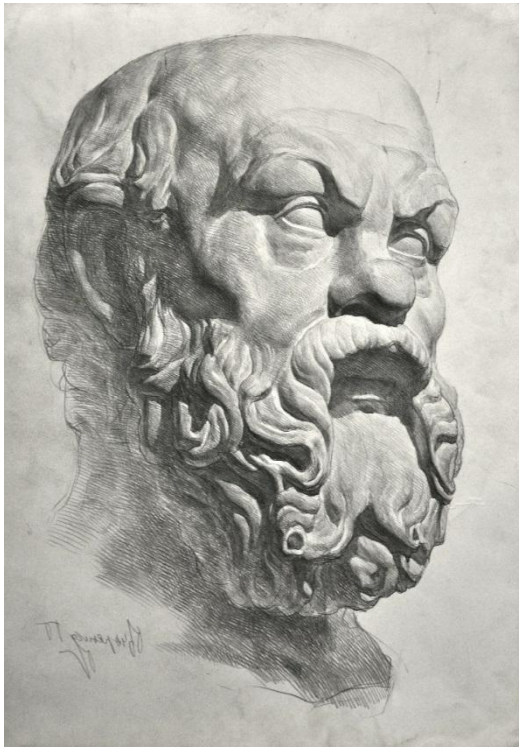


Сократ, мудрец

Инженерно-техническая безопасность

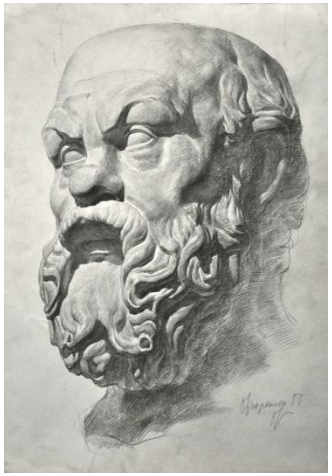
Комплексное противодействие атакам на информационные и материальные ресурсы бизнеса

Тема №13

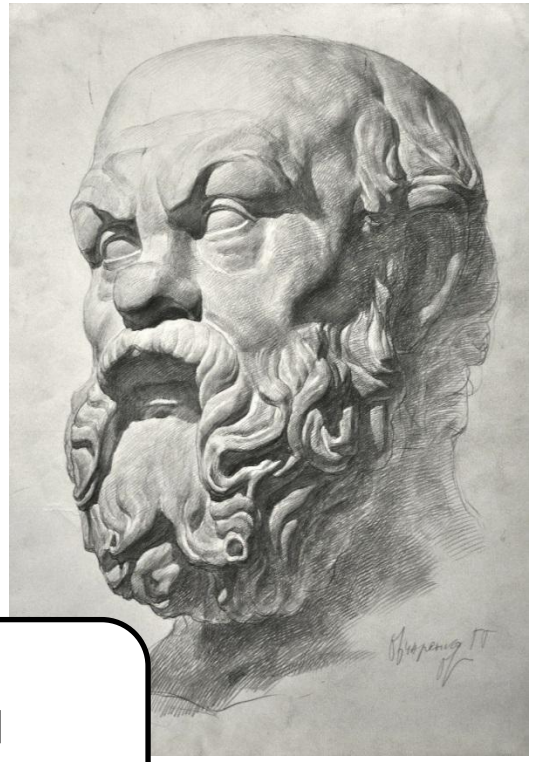
Организация системы инженерно-технической безопасности

Лекция , 2 часа

Оглавление



Функция инженерно-технической безопасности



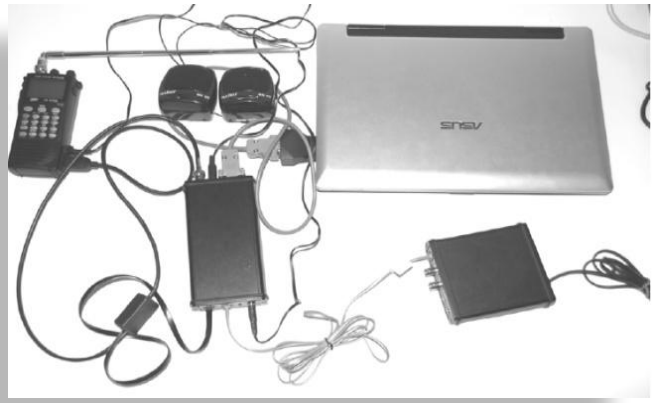
Сократ, мудрец

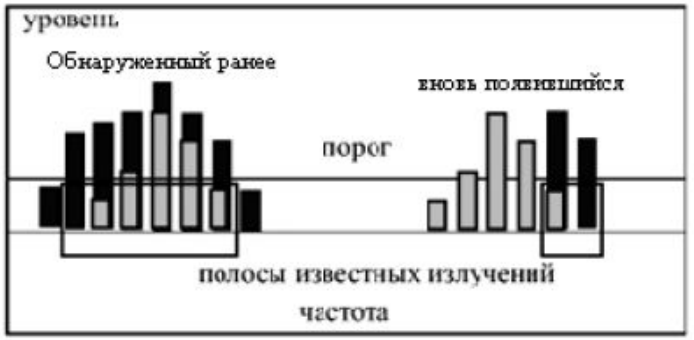
ФУНКЦИЯ ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ БЕЗОПАСНОСТИ

