Основы информационной безопасности критически важных объектов

Учебная дисциплина ОИБ КВО

Тема 10

Информационная безопасность и системы физической защиты критически важных объектов (ИБ и СФЗ КВО)

Толстой Александр Иванович

к.т.н., доцент

Кафедра «Информационная безопасность банковских систем»

Институт интеллектуальных кибернетических систем

Факультет «Кибернетика и информационная безопасность»

НИЯУ МИФИ

Москва, 2017

Содержание

Тема 10. ИБ и СФЗ КВО:

10.1.Введение

10.2. СФЗ как поддерживающая система обеспечения безопасности информации на объекте

10.3.Обеспечение безопасности информации в самой СФЗ.

10.4. Обеспечение ИБ СФЗ ядерных объектов

10.5. Обеспечение ИБ систем учета и контроля ядерных материалов

10.6. Обеспечение ИБ при использовании систем связи на ядерных объектах

Критически важные объекты

Критически важные объекты

↓

Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации

(Утверждены Президентом Российской Федерации Д.Медведевым 3 февраля 2012 г., № 803)

Критически важные объекты

↓

Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации

(Утверждены Президентом Российской Федерации Д.Медведевым 3 февраля 2012 г., № 803)

↑

Критически важный объект инфраструктуры Российской Федерации (далее - критически важный объект) - объект, нарушение (или прекращение) функционирования которого приводит к потере управления, разрушению инфраструктуры, необратимому негативному изменению (или разрушению) экономики страны, субъекта Российской Федерации либо административно- территориальной единицы или существенному ухудшению безопасности жизнедеятельности населения, проживающего на этих территориях, на длительный срок

Критически важные объекты

Рекомендации по гармонизации законодательства государств – членов Организации Договора о коллективной безопасности (ОДКБ) в сфере обеспечения безопасности критически важных объектов

(Приняты Постановление Парламентской Ассамблеи ОДКБ 27.11.2014 года № 7-5):

Государства – члены ОДКБ: Российская Федерация, Республика Белорусь, Республика Казахстан, Республика Таджикистан, Кыргызская Республика, Республика Армения.

Критически важные объекты - объекты социальной, производственной, инженерной, транспортной, энергетической, информационно-коммуникационной и иной инфраструктуры, нарушение функционирования которых в результате акта терроризма, также других негативных воздействий, может оказать влияние на принятие органами власти решений, воспрепятствовать политической или иной общественной деятельности, спровоцировать осложнение международных отношений или войну, устрашить население, дестабилизировать общественный порядок и (или) повлечь за собой человеческие жертвы, причинение вреда здоровью людей или окружающей среде, значительный материальный ущерб и нарушение условий жизнедеятельности людей.

Критически важные объекты

Рекомендации по гармонизации законодательства государств – членов Организации Договора о коллективной безопасности (ОДКБ) в сфере обеспечения безопасности критически важных объектов

(Приняты Постановление Парламентской Ассамблеи ОДКБ 27.11.2014 года № 7-5):

Государства – члены ОДКБ: Российская Федерация, Республика Белорусь, Республика Казахстан, Республика Таджикистан, Кыргызская Республика, Республика Армения.

Обеспечение безопасности критически важных объектов - реализация определяемой государством-членом ОДКБ системы правовых, экономических, организационных и иных мер, направленных на обеспечение состояния защищенности критически важных объектов.

Критически важные объекты

Рекомендации по гармонизации законодательства государств – членов Организации Договора о коллективной безопасности (ОДКБ) в сфере обеспечения безопасности критически важных объектов

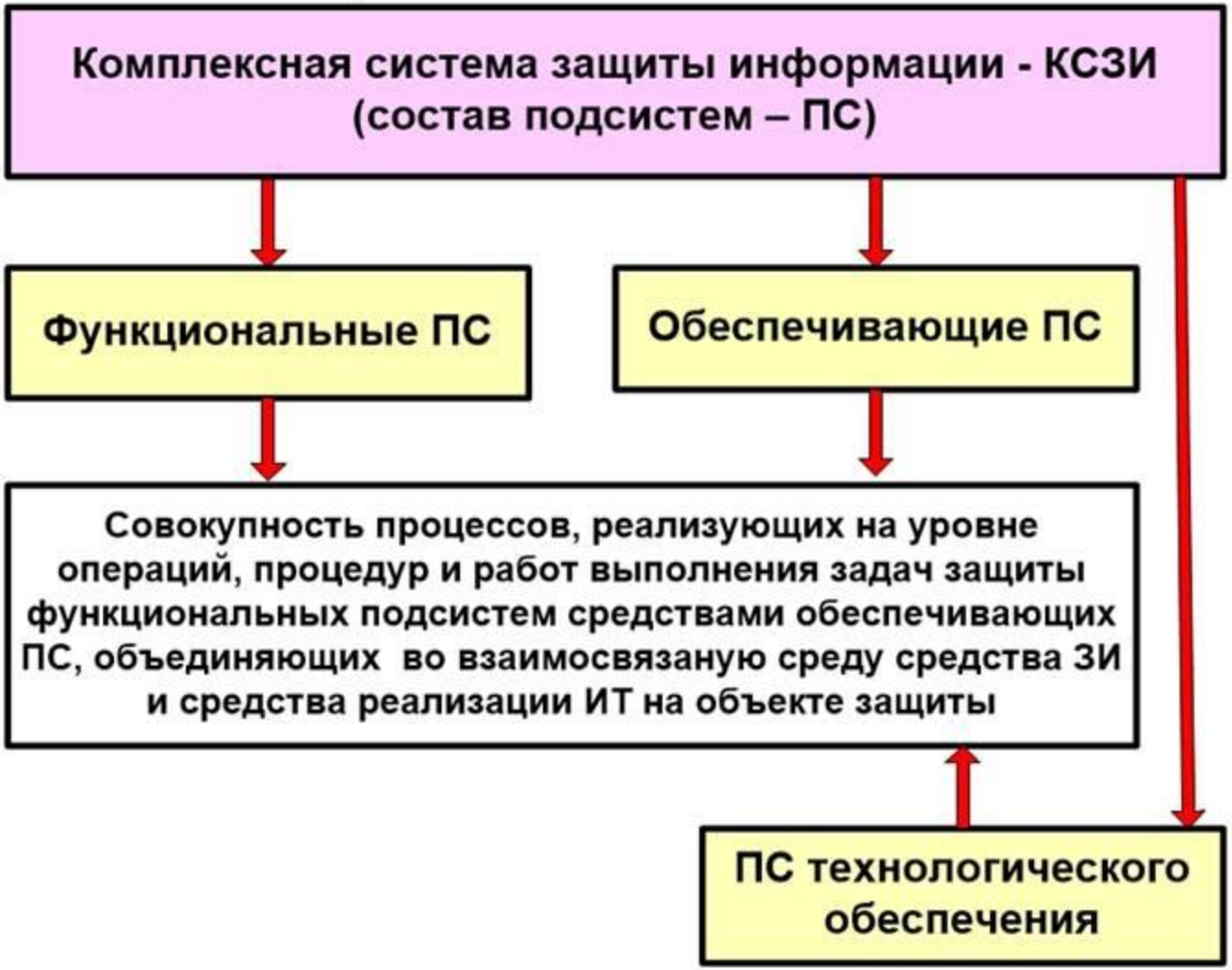
(Приняты Постановление Парламентской Ассамблеи ОДКБ 27.11.2014 года № 7-5):

Государства – члены ОДКБ: Российская Федерация, Республика Белорусь, Республика Казахстан, Республика Таджикистан, Кыргызская Республика, Республика Армения.

