Основы информационной безопасности критически важных объектов

Учебная дисциплина ОИБ КВО

Тема 9

Информационная безопасность автоматизированных систем критически важных объектов (ИБ АСУ 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

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

↓

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)

↑

Автоматизированная система управления производственными и технологическими процессами КВО инфраструктуры РФ - комплекс аппаратных и программных средств, информационных систем и информационно- телекоммуникационных сетей, предназначенных для решения задач оперативного управления и контроля за различными процессами и техническими объектами в рамках организации производства или технологического процесса КВО, нарушение (или прекращение) функционирования которых может нанести вред внешнеполитическим интересам РФ, стать причиной аварий и катастроф, массовых беспорядков, длительных остановок транспорта, производственных или технологических процессов, дезорганизации работы учреждений, предприятий или организаций, нанесения материального ущерба в крупном размере, смерти или нанесения тяжкого вреда здоровью хотя бы одного человека и (или) иных тяжелых последствий

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)

↑

Безопасность автоматизированной системы управления КВО - состояние автоматизированной системы управления КВО, при котором обеспечивается соблюдение проектных пределов значений параметров выполнения ею целевых функций (далее - штатный режим функционирования) при проведении в отношении ее компьютерных атак;

Компьютерная атака - целенаправленное воздействие на информационные системы и информационно-телекоммуникационные сети программно-техническими средствами, осуществляемое в целях нарушения безопасности информации в этих системах и сетях;

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.

Автоматизированная система управления технологическим процессом (АСУ ТП) **КВО**— комплекс программных и технических средств, предназначенный для автоматизации управления технологическим оборудованием на КВО.

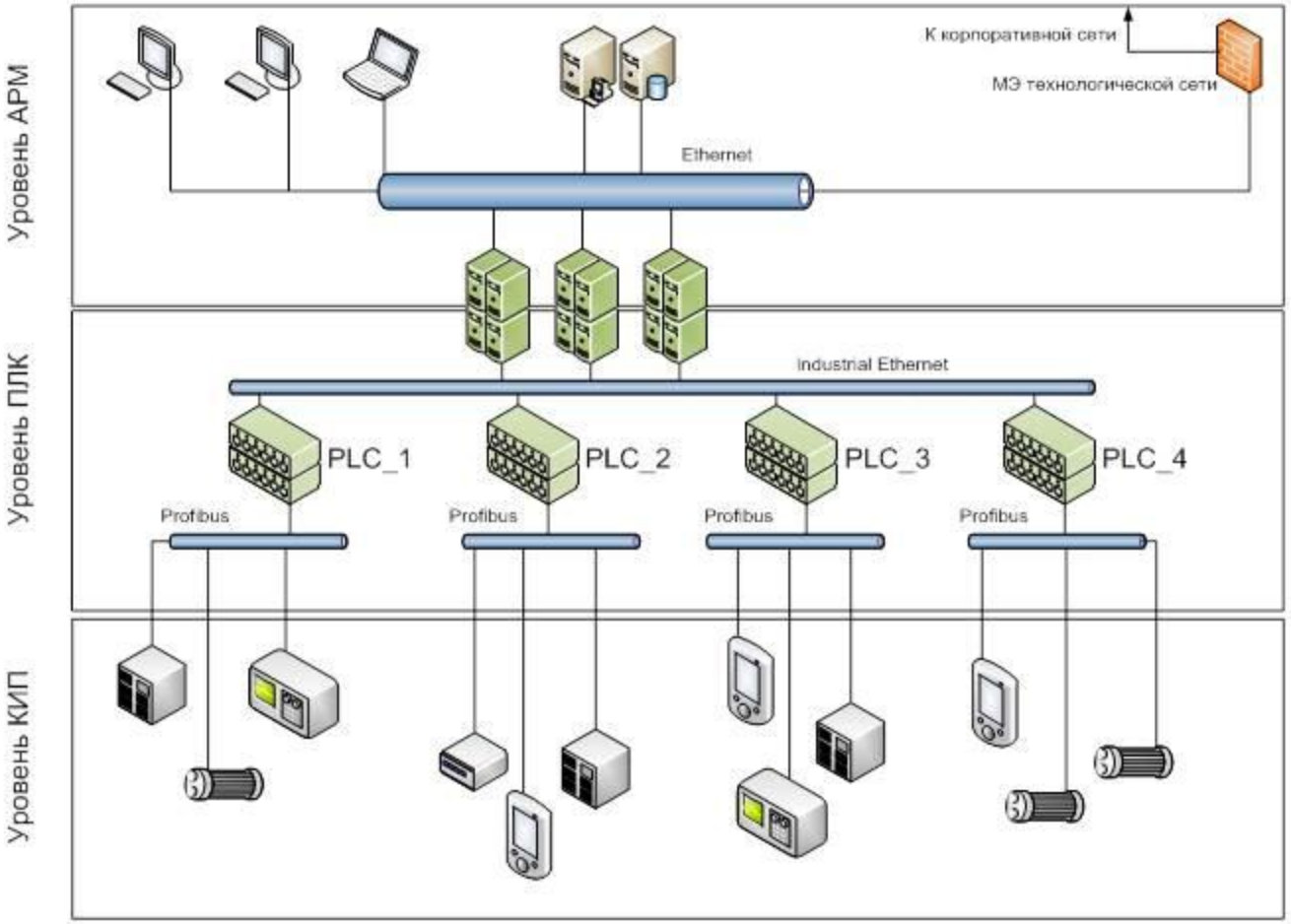
АСУ ТП характеризуются обеспечением комплексной автоматизацией технологических операций на всем производстве или отдельном участке КВО

