Security Management for Business

Инженерно-техническая безопасность предприятия

РОЛЬ И МЕСТО ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ В ОБЕСПЕЧЕНИИ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Система безопасности предприятия – это система выявления, предупреждения и пресечения посягательств на законные права предприятия, его имущество, интеллектуальную собственность, производственную дисциплину, технологическое лидерство, научные достижения и охраняемую информацию.

Укрупненные внешние и внутренние угрозы

- Угроза разглашения охраняемых сведений
- Угроза жизни и здоровью работников
- Угроза захвата собственности
- Угроза хищения материальных ценностей
- Угроза выбора несостоятельных контрагентов
- Угроза внешнего и внутреннего мошенничества
- Угроза промышленного шпионажа
- Угроза нарушения стабильности электронных ресурсов
- Угроза проникновения в персонал нежелательных лиц

Реализация решения – система мер противодействия угрозам

- Меры обеспечения физической безопасности
- Меры обеспечения инженерно-технической безопасности
- Меры обеспечения экономической безопасности
- Меры обеспечения финансовой безопасности
- Меры обеспечения информационной безопасности
- Меры обеспечения кадровой безопасности
- Меры мониторинга внешней и внутренней среды
- Меры взаимодействия внутри организации
- Меры взаимодействия за пределами организации

РОЛЬ И МЕСТО ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ В ОБЕСПЕЧЕНИИ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

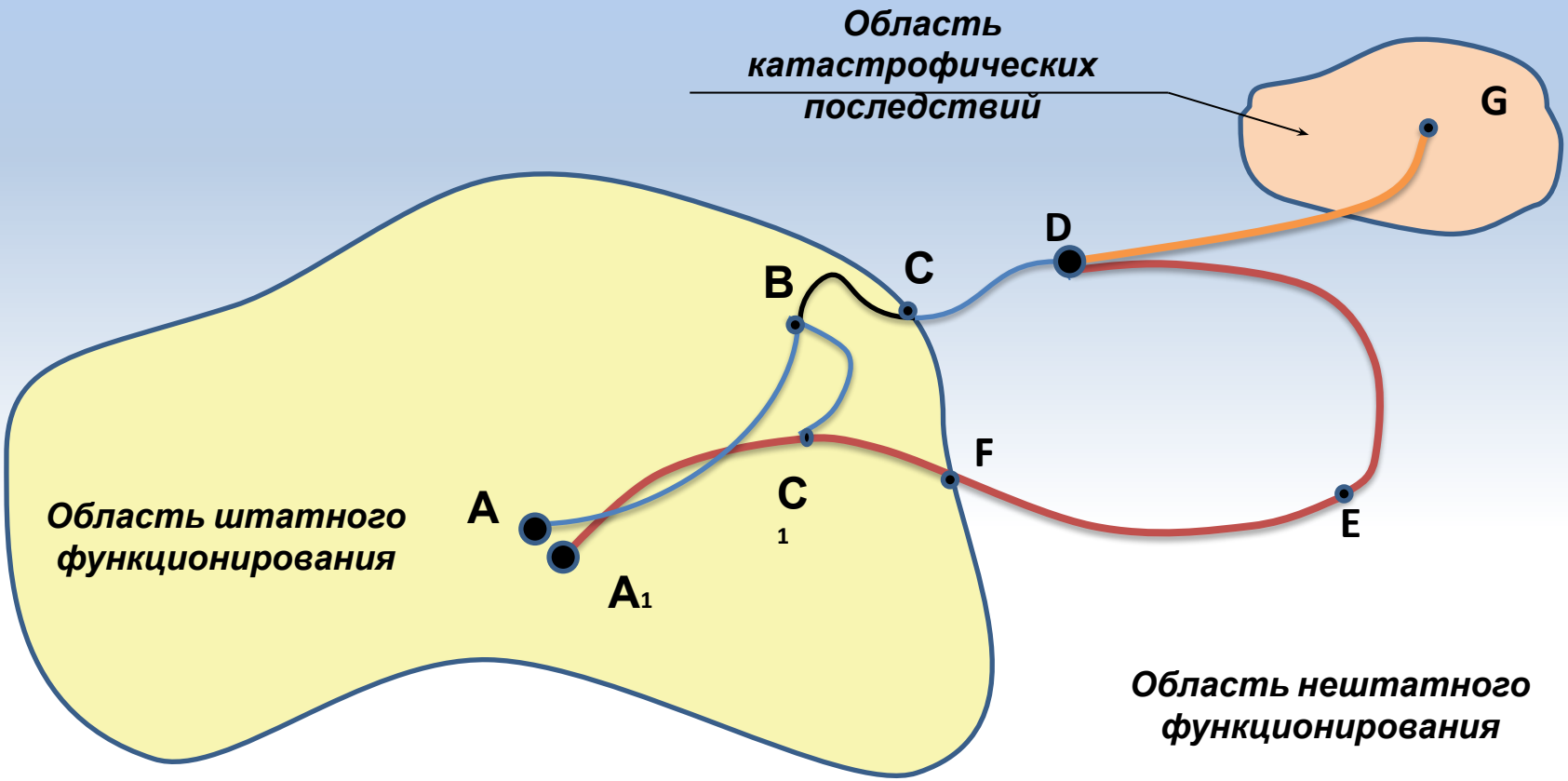
РОЛЬ И МЕСТО ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ В ОБЕСПЕЧЕНИИ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

ЭКСПЕРТНЫЕ ОЦЕНКИ ВЕРОЯТНОСТИ ОСУЩЕСТВЛЕНИЯ ОТДЕЛЬНЫХ ВИДОВ УГРОЗ ПРЕДПРИНИМАТЕЛЬСКОЙ ДЕЯТЕЛЬНОСТИ В РОССИЙСКОЙ ЭКОНОМИКЕ

№ п/п	Виды угроз	Вероятность осуществления угрозы, %
1	Экономическое подавление, в том числе:	
	срыв сделок и иных соглашений	48
	парализация деятельности предприятия с использованием гос. органов и средств массовой информации	31
	компрометация деятельности предприятия	11
	шантаж, компрометация руководителей и отдельных сотрудников	10
2	Физическое подавление, в том числе:	
	ограбление и разбойное нападение на офисы и склады	73
	угрозы физической расправы	22
	убийства	5
3	Промышленный шпионаж, в том числе:	
	подкуп сотрудников	43
	передача документов и разработок	10
	копирование программ и данных	24
	проникновение в ПЭВМ	18
	подслушивание переговоров	26
4	Финансовое подавление	нет данных
5	Психическое подавление	нет данных

РОЛЬ И МЕСТО ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ В ОБЕСПЕЧЕНИИ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

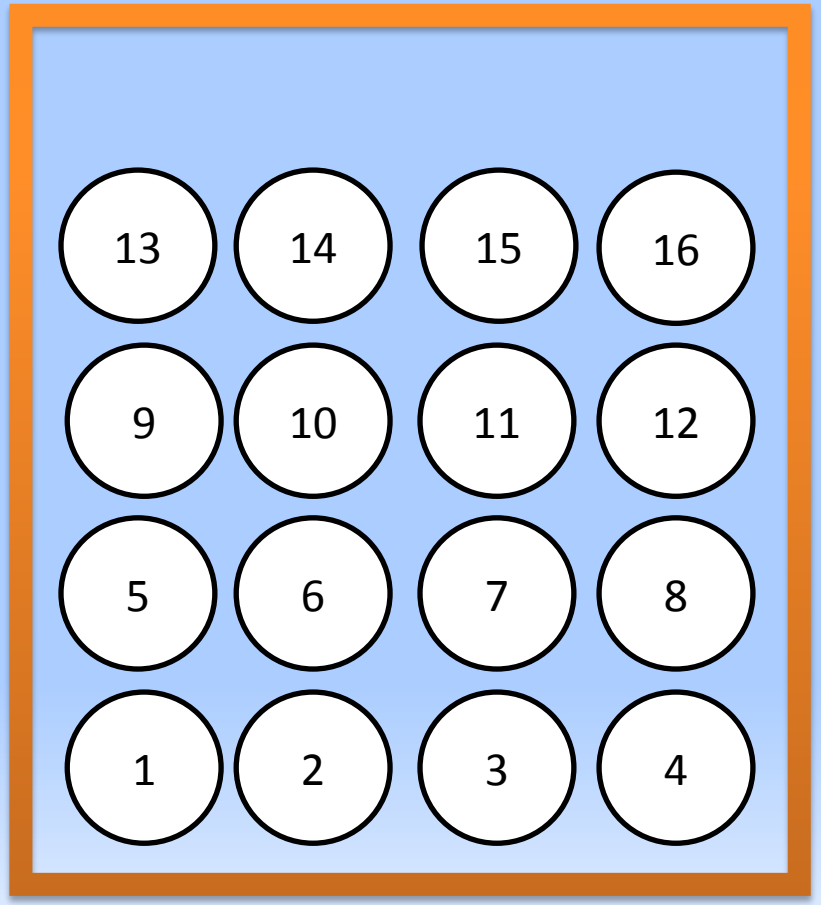
ФИЛОСОФИЯ ДЕЙСТВИЙ В НЕШТАТНЫХ СИТУАЦИЯХ



РОЛЬ И МЕСТО ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ В ОБЕСПЕЧЕНИИ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Целью обеспечения безопасности предприятия является комплексное воздействие на потенциальные и реальные угрозы, позволяющее ему успешно функционировать в нестабильных условиях внешней и внутренней среды.

