Риски кибербезопасности и их учет в процессах проектирования зданий

Владимир Голованов
АО «ИнфоТеКС»

Понятия «кибербезопасность» и «защита информации»

«Кибербезопасность» - сейчас везде, но это часть общей задачи

✓**Кибербезопасность (безопасность киберпространства):** сохранение конфиденциальности, целостности и доступности информации **в киберпространстве**.

Примечание: Кроме того, могут быть востребованы и другие свойства безопасности, такие как аутентичность, подотчетность, неотказуемость и *надежность*.
[**ISO/IEC 27032 Руководство по кибербезопасности**]

«Защита информации» и обеспечение «Безопасности информации»

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 50922— 2006

Защита информации

ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Издание официальное

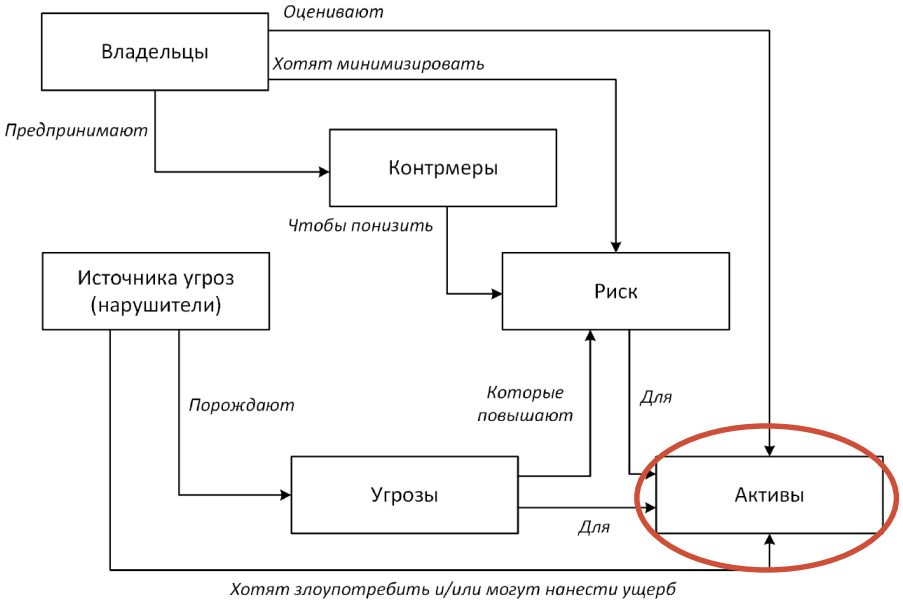
✓**Защита информации:** Деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.
[ГОСТ Р 50922-2006, п. 2.1.1]

✓**Защита информации от преднамеренного воздействия:** Защита информации, направленная на предотвращение преднамеренного воздействия, в том числе электромагнитного и (или) воздействия другой физической природы, осуществляемого в террористических или криминальных целях
[ГОСТ Р 50922-2006, п. 2.3.7]

✓**Безопасность информации:** Состояние защищенности информации [данных], при котором обеспечиваются ее [их] конфиденциальность, доступность и целостность.
[ГОСТ Р 50922-2006, п. 2.4.6]

Понятия «активы», «риски», «требования»