АСУ ТП представляет собой программно-аппаратный комплекс, состоящий из:

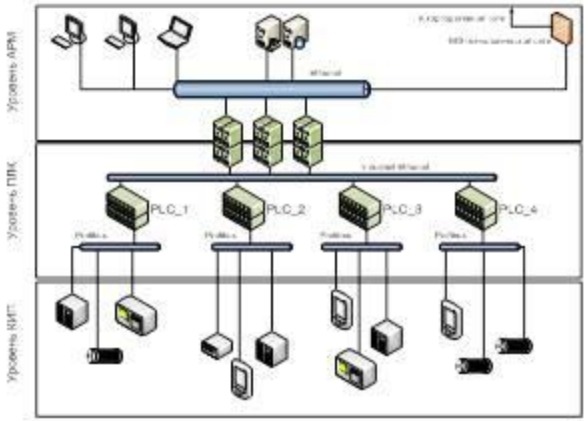
- автоматизированных рабочих мест (станция оператора, станция инженера, станция инженера КИП);
- программируемого логического контроллера (ПЛК);
- контрольно-измерительных приборов и автоматики (КИП).

АСУ ТП представляет собой программно-аппаратный комплекс, состоящий из:

- **автоматизированных рабочих мест (станция оператора, станция инженера, станция инженера КИП) – уровень АРМ;**
- **программируемого логического контроллера (ПЛК);**
- **контрольно-измерительных приборов и автоматики (КИП).**



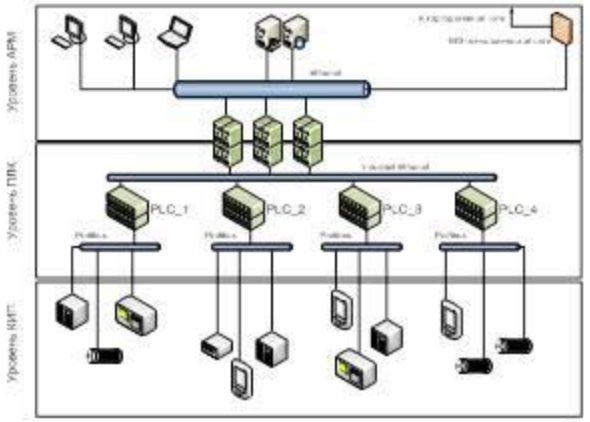
АСУ ТП - Уровень АРМ обеспечивает:



- диспетчерское наблюдение за технологическим процессом в реальном масштабе времени;
- расчет и выбор законов управления, настроек и установок, соответствующих заданным показателям качества управления и текущим (или прогнозным) параметрам объекта управления;
- хранение и дистанционную загрузку управляющих программ;
- ведение в реальном времени единой базы данных технологического процесса;
- конфигурирование комплекса для различных режимов работы (в том числе переход на резервную схему в нештатной ситуации);
- сбор, первичная обработка и накопление информации о параметрах технологического процесса и состоянии оборудования от промышленных контроллеров и других цифровых устройств, непосредственно связанных с технологической аппаратурой;
- отображение информации о текущих параметрах технологического процесса на экранах АРМ операторов и технического персонала в виде графических мнемосхем;
- отображение графиков текущих значений технологических параметров в реальном времени за заданный интервал;
- операторское управление технологическим процессом;
- обнаружение критических (аварийных) ситуаций;
- вывод на экраны АРМ операторов технологических и аварийных сообщений;
- архивирование истории изменения параметров технологического процесса;
- предоставление данных о параметрах технологического процесса для их использования в системах управления предприятием;
- связь с верхними уровнями системы управления предприятием.