ТЕОРИЯ И ПРАКТИКА ИСПОЛЬЗОВАНИЯ ИНЖЕНЕРНО-ТЕХНИЧЕСКИХ СРЕДСТВ



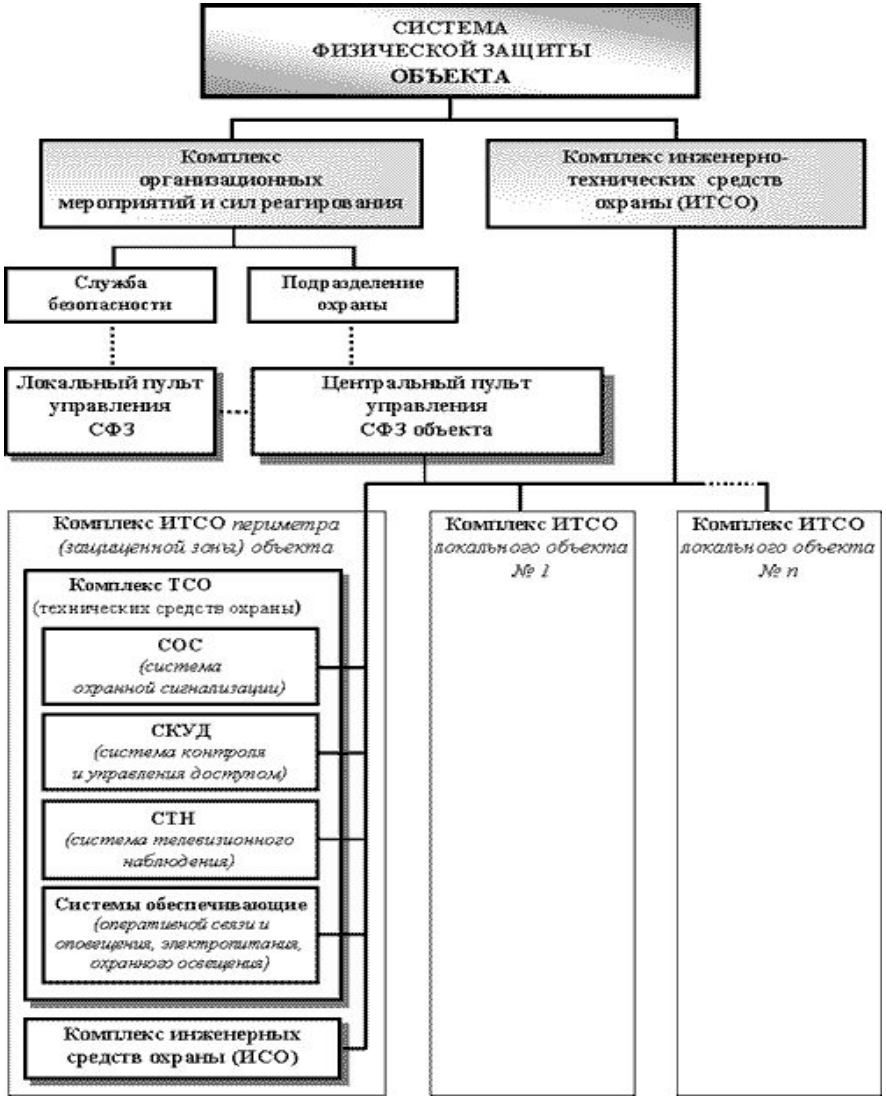
1. Система контроля и управления доступом
2. Внешние устройства охранной сигнализации
3. Внутренние устройства охранной сигнализации
4. Противопожарная сигнализация
5. Устройства подачи тревожных сигналов
6. Внешние устройства видео наблюдения
7. Внутренние устройства видео наблюдения
8. Инженерная защита выделенных зон
9. Активная и пассивная защита от несанкционированного съема информации техническими средствами
10. Спутниковая навигация и связь
11. Система радийной связи
12. Бронированные средства передвижения
13. Беспилотные летательные аппараты
14. Системы комплексного мониторинга
15. Система выявления взрывчатых веществ
16. Система поиска лиц по заданным параметрам

