ОРГАНИЗАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Лекция № 3.

Организационное обеспечение физической защиты объекта информатизации

Лекция № 3.
Организационное обеспечение физической защиты объекта информатизации

ЦЕЛЬ ЗАНЯТИЯ: Рассмотреть особенности организации внутриобъектового режима на объекте информатизации

ВОПРОС 1. Содержание режимных мер по защите информации
ВОПРОС 2. Основные принципы построения и оптимизации системы внутриобъектового режима
ВОПРОС 3. Основные направления построения системы внутриобъектового режима
ВОПРОС 4. Основные характеристики интегрированной технической системы охраны
ВОПРОС 5. Особенности создания интеллектуального здания
ВОПРОС 6. Особенности информационных систем интеллектуального здания
ВОПРОС 7. Основные требования к архитектуре ИТСО

ВВЕДЕНИЕ

ОБЪЕКТ ИНФОРМАТИЗАЦИИ — совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров.

Национальный стандарт Российской Федерации ГОСТ Р 51275-2006.

Защита информации.

Объект информатизации.

Факторы, воздействующие на информацию. Общие положения.

ВВЕДЕНИЕ

ЗАЩИЩАЕМЫЙ ОБЪЕКТ ИНФОРМАТИЗАЦИИ — объект информатизации, предназначенный для обработки защищаемой информации с требуемым уровнем ее защищенности.

Национальный стандарт Российской Федерации ГОСТ Р 51275-2006.

Защита информации.

Объект информатизации.

Факторы, воздействующие на информацию. Общие положения.

ВВЕДЕНИЕ

ФИЗИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ — защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.

ПРИМЕЧАНИЯ:

1. Организационные мероприятия по обеспечению физической защиты информации предусматривают установление режимных, временных, территориальных, пространственных ограничений на условия использования и распорядок работы объекта защиты.

2. К объектам защиты информации могут быть отнесены: охраняемая территория, здание (сооружение), выделенное помещение, информация и (или) информационные ресурсы объекта информатизации.

Национальный стандарт Российской Федерации ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

ВВЕДЕНИЕ

ФИЗИЧЕСКАЯ ЗАЩИТА — средства, используемые для обеспечения физической защиты ресурсов от преднамеренной или случайной угрозы

Государственный стандарт Российской Федерации ГОСТ Р ИСО 7498-2-99
"Информационная технология.
Взаимосвязь открытых систем.
Базовая эталонная модель.
Часть 2.
Архитектура защиты информации"

Лекция № 3.

Организационное обеспечение физической защиты объекта информатизации

ВОПРОС 1.

Содержание режимных мер по защите информации

ВОПРОС 1.
Содержание режимных мер по защите информации

РЕЖИМ - 1. Установленный порядок чего-нибудь,

2. Условия деятельности, работы, существования чего-нибудь.

ВОПРОС 1.
Содержание режимных мер по защите информации

Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» ОПРЕДЕЛЕНО, что защита информации представляет собой принятие упреждающего комплекса защитных мер.

ВОПРОС 1.
Содержание режимных мер по защите информации

При этом ОБЛАДАТЕЛЬ ИНФОРМАЦИИ, ОПЕРАТОР информационной системы в случаях, установленных законодательством, обязаны обеспечить РЕЖИМНЫЕ меры:

1) ПРЕДОТВРАЩЕНИЕ несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
2) своевременное ОБНАРУЖЕНИЕ фактов несанкционированного доступа к информации;
3) ПРЕДУПРЕЖДЕНИЕ возможности неблагоприятных ПОСЛЕДСТВИЙ нарушения порядка доступа к информации;
4) НЕДОПУЩЕНИЕ ВОЗДЕЙСТВИЯ на технические средства обработки информации, в результате которого нарушается их функционирование;
5) ВОЗМОЖНОСТЬ незамедлительного ВОССТАНОВЛЕНИЯ информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
6) ПОСТОЯННЫЙ КОНТРОЛЬ за обеспечением уровня защищенности информации.