АСУ ТП - Уровень ПЛК содержит:

- программируемые логические контроллеры, выполняющие функции автоматического управления ТП.



Управление технологическими процессами происходит на основе данных, получаемых от измерительных приборов, подключенных к контроллерам.

АСУ ТП - Уровень КИП содержит:

датчики, устройства измерения технологических параметров, приводы и исполнительные устройства, установленные на технологическом оборудовании и предназначенные для сбора первичной информации и реализации исполнительных воздействий.

Оборудование данного уровня непосредственно обеспечивает выполнение ТП.

Для надежного функционирования данного оборудования к нему предъявляются следующие требования:

- обеспечение работы системы в режиме реального времени;
- предельно высокая надежность;
- возможность встраивания аппаратуры в основное оборудование;
- возможность функционирования в цеховых условиях (загрязнённая атмосфера, большие перепады температур, сильные электромагнитные поля и помехи, ударные нагрузки, вибрация и т.д.).

Цель обеспечения ИБ в АСУ ТП:

обеспечение устойчивого функционирования АСУ ТП за счет предотвращения реализации угроз ИБ ее активам;

обеспечение определенного уровня ИБ АСУ ТП, рассчитанного на основе риск ориентированного подхода;

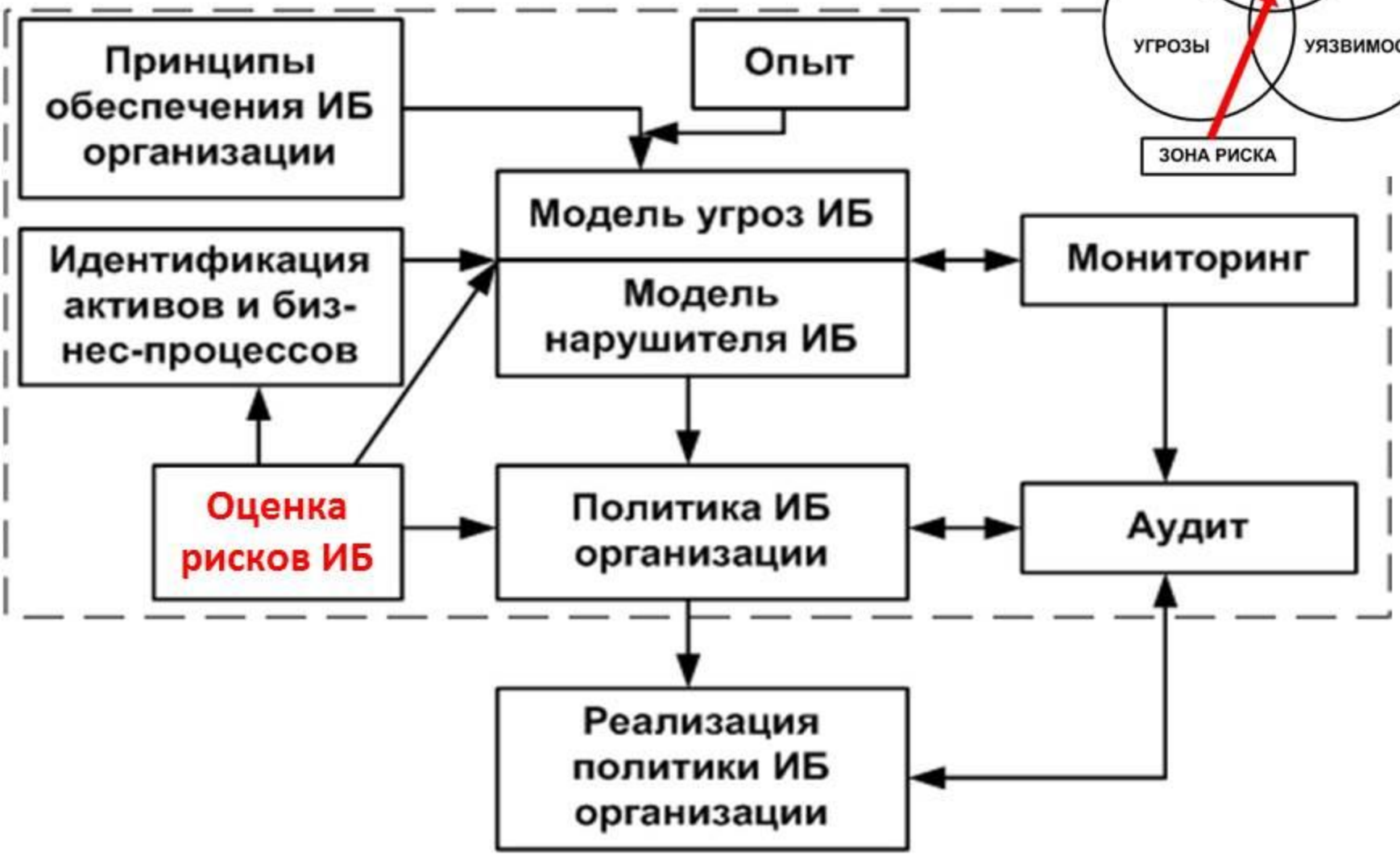
выработка планов восстановления после критических ситуаций и обеспечение непрерывности технологических процессов КВО;

достижение экономической целесообразности в выборе защитных мер.