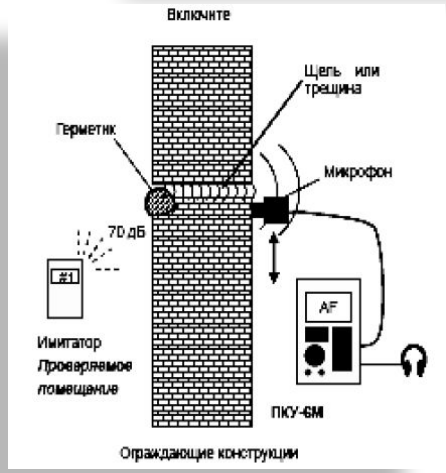
Кейс

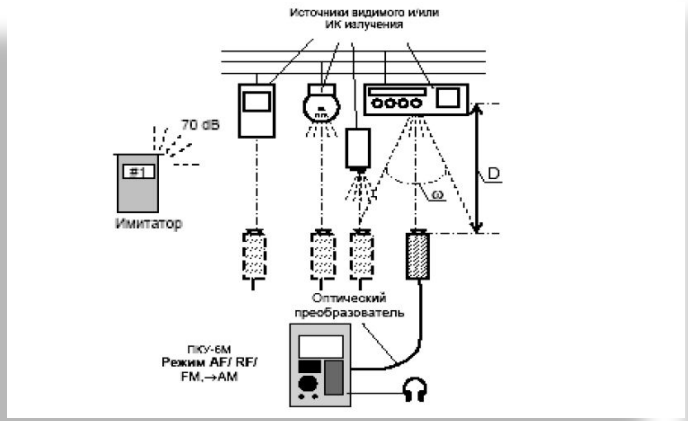
МЕТОДЫ ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

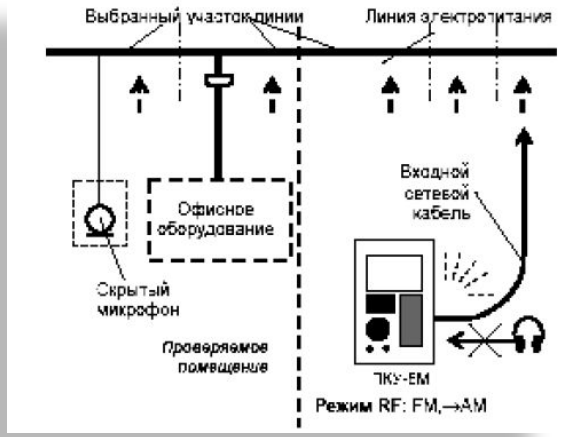
Комплекс RS turbo



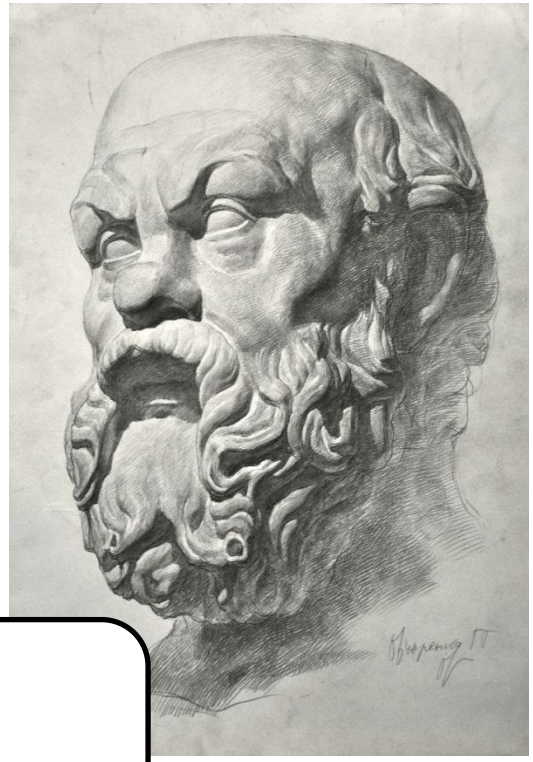








Концепция безопасности



Сократ, мудрец

КОНЦЕПЦИЯ БЕЗОПАСНОСТИ И ЕЕ ЗАДАЧИ

Концепция безопасности – основополагающий элемент концепции управления объектом, в задачи которой входит:

- **доскональное изучение объекта**
- **выявление потенциальных угроз**
- **постановка целей и задач разработчикам**
- **расстановка приоритетов**
- **экономия времени и бюджета**