Концепции безопасности и отношения. Угрозы, уязвимости, риски

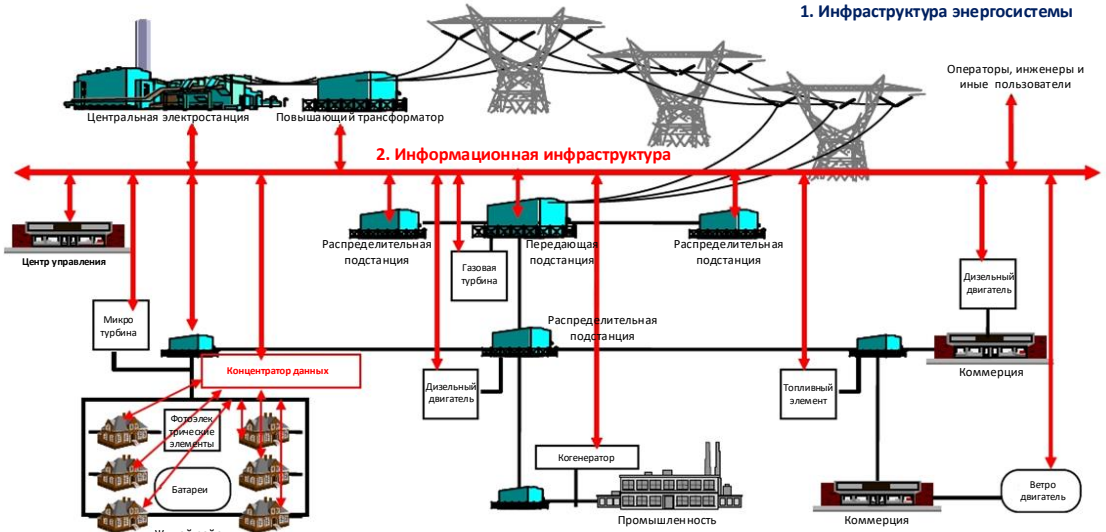


«…*угрозы создают риски для активов*, зависящие от вероятности реализации угрозы и размера ущерба активам при реализации рассматриваемой угрозы. Для того *чтобы уменьшить риски для активов, применяются средства защиты информации*……
Эти средства безопасности могут включать ИТ-средства безопасности,
а также меры не связанные с ИТ-средствами безопасности. Более широкое рассмотрение …… представлено в ИСО/МЭК 27001 и ИСО/МЭК 27002…»

ГОСТ Р ИСО/МЭК 15408-1-202x **Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель**

«Активы», «Информационная инфраструктура», «Информация»

- **Активы (asset):** Все, что имеет ценность для организации [ГОСТ Р ИСО/МЭК 13335-1-2006, п. 2.2]
- **Информационная инфраструктура:** Совокупность объектов информатизации, обеспечивающая доступ потребителей к информационным ресурсам [ГОСТ Р 53114-2008, п. 3.1.4]
- **Информация:** сведения (сообщения, данные) независимо от формы их представления [149-ФЗ «Об И, ИТ и ЗИ»]



IEC 62351 «Power systems management and associated information exchange - Data and communications security - Part 10: Security architecture guidelines»

infotecs

Делаем правильно!

«Информация» как объект и цель защиты

- **Общедоступная информация** - общеизвестные сведения, доступ к которым не ограничен.
- **Информация ограниченного доступа** - информация, доступ к которой ограничен в соответствии с федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

На основе **Статьи 5.** «Информация как объект правовых отношений» ФЗ от 27 июля 2006 г. № **149-ФЗ** «Об информации, информационных технологиях и о защите информации»

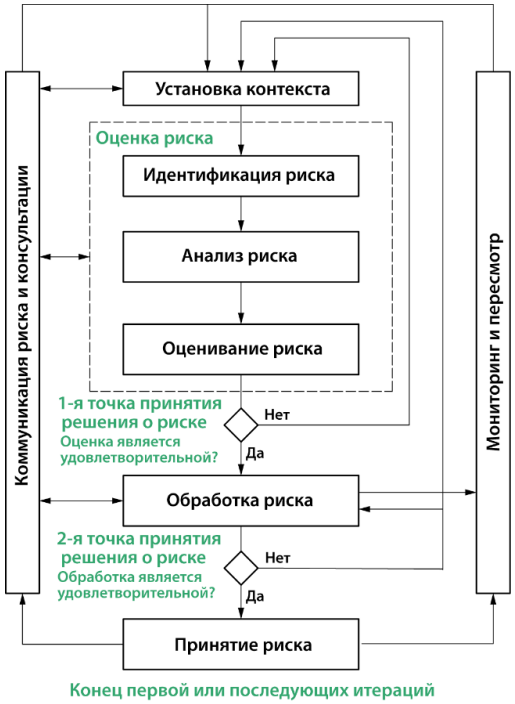
Категории информации ограниченного доступа