Современный подход к обеспечению ИБ

Основные идеи новой концептуальной схемы обеспечения ИБ:

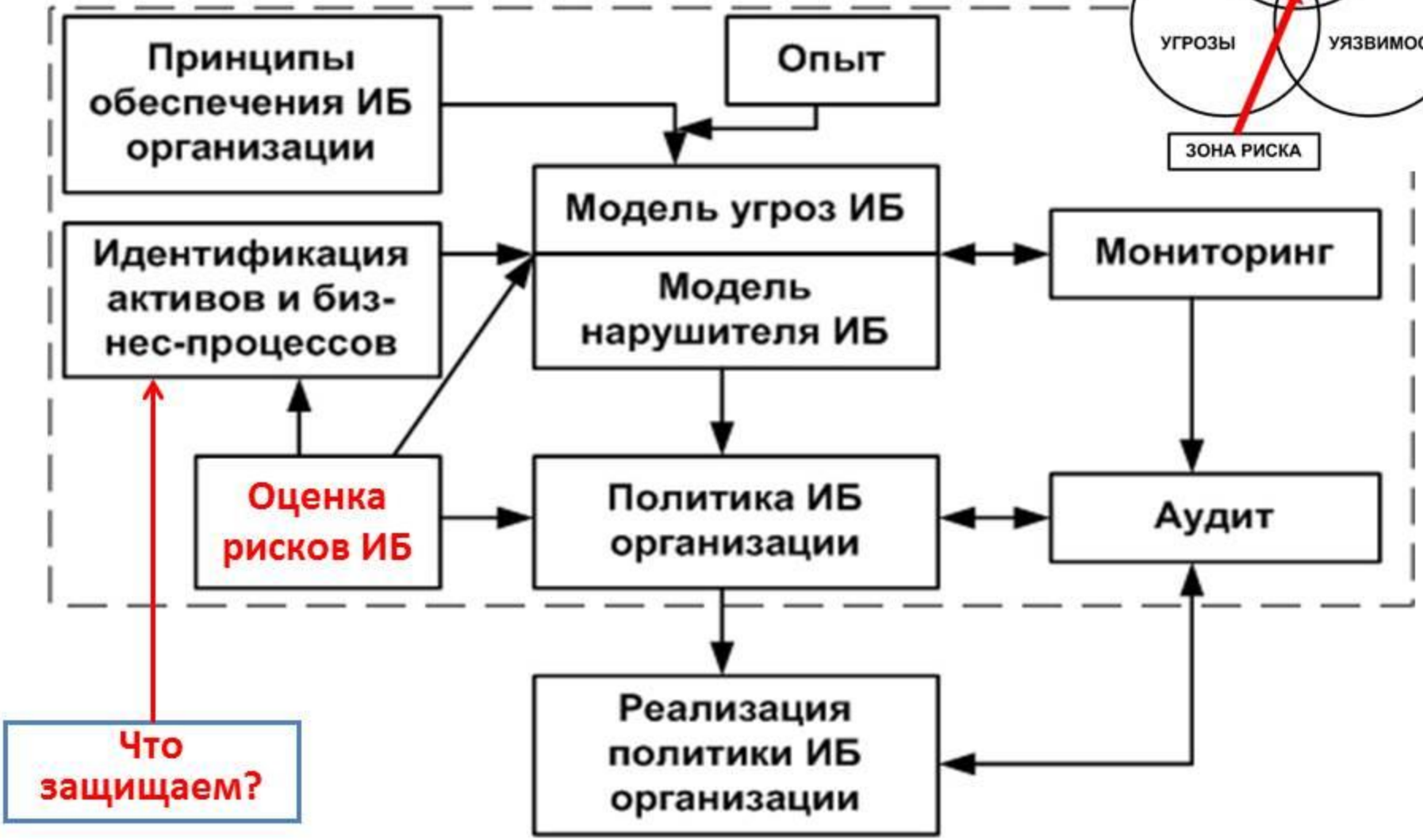
✓ **Менеджмент рисков ИБ – основа деятельности по обеспечению ИБ**



Современный подход к обеспечению ИБ

Основные идеи новой концептуальной схемы обеспечения ИБ:

✓ **Менеджмент рисков ИБ – основа деятельности по обеспечению ИБ**



Современный подход к обеспечению ИБ

Основные идеи новой концептуальной схемы обеспечения ИБ:

✓ **Менеджмент рисков ИБ – основа деятельности по обеспечению ИБ**

Принципы обеспечения ИБ организации

Опыт

От чего защищаем?