ВОПРОС 1.
Содержание режимных мер по защите информации

Физическая защита и защита от воздействий окружающей среды

1. Охраняемые зоны
2. Безопасность оборудования
3. Общие мероприятия по управлению информационной безопасностью
4. Административное управление защитой

ВОПРОС 1.
Содержание режимных мер по защите информации

1. Охраняемые зоны

ЦЕЛЬ УСТАНОВЛЕНИЯ ОХРАНЯЕМОЙ ЗОНЫ – предотвращение неавторизованного доступа, повреждения и воздействия в отношении помещений и информации организации.

Средства обработки критичной или важной служебной информации необходимо размещать в зонах безопасности, обозначенных определенным периметром безопасности, обладающим соответствующими защитными барьерами и средствами контроля проникновения.

Эти зоны должны быть физически защищены от неавторизованного доступа, повреждения и воздействия.

Уровень защищенности должен быть соразмерен с идентифицированными рисками.

С целью минимизации риска неавторизованного доступа или повреждения бумажных документов, носителей данных и средств обработки информации, рекомендуется внедрить политику "чистого стола" и "чистого экрана".

ВОПРОС 1.
Содержание режимных мер по защите информации

1. ОХРАНЯЕМЫЕ ЗОНЫ

1.1 Установление периметра охраняемой зоны

1.2 Организация контроля доступа в охраняемые зоны

1.3 Обеспечение безопасности зданий, производственных помещений и оборудования

1.4 Особенности выполнения работ в охраняемых зонах

1.5 Обеспечение безопасности зон приемки и отгрузки материальных ценностей

Лекция № 3.
Организационное обеспечение физической защиты объекта информатизации

ВОПРОС 2.

ОСНОВНЫЕ ПРИНЦИПЫ ПОСТРОЕНИЯ И ОПТИМИЗАЦИИ СИСТЕМЫ ВНУТРИОБЪЕКТОВОГО РЕЖИМА

ВОПРОС 2.
Основные принципы построения и оптимизации системы внутриобъектового режима

Формулируя концептуальные задачи обеспечения безопасности предприятия, следует выделить следующие принципы построения и оптимизации системы внутриобъектового режима объекта защиты:

1. **универсальность**, предполагающая, что все решения должны быть отработаны и унифицированы;
2. **комплексность**, предполагающая, что используемые приемы работы и применяемые ТС взаимоувязаны между собой, дополняют друг друга по функциональным и техническим показателям;
3. разумная **достаточность**, означающая, что мероприятия по обеспечению безопасности объекта должны быть адекватны возможным угрозам со стороны вероятного нарушителя по финансовым, материально-техническим и кадровым ресурсам;

ВОПРОС 2.
Основные принципы построения и оптимизации системы внутриобъектового режима

Формулируя концептуальные задачи обеспечения безопасности предприятия, следует выделить следующие принципы построения и оптимизации системы внутриобъектового режима объекта защиты:

4. оперативность, предполагающая приоритет методов и средств защиты, обеспечивающих быстрое обнаружение и последующую нейтрализацию возможных угроз;

5. адаптивность, предусматривающая, что методы и средства защиты могут быть достаточно гибко приспособлены к изменениям организационных и технических условий функционирования объекта;

6. непрерывность, систематичность, означающие, что выбранные решения обеспечат достаточно эффективную круглосуточную защиту объекта;

ВОПРОС 2.
Основные принципы построения и оптимизации системы внутриобъектового режима

Формулируя концептуальные задачи обеспечения безопасности предприятия, следует выделить следующие принципы построения и оптимизации системы внутриобъектового режима объекта защиты:

7. целеустремленность - сосредоточение усилий на защиту наиболее ценных ресурсов фирмы или наиболее уязвимых участков объекта;

8. многорубежность, предполагающая использование дополнительных пространственных рубежей безопасности или методов защиты для наиболее ответственных, с точки зрения безопасности, помещений и зон объекта;

9. равнопрочность создаваемых границ безопасности;

ВОПРОС 2.
Основные принципы построения и оптимизации системы внутриобъектового режима