- **Государственная тайна**: защищаемые государством сведения, распространение которых может нанести ущерб безопасности Российской Федерации
- **Режим секретности** - совокупность требований, правил, организационных, технических и иных мер, направленных на защиту сведений, составляющих государственную тайну
  [Закон РФ от 21 июля 1993 г. N 5485-I «О государственной тайне»].
- **Перечень сведений, относящихся к конфиденциальной информации**
  Примеры: Коммерческая тайна, ПДн, банковская тайна, медицинская тайна и т.п. – несколько десятков видов ИОД
  [Указ Президента РФ от 6 марта 1997 г. N 188 «Об утверждении перечня сведений конфиденциального характера»]
- **Информация ограниченного доступа**: Информация, не содержащая сведений составляющих государственную тайну, но подлежащая защите в соответствии с законодательством РФ

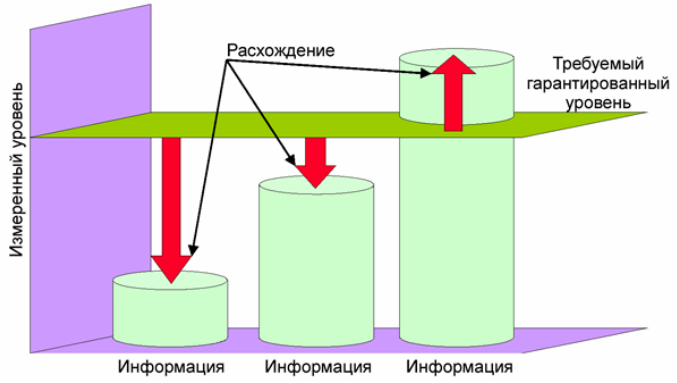
Чем мы обязаны руководствоваться?

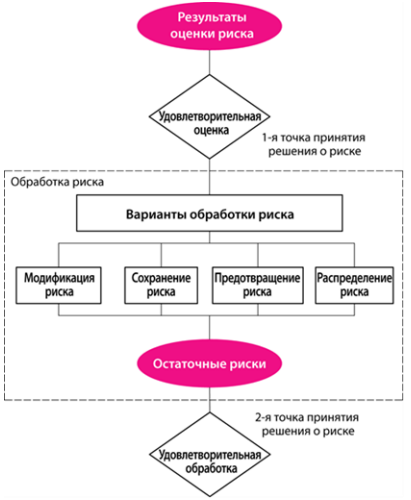
- Если присутствует «государственная тайна» - должны неукоснительно следовать **требованиям Государства.**
- Если присутствует ИОД, подлежащая защите в соответствии с законодательством РФ – должны исполняться требования Регуляторов (ФСБ России, ФСТЭК, Роскомнадзор и др.), а ***в дополнение к ним и с учетом специфики деятельности*** – возможны оценки в рамках риск-менеджмента ИБ.

Аналитическая модель управления рисками ИБ (ИСО/МЭК)



Идентификация, анализ, оценивание/ сопоставление с пороговыми значениями, обработка риска ИБ





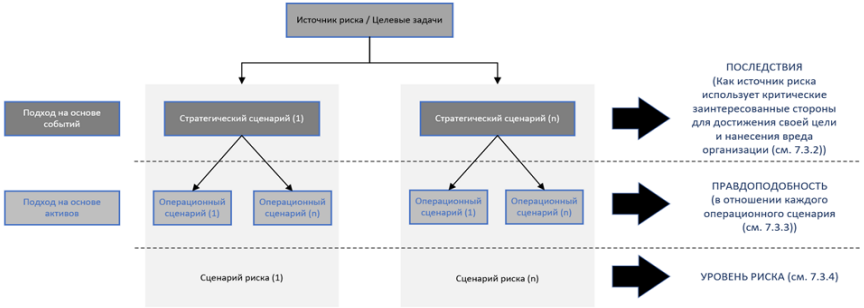
ISO/IEC 27005 Information technology – Security techniques – Information security risk management