Модель угроз ИБ

Идентификация активов и биз-нес-процессов

Модель нарушителя ИБ

Мониторинг

Оценка рисков ИБ

Политика ИБ организации

Аудит

Что защищаем?

Реализация политики ИБ организации

Современный подход к обеспечению ИБ

Основные идеи новой концептуальной схемы обеспечения ИБ:

✓ **Менеджмент рисков ИБ – основа деятельности по обеспечению ИБ**

Принципы обеспечения ИБ организации

Опыт

От чего защищаем?

Модель угроз ИБ

Идентификация активов и биз-нес-процессов

Модель нарушителя ИБ

Мониторинг

Оценка рисков ИБ

Политика ИБ организации

Аудит

Что защищаем?

Реализация политики ИБ организации

Как защищаем?

Современный подход к обеспечению ИБ

Основные идеи новой концептуальной схемы обеспечения ИБ:

✓ **Менеджмент рисков ИБ – основа деятельности по обеспечению ИБ**

Принципы обеспечения ИБ организации

Опыт

От чего защищаем?

Модель угроз ИБ

Идентификация активов и биз-нес-процессов

Модель нарушителя ИБ

Мониторинг

Как контролируем?

Оценка рисков ИБ

Политика ИБ организации

Аудит

Что защищаем?

Реализация политики ИБ организации

Как защищаем?

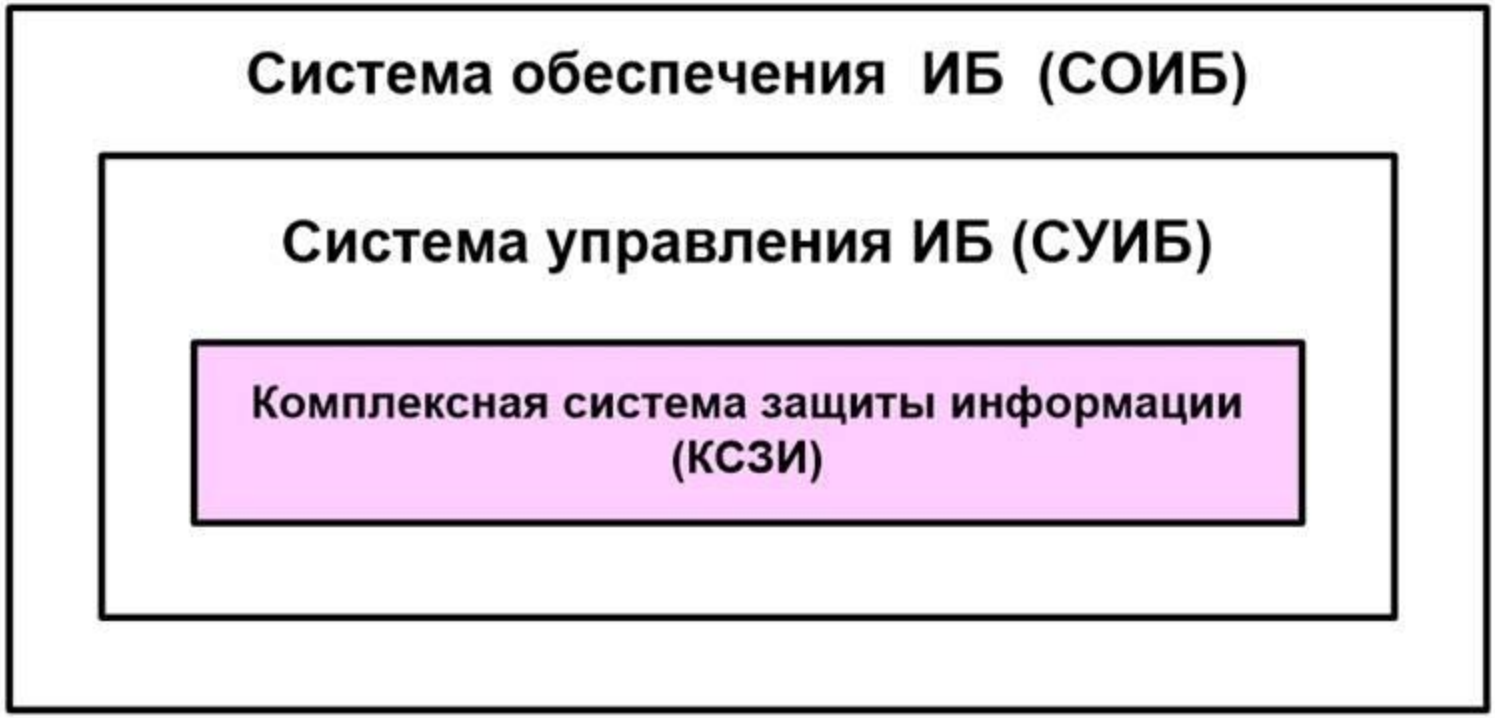
Задачи, которые необходимо решить для обеспечения ИБ в АСУ ТП:

- **Определить объекты защиты (что защищаем?)**
- **Описать угрозы ИБ (от чего защищаем?)**
- **Выбрать меры защиты (как защищаем?)**
- **Определить меры контроля (как контролируем?)**
- **Сформировать систему обеспечения ИБ, состоящую из комплексной системы защиты информации и систему управления ИБ**

Система обеспечения ИБ (СОИБ) =

Система управления ИБ (СУИБ) +

+ Комплексная система защиты информации (КСЗИ)



СОИБ = СУИБ + КСЗИ

Активы АСУ ТП, подлежащие защите:

1.Информация (данные):

- О производственном и (или) технологическом процессе,
- Об управляемом (контролируемом) объекте (в том числе данные о параметрах (состоянии) управляемого (контролируемого) объекта или процесса,
- Входная (выходная) информация,
- Команды управления,
- Контрольно-измерительная информация.

2.Объекты среды (программно-технический комплекс АСУ ТП):

- сеть передачи данных;
- автоматизированные рабочие места диспетчеров и управляющего персонала;
- серверы;
- управляющее оборудование.

Для объекта защиты

1.Информация (данные):

доступность, целостность, конфиденциальность

- О производственном и (или) технологическом процессе,
- Об управляемом (контролируемом) объекте (в том числе данные о параметрах (состоянии) управляемого (контролируемого) объекта или процесса,
- Входная (выходная) информация,
- Команды управления,
- Контрольно-измерительная информация.

2.Объекты среды (программно-технический комплекс АСУ ТП):

доступность, целостность

- сеть передачи данных;
- автоматизированные рабочие места диспетчеров и управляющего персонала;
- серверы;
- управляющее оборудование.

Источники угроз:

1.Антропогенные – связанные с непосредственными действиями потенциальных нарушителей:

Преднамеренные (У1)- внутренние и внешние;

Непреднамеренные (У2) - внутренние;

2.Техногенные (У3) – связанные с техногенными происшествиями;

3. Стихийные (У4) – связанные с природными явлениями;

Модель угроз:

угроза – источник угрозы – актив, на который направлена угроза – используемые уязвимости- способ реализации угрозы – ущерб – вероятность реализации угрозы