Критические элементы критически важных объектов - зоны, территории, административно-производственные здания и сооружения, конструктивные и технологические элементы критически важного объекта, элементы систем, оборудования или устройств потенциально опасной установки, места использования, хранения и уничтожения опасных веществ и материалов, несанкционированные действия в отношении которых приводят к прекращению нормального функционирования критически важно объекта, его повреждению или аварии, или созданию угрозы возникновения чрезвычайной ситуации.

СФЗ как поддерживающая система обеспечения безопасности информации на объекте

***«Комплексная система защиты информации» (КСЗИ)*- совокупность различных подсистем.**



СФЗ как поддерживающая система обеспечения безопасности информации на объекте

***«Комплексная система защиты информации» (КСЗИ)*- совокупность различных подсистем.**

Система физической защиты (ФЗ):

Комплекс: инженерно-технических средств и организационных мероприятий, направленных на обеспечение безопасности на объекте.

Совокупность: 1) организационных мероприятий ,
2) инженерно-технических средств, 3) действий подразделений охраны с целью обеспечение безопасности на объекте.

Б (защищаемого объекта) - состояние защищенности объекта от угроз причинения ущерба (вреда)……..
(ГОСТ Р 53704-2009 «Системы безопасности комплексные и интегрированные. Общие технические требования»).

Система физической защиты и обеспечение ИБ:

1. СФЗ как поддерживающая система обеспечения безопасности информации на объекте

2. Обеспечение безопасности информации в самой СФЗ

Система физической защиты и обеспечение ИБ:

1. СФЗ как поддерживающая система обеспечения безопасности информации на объекте

2. Обеспечение безопасности информации в самой СФЗ

10.2. СФЗ как поддерживающая система обеспечения безопасности информации на объекте

ГОСТ Р ИСО/МЭК 27002-2012 «ИТ. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента ИБ»:

9 Физическая безопасность и защита от воздействий окружающей среды

10.1 Зоны безопасности

12

10.2. СФЗ как поддерживающая система обеспечения безопасности информации на объекте

ГОСТ Р ИСО/МЭК 27002-2012 «ИТ. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента ИБ»:
9 Физическая безопасность и защита от воздействий окружающей среды
10.1 Зоны безопасности

Цель: Предотвращать неавторизованный физический доступ, повреждение и воздействие в отношении помещений и информации организации.

Средства обработки критической или чувствительной информации необходимо размещать в зонах безопасности, обозначенных определенным периметром безопасности, обладающим соответствующими защитными барьерами и средствами, контролирующими вход. Эти зоны должны быть физически защищены от неавторизованного доступа, повреждения и воздействия.

Уровень защищенности должен быть соразмерен выявленным рискам.

10.2. СФЗ как поддерживающая система обеспечения безопасности информации на объекте: ГОСТ Р ИСО/МЭК 27002-2012 (Физическая безопасность и защита от воздействий окружающей среды)

10.1.1 … Для защиты зон, которые содержат информацию и средства обработки информации, следует использовать периметры безопасности (барьеры, например стены, управляемые картами доступа ворота или турникеты, управляемые человеком).

10.1.2 … Зоны безопасности необходимо защищать с помощью соответствующих мер и средств контроля и управления входа, чтобы обеспечить уверенность в том, что доступ разрешен только авторизованному персоналу.

10.1.3 … Необходимо разработать и реализовать ФЗ зданий, производственных помещений и оборудования.

10.1.4 … Необходимо разработать и реализовать ФЗ от нанесения ущерба, который может явиться результатом пожара, наводнения, землетрясения, взрыва, общественных беспорядков и других форм природных или антропогенных бедствий.

10.1.5 … Необходимо разработать и реализовать ФЗ и рекомендации по работе в зонах безопасности.

10.1.6 Зоны общего доступа, приемки и отгрузки… должны быть изолированы от средств обработки информации, во избежание неавторизованного доступа.

10.2. СФЗ как поддерживающая система обеспечения безопасности информации на объекте: ГОСТ Р ИСО/МЭК 27002-2012 (Физическая безопасность и защита от воздействий окружающей среды)

10.2 Безопасность оборудования

Цель: Предотвращать потерю, повреждение, кражу или компрометацию активов и прерывание деятельности организации. Оборудование необходимо защищать от физических угроз и воздействия окружающей среды.

Обеспечение безопасности оборудования (включая используемое вне организации и выносимое имущество) необходимо для уменьшения риска неавторизованного доступа к информации и защиты ее от потери или повреждения.

При этом следует учесть размещение и утилизацию оборудования. Могут потребоваться специальные меры и средства контроля и управления для … защиты инфраструктуры поддерживающих услуг, например системы электропитания и кабельной разводки.

10.2. СФЗ как поддерживающая система обеспечения безопасности информации на объекте: ГОСТ Р ИСО/МЭК 27002-2012 (9 Физическая безопасность и защита от воздействий окружающей среды)

10.2 Безопасность оборудования

10.2.1 … Оборудование должно быть размещено и защищено так, чтобы уменьшить риски от угроз окружающей среды и возможности неавторизованного доступа.

10.2.2 … Оборудование необходимо защищать от перебоев подачи электроэнергии и других сбоев, связанных с перебоями в обеспечении поддерживающих услуг.

