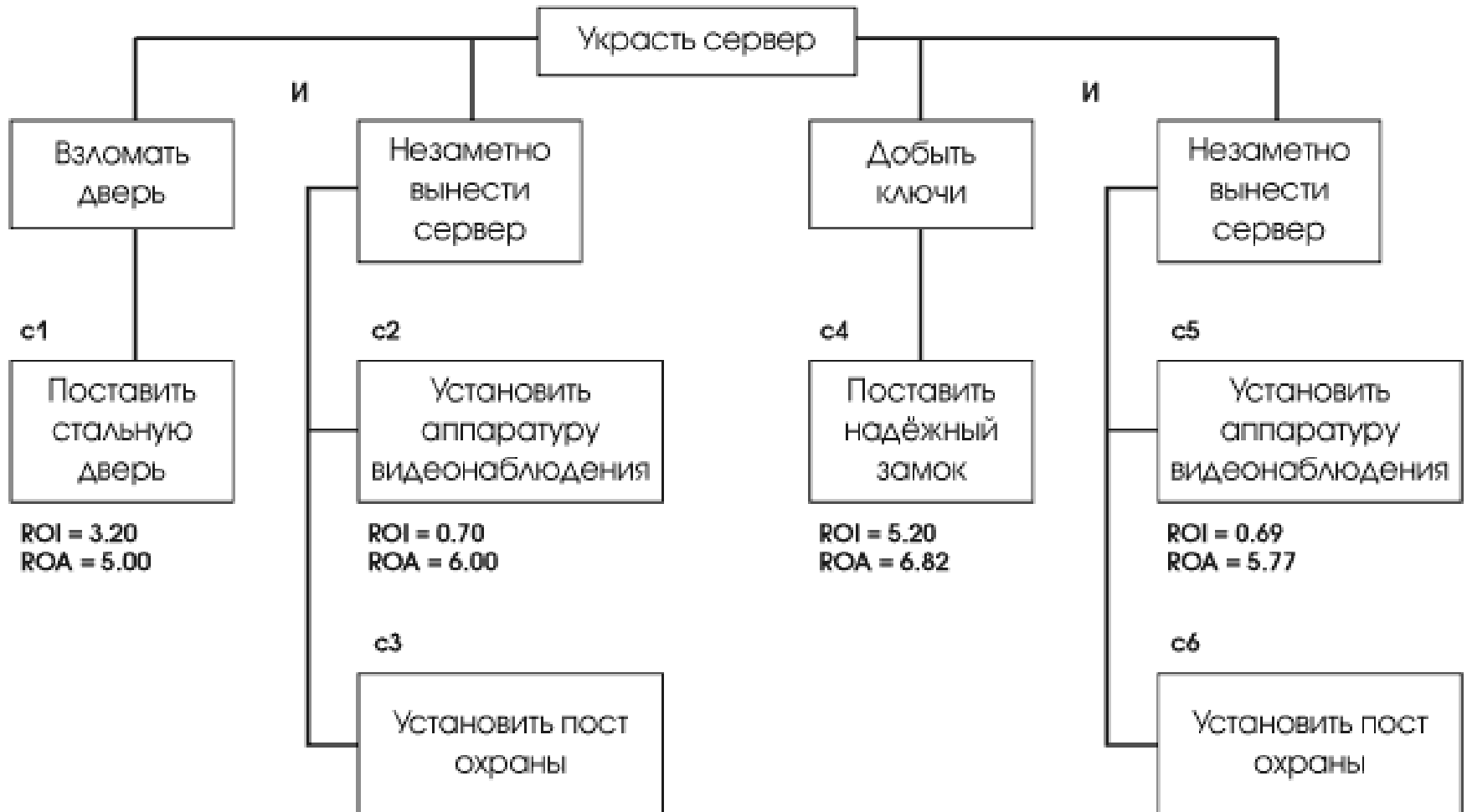
Способы моделирования угроз

- Простой перечень и описание.
- Деревья угроз.

Дерево угроз

- Показывает условия реализации угроз.
- Комбинированный эффект и взаимосвязь уязвимостей.
- Деревьев может быть много, в зависимости от числа угроз общего уровня:
 - Блокирование работы сервиса.
 - Кража информации на р.с. пользователей.
 - Несанкционированное изменение данных в БД.
 - ...
- Даёт оценку вероятности реализации угроз.

Дерево угроз



Модель нарушителя.

МОДЕЛИРОВАНИЕ ОКРУЖЕНИЯ

Модель нарушителя.