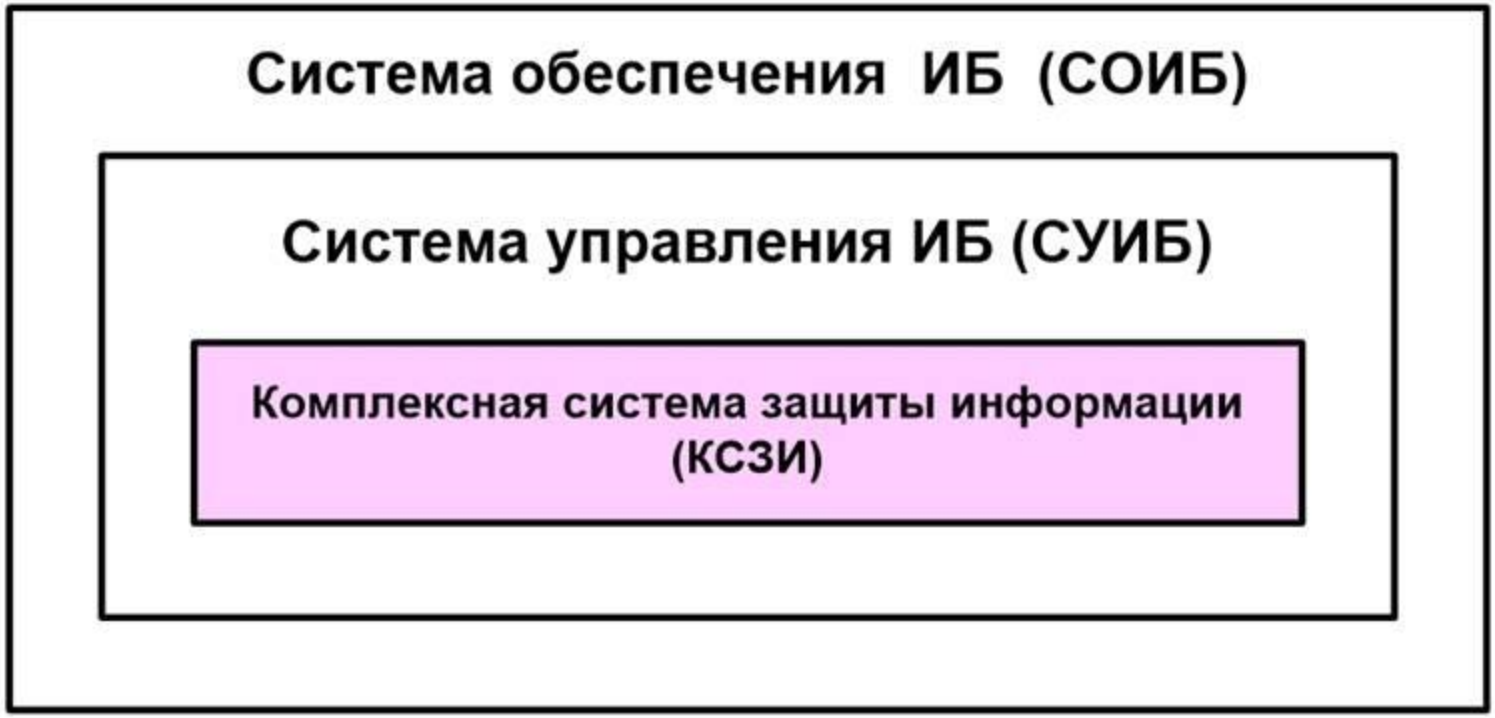
Модель нарушителя:

Вид нарушителя (внешний, внутренний) – права доступа - побудительные причины - цель – способ действия - квалификация - оснащение

Система обеспечения ИБ (СОИБ) =

Система управления ИБ (СУИБ) +

+ Комплексная система защиты информации (КСЗИ)



СОИБ = СУИБ + КСЗИ

Комплексная система защиты информации (КСЗИ) (состав подсистем):

- подсистема межсетевого экранирования;
- подсистема криптографической защиты каналов связи;
- подсистема разграничения доступа;
- подсистема антивирусной защиты;
- подсистема контроля целостности;
- подсистема регистрации и учета.

Система управления ИБ (СУИБ)

(состав подсистем):

- Подсистема контроля ИБ (обнаружение вторжений; анализ защищенности; контроль обновлений);
- Подсистема управления инцидентами;
- Подсистема управления рисками;
- Подсистема управления непрерывностью функционирования АСУ ТП (обеспечение готовности ИТ);
- ……

Использование средств защиты (пример):

Объект	Угроза	Средство защиты
АРМ диспетчеров и управляющего персонала	Доступ к операционной системе в процессе загрузки	Средства разграничения доступа. Средства усиленной аутентификации.
	Загрузка нештатной ОС с внешнего носителя	Средства разграничения доступа. Средства усиленной аутентификации. Датчики вскрытия корпуса системных блоков. Электронные замки.
	Несанкционированный доступ к ОС ТСОИ	Средства разграничения доступа. Средства усиленной аутентификации.
	Сканирование сетевой инфраструктуры	Межсетевые экраны. Средства обнаружения вторжений.
	Несанкционированный удаленный доступ к ТСОИ	Межсетевые экраны. Средства обнаружения вторжений. Средства разграничения доступа. Средства усиленной аутентификации.
	Внедрение ложного сетевого объекта (spoofing)	Межсетевые экраны. Средства обнаружения вторжений.
	Внедрение вредоносного ПО в ТСОИ	Средства антивирусной защиты. Средства обнаружения вторжений.
	Установка постороннего ПО на ТСОИ	Средства разграничения доступа.
	Предоставление доступа к ТСОИ посторонним лицам	Средства разграничения доступа. Средства усиленной аутентификации.