ПРИНЦИП СТАКАНА

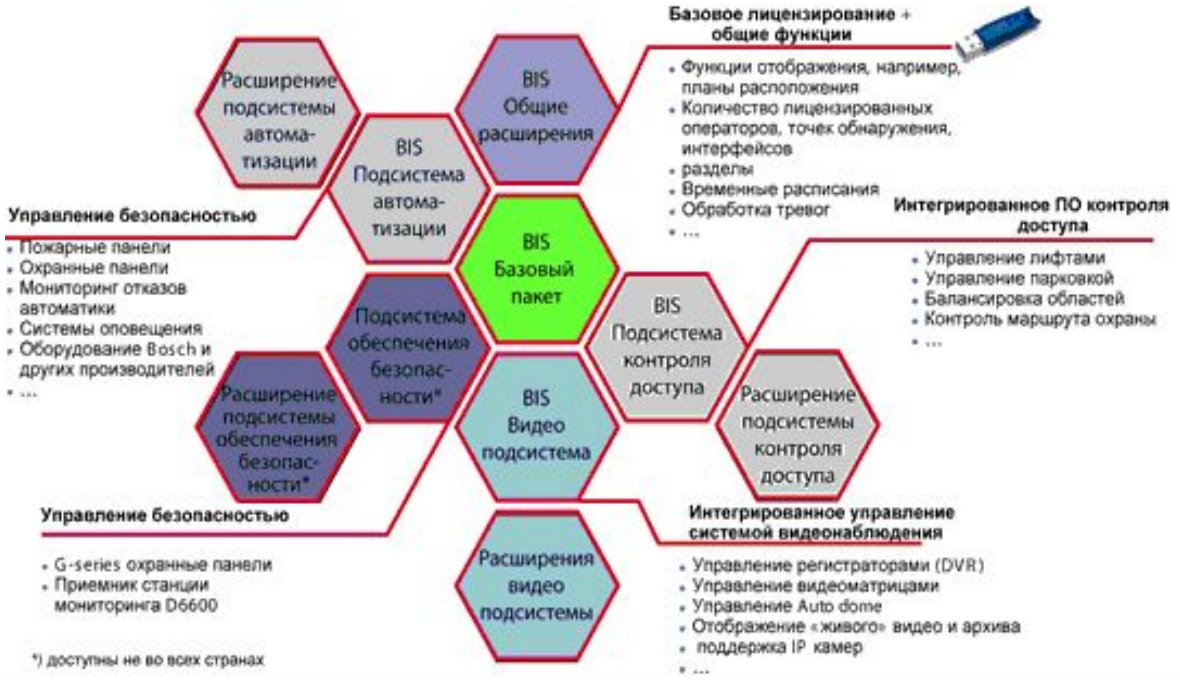
ТЕОРИЯ И ПРАКТИКА ИСПОЛЬЗОВАНИЯ ИНЖЕНЕРНО-ТЕХНИЧЕСКИХ СРЕДСТВ

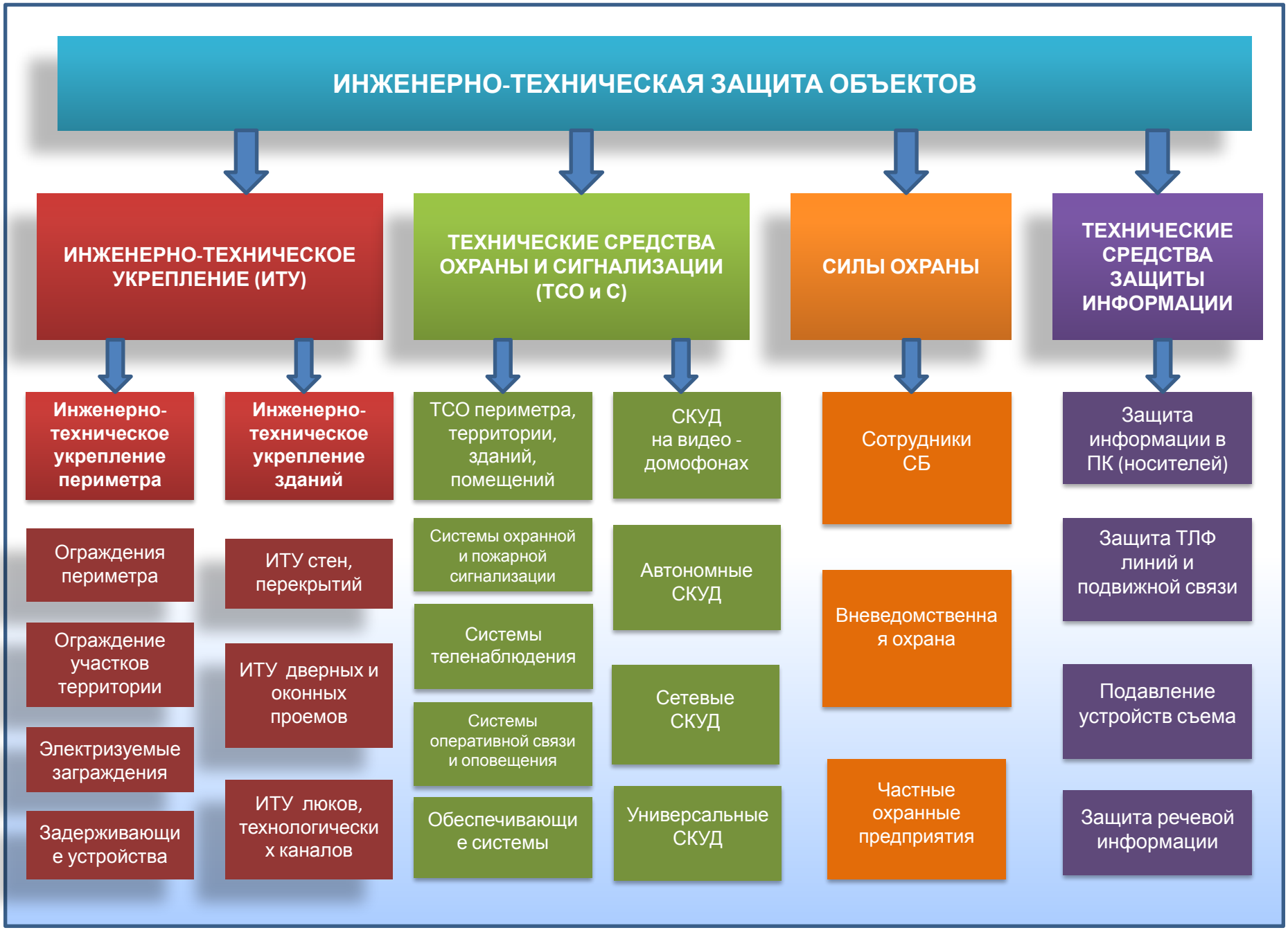
ОБЪЕКТЫ ЗАЩИТЫ

1. ***люди (персонал предприятия);***
2. ***имущество:***
   - важное или дефицитное технологическое оборудование;
   - секретная и конфиденциальная документация;
   - материальные и финансовые ценности;
   - готовая продукция;
   - интеллектуальная собственность (ноу-хау);
   - средства вычислительной техники (СВТ);
   - контрольно-измерительные приборы (КИП) и др.;
3. ***информация*** *конфиденциальная:* на материальных носителях, а также циркулирующая во внутренних коммуникационных каналах связи и информации, в кабинетах руководства предприятия, на совещаниях и заседаниях;
4. ***финансово-экономические ресурсы,*** обеспечивающие эффективное и устойчивое развитие предприятия (капитал, коммерческие интересы, бизнес-планы, договорные документы и обязательства и т. п.).



ТЕОРИЯ И ПРАКТИКА ИСПОЛЬЗОВАНИЯ ИНЖЕНЕРНО-ТЕХНИЧЕСКИХ СРЕДСТВ




ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯ ЗАЩИТА ОБЪЕКТОВ
ИНЖЕНЕРНО-ТЕХНИЧЕСКОЕ УКРЕПЛЕНИЕ (ИТУ)
ТЕХНИЧЕСКИЕ СРЕДСТВА ОХРАНЫ И СИГНАЛИЗАЦИИ (ТСО и С)
СИЛЫ ОХРАНЫ
ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ
Инженерно-техническое укрепление периметра
Инженерно-техническое укрепление зданий
ТСО периметра, территории, зданий, помещений
СКУД на видео - домофонах
Сотрудники СБ
Защита информации в ПК (носителей)
Ограждения периметра
ИТУ стен, перекрытий
Системы охранной и пожарной сигнализации
Автономные СКУД
Вневедомственная охрана
Защита ТЛФ линий и подвижной связи
Ограждение участков территории
ИТУ дверных и оконных проемов
Системы теленаблюдения
Сетевые СКУД
Подавление устройств съема
Электризуемые заграждения
ИТУ люков, технологических каналов
Системы оперативной связи и оповещения
Универсальные СКУД
Частные охранные предприятия
Защита речевой информации
Задерживающие устройства
Обеспечивающие системы

СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

Классы защиты объектов
(4-й класс защиты объектов – высший)

Группа объекта	Класс объекта	Класс защиты объекта
I	1	4
	2	3
II	1	4
	2	2
	3	1
III	1	3
	2	2
	3	1

I группа: критически важные и потенциально опасные объекты.
II группа: социально-значимые объекты.
III группа: объекты сосредоточения материальных ценностей.

В зависимости от вида и размеров ущерба, который может быть нанесен объекту, находящимся на нем людям и имуществу в случае реализации криминальных угроз, все объекты подразделяются на следующие классы:

класс 1 (высокая значимость) - ущерб в результате реализации криминальных угроз может приобрести федеральный или межрегиональный масштаб;

класс 2 (средняя значимость) - ущерб в результате реализации криминальных угроз может приобрести региональный или межмуниципальный масштаб;

класс 3 (низкая значимость) - ущерб в результате реализации криминальных угроз может приобрести муниципальный или локальный масштаб.

СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

ИДЕНТИФИКАТОРЫ

- механические - идентификационные признаки представляют собой элементы конструкции идентификаторов (перфорационные отверстия, элементы механических ключей и т.д.);

- магнитные - идентификационные признаки представляют собой намагниченные участки поверхности или магнитные элементы идентификатора (карты с магнитной полосой, карты Виганда и т. д.);

- оптические - идентификационные признаки представляют собой нанесенные на поверхности или внутри идентификатора метки, имеющие различные оптические характеристики в отраженном или проходящем оптическом излучении, помогающие осуществлять контроль доступа к охраняемому объекту (карты со штриховым кодом, голографические метки и т. д.);

- электронные - идентификационные признаки представляют собой электронный код , записанный в микросхеме идентификатора (дистанционные карты, электронные ключи и т. д.);

- акустические - идентификационные признаки представляют собой кодированный акустический сигнал;

- биометрические - идентификационные признаки для биометрических устройств представляют собой индивидуальные физические признаки человека (отпечатки пальцев, геометрия ладони, рисунок сетчатки глаза, голос, динамика подписи и т.д.);

Кейс

Использование СКУД в интересах работы с персоналом

В Московском банке ОАО «Сбербанк России» используется система контроля и управления доступом (СКУД). Она призвана обеспечить, в первую очередь, техническую составляющую пропускного и внутриобъектового режимов объектов данного финансово-кредитного учреждения. Архитектура СКУД позволяет получать фактографическую информацию за любой промежуток времени и с территории любого охраняемого объекта.
Данная система также, в интересах эффективного управления бизнесом, может быть использована и в других целях.