Формулируя концептуальные задачи обеспечения безопасности предприятия, следует выделить следующие принципы построения и оптимизации системы внутриобъектового режима объекта защиты:

10. последовательность в использовании соответствующих методов и средств при обнаружении, отражении и ликвидации угроз безопасности объекта (так называемая эшелонированность безопасности);
11. совместимость с существующими системами;
12. простота, экологическая чистота и незаметность ("дружественность"), предполагающие, что развертываемая система не создаст дополнительных препятствий для нормального функционирования организации, не потребует очень высокой квалификации и длительной подготовки обслуживающего персонала, не причинит вреда защищаемым ценностям объекта;

ВОПРОС 2.
Основные принципы построения и оптимизации системы внутриобъектового режима

Формулируя концептуальные задачи обеспечения безопасности предприятия, следует выделить следующие принципы построения и оптимизации системы внутриобъектового режима объекта защиты:

13. неуязвимость — способность противостоять предпринимаемым попыткам выведения системы из строя;
14. документированность, предполагающая регистрацию интересующих событий, связанных с защищаемым объектом, что необходимо для последующего анализа тревожных и нештатных ситуаций и достигнутого уровня защищенности объекта;
15. законность, означающая, что все применяемые меры организационного и технического характера легальны и юридически обоснованы.

Лекция № 3.
Организационное обеспечение физической защиты объекта информатизации

ВОПРОС 3.
Основные направления построения системы внутриобъектового режима

ВОПРОС 3.
Основные направления построения системы внутриобъектового режима

Оптимальная политика при создании системы внутриобъектового режима состоит в том, чтобы, исходя из выделенных ресурсов и намеченных приоритетов, проводить требуемые мероприятия, предусматривающие постепенное повышение эффективности всей системы обеспечения безопасности.

Следовательно, при имеющихся ресурсах необходимо стремиться к тому, чтобы обеспечить максимально достижимый на данный момент времени уровень защиты объекта.

При проведении конкретных мероприятий по развертыванию такой системы необходимо придерживаться концептуальных положений обеспечения безопасности, учитывать и особенности защищаемого объекта и оперативную обстановку на текущий момент времени, что позволит достичь достаточно высокого уровня безопасности.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (организации) — формальное изложение правил поведения, процедур, практических приемов или руководящих принципов в области информационной безопасности, которыми руководствуется организация в своей деятельности.

ПРИМЕЧАНИЕ:

Политики должны содержать:

- **предмет, основные цели и задачи политики безопасности;**
- **условия применения политики безопасности и возможные ограничения;**
- **описание позиции руководства организации в отношении выполнения политики безопасности и организации режима информационной безопасности организации в целом;**
- **права и обязанности, а также степень ответственности сотрудников за выполнение политики безопасности организации;**
- **порядок действия в чрезвычайных ситуациях в случае нарушения политики безопасности.**

Национальный стандарт Российской Федерации ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ — совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

Национальный стандарт Российской Федерации ГОСТ Р 53113.1-2008. Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения

ВОПРОС 3.
Основные направления построения системы внутриобъектового режима

Разноплановые задачи по обеспечению состояния защищенности экономического пространства хозяйствующего субъекта обуславливают необходимость принятия комплексных, интегрированных решений.

Определенный уровень безопасности объекта может быть достигнут различными способами, например, путем использования многочисленного штата сотрудников охранных структур или установки нескольких автономных технических систем безопасности (ТСБ) разного типа.

ВОПРОС 3.
Основные направления построения системы внутриобъектового режима

В целях блокирования угроз применяются обычно такие традиционные ТСБ, как:

- **система контроля и управления доступом (СКУД);**
- **система пожарной сигнализации (включая аварийное оповещение и управление эвакуацией персонала и посетителей) (СПС);**
- **система охранной сигнализации (включая защиту периметра объекта и тревожное оповещение) (СОС);**
- **система видеоконтроля (СВК).**

ВОПРОС 3.
Основные направления построения системы внутриобъектового режима

Развертывание какой-либо отдельной автономной ТСБ требует, как правило, сравнительно небольших финансовых затрат за счет использования традиционной аппаратной базы и опробованных технических решений.