СТРУКТУРА КОНЦЕПЦИИ БЕЗОПАСНОСТИ

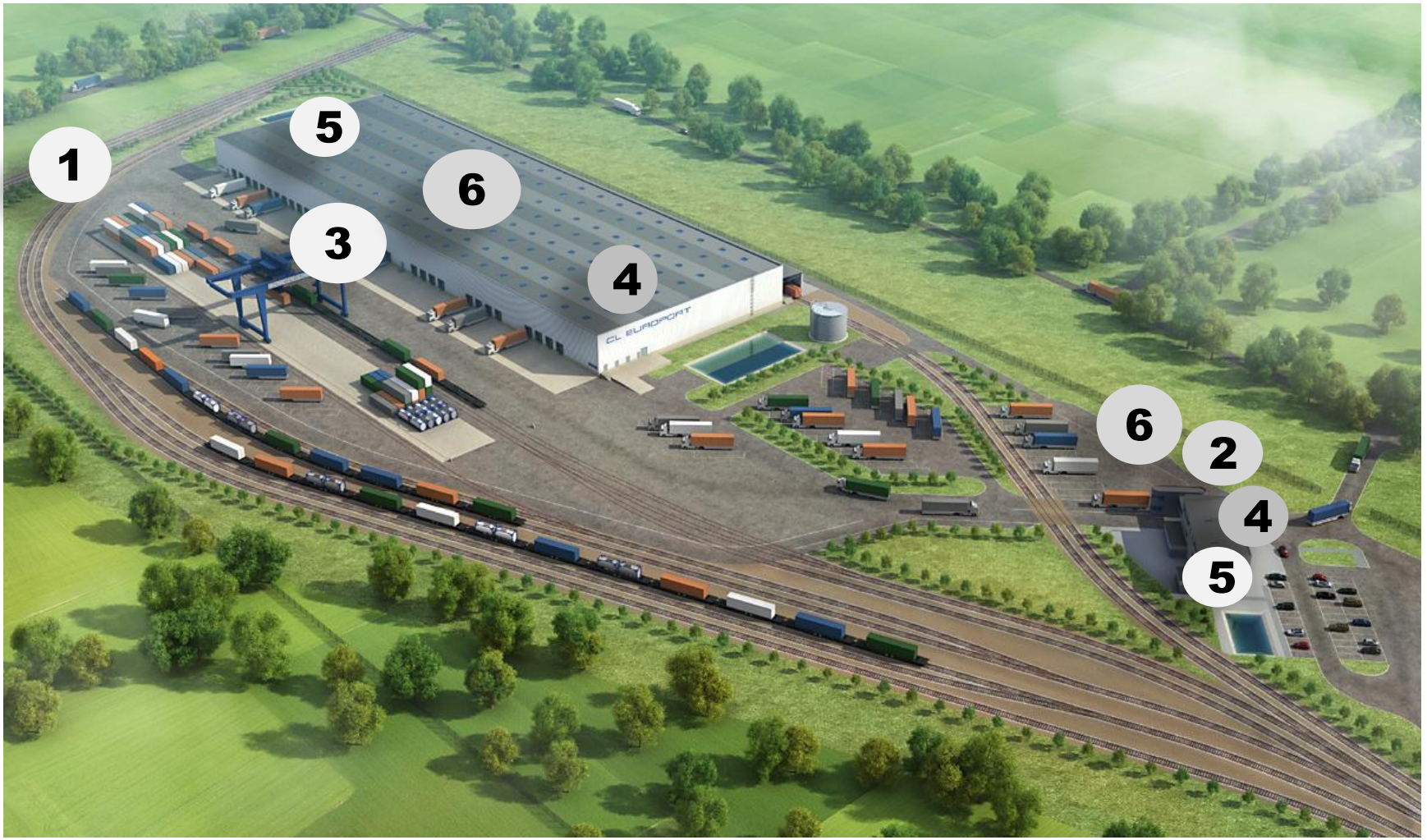
1. Классификация объекта по категориям: от незначительного до критического
2. Классификация зон охраны (с учетом специфики объекта)
3. Определение рисков и угроз, разграничение их по типам: криминальные, техногенные, природные, террористические и др.
4. Разработка модели нарушителя, а также сценариев нарушений по категориям нарушителей
5. Разработка сценариев проникновения на объект
6. Разработка модели обеспечения безопасности
7. Разработка и проработка контрольных сценариев (описывается последовательность действий и затраты времени для пресечения действий

КЛАССИФИКАЦИЯ ОБЪЕКТОВ ПО КАТЕГОРИЯМ

Категория	Объект защиты	Характеристика объекта	Возможный ущерб
1	Жизнь и здоровье собственников и ТОП-менеджмента		Уровень ущерба от значительного до критического
2 3	Жизнь и здоровье сотрудников компании и посетителей		Уровень ущерба от значительного до критического
4	Недвижимое имущество компании	Здания, хозяйственные постройки, хранилища и другие капитальные сооружения, находящиеся в собственности, или в долевой собственности. **Не может быть перемещено, может быть только разрушено полностью или частично**	Уровень ущерба от значительного до критического
5	Имущество и ТМЦ, принадлежащее компании.	Транспортные средства, материальные ценности, наличные деньги, ценные бумаги, электроника, персональные компьютеры, объекты хранения на складах. **Может быть повреждено, украдено, разрушено**	Уровень ущерба от незначительного до очень значительного
6	Конфиденциальная информация	Информация, потеря, разглашение которой может привести к возникновению угроз жизни и здоровья собственников и сотрудников компании, материальным потерям, порче деловой репутации компании	Уровень ущерба от незначительного до очень значительного