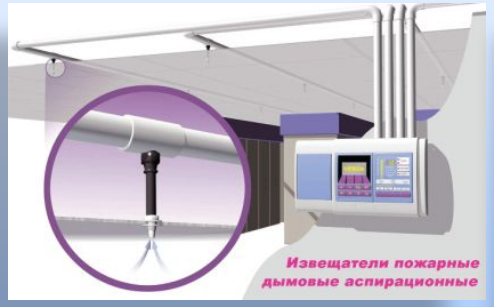
Так, Департамент внутреннего контроля, ревизий и аудита центрального аппарата в 2010 году проверял организацию кредитования юридических лиц в Московском банке. В ходе проверки у ревизоров возникли обоснованные подозрения в подлинности нескольких актов проверки залогового имущества. Проверяющие попросили службу безопасности банка предоставить заверенные распечатки данных СКУД по 3 кредитным инспекторам и 2 инспекторам экономической безопасности, которые якобы совместно (по 2 человека) проверяли наличие залога у заемщиков-юридических лиц. В одном из случаев оказалось, что кредитный инспектор и инспектор экономической безопасности в конкретный день на проверку не выезжали, однако составили акт о том, что проверка произведена и залог сохранен. Распечатка данных СКУД показала, что оба сотрудника в день проверки утром прошли на работу, а после 18.00 покинули ее. Ознакомившись с эти объективными данными, оба сотрудника признались в служебном проступке, написали соответствующие объяснения. По итогам проверки им были объявлены дисциплинарные взыскания, оба были лишены квартальной премии.

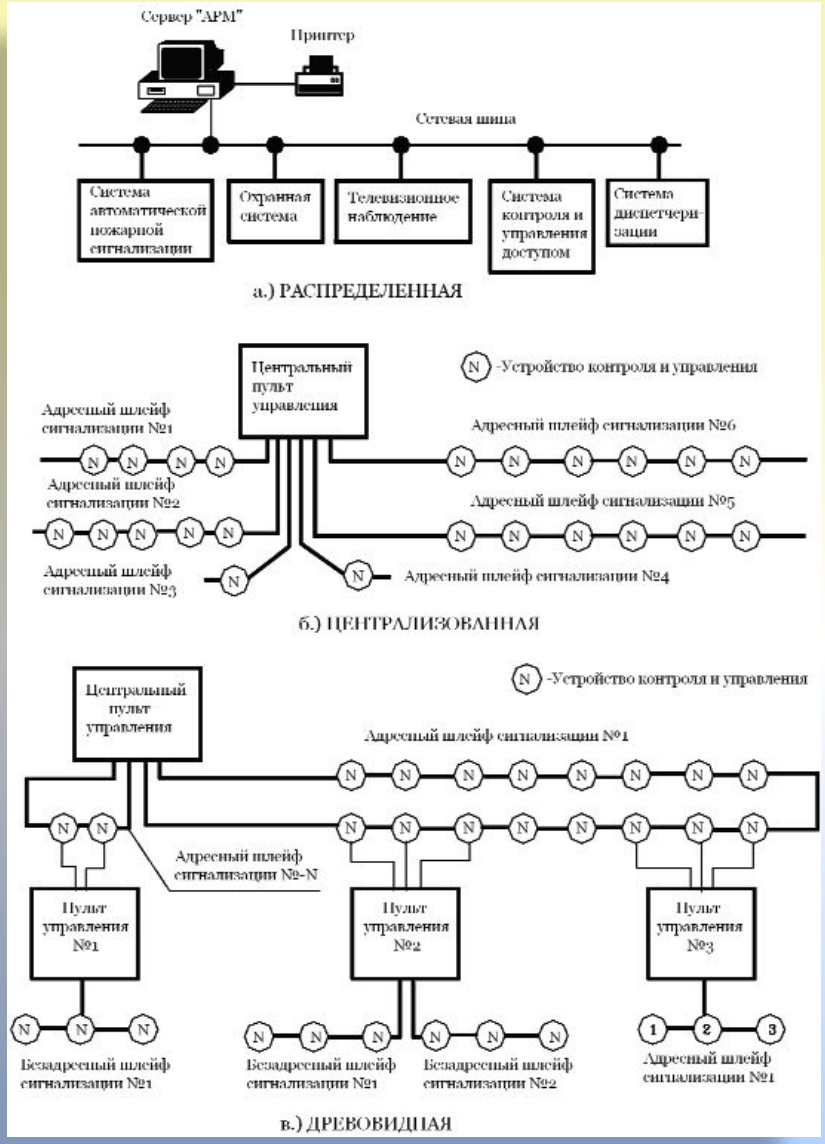
Руководители подразделений этого банка часто запрашивают в службе безопасности распечатки данных СКУД по подчиненным сотрудникам и используют эти материалы в мероприятиях по укреплению трудовой дисциплины. В отдельных случаях работников банка увольняют с работы за однократное грубое нарушение трудовой дисциплины (отсутствие на работе более 3 часов без уважительной причины).

ПРОТИВОПОЖАРНЫЕ СИСТЕМЫ

СТРУКТУРА ПОЖАРНОЙ БЕЗОПАСНОСТИ

в соответствии с ФЗ РФ от 22 июля 2008 г. N 123-ФЗ "Технический регламент о требованиях пожарной безопасности"





Кейс

- **В России не представляет проблем найти грамотных технических специалистов практически в любой области;**
- **Уровень подготовки многих технических специалистов, существующих в России, позволяет им решать сложные и нестандартные проблемы, которые не в состоянии решить основная масса специалистов того же профиля в других странах;**
- **Большое количество жителей России не является законопослушными гражданами и ищут незаконные способы получения денег;**
- **В России существует КУЛЬТУРА НАРУШЕНИЯ ЗАПРЕТОВ. В том числе, КУЛЬТУРА ПРЕОДОЛЕНИЯ СИСТЕМ БЕЗОПАСНОСТИ ОБЪЕКТОВ.**

В 90-х годах ГУВО МВД РФ провело статистическое исследование состава групп, осуществляющих кражи в музеях. Результат:

- **Научные сотрудники - 20%**
- **Инженерно-технические работники - 40%**
- **Сотрудники музеев - 30 %**
- **Профессиональные воры - 10%**

(ПРИМЕЧАНИЕ: Цифры не точные, но порядок правильны.)

Налицо, вполне грамотно сформированный состав рабочей группы - идеологи, технические специалисты, наводчики и конечные исполнители.

Промышленные объекты гораздо более интересны криминальным элементам, чем музеи. В первую очередь, это связано с тем, что промышленные предприятия представляют для криминалитета не разовый, а постоянный источник доходов. Организация работы криминальных структур здесь, часто, поставлена на поток. В незаконной деятельности могут принимают участие сотрудники любых подразделений предприятия, от сотрудников службы охраны, до высшего руководства.

На некоторых заводах теневой оборот сравним с официальным оборотом предприятия.

Таким образом, **ОСНОВНОЕ ТРЕБОВАНИЕ К СИСТЕМЕ БЕЗОПАСНОСТИ ПРОИЗВОДСТВЕННЫХ ОБЪЕКТОВ**:

СИСТЕМА БЕЗОПАСНОСТИ ПРОИЗВОДСТВЕННЫХ ОБЪЕКТОВ ДОЛЖНА ОБЕСПЕЧИВАТЬ ЗАЩИТУ ОТ ПРОТИВОПРАВНЫХ ДЕЙСТВИЙ* ПРОФЕССИОНАЛЬНО ПОДГОТОВЛЕННЫХ *КРИМИНАЛЬНЫХ ГРУПП.

СИСТЕМЫ ОХРАНЫ ПЕРИМЕТРА

Задачи, решаемые при оборудовании периметра техническими средствами охраны

✔Обнаружение факта попытки проникновения нарушителя.

✔Определение места проникновения нарушителя.

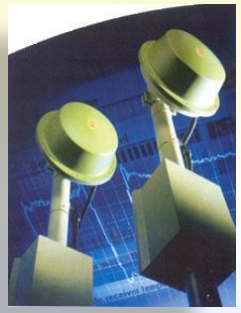
✔Оповещение группы реагирования.