Применение тех или иных систем продиктовано зачастую определенным консерватизмом в области обеспечения безопасности и сложившимися предпочтениями заказчика и исполнителя работ по их установке.

Кроме того, подрядчик, выполняющий проектирование и монтаж ТСБ, склонен предлагать известные ему, обеспеченные ресурсами и опробованные (но часто не самые оптимальные) технические решения и аппаратные средства.

ВОПРОС 3.
Основные направления построения системы внутриобъектового режима

Установка всех необходимых для обеспечения эффективной защиты объекта систем требует, как правило, значительных затрат и приводит как к ненужному дублированию функций и высоким эксплуатационным расходам, так и к нестыковкам (отсутствию взаимодействия между отдельными системами).

В результате создается комплекс сложных в управлении, дорогостоящих систем безопасности, но с ограниченными возможностями.

При построении действительно эффективной комплексной технической системы охраны ее, как и всякую другую систему, необходимо рассматривать в целом, как единство организационно-технических мер, направленных на защиту объекта.

ВОПРОС 3.
Основные направления построения системы внутриобъектового режима

Глубокая интеграция ТСБ возможна только при поддержании на объекте основных, базовых уровней интеграции, опирающихся на организационно-административные способы защиты объекта, а также средства и методы инженерно-технической защиты.

Эти методы и средства носят универсальный характер.

Они обеспечивают защиту всех видов ценностей объекта при привлечении, как правило, минимально возможных ресурсов.

Базовые уровни особенно эффективны благодаря тому, что способствуют предотвращению угроз за счет создания тех или иных преград (физического или психологического характера) для потенциального нарушителя.

Лекция № 3.
Организационное обеспечение физической защиты объекта информатизации

ВОПРОС 4.
Основные характеристики интегрированной технической системы охраны

ВОПРОС 4. Основные характеристики интегрированной технической системы охраны

Интегрированная техническая система охраны (ИТСО) хозяйствующего субъекта, созданная на базе традиционных подсистем СКУД, СПС, СОС и СВК, обеспечивает, например, следующие виды взаимодействия между подсистемами:

- разблокировка дверей и проходов (СКУД), используемых при эвакуации, в зонах возможного пожара или по всему объекту при получении сигнала пожарной тревоги (от СПС);
- блокировка охранных зон, тамбуров и шлюзов (СКУД) при срабатывании различных охранных детекторов (в СОС) или детекторов активности от видеокамер (в СВК);
- использование тревожных сигналов (от СПС, СКУД и СОС) для подключения соответствующих видеокамер (СВК), что позволяет уточнить и документировать обстановку в зоне тревоги.

ВОПРОС 4. Основные характеристики интегрированной технической системы охраны

По сравнению с простой совокупностью отдельных систем и средств защиты применение интегрированных систем безопасности для организации внутриобъектового режима на предприятии обеспечивает следующие преимущества:

- более быструю и точную реакцию на происходящие события;
- оптимальный анализ текущих ситуаций;
- значительное снижение риска, связанного с "человеческим фактором" - ошибками и возможными недобросовестными действиями обслуживающего персонала и сотрудников фирмы;

ВОПРОС 4. Основные характеристики интегрированной технической системы охраны

По сравнению с простой совокупностью отдельных систем и средств защиты применение интегрированных систем безопасности для организации внутриобъектового режима на предприятии обеспечивает следующие преимущества:

- уменьшение затрат на оборудование ввиду многофункционального использования отдельных ТС и более полной их загрузки;
- облегчение работы обслуживающего персонала за счет автоматизации процессов управления, контроля и принятия решений по обеспечению безопасности;
- снижение затрат на монтаж и эксплуатацию системы безопасности, сокращение обслуживающего персонала и затрат на его обучение и содержание.