АСУ ТП = объект информатизации (ОИ)

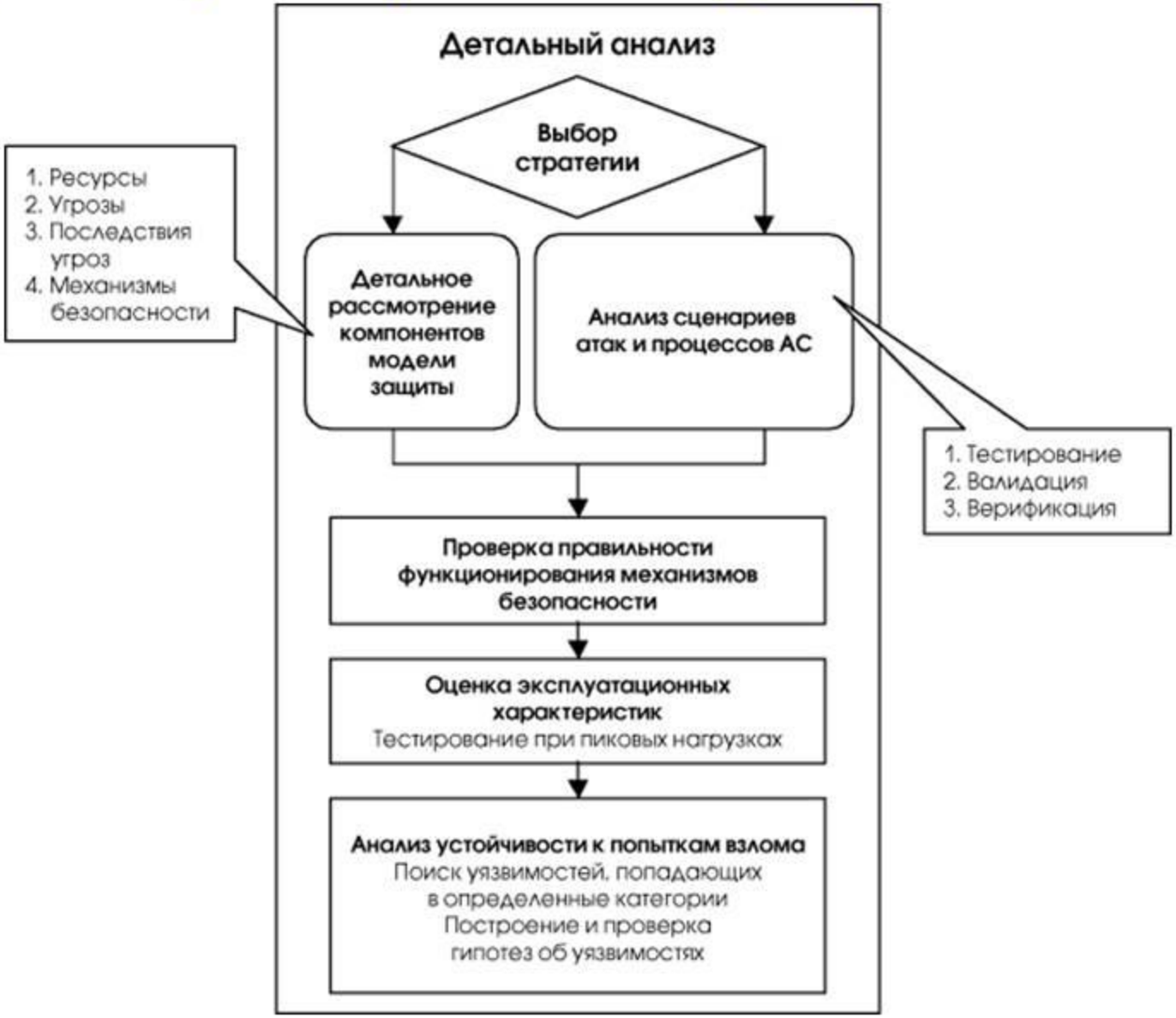
Аттестация АС по требованиям безопасности информации (опыт РФ)

Под аттестацией ОИ понимается комплекс организационно-технических мероприятий, в результате которых посредством специального документа (Аттестат соответствия) подтверждается, что объект отвечает требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных ФСТЭК России.

Состав нормативной и методической документации для аттестации конкретных АС определяется органом по аттестации в зависимости от вида и условий функционирования ОИ на основании анализа исходных данных по аттестуемой АС. Аттестат соответствия выдается владельцу АС на период, в течение которого обеспечивается неизменность условий функционирования системы и технологии обработки защищаемой информации, могущих повлиять на характеристики, определяющие безопасность информации (состав и структура технических средств, условия размещения, используемое ПО, режимы обработки информации, средства и меры защиты), но не более чем на 3 года.

Процедура аттестации АС по требованиям информационной безопасности

Процедура аттестации АС по требованиям информационной безопасности



Благодарю за внимание!

Толстой Александр Иванович

AlTolstoj@mephi.ru