В отдельных случаях, могут решаться дополнительные задачи:

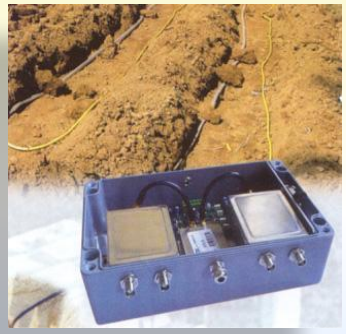
✔Оптимизация действий группы реагирования - формирование рекомендаций по реагированию в конкретной ситуации, включение освещения участков, на которых обнаружены действия нарушителей.

✔Психологическое воздействие на нарушителя - формирование звуковых и световых сигналов тревоги, передача в зоне деятельности нарушителя голосовых сообщений по громкоговорящей связи и т.п.

Радиолучевые системы

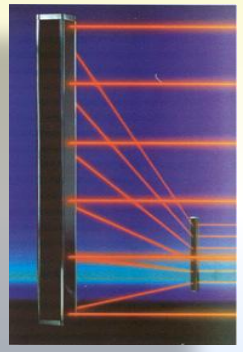


Радиоволновые системы



Вибрационно-чувствительные системы с сенсорными кабелями

Активные лучевые ИК-датчики



СВЧ датчик

Системы с волоконно-оптическими

Пассивные ИК-датчики

Автономные и быстроразворачиваемые системы

Кейс

Можно сделать сколь угодно хорошую техническую укрепленность объекта,
но при отсутствии технических средств охраны группа реагирования никогда не узнает о том,
что на объект совершено нападение.
Можно сделать замечательную укрепленность и технические средства охраны, но если террористу
необходимо 5 минут для того, чтобы достигнуть здания, которое он собирается взорвать,
а группе реагирования 10, то система бесполезна, т.к. здание будет взорвано.и т.п.

ПРИМЕРЫ

1. Калужский музей изобразительных искусств. Здание и экспозиция музея оборудованы тремя рубежами охраны - охраняются окна, объем залов и отдельные картины. Музей расположен на центральной площади города напротив здания Вневедомственной охраны. **НО**... окна здания не оборудованы решетками.
Действия нарушителей: Быстро разбить окно, вломиться в помещение, сорвать картину и убежать.
Все рубежи сигнализации сработали. Вневедомственная охрана приехала через 2 минуты после сигнала тревоги.
Но к тому моменту грабителям удалось скрыться.
Система безопасности оказалась не эффективной. Этой ситуация могла не произойти, если бы окна были оборудованы решетками. Время преодоления решетки составляет более 2 минут и обеспечивает задержку нарушителей на время, достаточное для прибытия группы реагирования.

2. В одном из подмосковных городов здание банка и отдельные его помещения оборудованы бронестеклами. **НО...**
Бронестекла вставлены в алюминиевые рамы. Такое техническое решение сводит на нет защиту, реализованную бронестеклами. На то 2 причины:

- Дюралевая рама пробивается выстрелами из автомата. Т.е. по служащим банка можно вести огонь из-за стекла.
- Бронестекло выбивается вместе с рамой. Для этого достаточно въехать в него на автомобиле.

ВСЕ ФУНКЦИОНАЛЬНЫЕ ЭЛЕМЕНТЫ СИСТЕМЫ БЕЗОПАСНОСТИ ДОЛЖНЫ БЫТЬ СБАЛАНСИРОВАНЫ И РАССЧИТАНЫ НА ОДИН УРОВЕНЬ ЗАЩИЩЕННОСТИ.

ВИДЕОНАБЛЮДЕНИЕ В СИСТЕМАХ ОХРАНЫ

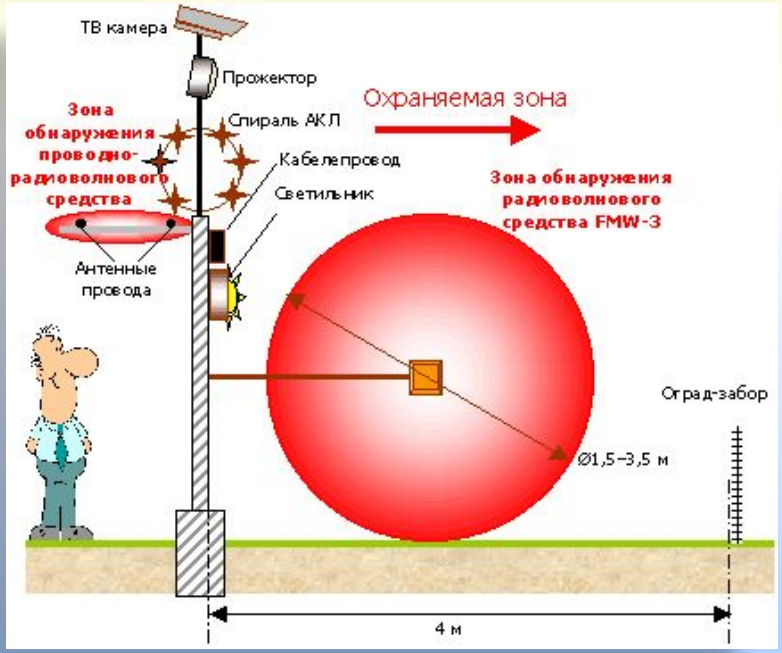
ОСНОВНЫЕ ПОДХОДЫ К ОСНАЩЕНИЮ ПЕРИМЕТРА СИСТЕМАМИ ВИДЕОКОНТРОЛЯ:

Объект особой важности — двухрубежная система периметровой сигнализации плюс система глобального теленаблюдения.

Важный объект — видеоконтроль отдельных зон, где вероятность нарушения наиболее высока. Обычно это зоны ворот, стыки с водоемами, с соседними зданиями, участки, где гипотетически возможна заблаговременная подготовка преступной акции.

Прочие объекты с небольшой протяженностью периметра — здесь наиболее эффективным будет телевизионный контроль всей трассы периметра, вкупе с некоторыми, прилегающими к участку, наружными зонами.

Пример применения видеонаблюдения для охраны объекта особой важности



ПОКОЛЕНИЯ СИСТЕМ ВИДЕОНАБЛЮДЕНИЯ

Системы первого поколения:
Детектор движения. **Традиционно интегрирован в цифровые видеорегистраторы. Обнаружение угроз происходит при сравнении пиксельных изменений между кадрами.**

Системы второго поколения:
Интеллектуальное видео. **Постоянно определяет и переопределяет изменения фона, которые происходят в поле зрения камеры и отделяет динамически меняющийся фон (т.е. нормальное поведение) от аберрантного (т.е. ненормального) поведения цели). Это позволяет отделять естественную активность окружающей среды , такой как качание деревьев под действием ветра, от активности, вызванной движением целей.**

Системы третьего поколения:
Географическое реагирование **. Интеллектуальное видео, которое выполняет все свои функции плюс отслеживает цели (с передачей целей от камеры к камере, при необходимости) и показывает контуры, расположение и движение всех целей на географической карте или карте объекта.**

ВИДЕОНАБЛЮДЕНИЕ В СИСТЕМАХ ОХРАНЫ

ОСНОВНЫЕ ФУНКЦИИ СОТ, ТРЕБУЮЩИЕ ПРИСУТСТВИЯ ОПЕРАТОРА

1. Оперативное наблюдение за охраняемой территорией, зданиями и помещениями. *Обнаружение нарушителя возложено на оператора.*
2. Оценка сигнала тревоги. *Телекамера используется совместно с техническим средством охраны для подтверждения факта срабатывания последнего.*
3. Телевидение может использоваться совместно с системой управления доступом.
4. Психологическое воздействие на нарушителя. *Телекамеры, даже неработающие, могут оказывать «отпугивающее» действие, выполняя таким образом предупредительно-профилактическую функцию.*
5. Документирование событий на объекте. *Материал видеоархивов может оказаться полезным в качестве доказательной базы при расследовании несанкционированных действий.*