ВОПРОС 4. Основные характеристики интегрированной технической системы охраны

При построении и оптимизации ИТСО необходимо учитывать, что современным системам безопасности присущи все характерные признаки сложных человеко-машинных систем:

- наличие большого числа взаимосвязанных элементов;
- неопределенность из-за неполной информации о потенциальном нарушителе и его действиях;
- субъективизм, связанный с необходимостью принятия человеком важных оперативных решений;
- многообразие условий функционирования (различные условия эксплуатации, наличие естественных и промышленных помех).

ВОПРОС 4. Основные характеристики интегрированной технической системы охраны

При рассмотрении взаимодействия ИТСО и других систем объекта необходимо исходить из следующих положений:

- **всякая система является иерархической структурой, элементами и связями которой (как внутренними, так и внешними) нельзя пренебрегать;**
- **накопление и объединение свойств элементов системы приводит к появлению качественно новых свойств, не характерных для ее отдельных элементов;**
- **система работает тем лучше и устойчивее, чем меньше ее отдельные части взаимодействуют между собой и с окружающей средой.**

ВОПРОС 4. Основные характеристики интегрированной технической системы охраны

Любая система — составная часть влияющей на ее структуру и функционирование более сложной системы.

К такой системе более высокого уровня (по сравнению с ИТСО) можно отнести интегрированную техническую систему безопасности (ИТСБ), которая служит составной частью единой интегрированной системы объекта, объединяющей все инженерно-технические системы хозяйствующего субъекта.

ВОПРОС 4. Основные характеристики интегрированной технической системы охраны

ИНТЕГРИРОВАННАЯ ТЕХНИЧЕСКАЯ СИСТЕМА БЕЗОПАСНОСТИ
может охватывать такие системы, как:

- **информационно-аналитическая система, обеспечивающая задачи анализа рисков, возможных угроз, юридической защиты;**
- **система экономической безопасности, выполняющая задачи проверки клиентов, возврата кредитов, защиты от недобросовестной конкуренции;**
- **система собственной безопасности, обеспечивающая выполнение задач проверки сотрудников на лояльность, досмотра посетителей, персонала и корреспонденции, контроля систем жизнеобеспечения объекта, экологического мониторинга;**

ВОПРОС 4. Основные характеристики интегрированной технической системы охраны

ИНТЕГРИРОВАННАЯ ТЕХНИЧЕСКАЯ СИСТЕМА БЕЗОПАСНОСТИ может охватывать такие системы, как:

- система защиты информации в информационно-вычислительных и телекоммуникационных сетях;
- система защиты информации от утечки по техническим каналам;
- система автоматического пожаротушения и дымоудаления;
- система физической охраны объекта;
- система обеспечения безопасности автоперевозок.

Лекция № 3.
Организационное обеспечение физической защиты объекта информатизации

ВОПРОС 5.
Особенности создания интеллектуального здания

ВОПРОС 5.
Особенности создания интеллектуального здания

Наиболее эффективные решения интегрированной системы здания находятся в области концепции "интеллектуального здания" (ИЗ), когда на базе новейших информационных технологий интегрируются не только системы инженерного обеспечения здания, но и телекоммуникационные, вычислительные системы, а также технические системы безопасности.

"Интеллектуальное здание" обеспечивает эффективное использование рабочего пространства благодаря оптимизации всех его структур, систем, служб и связей между ними.

ВОПРОС 5.
Особенности создания интеллектуального здания

Неотъемлемая часть ИЗ — структурированная кабельная сеть (СКС) — иерархическая базовая кабельная система здания, являющаяся, по существу, элементом его капитального строительства.

СКС позволяет объединить в единую систему все проводные системы объекта.

Структурированная сеть требует значительных первоначальных затрат, что обусловлено использованием достаточно дорогого оборудования (категорированного высокочастотного кабеля, коммутационной аппаратуры, качественных кабелепроводов).

ВОПРОС 5.
Особенности создания интеллектуального здания

Кабелепроводы СКС и розетки различного назначения позволяют подключать офисную и информационно-вычислительную аппаратуру, телекоммуникационную технику, электробытовые приборы, ТС безопасности, датчики систем жизнеобеспечения.

Интеллектуальное здание конфигурируется так, чтобы функциональные возможности всех его систем можно было бы наращивать по мере появления дополнительных средств или потребностей.