КЛАССИФИКАЦИЯ ЗОН ОХРАНЫ

КЛАССИФИКАЦИЯ ЗОН ОХРАНЫ



ЗАДАЧИ ЗОН БЕЗОПАСНОСТИ (пример)

- **ЗОНА БЕЗОПАСНОСТИ – 1 - не допустить проникновения посторонних лиц на территорию объекта через периметральные заграждения, технологические проходы и проезды, и КПП;**

- **ЗОНА БЕЗОПАСНОСТИ – 2 - в случае проникновения нарушителя – принять меры к его локализации и задержанию (нейтрализации); противодействие целому ряду техногенных и криминальных угроз**

РИСКИ И УГРОЗЫ

К этим группам отнесены:

1. **Природные риски и угрозы** – являющиеся следствием природных явлений

2. **Техногенные риски и угрозы** – связанные с авариями, выходом из строя обеспечивающих инженерных систем, электрического оборудования и т.п.

3. **Криминальные угрозы** – связанные с незаконными действиями отдельных лиц или групп людей

4. **Террористические угрозы** – маловероятная, но учитываемая в концепции группа угроз имеющая «пересечения» с криминальными угрозами в некоторых сценариях реализации угроз

ТЕХНОГЕННЫЕ РИСКИ И УГРОЗЫ

Наименование рисков и угроз	Факторы риска
1. **Пожары** **Основные объекты риска:** • Кабинеты руководителей и сотрудников комплекса; • Складские помещения, хранилища • Административные и технологические помещения (котельная, погрузочные терминалы • Гаражи, парковочные комплексы • Железнодорожные подъезды	• отсутствие контроля состояния систем электроснабжения; • отсутствие наличия систем ПС на объектах; • отсутствие наличия первичных средств пожаротушения и навыков обращения с ними; • отсутствие своевременного информирования экстренных служб

КРИМИНАЛЬНЫЕ РИСКИ И УГРОЗЫ

Наименование рисков и угроз	Факторы риска
1. **Покушение на жизнь и здоровье собственников и сотрудников комплекса** **Факторы, снижающие риск:** • минимизация времени проезда КПП; • информирование охраны о движении/прибытии машины; • видеонаблюдение вдоль периметрального заграждения с возможностью контроля наружной прилегающей территории	• одно направление подъезда, • узкая дорога – отсутствие возможности маневра, • «лежачий полицейский» - снижение скорости, • площадка перед КПП – возможность нахождения посторонних людей.

КРИМИНАЛЬНЫЕ РИСКИ И УГРОЗЫ

Наименование рисков и угроз	Факторы риска
1. **Покушение на жизнь и здоровье собственников и сотрудников комплекса** **Факторы, снижающие риск:** • минимизация времени проезда КПП; • информирование охраны о движении/прибытии машины; • видеонаблюдение вдоль периметрального заграждения с возможностью контроля наружной прилегающей территории	• одно направление подъезда, • узкая дорога – отсутствие возможности маневра, • «лежачий полицейский» - снижение скорости, • площадка перед КПП – возможность нахождения посторонних людей.

МОДЕЛЬ НАРУШИТЕЛЯ

Структура раздела :

1. **Общая классификация**
2. **Деление нарушителей на группы**
3. **Описание каждого вида нарушителей**
4. **Характеристика нарушителей (по типу осведомленности, тактики проникновения на объект, мотивам и пр.)**
5. **Потенциальные типы нарушителей, способные реализовать угрозы.**

Группа	Характеристика
Внешние нарушители	Лица, не являющиеся сотрудниками логистического комплекса или охраны и не относящиеся к персоналу, доставляющему грузы, а также к посетителям
Внутренние (потенциальные) нарушители	Лица, входящие в состав персонала логистического комплекса и его охраны;
Временные, внутренние (потенциальные нарушители)	Лица, временно находящиеся на территории комплекса, как экспедиторы или водители, а также гости (посетители).

ПРИМЕР СЦЕНАРИЯ ПРОНИКНОВЕНИЯ

Описание ситуации

Подготовленный нарушитель, знающий топографию объекта перелезает через ограждение в углу логистического комплекса (вблизи ж/д переезда) и движется к разгрузочному терминалу расположенному в дальнем углу комплекса с целью совершить кражу. Нарушитель намеревается покинуть объект тем же путем.