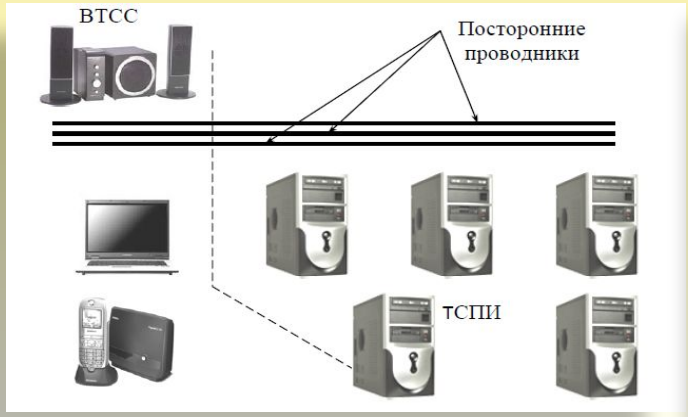
ИНТЕЛЛЕКТУАЛЬНЫЕ ФУНКЦИИ СОТ

1. Обнаружение перемещения в зоне наблюдения (видеодетекция). *Такие устройства часто встраиваются в стандартные мультиплексоры. При этом оператор может задавать зону на экране монитора, движение в которой вызывает сигнал тревоги.*
2. Распознавание (классификация) объектов. *Система должна отличить человека от животного и от качания веток деревьев.*

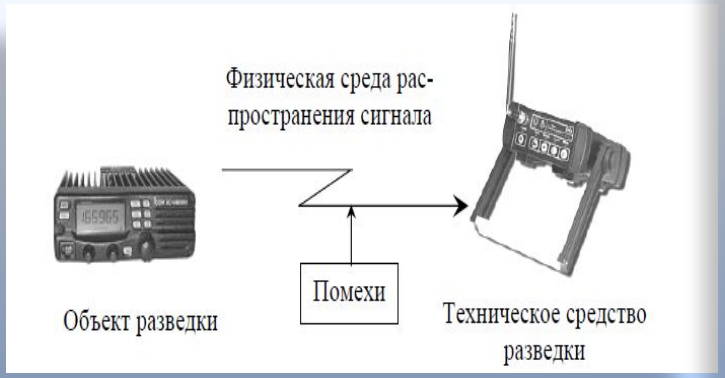
Типовая схема применения комплекса СОТ

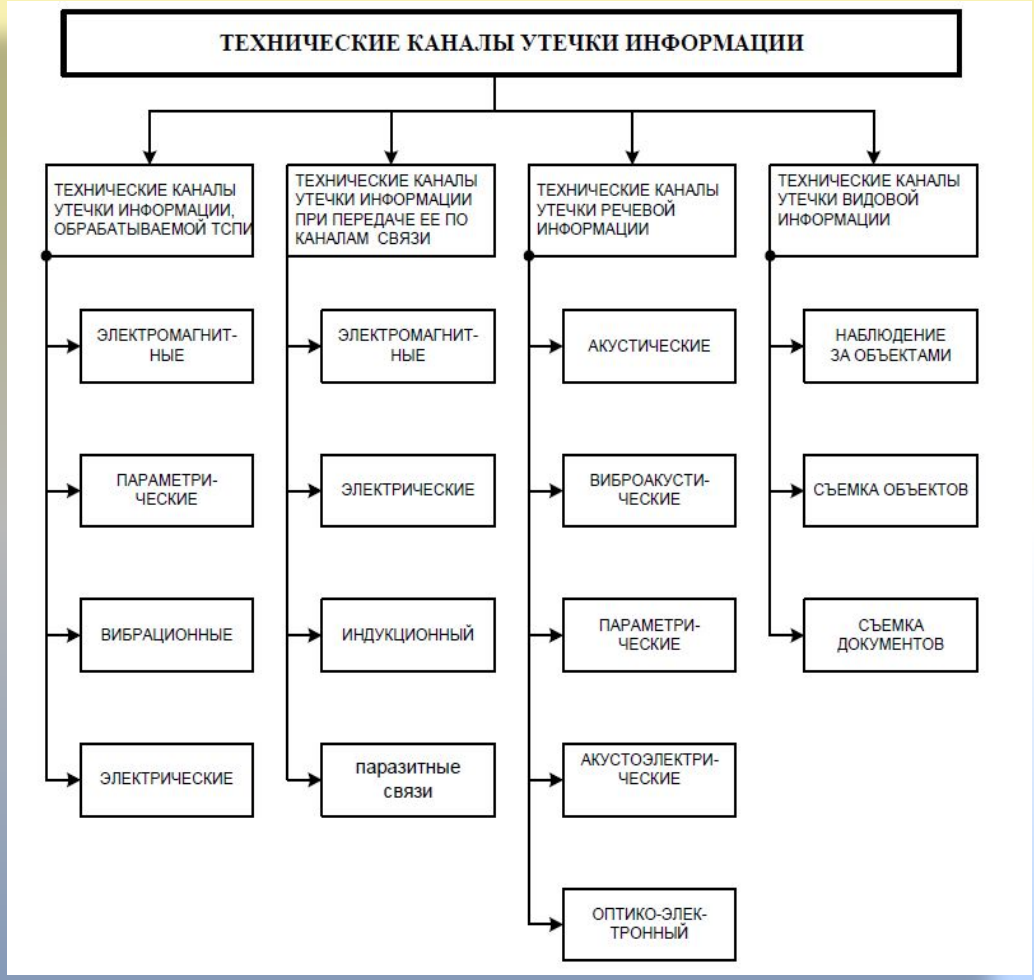
ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

Источники образования возможных каналов утечки информации



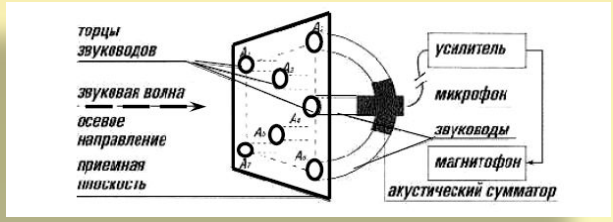
Технический канал утечки информации





ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

Плоская фазированная решетка



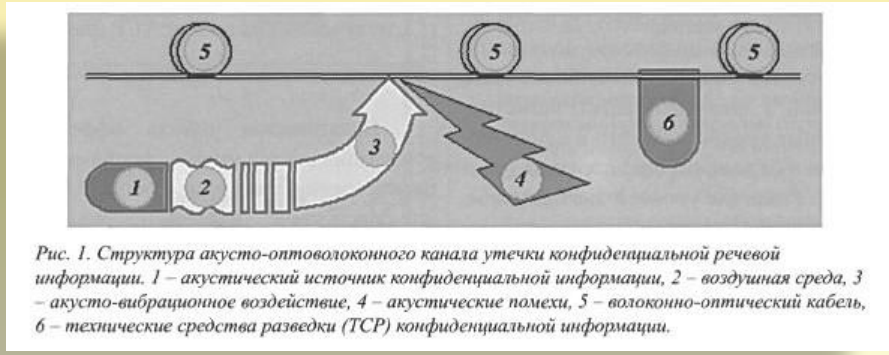
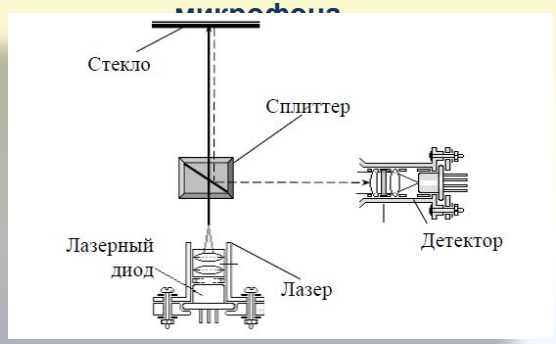


Рис. 1. Структура акусто-оптоволоконного канала утечки конфиденциальной речевой информации. 1 – акустический источник конфиденциальной информации, 2 – воздушная среда, 3 – акусто-вибрационное воздействие, 4 – акустические помехи, 5 – волоконно-оптический кабель, 6 – технические средства разведки (ТСР) конфиденциальной информации.