Важно также, что ИЗ готово к восприятию новых технологий и последовательной модернизации своих систем в течение весьма длительного периода (15-20 лет).

ВОПРОС 5.
Особенности создания интеллектуального здания

Концепция ИЗ предполагает интеграцию самых разнообразных инженерно-технических и организационно-административных систем.

Такая интеграция способствует оптимизации деловых процессов фирмы, в которые вовлечены кадровые, материальные, финансовые и информационные ресурсы, и значительному повышению эффективности работы фирмы за счет реинжиниринга бизнеса.

ВОПРОС 5.
Особенности создания интеллектуального здания

Информационные системы объекта представляют собой проводные слаботочные системы (могут быть также системы, использующие радио и оптический каналы) не энергетического назначения, отличающиеся по следующим направлениям использования:

- **связь и передача информации;**
- **управление эксплуатацией здания;**
- **обеспечение безопасности объекта;**
- **обеспечение бизнес-процессов фирмы;**
- **обеспечение отдыха и комфортных условий работы.**

Лекция № 3.
Организационное обеспечение физической защиты объекта информатизации

ВОПРОС 6.
ОСОБЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ИНТЕЛЛЕКТУАЛЬНОГО ЗДАНИЯ

ВОПРОС 6.
Особенности информационных систем интеллектуального здания

Информационные системы интеллектуального здания хозяйствующего субъекта можно условно разделить на следующие системы:

1. Информационно-телекоммуникационная система (ИТКС) в ориентировочном составе:

- **локальная вычислительная сеть (ЛВС);**
- **система учрежденческой автоматической телефонной связи, обеспечивающая коммутируемую и прямую телефонную связь, диспетчерскую связь, конференц-связь.**

ВОПРОС 6.
Особенности информационных систем интеллектуального здания

Информационные системы интеллектуального здания хозяйствующего субъекта можно условно разделить на следующие системы:

2. Система управления эксплуатацией (СУЭ) объекта - ориентировочно в ее состав могут входить следующие системы:

- **управления водоснабжением и канализацией;**
- **обеспечения кондиционирования и вентиляции воздуха;**
- **управления лифтовым оборудованием;**
- **контроля основных энергетических показателей;**
- **обеспечения экологического мониторинга;**
- **предотвращения оледенения элементов строительных конструкций и дренирования ливневых вод;**
- **управления автостоянками.**

ВОПРОС 6.
Особенности информационных систем интеллектуального здания

Информационные системы интеллектуального здания хозяйствующего субъекта можно условно разделить на следующие системы:

3. Интегрированная техническая система охраны - в ее состав ориентировочно входят системы:

- **контроля и управления доступом (СКУД);**
- **пожарной сигнализации (СПС);**
- **аварийного оповещения и управление эвакуацией персонала и посетителей (СОУЭ);**
- **охранной сигнализации (включая защиту периметра и тревожную сигнализацию) (СОС);**
- **видеоконтроля (СВК).**

ВОПРОС 6.
Особенности информационных систем интеллектуального здания

Информационные системы интеллектуального здания хозяйствующего субъекта можно условно разделить на следующие системы:

4. Технологические системы объекта, например, такие системы, как:

- **робототехнических производственных линий для заводов;**
- **обеспечения дилинг-процессов банков;**
- **досмотра покупателей и предотвращения краж магазинов;**
- **вызова, связи и сигнализации больниц;**
- **замкнутого телевидения для учебных заведений.**

ВОПРОС 6.
Особенности информационных систем интеллектуального здания

Информационные системы интеллектуального здания хозяйствующего субъекта можно условно разделить на следующие системы:

5. Обеспечивающие системы - ориентировочно они могут включать системы:

- **электрочасофикации и синхронизации;**
- **проводной радиотрансляции;**
- **управления звуком, обеспечивающая местное громкоговорящее вещание и оповещение, озвучивание залов заседаний и переговорных комнат;**
- **коллективного приема телевизионных сигналов.**