Аналитическая модель управления рисками ИБ (ИСО/МЭК). Примеры 27005

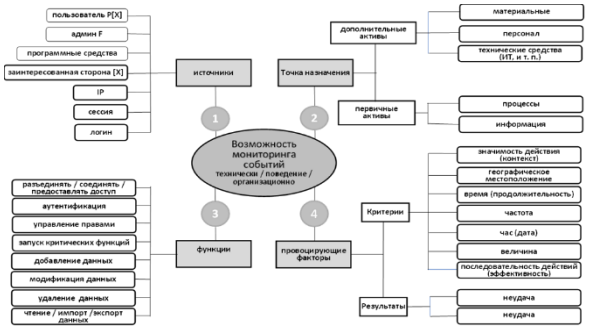
Событийный подход

Пример графика зависимости активов

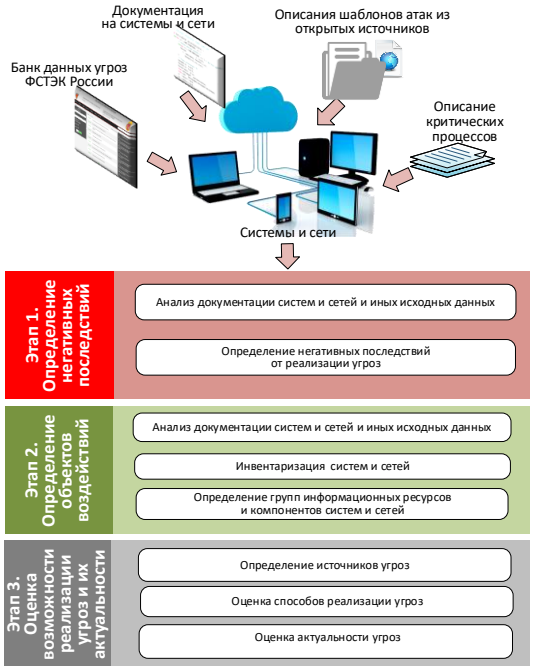
Оценка риска на основе сценариев риска



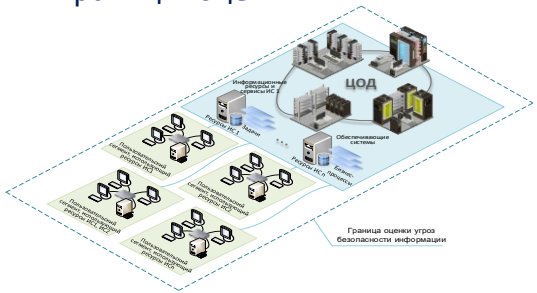
Пример применения модели SFDT («source-function-destination-trigger»)



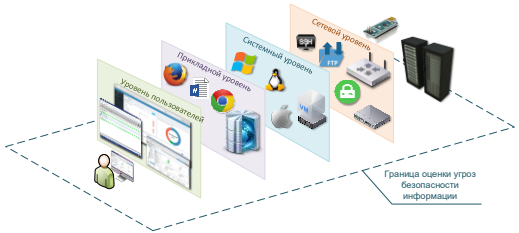
Рекомендации по моделированию угроз (≡ анализ и оценка рисков)



Границы оценки



Уровни ИТ архитектуры



Граница моделирования угроз безопасности информации: совокупность информационных ресурсов и компонентов систем и сетей, в пределах которой обеспечивается защита информации в соответствии с едиными правилами и процедурами, а также контроль за реализованными мерами защиты информации [МД. «Методика моделирования угроз безопасности информации» (проект)]

Что в части требований к зданиям и помещениям? Пример

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 27002— 2021

Информационные технологии

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Свод норм и правил применения мер обеспечения информационной безопасности

(ISO/IEC 27002:2013, IDT)