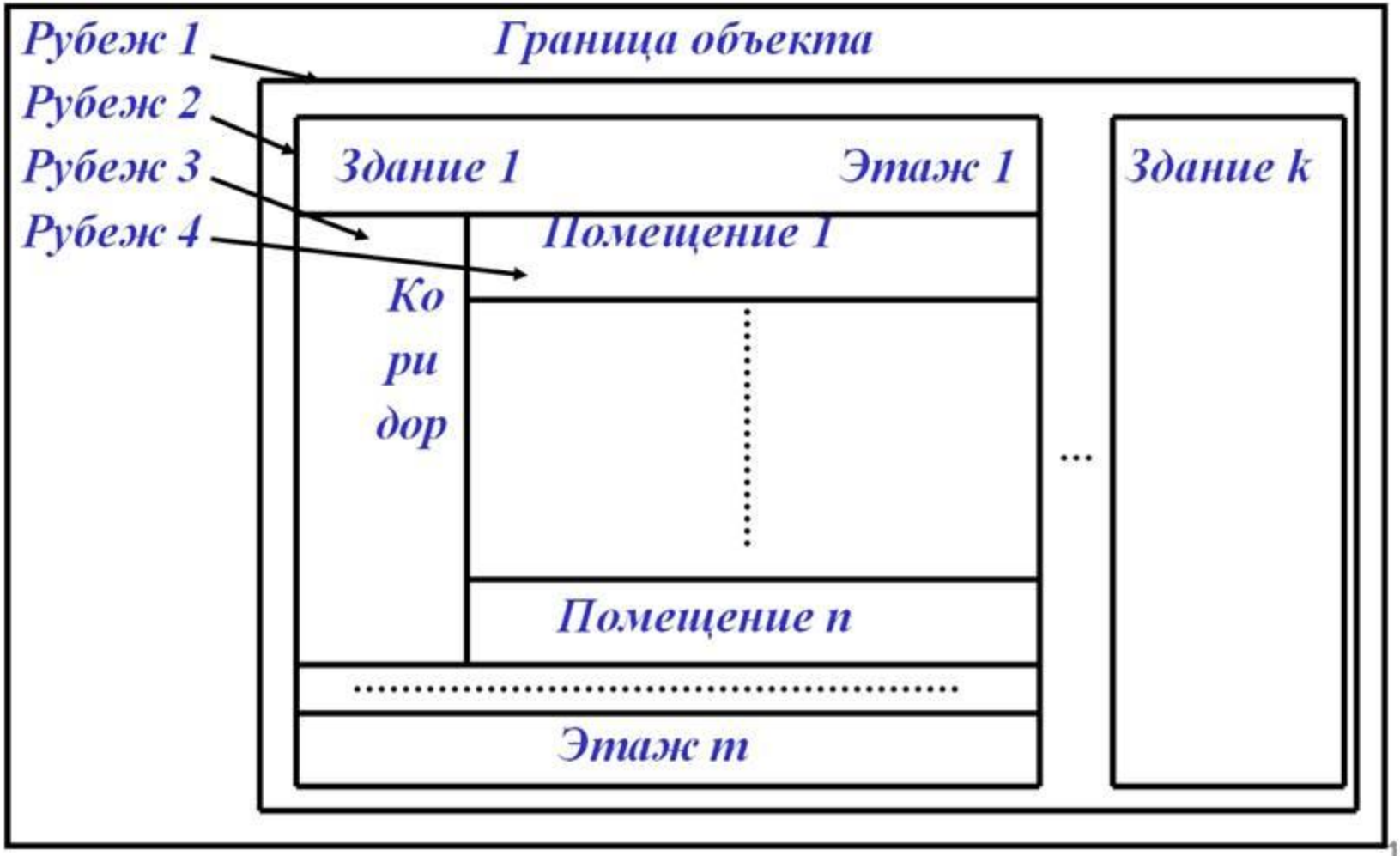
10.2.3 … Силовые и телекоммуникационные кабельные сети, по которым передаются данные или поддерживающие информационные услуги, необходимо защищать от перехвата информации или разрушения.

10.2.4 … Должно проводиться надлежащее техническое обслуживание оборудования для обеспечения его непрерывной доступности и целостности.

10.2.6 … (при утилизации) Все компоненты оборудования, содержащие носители данных, следует проверять с целью обеспечения уверенности в том, что любые чувствительные данные и лицензионное программное обеспечение были удалены или перезаписаны безопасным образом до их утилизации.

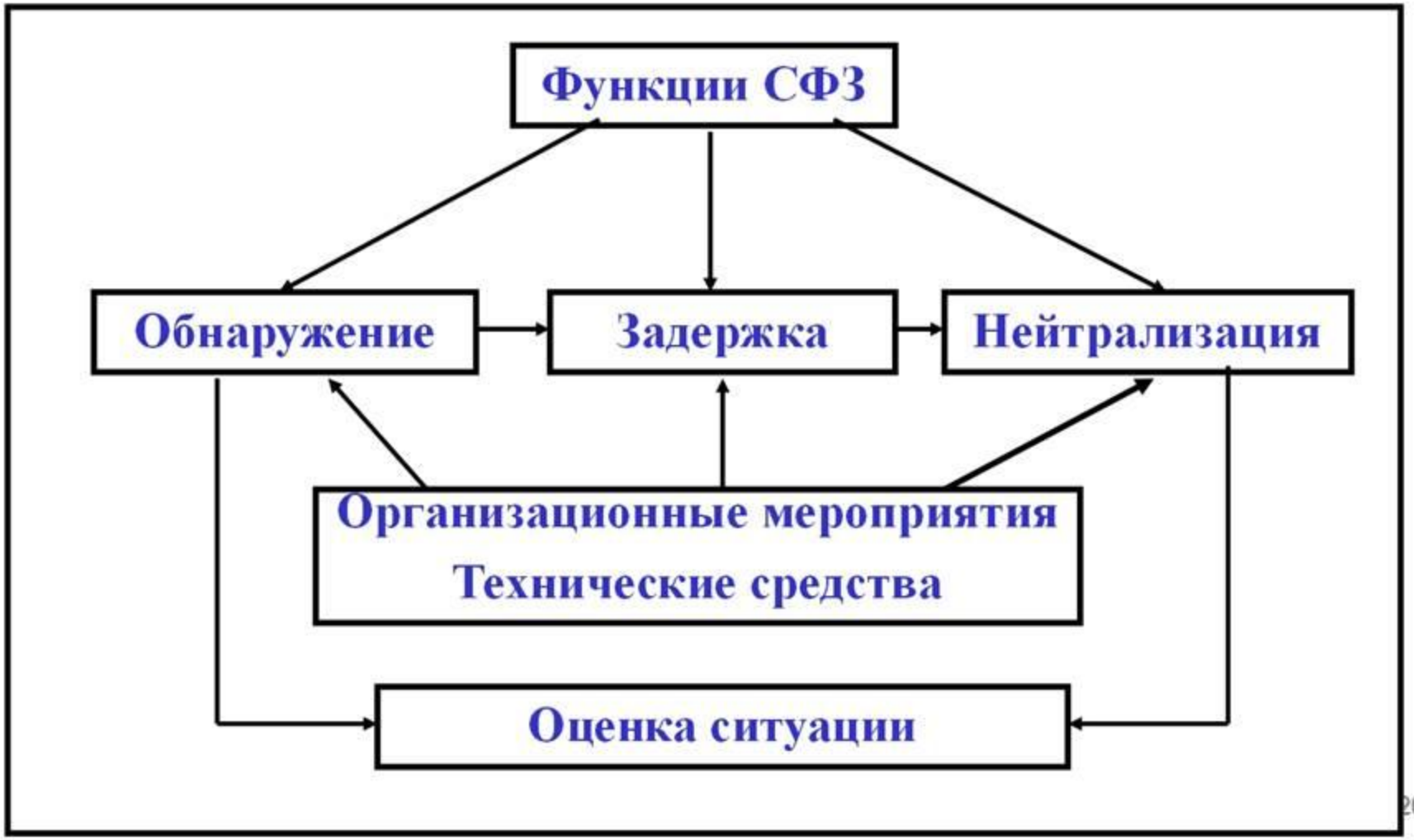
10.2. СФЗ как поддерживающая система обеспечения безопасности информации на объекте:

Принцип построения СФЗ: рубежность, эшелонирование, равнопрочность



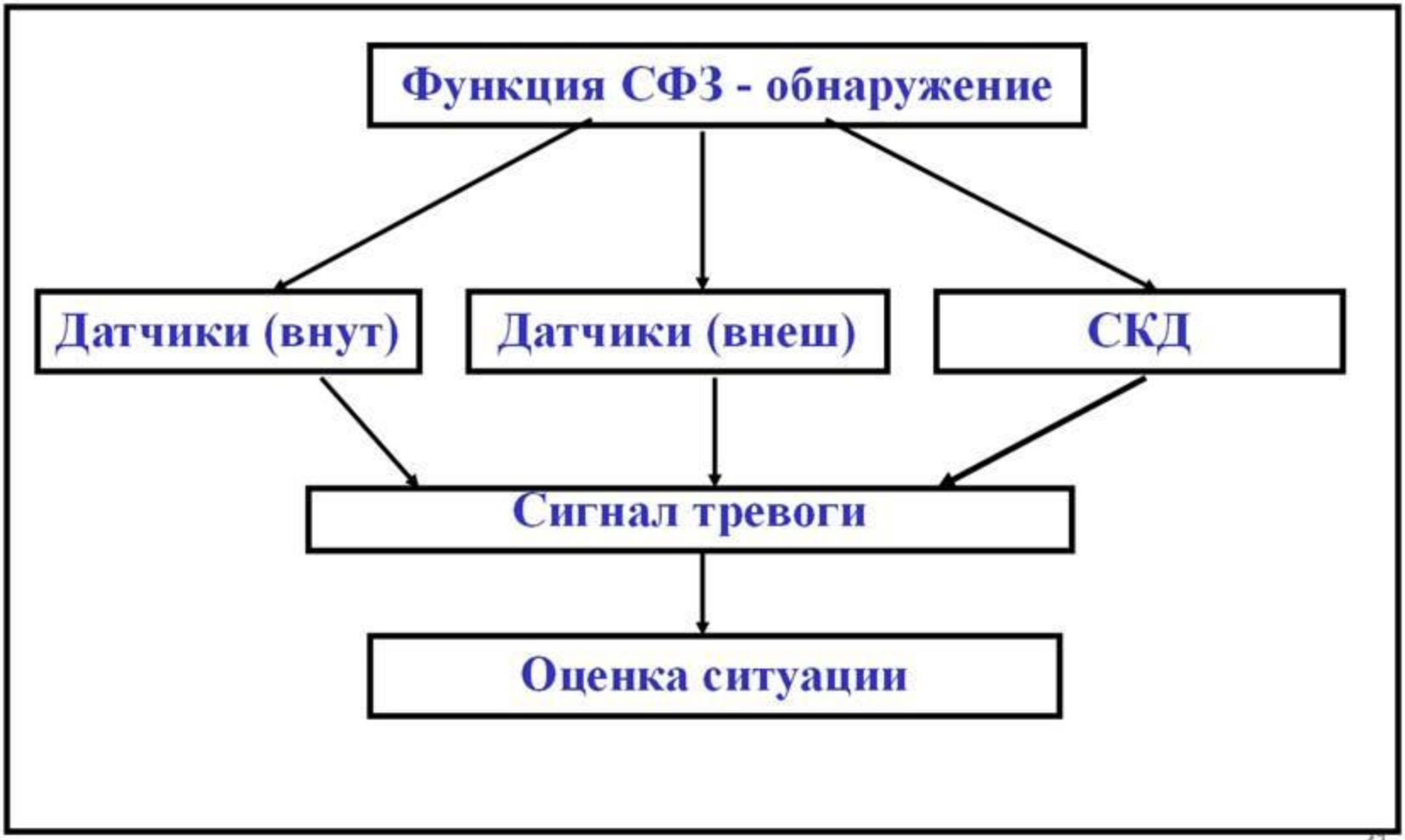
10.2. СФЗ как поддерживающая система обеспечения безопасности информации на объекте:

Функции СФЗ



10.2. СФЗ как поддерживающая система обеспечения безопасности информации на объекте:

Функции СФЗ: «обнаружение»



10.2. СФЗ как поддерживающая система обеспечения безопасности информации на объекте:

Структура СФЗ

10.2. СФЗ как поддерживающая система обеспечения безопасности информации на объекте:

Дополнительная информация (самостоятельное изучение):

Физическая защита ядерных объектов: Учебное пособие для вузов/ П.В.Бондарев, А.В.Измайлов, А.И.Толстой; Под ред. Н.С.Погожина.- М.: МИФИ, 2008.- 584 с.