ВОПРОС 6.
Особенности информационных систем интеллектуального здания

Правильно построенная ИТСО взаимодействует с другими техническими системами здания по следующим позициям:

- **формирование необходимой структуры и конфигурирование системы при использовании кабелепроводов, проводных каналов и коммутационных возможностей СКС объекта;**
- **обеспечение бесперебойного и защищенного электропитания системы при подключении к промышленной сети электроснабжения, системам резервированного питания, заземления и молниезащиты;**
- **создание надежного распределенного управления системой при подключении к ЛВС;**
- **удаленный контроль системы при использовании телекоммуникационных линий и сетей;**

ВОПРОС 6.
Особенности информационных систем интеллектуального здания

Правильно построенная ИТСО взаимодействует с другими техническими системами здания по следующим позициям:

- **блокировка или активация отдельных ТС и систем при обнаружении угроз (принудительный пуск всех лифтов вниз и их отключение, переключение огнезадерживающих и герметизирующих заслонок и клапанов на воздуховодах, отключение систем вентиляции);**

- **активация систем защиты информации (ограничение доступа к ресурсам информационно-вычислительных сетей, обнаружение и подавление средств несанкционированного съема информации) в соответствующих зонах при обнаружении тревожных ситуаций.**

ВОПРОС 6.
Особенности информационных систем интеллектуального здания

Правильно построенная ИТСО взаимодействует с другими техническими системами здания по следующим позициям:

- повышение эффективности визуального контроля, надежности и оперативности выполнения эвакуационных мероприятий при привлечении возможностей системы освещения;
- оповещение внешних организаций с целью ликвидации угроз объекту при подключении к городской телефонной сети;
- запуск систем пожаротушения и дымоудаления при обнаружении возгораний;

Лекция № 3.
Организационное обеспечение физической защиты объекта информатизации

ВОПРОС 7.
Основные требования к архитектуре ИТСО

ВОПРОС 7.
Основные требования к архитектуре ИТСО

Архитектура Интегрированной технической системы охраны должна удовлетворять следующим основным требованиям

- **открытая расширяемая архитектура с возможностью наращивания аппаратных средств и количества пользователей;**
- **возможность работы в сети типа клиент-сервер;**
- **открытое программное обеспечение (работающее в среде надежной операционной системы) с возможностью расширения функций и наращивания пользовательских модулей, допускающее автономную работу контроллеров при нарушении связи с центральным компьютером системы;**

ВОПРОС 7.
Основные требования к архитектуре ИТСО

Архитектура Интегрированной технической системы охраны должна удовлетворять следующим основным требованиям

- **интерактивный, графический, ориентированный на работу с меню интерфейс оператора, позволяющий отображать планы помещений объекта с точками управления и контроля;**
- **возможность конфигурирования системы - настройки всех реакций системы, графического изображения, содержания текстовых, речевых и звуковых сообщений;**
- **защита доступа к функциям системы и ее информационным ресурсам;**

ВОПРОС 7.
Основные требования к архитектуре ИТСО

Архитектура Интегрированной технической системы охраны должна удовлетворять следующим основным требованиям

- защита доступа к функциям системы и ее информационным ресурсам;
- обработка и ведение журнала событий и других баз данных системы и вывод результатов на печать в виде отчетов;
- обеспечение программных приложений для отдельных подсистем ИТСО;
- ввод, редактирование и архивирование текстовых и фотографических данных, а также видеосигналов;
- возможность обучение и консультирования оператора.

ВОПРОС 7.
Основные требования к архитектуре ИТСО

В качестве линий связи Интегрированной технической системы охраны ИТСО можно использовать:

- **радиолинии;**
- **силовые провода переменного тока сети электроснабжения;**
- **стандартные телефонные провода;**
- **коаксиальные кабели;**
- **оптоковолоконные кабели;**
- **проводные витые пары**

ВОПРОС 7.
Основные требования к архитектуре ИТСО

Особое внимание необходимо обратить на выбор оборудования с высокой эксплуатационной надежностью, большим гарантийным сроком эксплуатации и хорошей технической поддержкой в процессе эксплуатации.