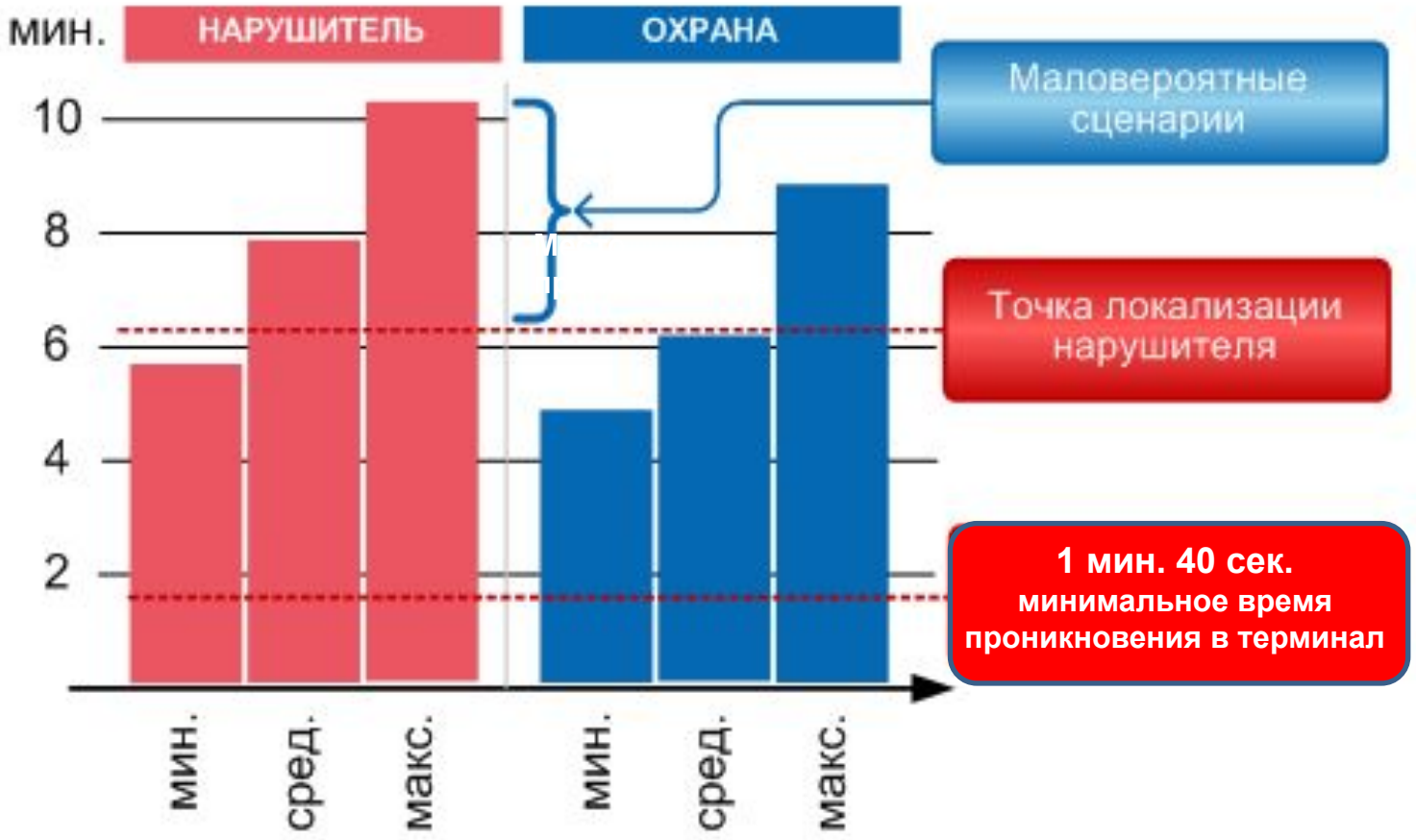
ПОСЛЕДОВАТЕЛЬНОСТЬ ДЕЙСТВИЙ И ЗАТРАТЫ ВРЕМЕНИ ПОТЕНЦИАЛЬНОГО НАРУШИТЕЛЯ

НАРУШИТЕЛЬ		ТСО	СОТРУДНИКИ ОХРАНЫ	
Действия	**Затраты времени**	**Функции**	**Действия**	**Затраты времени**
Преодоление ограждения без специальных приспособлений	20-40 сек.	Срабатывание периметральной сигнализации	Реагирование охранника на звуковой сигнал тревоги.	10 -15 сек.
Перемещение по территории в направление терминала.	20-30 сек.	Автоматический вывод на экран изображения из зоны вторжения	Сотрудник 1. Определение зоны проникновения, визуальное изучение обстановки Сотрудник 2 и 3: экипировка	30-60 сек.