Стр. 8 - 32

Глава 1. Методологические основы построения СФЗ объектов

Система физической защиты и обеспечение ИБ:

1. СФЗ как поддерживающая система обеспечения безопасности информации на объекте

2. Обеспечение безопасности информации в самой СФЗ

Система физической защиты и обеспечение ИБ:

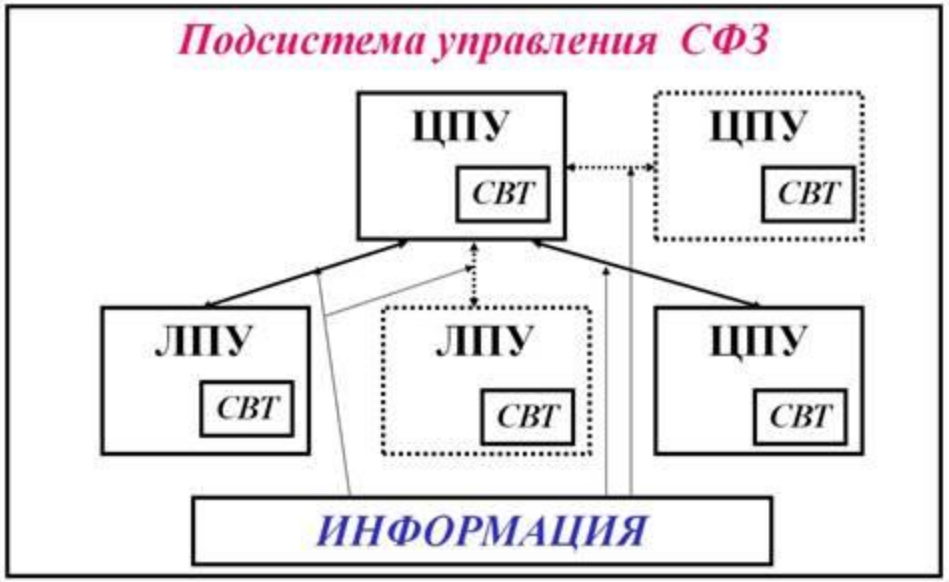
1. СФЗ как поддерживающая система обеспечения безопасности информации на объекте

2. Обеспечение безопасности информации в самой СФЗ

10.3. Обеспечение безопасности информации в самой СФЗ

Структура объекта защиты

СФЗ – совокупность подсистем



Подсистема управления СФЗ:
СВТ (ЦПУ и ЛПУ) +
каналы связи +
информация +
человек

10.3. Обеспечение безопасности информации в самой СФЗ

СФЗ – совокупность подсистем

10.3. Обеспечение безопасности информации в самой СФЗ

СФЗ – совокупность подсистем

Реализация подсистем ФЗ:

- Средства вычислительной техники;
- Микропроцессорные устройства;
- Средства телекоммуникации;
- Средства связи;
- Средства управления;
- Средства отображения;
- Средства документирования;
- Средства обработки, хранения и отображения видеоинформации;
- Средства управления доступом.

Функционирование СФЗ:

обязательное участие человека

10.3. Обеспечение безопасности информации в самой СФЗ

СФЗ – совокупность подсистем

Реализация подсистем ФЗ:

- Средства вычислительной техники;
- Микропроцессорные устройства;
- Средства телекоммуникации;
- Средства связи;
- Средства управления;
- Средства отображения;
- Средства документирования;
- Средства обработки, хранения и отображения видеоинформации;
- Средства управления жоступом.

Функционирование СФЗ:

обязательное участие человека

*свойства информации (ИБ):

Ц – целостность; Д – доступность,

К - конфиденциальность

СФЗ – это объект информатизации

СФЗ – это автоматизированная система (АС)

СФЗ – это автоматизированная система управления технологическим процессом (АСУ ТП)

Особенность АС СФЗ:

- наличие чувствительной информации;
- нарушение свойств информации* (Ц, Д, К) может привести к снижению эффективности функционирования СФЗ

10.3. Обеспечение безопасности информации в самой СФЗ

Функции АС СФЗ:

- Получение достоверной информации о действиях субъектов;
- Разграничение потоков информации;
- Обработка и визуализация информации;
- Управление техническими средствами и подсистемами СФЗ;
- Документирование информации о деятельности СФЗ
- Обмен информации с другими системами обеспечения безопасности объекта

АС СФЗ = АСУ ТП

10.3. Обеспечение безопасности информации в самой СФЗ

Характерные свойства АС СФЗ:

- **Наличие информации, ограниченного доступа:**
  - **конфиденциальной информации о СФЗ;**
  - **служебной информации о системах защиты информации от НСД в СФЗ;**
  - **информации, составляющую служебную тайну;**
  - **информации, составляющую государственную тайну (КВО);**
- **Территориальное размещение компонентов АС СФЗ;**
- **Размещение компонентов СФЗ в транспортных средствах (при транспортировании активов);**
- **Разделение функциональных обязанностей персонала;**
- **Относительное постоянство и узкая специализация ПО;**
- **Отсутствие у части персонала, обслуживающего СФЗ, доступа в охраняемую зону.**

10.3. Обеспечение безопасности информации в самой СФЗ

Объекты защиты в АС СФЗ (активы):

1.Информационные активы:

- конфиденциальной информации о СФЗ;
- служебной информации о системах защиты информации от НСД в СФЗ;
- информации, составляющую служебную тайну;
- информации, составляющую государственную тайну (КВО);

2.Объекты среды (программно-технический комплекс АС СФЗ):

- средства ФЗ (средства обнаружения, средства видеонаблюдения, средства контроля доступа, управляющее оборудование);
- сеть передачи данных;
- средства обработки информации;
- автоматизированные рабочие места диспетчеров и управляющего персонала.

10.3. Обеспечение безопасности информации в самой СФЗ

Угрозы АС СФЗ:

- Нарушение конфиденциальности информации (разглашение, утрата, хищение, утечка и перехват);
- Нарушение целостности информации (уничтожение, искажение, подделка);
- Нарушение санкционированной доступности информации;
- Нарушение целостности объектов среды (кража, уничтожение, подделка);
- Нарушение санкционированной доступности к объектам среды;
- Нарушение работоспособности средств ФЗ.

10.3. Обеспечение безопасности информации в самой СФЗ

Источники угроз АС СФЗ:

- Стихийные бедствия и катастрофы;
- Отказы и неисправности технических средств и средств информатизации АС СФЗ;
- Непреднамеренная деятельность человека, влияющая на ИБ АС СФЗ (внутренний нарушитель);
- Преднамеренная деятельность человека, влияющая на ИБ АС СФЗ (внутренний или внешний нарушитель, сговор внутреннего и внешнего нарушителя) ;

10.3. Обеспечение безопасности информации в самой СФЗ

Источники угроз АС СФЗ: отказы и неисправности технических средств и средств информатизации:

- **Отказы и неисправности техническим средств различных подсистем СФЗ;**
- **Отказы из-за нарушений в системе электропитания;**
- **Отказы и неисправности средств защиты информации;**
- **Отказы и неисправности технических средств контроля эффективности принятых мер по ЗИ;**
- **Сбои программного обеспечения и программных средств защиты информации;**
- **Сбои программных средств контроля эффективности принятых мер по ЗИ.**

10.3. Обеспечение безопасности информации в самой СФЗ

Источники угроз АС СФЗ: непреднамеренная деятельность человека, влияющая на ИБ АС СФЗ (внутренний нарушитель):