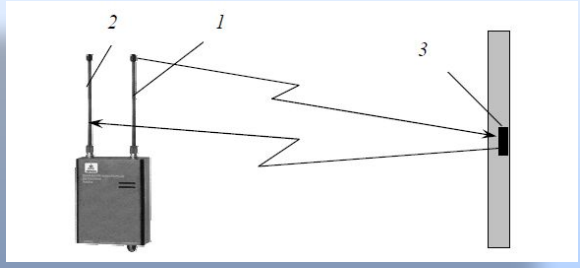
Схема простейшего лазерного микрофона



Закамуфлированная цифровая микрофотокамера

Зрительная труба

Схема аудио-транспордера



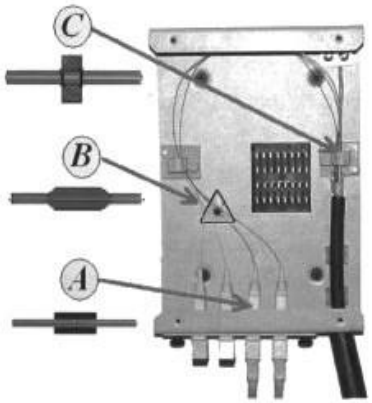
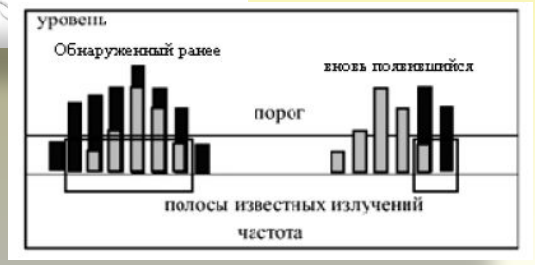
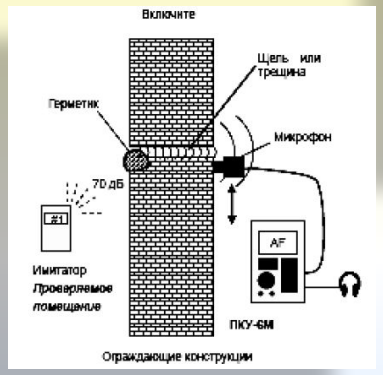


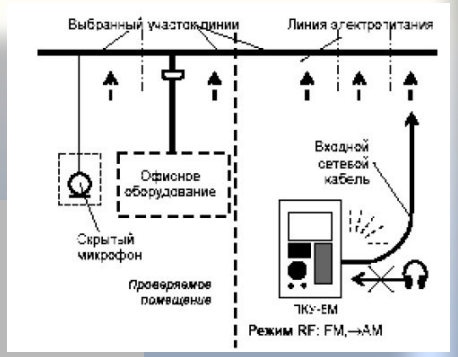
Рис. 2. Угрозы формирования канала утечки речевой информации типов A, B, C на примере отдельных волоконно-оптических элементов структурированной кабельной системы.

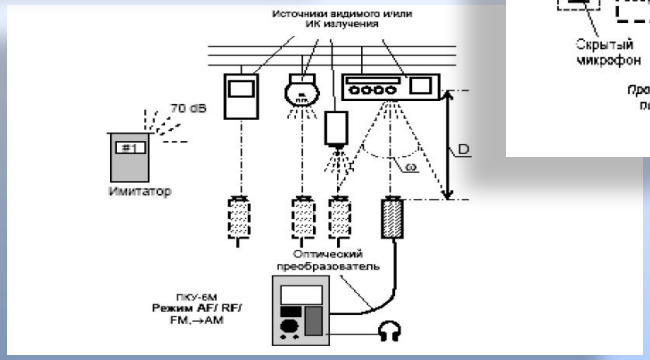
ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

Комплекс RS turbo







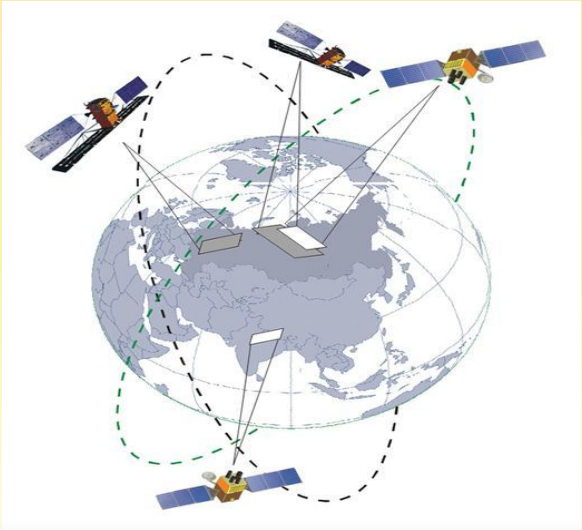


НОВНЫЕ НАПРАВЛЕНИЯ ЗАЩИТЫ ФОРМАЦИИ ОТ УТЕЧКИ ПО НО-ОПТИЧЕСКОМУ КАНАЛУ:

- **располагать объекты защиты так, чтобы исключить отражение света в сторону возможного расположения злоумышленника;**
- **уменьшить отражательные свойства объекта защиты;**
- **уменьшить освещенность объекта защиты;**
- **использовать средства преграждения или значительного ослабления отраженного света: ширмы, шторы, ставни, темные стекла, преграды;**
- **применять средства маскирования, имитации и другие с целью введения в заблуждение злоумышленника;**
- **использовать средства пассивной и активной защиты источника от неконтролируемого распространения отраженного или излученного света и других излучений;**
- **осуществлять маскировку объектов защиты, варьируя отражательными свойствами и контрастом фона;**
- **применять маскирующие средства сокрытия объектов можно в виде аэрозольных завес и маскирующих сеток, красок, укрытий.**

ИСПОЛЬЗОВАНИЕ СРЕДСТВ КОСМИЧЕСКОГО ОБНАРУЖЕНИЯ И КОНТРОЛЯ

(По материалам ОАО «Российские космические системы»)



НАИБОЛЕЕ ЗНАЧИМЫЕ ПРОБЛЕМЫ, И ВОЗМОЖНЫЕ ИХ РЕШЕНИЯ

Отсутствие отработанных средств автоматизации создания большинства стандартных и тематических продуктов ДЗЗ без участия экспертов, в силу специфики информационных свойств исходных данных → **Недостаточная оперативность** предоставления конечных продуктов потребителям и необходимость привлечения обширных интеллектуальных ресурсов

Отсутствие технологических возможностей самостоятельной интерпретации первичных информационных продуктов (например, гиперкуба или интерферометрических пар радиолокационных изображений) у большинства потребителей → **Потенциальная невостребованность** новых видов информационных продуктов ДЗЗ

Отсутствие единых требований (стандартов) потребителей к конечным информационным продуктам (виду, формату и средствам их представления) → **Необходимость средств адаптации** продуктов ДЗЗ на входе в информационно-аналитические системы потребителей

→ **Требуется разработка в составе НКПОР Оператора КС ДЗЗ** нового поколения методико-алгоритмического обеспечения и максимально автоматизированных программно-аппаратных комплексов стандартной и тематической обработки первичной информации, архивации и распространения базовых информационных продуктов ДЗЗ межведомственного использования, ***с привлечением научно-практического потенциала ведущих институтов РАН и отраслевых центров мониторинга***

Тип КА	Тип аппаратуры ДЗЗ	Линейное разрешение (метры)	Спектральные диапазоны (мкм)	Прием данных ДЗЗ
Ресурс - ДК	Оптико-электронная: • панхроматическая; • многозональная	до 3 от 3,0 до 4,0	Панхроматический - 0,58 ÷ 0,8 Ближний ИК - 0,7 ÷ 0,8	До 6 раз в сутки, около 20 тыс. кв. км ежесуточно
Метеор - М	Оптико-электронная : • видимый диапазон; • инфракрасная; • многозональная	1000 4000 60 и 120	0,5 ÷ 0,6 3,5 ÷ 12,5 (6 каналов) 0,370 ÷ 0,900 (6 каналов)	2 раза в сутки. Глобальная съемка Земли в течение суток, до 8 сеансов. Съемка всей территории России в течение 4 сут.
Электро - Л	Оптико-электронная: • многозональная; • инфракрасная	1000 4000	0,5 ÷ 0,9 3,5 ÷ 12,5 (10 каналов)	Глобальная съемка восточного полушария Земли каждые 30 мин
Ресурс - П	Оптико-электронная: • панхроматическая; • многозональная; • гиперспектральная	0,9, 12, 60, 24 ÷120 30	0,58 ÷ 0,80 0,45 ÷ 0,90 (5 каналов) 0,40 ÷ 1,10 (до 150 каналов)	До 18 раз в сутки, около 250 тыс. кв. км ежесуточно
Канопус - В	Оптико-электронная: • панхроматическая; • многозональная.	2,5 12,0	0,58 ÷ 0,86 0,46 ÷ 0,84 (4 канала)	До 18 раз в сутки, около 100 тыс. кв. км ежесуточно
МКА ФКИ	Оптико-электронная: • многозональная; • гиперспектральная	120 50	0,48 ÷ 0,95 (4 канала) 0,40÷ 1,10 (до 150 каналов)	До 4 раз в сутки, ежесуточно 400 тыс. кв. км 35 тыс. кв. км
Кондор - Э	Радиолокационная	1 ÷ 2 – детальный режим 3 ÷ 5 – обзорный полосовой режим 5 ÷ 30 – обзорный маршрутный режим	S (10 см)	До 6 раз в сутки, около 110 тыс. кв. км высокого разрешения ежесуточно