Характерные особенности отечественных ТС - относительная дешевизна, адаптированность к отечественным нормам и стандартам, возможность работы по отечественным сетям, каналам и линиям связи, хорошая ремонтно-сервисная база, возможность поставки доработанных средств или программного обеспечения по особому заказу.

ВОПРОС 7.
Основные требования к архитектуре ИТСО

Вместе с тем они имеют такие (чисто российские) недостатки:

— неполнота эксплуатационной и конструкторской документации

— несоответствие ее требованиям отдельных стандартов,

— невысокая надежность вследствие упрощенного подхода к их разработке,

— слабая отработка технологических процессов.

Импортные ТС отличаются, как правило, более высокими потребительскими характеристиками и надежностью в эксплуатации, расширенным пользовательским сервисом и автоматизацией.

ВОПРОС 7.
Основные требования к архитектуре ИТСО

Вместе с тем необходимо учитывать, что при использовании зарубежных ТС может возникнуть ряд трудностей, в том числе:

- **неприспособленность к условиям эксплуатации в России (иные климатические факторы, перебои в электропитании, несовершенные линии связи, вандализм);**

- **отсутствие русифицированного программного обеспечения и документации, несоответствие отечественным стандартам;**

- **несовершенство гарантийного и послегарантийного обслуживания ввиду недостаточного опыта работы отечественных фирм-поставщиков с зарубежными ТС или потерь времени и средств при прямом обращении к фирме-изготовителю;**

ВОПРОС 7.
Основные требования к архитектуре ИТСО

- необходимость содержания сертифицированных специалистов, прошедших обучение для работы с зарубежными ТС и системами, либо отсутствие системы обучения персонала особенностям эксплуатации ТС;
- трудности сопряжения с уже находящейся в эксплуатации отечественной аппаратурой;
- невозможность сертификации ТС и систем из-за несоответствия отдельных параметров аппаратуры действующим требованиям или отказа зарубежных производителей предоставить необходимые данные;
- возможность установки программных или аппаратных закладных устройств несанкционированного съема конфиденциальной информации (что особенно опасно для отдельных пользователей).

ВОПРОС 7.
Основные требования к архитектуре ИТСО

При выборе ТС и построении системы предпочтение следует отдавать тем из них, которые обеспечивают:

- **наиболее эффективные технические решения при прогнозировании и предупреждении возможных угроз;**
- **минимизацию времени, необходимого для обнаружения угрозы;**
- **повышение надежности функционирования и обеспечению высокой живучести системы.**

ВОПРОС 7.
Основные требования к архитектуре ИТСО

Всякая система охраны (система раннего обнаружения угроз) так или иначе сводится к следующим устройствам:

- **чувствительные охранные детекторы-извещатели, обнаруживающие угрозы безопасности объекта;**
- **устройства доставки, сбора и обработки информации от извещателей и принятия решений по тревожным ситуациям;**
- **регистрирующие и оповещающие устройства.**

ВОПРОС 7.
Основные требования к архитектуре ИТСО

В качестве чувствительного детектора в технических системах безопасности - подсистемах ИТСО выступают такие устройства, как пожарные извещатели, охранные детекторы или видеокамеры.

Тенденция развития охранных систем заключается в своеобразной "конвергенции" указанных ТС в многопараметрические датчики, отслеживающие процессы наступления угроз объекту и принимающие решение о тревоге в ходе многокритериального анализа.

ВОПРОС 7.
Основные требования к архитектуре ИТСО

Устройствами обработки информации могут служить как собственные ТС отдельных ТСБ — подсистем ИТСО, так и общий компьютер системы.

ИТСО регистрирует все тревожные ситуации на выбранных носителях (специальный видеомагнитофон круглосуточной записи, магнитные носители компьютера).

Оповещение о тревожных ситуациях может быть как внутренним — в пределах зоны обнаружения тревоги (на выделенных мониторах и звуковых терминалах), так и внешним — по существующим каналам информационных и телекоммуникационных сетей.

СПАСИБО ЗА ВНИМАНИЕ