- **Некомпетентная деятельность персонала, приводящая к пожарам и авариям;**
- **Некомпетентные действия и ошибки, допущенные при проектировании АС СФЗ, включая подсистему ЗИ;**
- **Некомпетентные или ошибочные действия пользователей и обслуживающего персонала АС СФЗ;**
- **Некомпетентные или неосторожные действия персонала при профилактике, техническом обслуживании и ремонте технических средств АС СФЗ;**
- **Неправильное обращение с магнитными носителями при их использовании и хранении;**
- **Халатность и недостаточно четкое исполнение служебных обязанностей.**

10.3. Обеспечение безопасности информации в самой СФЗ

Источники угроз АС СФЗ: преднамеренная деятельность человека, влияющая на ИБ АС СФЗ (внешний или внутренний нарушитель:

- **Деятельность разведывательных и специальных служб по добыванию информации, навязыванию ложной информации, нарушающих работоспособность АС СФЗ;**
- **Противозаконная и преступная деятельность групп и отдельных лиц, направленная на проникновение на КВО, хищение активов КВО и диверсионные действия против КВО и его активов;**
- **Нарушение пользователями и обслуживающим персоналом АС СФЗ установленных регламентов сбора, обработки и передачи информации, а также требований ИБ.**

10.3. Обеспечение безопасности информации в самой СФЗ

Результаты преднамеренной деятельности человека, влияющие на ИБ АС СФЗ (начало):

- Хищение оборудования;
- Хищение магнитных носителей;
- Разрушение оборудования, магнитных носителей и дистанционное стирание информации;
- НСД к информации с использованием терминалов, оставленных без присмотра;
- Модификацию информации;
- Считывание или уничтожение информации;
- Несанкционированное изменение полномочий;
- Сбор и анализ используемых распечаток;
- Визуальный перехват информации;
- Перехват электромагнитного излучения;
- Копирование информации при подключении к кабелю ЛВС или приеме ЭМ излучения от сетевого адаптера;

10.3. Обеспечение безопасности информации в самой СФЗ

Результаты преднамеренной деятельности человека, влияющие на ИБ АС СФЗ (окончание):

- Выявление паролей при подключению к кабелю ЛВС и имитации запроса сетевой ОС;
- Установка скрытых передатчиков с целью копирования данных;
- Использование программных закладок с целью разрушения информации;
- Воздействие на объекты систем и сетей связи в виде манипуляций с сообщениями;
- Проникновение в систему через внешний канал связи с присвоением полномочий легального пользователя;
- Проникновение в систему через телефонную сеть при перекоммутации канала на модем злоумышленника;
- Визуальное наблюдение за ЯО.

10.3. Обеспечение безопасности информации в самой СФЗ

Результаты преднамеренной деятельности человека, влияющие на ИБ АС СФЗ (сговор внутреннего и внешнего нарушителя):

- Изменение параметров технических средств АС СФЗ;
- Изменение направления и радиуса действия средств АС СФЗ;
- Замена элементов обнаружения технических средств АС СФЗ;
- Вывод аппаратуры АС СФЗ из строя;
- Изменение характеристик систем обработки сигналов тревоги и передачи данных;
- Вывод из строя резервных систем;
- Помощь успешному прохождению к уязвимым местам КВО с учетом времени развертывания сил реагирования

10.3. Обеспечение безопасности информации в самой СФЗ

Способ нарушения ИБ АС СФЗ – информационный:

- Противозаконный сбор, распространение и использование информации;
- Манипулирование информацией (дезинформация, сокрытие или искажение);
- Незаконное копирование данных и программ;
- Незаконное уничтожение информации;
- Хищение информации из баз данных;
- Нарушение адресности и оперативности информационного обмена;
- Нарушение технологии обработки данных и информационного обмена.

Способ нарушения ИБ АС СФЗ - программно-математический:

- Внедрение программ-вирусов и других вредоносных программ;
- Внедрение «программных закладок» для осуществления НСД или воздействия на информацию и на средства защиты.

10.3. Обеспечение безопасности информации в самой СФЗ

Способ нарушения ИБ АС СФЗ - физический:

- Уничтожение, хищение и разрушение средств обработки и защиты информации, средств связи, внесение в них неисправностей;
- Уничтожение, хищение и разрушение машинных или других оригиналов носителей информации;
- Хищение ключей (ключевых документов, криптографических ключей, программных или аппаратных ключей);
- Воздействие на обслуживающий персонал и пользователей системы;
- Диверсионные действия по отношению к объектам информатизации.

10.3. Обеспечение безопасности информации в самой СФЗ

Способ нарушения ИБ АС СФЗ - радиоэлектронный:

- Перехват информации в технических каналах утечки;
- Перехват информации в сетях передачи данных и линиях связи;
- Внедрение электронных устройств перехвата информации в технические средства и помещения;
- Навязывание ложной информации по сетям передачи данных и линиям связи;
- Радиоэлектронное подавление линий связи и систем управления.

Способ нарушения ИБ АС СФЗ - организационно-правовой:

- Невыполнение требований законодательства;
- Невыполнение требований нормативных документов;
- Задержка в разработке и принятии необходимых нормативных документов.

10.3. Обеспечение безопасности информации в самой СФЗ

Цель обеспечения ИБ АС СФЗ:

- Обеспечить непрерывность функционирования АС СФЗ в условиях существования угроз в информационной сфере.

Задачи, которые должны быть решены для достижения этой цели:

- Обеспечить конфиденциальность (разглашение, утрата, хищение, утечка и перехват), целостность (уничтожение, искажение, подделка) и доступность информации;
- Обеспечить доступность и целостность объектов среды обработки информации в АС СФЗ.

Данные задачи необходимо решить в рамках создания и эксплуатации подсистемы обеспечения ИБ АС СФЗ (ПИБ), которая должна включить в себя совокупность мер и средств защиты информации (КСЗИ) и систему управления ИБ

10.3. Обеспечение безопасности информации в самой СФЗ

КСЗИ (как часть ПИБ) АС СФЗ объединяет следующие меры и средства (начало):

- Физическая защита пунктов управления СФЗ, жизненно-важных объектов и технических средств информатизации;
- Разрешительная система допуска исполнителей к работам, документам и информации;
- Ограничение доступа персонала в здания и помещения, где размещены средства информатизации;
- Разграничение доступа к данным, ПО и средствам ЗИ;
- Регистрация пользователей информационных систем, контроль за НСД;
- Учет документов и информационных массивов;
- Применение криптографических методов и средств;
- Надежное хранение традиционных и машинных носителей информации, ключей и безопасное их обращение;

10.3. Обеспечение безопасности информации в самой СФЗ

КСЗИ (как часть ПИБ) АС СФЗ объединяет следующие меры и средства (окончание):