Издание официальное

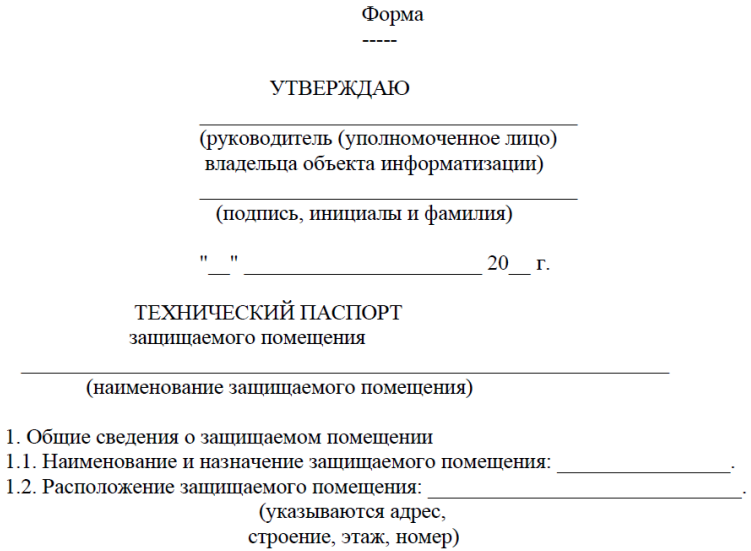
Пример требований (публичные)

ГОСТ Р ИСО/МЭК 27002-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности»

Раздел 11 «**Физическая безопасность и защита от воздействия окружающей среды**», что рассматривается:

- ✓ физический периметр безопасности;
- ✓ меры и средства контроля и управления физическим доступом;
- ✓ политика «чистого стола» и «чистого экрана»
- ✓ безопасность зданий, помещений и оборудования;
- ✓ защита от внешних угроз и угроз со стороны окружающей среды (техногенные, природные и т.п.);
- ✓ работа в зонах безопасности;
- ✓ зоны погрузки и разгрузки;
- ✓ размещение и защита оборудования и т.п.

Российская практика в соответствии с установленными требованиями



Форма

УТВЕРЖДАЮ

_____
(руководитель (уполномоченное лицо)
владельца объекта информатизации)

_____
(подпись, инициалы и фамилия)

"__" _____ 20__ г.

ТЕХНИЧЕСКИЙ ПАСПОРТ
защищаемого помещения

_____
(наименование защищаемого помещения)

1. Общие сведения о защищаемом помещении
1.1. Наименование и назначение защищаемого помещения: _____.
1.2. Расположение защищаемого помещения: _____.
(указываются адрес,
строение, этаж, номер)

- **Защищаемые помещения (ЗП):** помещения (служебные кабинеты, актовые, конференц-залы и т.д.), специально предназначенные для проведения конфиденциальных мероприятий (совещаний, обсуждений, конференций, переговоров и т.п.).
- **Контролируемая зона:** пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.
- **Защищаемый объект информатизации:** объект информатизации, предназначенный для обработки защищаемой информации с требуемым уровнем ее защищенности.

Каналы утечки «информации». Куда могут «убежать секреты»

- ✓ Установка систем ограничения и контроля доступа на объектах размещения и в выделенных помещениях;
- ✓ Экранирование техники и соединительных линий средств;
- ✓ Заземление техники и экранов соединительных линий приборов;
- ✓ Звукоизоляция выделенных помещений;
- ✓ Встраивание в средства связи, обладающие «микрофонным» эффектом и имеющие выход за пределы контролируемой зоны, специальных фильтров;
- ✓ Ввод автономных и стабилизированных источников, а также устройств гарантированного питания в цепи электроснабжения техники;
- ✓ Монтаж в цепях электропитания техники, а также в электросетях выделенных помещений помехоподавляющих фильтров…….
- ✓ и т.п.

Краткое резюме

- **Категория защищаемой информации** – главный критерий применимости того или иного подхода к оценке рисков.
- При обработке на объекте сведений, **составляющих государственную тайну**, при проектировании и в процессе строительства зданий и сооружений привлекаем экспертную организацию!!!!
- При обработке на объекте **сведений конфиденциального характера** запрашиваем Заказчика строительства сведения по планам размещения и необходимости учета помещений в соответствии с установленными требованиями по защите информации ограниченного доступа.
- *Потом риск-менеджмент ИБ!*

Спасибо за внимание!

Vladimir.Golovanov@infotecs.ru

Подписывайтесь на наши соцсети

vk.com/infotecs_news

t.me/infotecs_news

rutube.ru/channel/24686363