ОСОБЕННОСТИ КОМПЛЕКСНОГО ПОДХОДА К ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ОСОБО ВАЖНЫХ ОБЪЕКТОВ

ПРЕДПРИЯТИЯ И ОРГАНИЗАЦИИ С ОСОБЫМИ УСТАВНЫМИ ЗАДАЧАМИ

- Места производства и хранения денег
- Места производства и хранения оружия, боеприпасов и военной техники
- Эксплуатация магистральных нефте- и газопроводов
- Особо опасные экологические производства
- Частные охранные предприятия
- Охрана природы и природных ресурсов

ОСОБЕННОСТИ КОМПЛЕКСНОГО ПОДХОДА К ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ОСОБО ВАЖНЫХ ОБЪЕКТОВ

СПЕЦИФИЧЕСКИЕ ЦЕЛЕВЫЕ РЕШЕНИЯ В ОБЛАСТИ БЕЗОПАСНОСТИ ДЛЯ ТЕХНОГЕННЫХ ОБЪЕКТОВ

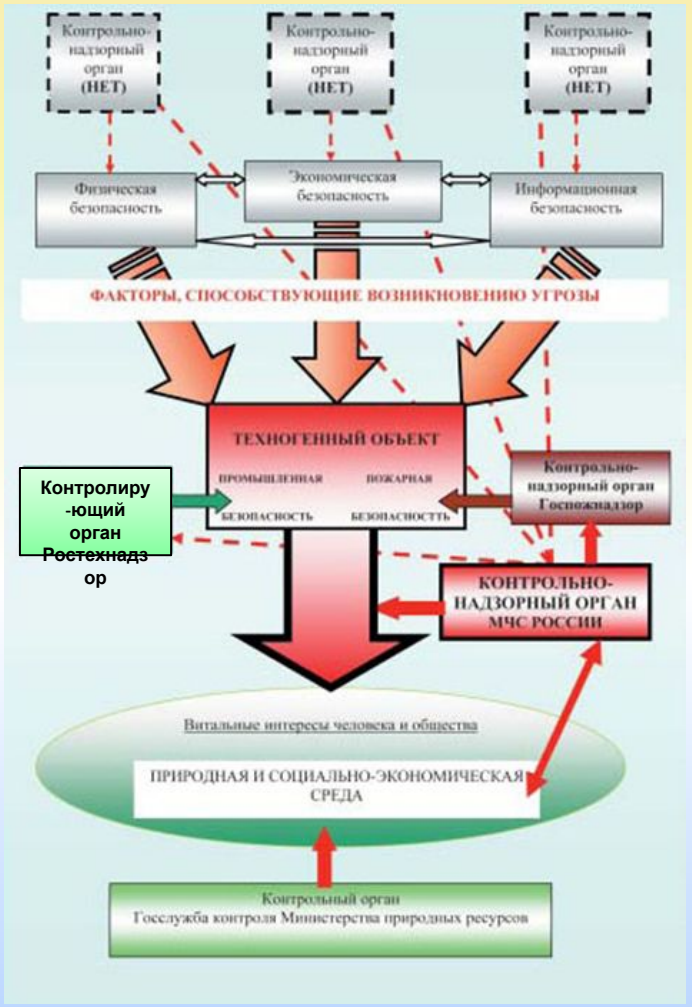
1) разработка и принятие адекватных организационных, административных и технических мер по вопросам применения технических средств и систем обеспечения безопасного функционирования объекта не только до совершения террористического акта, но и в период угрозы возникновения и наступления чрезвычайной ситуации, связанной с ним;

2) разработка и определение в окружающей обстановке и поведении лиц признаков, указывающих на совершение действий, направленных на подготовку и проведение террористического акта,, а также применение имеющихся и вновь создаваемых технических средств и систем обеспечения безопасности для их вы явления и пресечения;

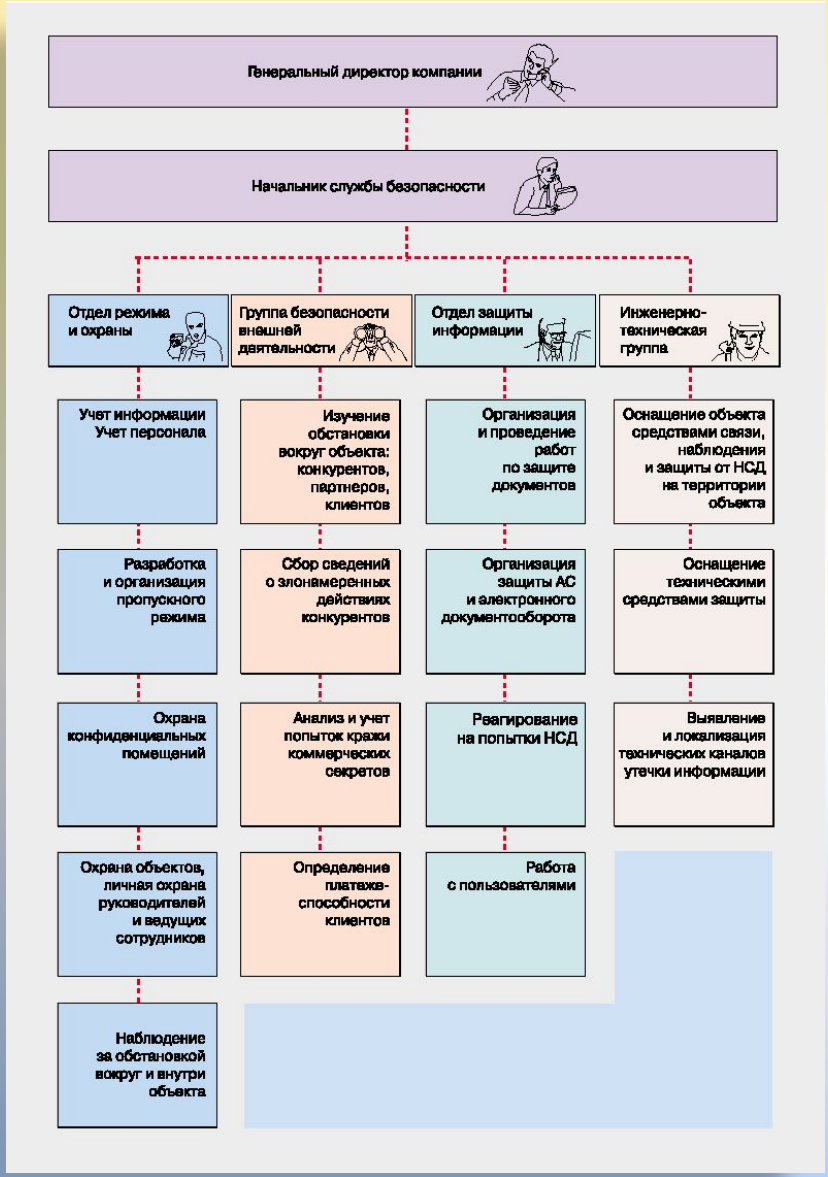
3) определение мест:
а) наиболее уязвимых с точки зрения возможности проведения террористических актов;
б) наиболее опасных по негативным последствиям в случае проведения на них терактов и диверсий, а также по оснащению этих мест техническими средствами и системами обеспечения безопасности;

4) обеспечение взаимодействия всех служб объекта, задействованных в организации антитеррористической защищенности объекта;

5) обеспечение надежной связи и взаимодействия службы безопасности объекта с правоохранительными органами, являющимися субъектами антитеррористической борьбы.



ПОДРАЗДЕЛЕНИЯ ТЕХНИЧЕСКОЙ ЗАЩИТЫ В СТРУКТУРЕ СБ ПРЕДПРИЯТИЯ РАЗГРАНИЧЕНИЕ ПОЛНОМОЧИЙ



ОСНОВНЫЕ ЗАДАЧИ ПОДРАЗДЕЛЕНИЯ ТЕХНИЧЕСКОЙ ЗАЩИТЫ

- 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 обеспечивающих требования безопасности.

Рекомендуемая литература