- Применение резервирования технических средств и дублирование информации;
- Снижение уровня и информативности ПЭМИН;
- Снижение уровня акустических излучений;
- Электрическая развязка цепей питания и заземления;
- Активное зашумление в различных диапазонах;
- Противодействие оптическим средствам наблюдения и лазерным средствам перехвата;
- Предотвращение внедрения в АС программ-вирусов и программных закладок.
- Применение сертифицированных по требованиям безопасности информации технических и программных средств;

10.3. Обеспечение безопасности информации в самой СФЗ

Система управления ИБ АС СФЗ (как часть ПИБ) объединяет следующие процессы:

- **Мониторинг ИБ;**
- **Проверка эффективности ПИБ;**
- **Управление инцидентами ИБ;**
- **Категорирование помещений;**
- **Категорирование технических средств и систем обработки информации;**
- **Классификация АС СФЗ;**
- **Классификация систем радиосвязи.**

10.3. Обеспечение безопасности информации в самой СФЗ

Дополнительная информация (самостоятельное изучение):

Физическая защита ядерных объектов: Учебное пособие для вузов/ П.В.Бондарев, А.В.Измайлов, А.И.Толстой; Под ред. Н.С.Погожина.- М.: МИФИ, 2008.- 584 с.

Глава 8. Особенности СФЗ ядерных объектов

Стр. 298-335

Глава 12. Информационная безопасность СФЗ ядерных объектов

Стр. 389-489

10.4. Обеспечение информационной безопасности СФЗ ядерных объектов

Постановления Правительства РФ от 14.03.2014 N 191 «Об утверждении Правил физической защиты ядерных материалов, ядерных установок и пунктов хранения ядерных материалов» (в ред. Постановлений Правительства РФ от 22.04.2009 N 351, от 08.010.2010 N 702, от 04.02.2011 N 48, от 16.05.2011 N 364, от 28.08.2012 N 863, от 16.02.2013 N 127, от 18.02.2014 N 125, от 14.03.2014 N 191):

I. ОБЩИЕ ПОЛОЖЕНИЯ

II. ГОСУДАРСТВЕННАЯ СИСТЕМА ФИЗИЧЕСКОЙ ЗАЩИТЫ

III. ОРГАНИЗАЦИЯ И ОСУЩЕСТВЛЕНИЕ ФИЗИЧЕСКОЙ ЗАЩИТЫ НА ЯДЕРНОМ ОБЪЕКТЕ

IV. ОСНОВНЫЕ ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ ФИЗИЧЕСКОЙ ЗАЩИТЫ ЯДЕРНЫХ МАТЕРИАЛОВ, ЯДЕРНЫХ УСТАНОВОК ПРИ ПЕРЕВОЗКЕ И ТРАНСПОРТИРОВАНИИ

V. ГОСУДАРСТВЕННЫЙ НАДЗОР, ВЕДОМСТВЕННЫЙ И ОБЪЕКТОВЫЙ КОНТРОЛЬ ЗА ФИЗИЧЕСКОЙ ЗАЩИТОЙ

VI. УВЕДОМЛЕНИЕ О НЕСАНКЦИОНИРОВАННЫХ ДЕЙСТВИЯХ

Приложение 1: КАТЕГОРИИ ЯДЕРНЫХ МАТЕРИАЛОВ

Приложение 2: КАТЕГОРИИ ПОСЛЕДСТВИЙ НЕСАНКЦИОНИРОВАННЫХ ДЕЙСТВИЙ В ОТНОШЕНИИ ПРЕДМЕТОВ ФИЗИЧЕСКОЙ ЗАЩИТЫ

Приложение 3: ТРЕБОВАНИЯ К РАЗМЕЩЕНИЮ ПРЕДМЕТОВ ФИЗИЧЕСКОЙ ЗАЩИТЫ НА ЯДЕРНОМ ОБЪЕКТЕ

10.4. Обеспечение информационной безопасности СФЗ ядерных объектов

Постановления Правительства РФ от 14.03.2014 N 191 «Об утверждении Правил физической защиты ядерных материалов, ядерных установок и пунктов хранения ядерных материалов» (в ред. Постановлений Правительства РФ от 22.04.2009 N 351, от 08.010.2010 N 702, от 04.02.2011 N 48, от 16.05.2011 N 364, от 28.08.2012 N 863, от 16.02.2013 N 127, от 18.02.2014 N 125, от 14.03.2014 N 191):

"ядерный объект" - предприятие (организация, воинская часть), на территории которого используется или хранится ядерный материал либо размещается и (или) эксплуатируется ядерная установка или пункт хранения, в том числе ядерное оружие, ядерная энергетическая установка военного назначения, стенд - прототип ядерной энергетической установки военного назначения, исследовательская ядерная установка, предназначенная для создания ядерного оружия и (или) ядерных энергетических установок военного назначения.

3. Деятельность в области использования атомной энергии без обеспечения физической защиты в соответствии с настоящими Правилами запрещается.

Ядерный объект – типичный КВО

10.4. Обеспечение информационной безопасности СФЗ ядерных объектов

Постановления Правительства РФ от 14.03.2014 N 191 «Об утверждении Правил физической защиты ядерных материалов, ядерных установок и пунктов хранения ядерных материалов»
(в ред. Постановлений Правительства РФ от 22.04.2009 N 351, от 08.010.2010 N 702, от 04.02.2011 N 48, от 16.05.2011 N 364, от 28.08.2012 N 863, от 16.02.2013 N 127, от 18.02.2014 N 125, от 14.03.2014 N 191):

4. СФЗ представляет собой единую систему планирования, координации, контроля и реализации комплекса технических и организационных мер для осуществления ФЗ.

В состав государственной системы физической защиты входят:

а) федеральные органы исполнительной власти, осуществляющие управление (координацию) деятельностью ЯО;

б) федеральные органы исполнительной власти, участвующие в создании, совершенствовании, осуществлении и обеспечении ФЗ;

в) федеральные органы исполнительной власти, осуществляющие государственный надзор за ФЗ;

г) ядерные объекты;

10.4. Обеспечение информационной безопасности СФЗ ядерных объектов

Дополнительная информация (самостоятельное изучение):

Физическая защита ядерных объектов: Учебное пособие для вузов/ П.В.Бондарев, А.В.Измайлов, А.И.Толстой; Под ред. Н.С.Погожина.- М.: МИФИ, 2008.- 584 с.