Модель нарушителя определяет:

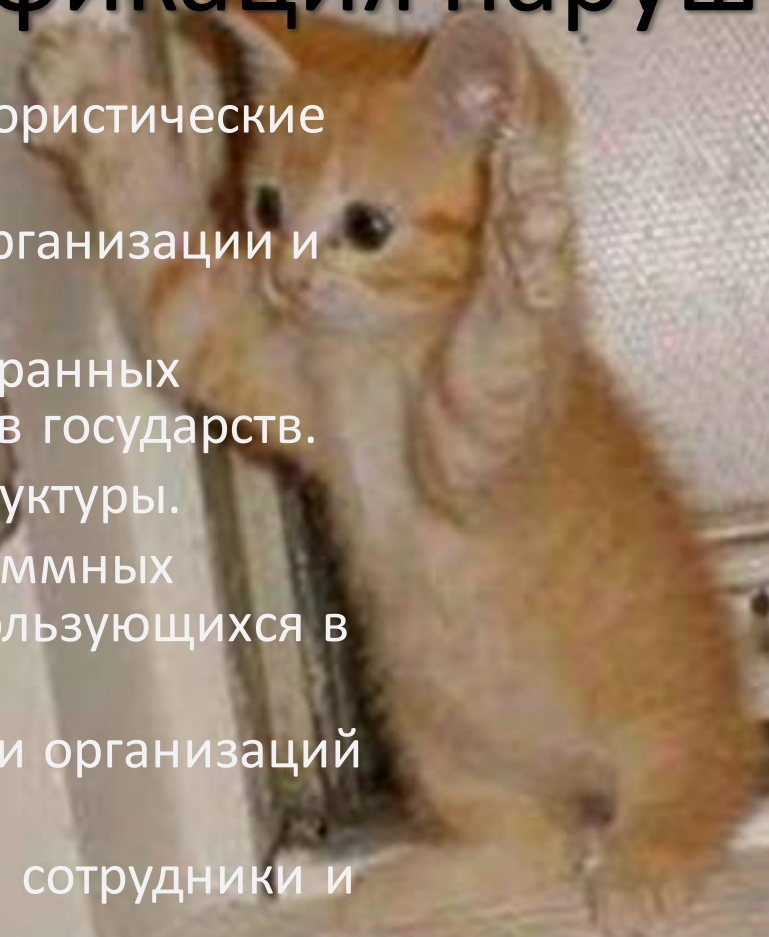
- категории (типы) нарушителей, которые могут воздействовать на объект;
- цели, которые могут преследовать нарушители каждой категории и их описание;
- типовые сценарии возможных действий нарушителей, описывающие последовательность (алгоритм) действий групп и отдельных нарушителей, способы их действий на каждом этапе.

Пример простой модели нарушителя ИБ

| Наименование | Тип нарушителя | Описание возможностей |
|--|----------------|--|
| Основной/вспомогательный персонал | Внутренний | Обладают хорошими знаниями в области эксплуатации ПО и технических средств, знакомы со спецификой |
| Представители служб безопасности, технический персонал | Внутренний | Хорошо знакомы со структурой, основными функциями и принципами работы программно-аппаратных средств ЗИ |
| Лица, распространяющие вирусы/вредоносные программы, другие лица, осуществляющие НСД | Внешний | Обладают достаточными знаниями в области осуществления НСД к ресурсам ИС |
| Представители менеджмента организации | Внутренний | Являются наиболее актуальными источниками угроз на уровне бизнес-процессов |
| Поставщики различных услуг, персонал надзорных организаций и аварийных служб | Внешний | Возможные реализуемые угрозы: уничтожение, блокирование, искажение информации. Действия совершаются по незнанию, невнимательности или халатности, но без злого умысла. |
| Недобросовестные партнеры, хакеры | Внешний | Способны умышленно дезорганизовать работу, вывести системы из строя, разгласить и исказить конф. информации за счет НСД к информации и утечки по ТКУИ |
| Клиенты | Внешний | Могут нанести ущерб намеренно или по незнанию |

Классификация нарушителей

- Террористы и террористические организации.
- Конкурирующие организации и структуры.
- Спецслужбы иностранных государств и блоков государств.
- Криминальные структуры.
- Взломщики программных продуктов ИТ, использующихся в системах связи.
- Бывшие сотрудники организаций связи.
- Недобросовестные сотрудники и партнеры.
- Пользователи услугами связи и др.



Классификация нарушителей. Основные типы.

- Разработчик.
- Обслуживающий персонал (системный администратор, сотрудники обеспечения ИБ).
- Пользователи.
- Сторонние лица.

Мотивы нарушителей

- Месть.
- Достижение денежной выгоды.
- Хулиганство и любопытство.
- Профессиональное самоутверждение.