ПОСЛЕДОВАТЕЛЬНОСТЬ ДЕЙСТВИЙ И ЗАТРАТЫ ВРЕМЕНИ ПОТЕНЦИАЛЬНОГО НАРУШИТЕЛЯ (ПРОДОЛЖЕНИЕ)

НАРУШИТЕЛЬ		ТСО	СОТРУДНИКИ ОХРАНЫ	
Действия	**Затраты времени**	**Функции**	**Действия**	**Затраты времени**
Минимальное время проникновения нарушителя в погрузочный терминал	**1 мин. 40 секунд.**		**Минимальное время локализации (нахождения) нарушителя:**	**4 мин. 40 сек.**
Максимальное:	**5 мин. 40 сек.**		**Максимальное:**	**8 мин. 45 сек.**
Среднее:	**3 мин. 40 сек.**		**Среднее:**	**6 мин. 45 сек.**
Нахождение на объекте (минимальное)	180 сек.			
Отход к автомобилю (суммарно)	60-90 сек.			
Итого (среднее):	**8 минут.**			

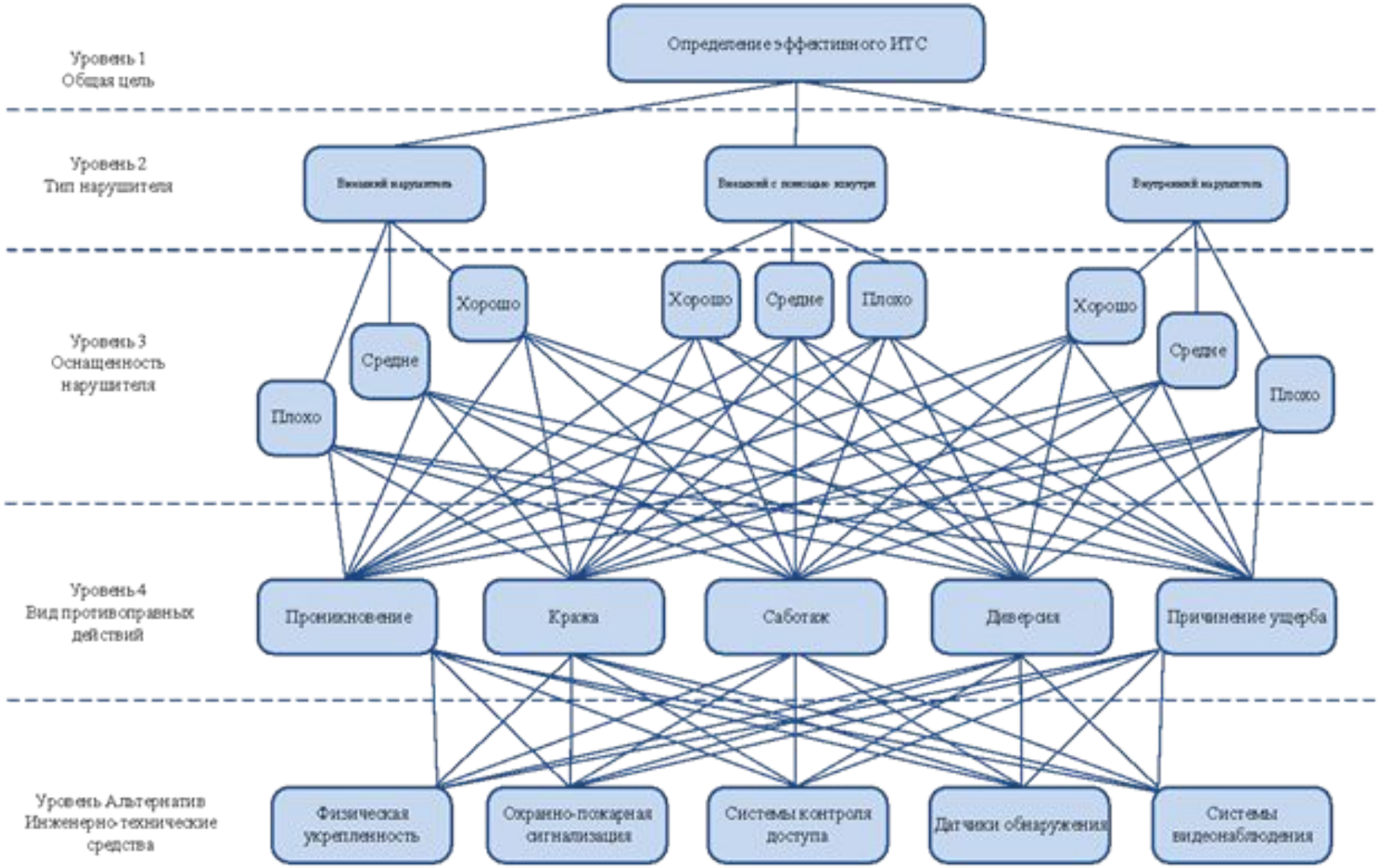
АНАЛИЗ КОНТРОЛЬНОГО СЦЕНАРИЯ



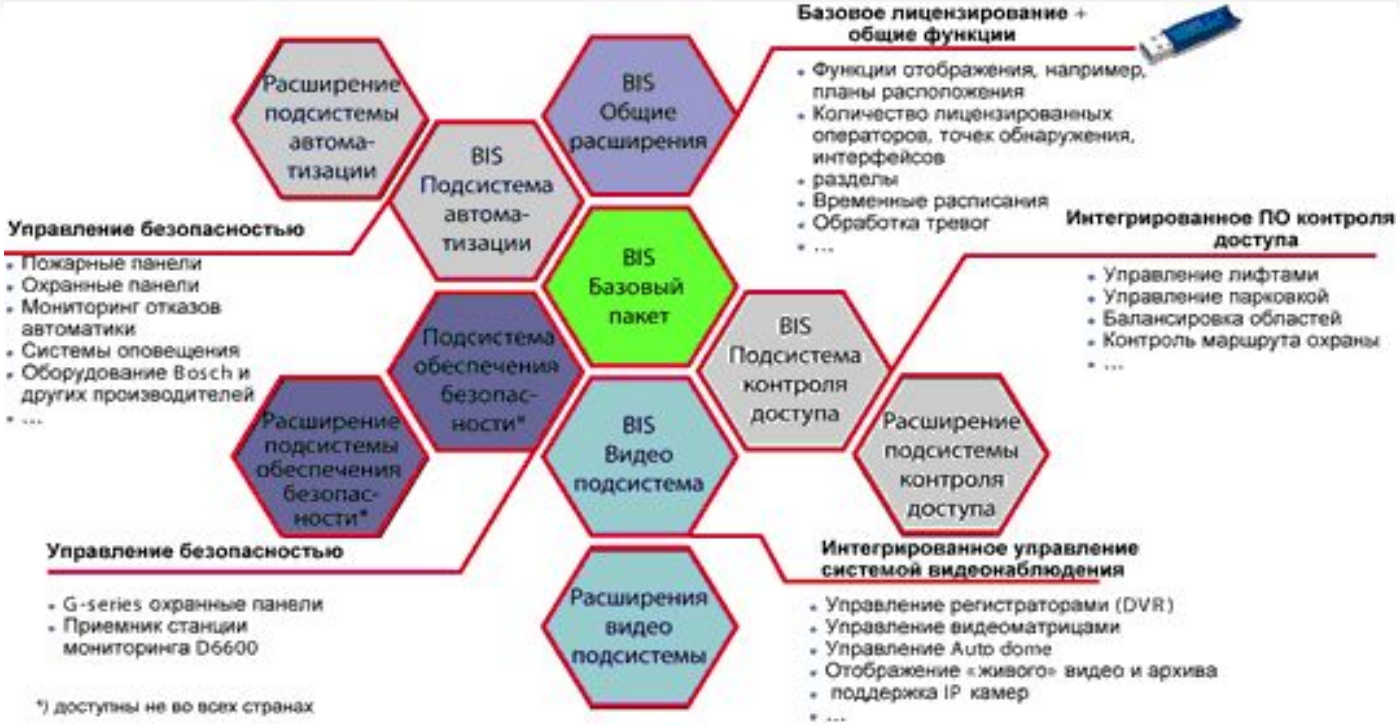
МОДЕЛЬ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Модель обеспечения безопасности логистического комплекса

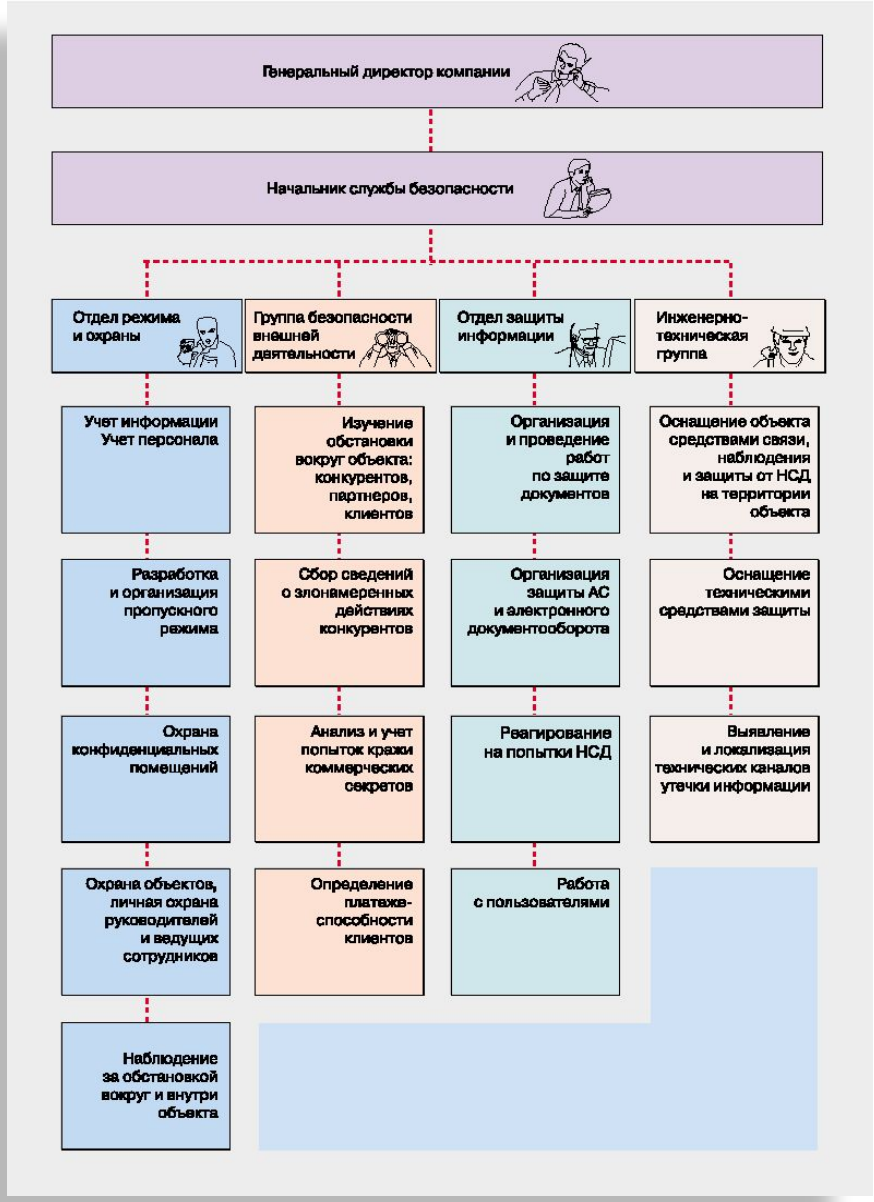
МЕТОДОЛОГИЯ ВЫБОРА КОМПЛЕКСА СРЕДСТВ ИТБ