Глава 8. Особенности СФЗ ядерных объектов

Стр. 298-335

Глава 12. Информационная безопасность СФЗ ядерных объектов

Стр. 389-489

10.5. Обеспечение информационной безопасности систем учета и контроля ядерных материалов

Система учета и контроля ядерных материалов (СУиК ЯМ) = АС

Особенности АС УиК ЯМ:

- АС УиК ЯМ – это локальные информационные вычислительные сети с АРМ в виде рабочих станций на принципах “клиент-сервер”;
- Отдельные составляющие АС УиК могут быть автономными АРМ на базе ВТ;
- Базы данных ведутся на серверах;
- Базовое программное обеспечение: СУБД (например, СУБД SQL Server);
- Информация о количественных и качественных характеристиках ЯМ составляет государственную тайну.

10.5. Обеспечение информационной безопасности систем учета и контроля ядерных материалов

Система учета и контроля ядерных материалов (СУиК ЯМ) = АС УиК ЯМ

Особенности АС УиК ЯМ:

- **Определенные уровни секретности (конфиденциальности) защищаемых информационных ресурсов: или строго один уровень доступа, или разные уровни доступа.**
- **Определенные уровни доступа к штатным средствам АС УиК для лиц, обладающих разными уровнями полномочий: все субъекты доступа имеют или равные права доступа, или разные права доступа. Формируется матрица доступа или полномочий субъектов доступа по отношению к информационным ресурсам в АС УиК.**
- **Определенный режим обработки данных: все СВТ АС УиК размещаются или в контролируемой зоне и не имеют внешних физических информационных связей, или в одной или нескольких контролируемых зон и не имеют незащищенных внешних физических информационных связей, или в контролируемой зоне и имеют внешние физические информационные связи со СВТ, не относящимся к АС УиК.**

10.5. Обеспечение информационной безопасности систем учета и контроля ядерных материалов

Особенности обеспечения ИБ АС УиК ЯМ:

- Определяются особенностями АС УиК ЯМ.
- Обеспечение ИБ АС УиК ЯМ является составной частью обеспечения ИБ ядерного объекта.
- Основными направлениями обеспечения ИБ АС УиК ЯМ является: ЗИ от НСД (как часть общей проблемы ЗИ от НСД на ЯО); ЗИ от утечки по техническим каналам утечки - ТКУИ (особенно от утечки за счет ПЭМИН, от технических средств разведки, от воздействия на АС УиК по ТКУИ).
- В АС УиК ЯО должна быть создана подсистема ИБ (ПИБ), состоящая из следующих частей (подсистем): подсистемы управления доступом; подсистемы регистрации и учета; криптографической подсистемы; подсистемы обеспечения целостности.

10.5. Обеспечение информационной безопасности систем учета и контроля ядерных материалов

Особенности обеспечения ИБ АС УиК ЯМ:

- АС УиК ЯМ должна пройти аттестацию (сертификацию) на уровень обеспечения ИБ с присвоением определенного класса.
- Деление на классы учитывает особенности АС УиК ЯМ и проводится для выбора мер защиты информации. Каждый класс – свой набор мер и свои требования к подсистемам ПИБ. К каждому классу АС УиК предъявляется минимально необходимый набор требований по защите информации.
- В РФ устанавливается три класса защищенности СУиК (III, II, I);

10.5. Обеспечение информационной безопасности систем учета и контроля ядерных материалов

Классификация АС УиК ЯМ: подсистема контроля доступа

Требования	III	II	I
1.1. Идентификация, проверка подлинности и контроль доступа субъектов:			
. При входе в ОС;	+	+	+
. При доступе к СУБД	+	+	+
. При доступе к объектам ОС	+	+	+
1.2. Контроль передаваемых (принимаемых) данных в сети	-	+	+
1.3.Ограничение процессов для доступа к данным	-	+	+
1.4.Управление потоками информации	-	+	+

10.5. Обеспечение информационной безопасности систем учета и контроля ядерных материалов

Классификация АС УиК ЯМ: подсистема регистрации и учета (начало)

Требования	III	II	I
2.1. Регистрация и учет (начало):			
. Входа (выхода) субъекта в ОС;	+	+	+
. Выдачи печатных выходных документов;	+	+	+
. Запуска (завершения) всех программ;	+	+	+
. Доступа программных средств к защищаемым файлам и каталогам;	+	+	+
. Доступа программных средств к фрагментам и узлам сети;	-	+	+
. Доступа к объектам СУБД;	+	+	+
. Изменения полномочий субъектов доступа и их статуса;	-	-	+

10.5. Обеспечение информационной безопасности систем учета и контроля ядерных материалов

Классификация АС СУиК ЯМ: подсистема регистрации и учета (окончание)

Требования	III	II	I
2.1.Регистрация и учет (окончание): . Создаваемых защищаемых объектов доступа; . Всех нарушений при обмене данных по сети; . Установления соединения между удаленными процессами	- - -	+ + -	+ + +
2.2. Учет носителей информации	+	+	+
2.3. Очистка освобождаемых областей ОЗУ и внешних накопителей	-	+	+
2.4.Сигнализация попыток нарушения защиты	-	-	+

10.5. Обеспечение информационной безопасности систем учета и контроля ядерных материалов

Классификация АС УиК ЯМ: криптографическая подсистема

Требования	III	II	I
3.1. Шифрование секретной информации	-	-	+
3.2. Использование сертифицированных криптографических средств	-	-	+

10.5. Обеспечение информационной безопасности систем учета и контроля ядерных материалов

Классификация АС УиК ЯМ: подсистема обеспечения целостности (начало)

Требования	III	II	I
4.1. Обеспечение целостности программных средств и обрабатываемой информации	+	+	+
4.2.Обеспечения целостности соединения	-	-	+
4.3. Доказательство передачи и доставки данных	-	-	+
4.4. Физическая защита помещений, СВТ и носителей информации	+	+	+
4.5.Наличие администратора (служ-бы) защиты информации в СУиК	-	+	+

10.5. Обеспечение информационной безопасности систем учета и контроля ядерных материалов

Классификация АС УиК ЯМ: подсистема обеспечения целостности (окончание)

Требования	III	II	I
4.6. Периодическое тестирование СЗИ НСД	+	+	+
4.7. Наличие средств восстановления СЗИ НСД	+	+	+
4.8. Использование защищенных линий связи	-	+	+
4.9. Применение сертифицированных межсетевых экранов	-	-	+
4.10. Использование сертифицированных средств защиты	+	+	+

10.6. Обеспечение информационной безопасности при использовании систем связи на ядерных объектахсистем учета и контроля ядерных материалов

Дополнительная информация (самостоятельное изучение):

Физическая защита ядерных объектов: Учебное пособие для вузов/ П.В.Бондарев, А.В.Измайлов, А.И.Толстой; Под ред. Н.С.Погожина.- М.: МИФИ, 2008.- 584 с.

Глава 12. Информационная безопасность СФЗ ядерных объектов

Стр. 389-489

Благодарю за внимание!

Толстой Александр Иванович

AlTolstoj@mephi.ru