ПРАКТИКА ИНТЕГРАЦИИ ИНЖЕНЕРНО-ТЕХНИЧЕСКИХ СРЕДСТВ



ПОДРАЗДЕЛЕНИЯ ИТБ В СТРУКТУРЕ СБ ПРЕДПРИЯТИЯ
РАЗГРАНИЧЕНИЕ ПОЛНОМОЧИЙ

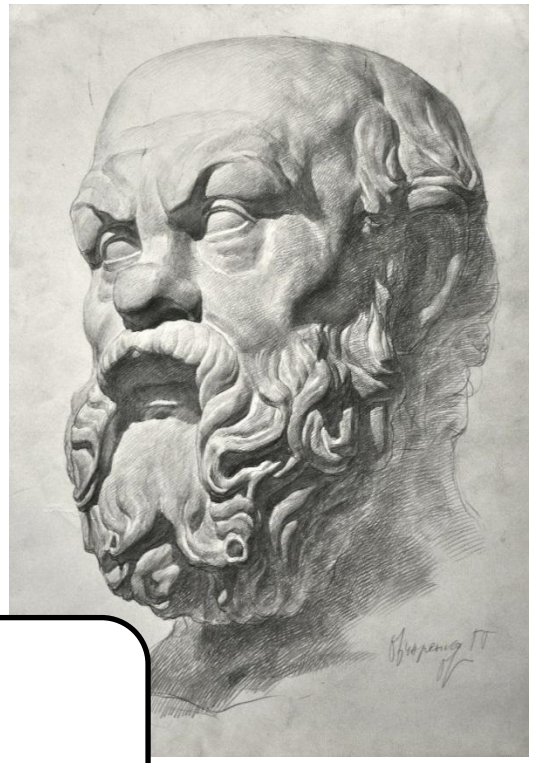


ОСНОВНЫЕ ЗАДАЧИ ПОДРАЗДЕЛЕНИЯ ИТБ

- обследование выделенных помещений с целью установления потенциально возможных каналов утечки конфиденциальной информации через технические средства, конструкции зданий и оборудования.
- выявление и оценка степени опасности технических каналов утечки информации.
- разработка мероприятий по ликвидации (локализации) установленных каналов утечки информации организационными, организационно-техническими или техническими мерами, используя для этого физические, аппаратные и программные средства и математические методы защиты.
- организация контроля (в том числе и инструментального) за эффективностью принятых защитных мероприятий. Проведение обобщения и анализа результатов контроля и разработка предложений по повышению надежности и эффективности мер защиты.

ПРАВА ПОДРАЗДЕЛЕНИЯ ТЕХНИЧЕСКОЙ ЗАЩИТЫ

- обеспечение приобретения, установки, эксплуатации и контроля состояния технических средств защиты информации.
- проверять наличие технических средств обеспечения производственной деятельности в выделенных помещениях, измерять их параметры на соответствие требованиям безопасности;
- устанавливать технические средства защиты каналов утечки информации через технические средства обеспечения производственной деятельности;
- запрещать использование технических средств, не



Сократ, мудрец

Библиография

Основная литература

1. Шульц В.Л., Рудченко А.Д., Юрченко А.В. Безопасность предпринимательской деятельности. М.: Издательство «Юрайт», 2016;
2. Шульц В.Л., Рудченко А.Д., Юрченко А.В. Пособие для обучения на майноре. (на начальном этапе)

Дополнительная литература

1. Ворона В.А., Тихонов В.А. Концептуальные основы создания и применения системы защиты объектов. 2012. М. Горячая линия – Телеком, С 65

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА