Тема 1 Организация безопасного удаленного доступа

Лекция 2. Основы мониторинга информационной безопасности АСУ ТП

Дисциплина: Анализ информационных потребностей подразделений информационно-аналитического мониторинга

Доцент: Кирьянов Александр Владимирович
email:kiryanov_a@mirea.ru

Учебные вопросы:

1. Основные понятия, жизненный цикл объектов мониторинга
2. Требования к мониторингу информационной безопасности на этапе разработки безопасного программного обеспечения
3. Объекты мониторинга информационной безопасности
4. Основные понятия и определения в области АСУ ТП

Вопрос 1

Основные понятия,
жизненный цикл объектов мониторинга

Основные понятия

Безопасность информации –

состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность

ГОСТ Р 50922-2006 Защита информации. Основные термины и определения

Угроза (безопасности информации) –

совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации

ГОСТ Р 50922-2006 Защита информации. Основные термины и определения

Уязвимость –

свойство информационной (автоматизированной) системы, обуславливающее возможность реализации угроз безопасности обрабатываемой в ней информации

ГОСТ Р 59547-2021 Защита информации. Мониторинг информационной безопасности. Общие положения

Основные понятия

Мониторинг информационной безопасности –

процесс постоянного наблюдения и анализа результатов регистрации событий безопасности и иных данных с целью выявления нарушений безопасности информации, угроз безопасности информации и уязвимостей

Источник: ГОСТ Р 59547-2021 Защита информации. Мониторинг информационной безопасности. Общие положения

Особенности терминологии

Событие безопасности – зафиксированное в обрабатываемом виде состояние объекта мониторинга, указывающее на возможное нарушение безопасности информации, а также на сбой в работе средства защиты/обработки информации или иную ситуацию, которая может быть значимой для безопасности информации

Инцидент информационной безопасности – событие, которое **привело или может привести** к нарушению или возникновению угроз

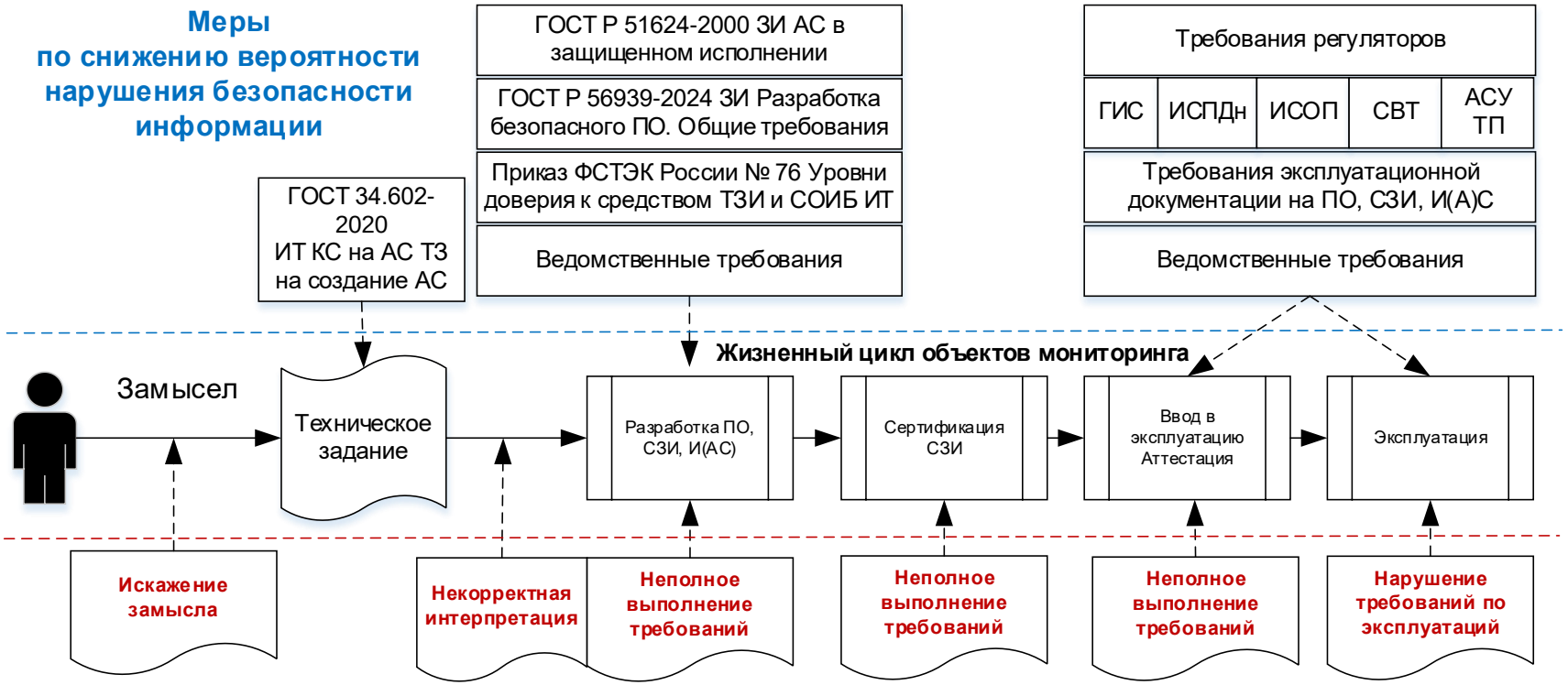
Компьютерный инцидент (КИ) – **факт** нарушения (прежде всего, в результате **компьютерной атаки**)

Жизненный цикл объектов мониторинг

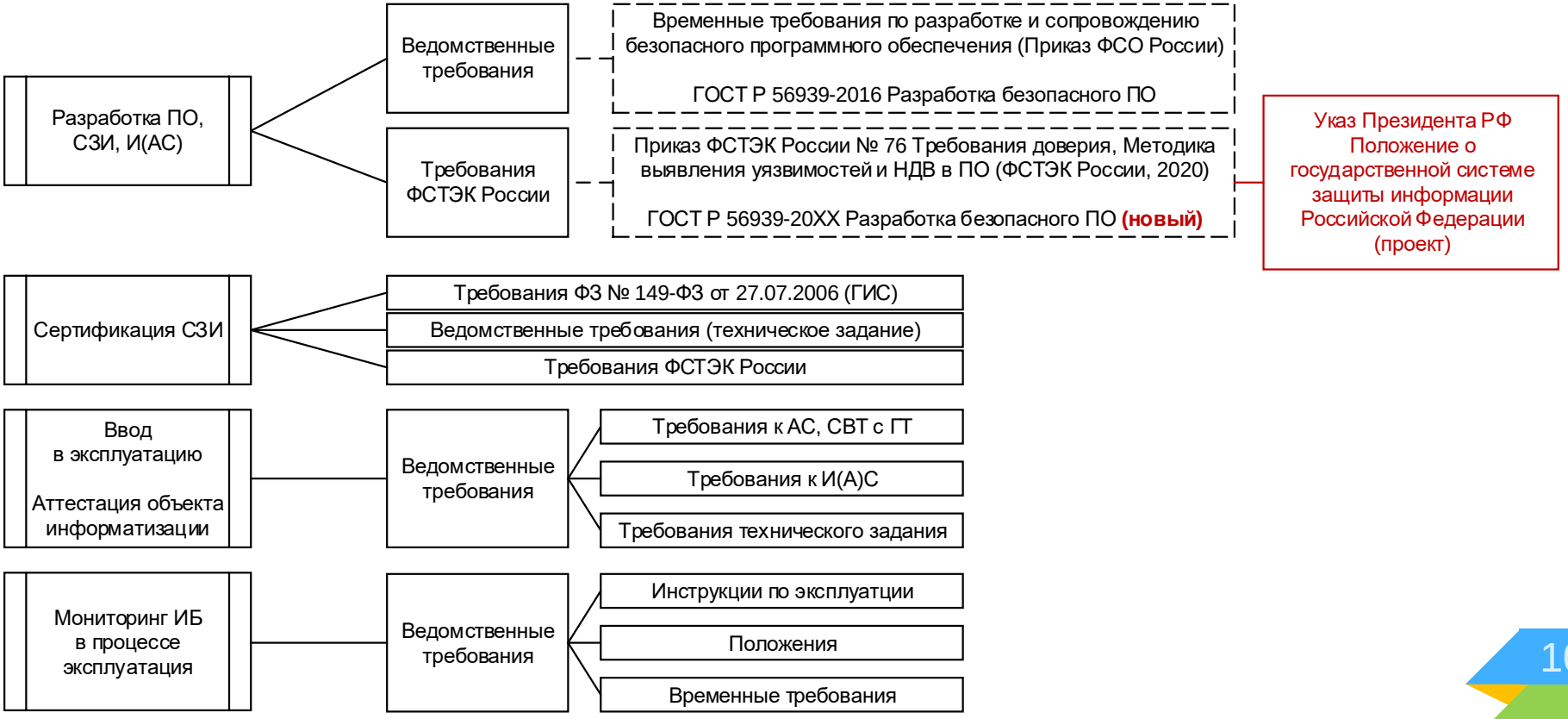
Вопрос 2

Требования к мониторингу информационной безопасности на этапе разработки безопасного программного обеспечения

Механизмы появления уязвимостей И(А)С



Требования к элементам системы мониторинга информационной безопасности



РБПО : разработка безопасного программного обеспечения

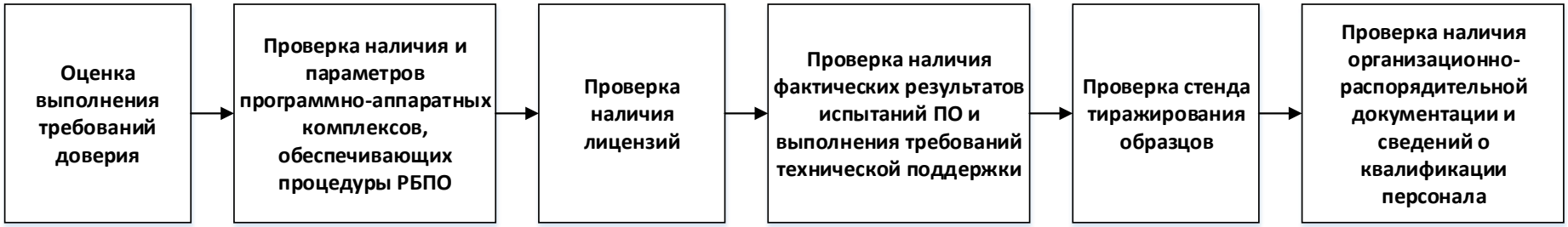
Требования ФСО России:

- **Приказ ФСО России (ДСП) Временные требования по разработке и сопровождению безопасного программного обеспечения**

Требования ФСТЭК России:

- **Приказ ФСТЭК России № 76 (2020) Требования доверия**
- **Методика выявления уязвимостей и недекларированных возможностей в программном обеспечении (ФСТЭК России, 2020)**
- **Порядок проведения сертификации процессов безопасной разработки ПО СЗИ (Приказ № 240 ФСТЭК России от 01.12.2023)**

РБПО Требования к РБПО ФСТЭК России



Приказ ФСТЭК России № 76 (2020) Требования доверия

Методика ВУ и НДВ в ПО (ФСТЭК России, 2020)

Требования стандартов СМК (система менеджмента качества)

1. Приказ ФСТЭК России от 03.04.2018 № 55 Об утв. Положения о системе сертификации средств защиты информации
2. Приказ ФСТЭК России от 02.06.2020 г. № 76 (дсп) Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий с приложением Методика выявления уязвимостей и недекларированных возможностей в программном обеспечении (утв. ФСТЭК России 25.12.2020 г. (дсп))
3. ГОСТ Р 56939-2024 Защита информации. Разработка безопасного программного обеспечения. Общие требования
4. Стандарты серии ГОСТ 19.XXX (101, 201, 402, 404) Единая система программной документации

РБПО Нормативное обеспечение

Национальные стандарты

- ГОСТ Р 56939-2024 ЗИ РБПО Общие требования
- ГОСТ Р 58412-2019 ЗИ РБПО Угрозы БИ при разработке ПО
- ГОСТ Р 71206-2024 ЗИ РБПО Безопасный компилятор языков Си Си++. Общие требования
- ГОСТ Р 71207-2024 ЗИ РБПО Статический анализ программного обеспечения. Требования

Национальные стандарты (проекты)

- ГОСТ Р (проект) ЗИ РБПО Руководство по оценки безопасности разработки программного обеспечения
- ГОСТ Р (проект) ЗИ РБПО Руководство по реализации мер по разработке безопасного программного обеспечения
- ГОСТ Р (проект) ЗИ РБПО Руководство по проведению динамического анализа программного обеспечения

ФСТЭК России (проекты)

- Приказ ФСТЭК России от 02.06.2020 г. № 76 (3-я редакция) *с требованиями к ИИ*
- Методика выявления уязвимостей и недекларированных возможностей в программном обеспечении (3-я редакция)

Этап	Состав сведений, предоставляемых разработчиком безопасного ПО
	Технические условия, комплект программной документации
	Сборочная среда
	Дистрибутив
КАО.1	**Результаты анализа безопасности** архитектуры • настройки средств анализа (контроля) защищенности (сканеров безопасности) • результаты анализа сетевых интерфейсов, конфигурационных файлов ОО (объект оценки) и т.п. • принятые меры по исправлению подтвержденных уязвимостей • меры по устранению уязвимостей в формальной модели безопасности
КАО.2	**Методика и результаты** анализа безопасности заимствованного и привлекаемого программного обеспечения (не реже 1 раза в месяц)
КАО.2	**Методика и результаты** анализа безопасности на основе открытых источников, обоснование неактуальности уязвимостей, принятые меры по исправлению уязвимостей
КАО.2	**Методика, тесты и результаты** тестирования на проникновение, принятые меры по исправлению уязвимостей
САО.1	**Методика и результаты** статического анализа кода (настройки статических анализаторов, предупреждения о потенциальных уязвимостях кода, полученные от статического анализатора, разметка полученных предупреждений, принятые меры по исправлению уязвимостей)
ДАО.1	**Функциональные тесты** (системные (интеграционные), регрессионные, модульные тесты) **Методики** функционального тестирования **Результаты** функционального тестирования (а именно: системные (интеграционные), регрессионные, модульные тесты, журналы выполнения тестов, принятые меры по исправлению уязвимостей)
ДАО.2	**Методика и результаты** фаззинг-тестирования (конфигурационные параметры фаззинг-тестирования, наборы входных данных (словари и модели), журналы работы фаззера, выявленные уязвимости, принятые меры по исправлению)
ДАО.3	**Методика и результаты** системного тестирования

РБПО Материально-техническое обеспечение

Программное обеспечение

- не менее двух сертифицированных средств антивирусной защиты от различных разработчиков (в случае отсутствия для среды таковых, допускается использовать иные) **~20 000 ₽/год**
- средство мониторинга сетевого трафика
- средство расчета контрольных сумм (рекомендуется использовать программы контрольного суммирования, допускающие эффективную эксплуатацию в среде функционирования ОО)) **~1 000 ₽/год**
- средство контроля системных вызовов, относящихся к работе с объектами файловой системы
- средства формальной верификации модели безопасности
- инструментальные средства анализа **~5 000 000 – 15 000 000 ₽/год**
- средства анализа сетевых интерфейсов | средства анализа конфигурационных файлов
- средства тестирования на проникновение | статические анализаторы | средства фаззинг-тестирования | средство анализа трасс

Примечание:

- Должны применяться инструментальные средства анализа и контроля, имеющие техническую поддержку и возможность адаптации (доработки) под особенности среды сборки и проводимые испытания ОО либо свободно распространяемые в исходных код
- Рекомендуется применять инструментальные средства анализа и контроля, не имеющие каких-либо ограничений по их применению, адаптации (доработки) на территории Российской Федерации

Технические средства

- система управления средой виртуализации **~500 000 – 2 000 000 ₽**
- система хранения данных **~300 000 – 1 000 000 ₽**
- источник бесперебойного питания **~80 000 – 150 000 ₽**
- телекоммуникационное оборудование **~50 000 – 200 000 ₽**

Доступ к сети Интернет

Аренда помещений

РБПО Инструментальные средства

Тип средства	Наименование
Средства антивирусной защиты	**Kaspersky Endpoint Security, Антивирус Dr Web Desktop Security**
Средства мониторинга сетевого трафика	**Wireshark, tcpdump**
Средства расчета контрольных сумм	**ФИКС-UNIX 1.0, ФИКС 2.0.2, ПИК-Эшелон, gostsum, md5sum**
Средства контроля системных вызовов	**trace, dtrace, ptrace (*trace)**
Средства формальной верификации	**TLA+/TLC, Event-B, Alloy**
Сканеры уязвимостей	**Nessus, Nexpose, XSpider, Metasploit Express, Nmap, Greenbone Security Assistant, Nikto, Netsparker, Acunetix, RedCheck, Сканер-ВС, Vuls, grype**
Средства тестирования на проникновение	**Metasploit-Framework, Hydra**
Средства статического анализа и разметки	**Svace и Svacer, Solar appScreener, АК-ВС, PT Application Inspector, PVS Studio, Clang Analyzer**
Средства фаззинг-тестирования	**AFL++, LibFuzzer, Crusher, go-fuzz, Syzkaller, afl-cov, afl-utils, lcov, gcov**
Средства анализа трасс и поверхности атаки	**Natch, Блесна**
Средства обратной разработки и отладки	**IDA Pro, Radare2, GDB**
Система контроля версий	**git (Gitlab), SVN, Mercurial**
Средство облачного хранения данных	**Nextcloud, Яндекс.Диск**
Средство управления проектами	**Redmine, Jira, Mattermost**

#	Тип средства защиты информации	Дата и номер Приказа ФСТЭК России	Типы
1	Операционные системы (ОС)	19.08.2016 № 119	А, Б, В
2	Средства обнаружения вторжений (СОВ)	06.12.2011 № 638	С, У
3	Средства антивирусной защиты (АВЗ)	20.03.2012 № 28	А, Б, В, Г
4	Средства доверенной загрузки (СДЗ)	27.09.2013 № 119	УБ, ПР, ЗЗ
5	Средства контроля съемных машинных носителей информации (СКСМНИ)	28.07.2014 № 87	Н, П
6	Средства межсетевого экранирования (МСЭ)	09.02.2016 № 9	А, Б, В, Г, Д
7	Средства контейнеризации (СК)	04.07.2022 № 118	–
8	Средства виртуализации (СВ)	27.10.2022 № 187	–
9	Требования к СЗИ от воздействий, направленных на отказ в обслуживании И(А)С	30.07.2018 № 132	–
10	Требования к многофункциональным межсетевым экранам уровня сети	07.03.2023 № 44	–
11	Требования к системам управления базами данных (СУБД)	14.04.2023 № 64	–
12	Требования к средствам обнаружения и реагирования уровня узла (EDR)	Разрабатываются (2024)	
13	Требования к среде выполнения интерпретируемого (компилируемого в промежуточное представление) кода	Разрабатываются (2024)	

Выводы по 2 учебному вопросу

1. Важным элементов государственной системы защиты информации РФ является система лицензирования участников систем обязательной сертификации средств защиты информации и техническое регулирование вопрос защиты информации
2. Как к разработчикам, так и к испытательным лабораториям, проводящим сертификационные испытания, предъявляются нормативные требования по применению конкретных методов и испытательных средств в целях снижения вероятности реализации угроз безопасности информации, обусловленных наличием уязвимостей в объектах защиты

Вопрос 3

Объекты мониторинга информационной безопасности

Объекты мониторинга

- автоматизированные рабочие места
- серверное оборудование
- телекоммуникационное оборудование
- технологическое и (или) производственное оборудование (исполнительные устройства);
- средства ЗИ
- иные объекты мониторинга, определенные оператором информационных (автоматизированных) систем

ГОСТ Р 59547-2021 Защита информации. Мониторинг информационной безопасности. Общие положения

Ведомственные объекты защиты

СВТ, обрабатывающие информацию ограниченного доступа (не ГТ)

«Временный порядок обеспечения безопасности информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, с использованием средств вычислительной техники …»

(приказ 2023 г)

Объекты ВТ с ГТ

Инструкция … (приказ)

И(А)С

Техническое задание

МСС, ЗВС

Требования по обеспечению ИБ (приказы)

Объекты КИИ

Законодательство в сфере обеспечения безопасности ЗОКИИ (значимых объектов критической информационной инфраструктуры)

Положение о государстенной системы защиты информации Российской Федерации (проект Указа Президента РФ)

Особенности:

- И(А)С ФОИВ (федеральных органов исполнительной власти) должны быть приведены в соответствие с требованиями Приказа ФСТЭК России № 17
- СЗИ в составе И(А)С ФОИВ должны быть сертифицированы
- ОИ (объекты информатизации) должны быть аттестованы
- ГОС ЗИ РФ взаимодействует с ГосСОПКА
- ФОИВ разрабатывает план мероприятий по ЗИ
- ФОИВ разрабатывает отчет о выполнении мероприятий по ЗИ и представляет его во ФСТЭК России
- в ФОИВ должны быть утвержден Порядок организации и управления ЗИ в органе

Примечание: ФСО России является ФОИВ

Статья 1 Указа Президента РФ от 07.08.2004 №1013 «Вопросы ФСО РФ»

Процесс управления уязвимостями

Задачи, решаемые на этапах управления уязвимостями:

1. Осуществляется выявление уязвимостей на основании данных, получаемых из внешних и внутренних источников, и принятие решений по их последующей обработке
2. Определяется уровень критичности уязвимостей применительно к информационным системам органа (организации)
3. Определяется приоритетность устранения уязвимостей и выбираются методы их устранения: обновление программного обеспечения и (или) применение компенсирующих мер защиты информации
4. Принимаются меры, направленные на устранение или исключение возможности использования (эксплуатации) выявленных уязвимостей
5. Осуществляется сбор и обработка данных о процессе управления уязвимостями и его результатах, а также принятие решений по улучшению данного процесса

ФСТЭК Методический документ Руководство по организации процесса управления уязвимостями в органе (организации) Утв. 17.05.2023

Основные процессы и процедуры органа (организации), связанные с управлением уязвимостями

- **Мониторинг информационной безопасности**
  Процесс постоянного наблюдения и анализа результатов регистрации событий безопасности и иных данных с целью выявления нарушений безопасности информации, угроз безопасности информации и уязвимостей
- **Оценка защищенности**
  Анализ возможности использования обнаруженных уязвимостей для реализации компьютерных атак на информационные системы органа (организации)
- **Оценка угроз безопасности информации**
  Выявление и оценка актуальности угроз, реализация (возникновение) которых возможна в информационных системах органа (организации)
- **Управление конфигурацией**
  Контроль изменений, состава и настроек программного и программно-аппаратного обеспечения информационных систем
- **Управление обновлениями**
  Приобретение, анализ и развертывание обновлений программного обеспечения в органе (организации)
- **Применение компенсирующих мер защиты информации**
  Разработка и применение мер защиты информации, которые применяются в информационной системе взамен отдельных мер защиты информации, подлежащих реализации в соответствии с требованиями по защите информации, в связи с невозможностью их применения

Рекомендуемые сроки устранения уязвимостей

• критический уровень опасности	до 24 часов
• высокий уровень опасности	до 7 дней
• средний уровень опасности	до 4 недель
• низкий уровень опасности	до 4 месяцев

в соответствии с **Методикой оценки уровня критичности уязвимостей программных, программно-аппаратных средств, утвержденной ФСТЭК России 28 октября 2022 г.**

Основание создания ЦМИБ

Указ Президента Российской Федерации от 07 мая 2017 года № 204

«О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года»

в рамках национальной программы
«Цифровая экономика Российской Федерации»

Цель создания ЦМИБ

поддержание проектного уровня информационной безопасности, обнаружения, оперативного реагирования на сетевые компьютерные атаки, компьютерные инциденты и проведение мероприятий по ликвидации их последствий в *объектовых* автоматизированных системах

Нормативно-техническая документация

- Федеральный закон Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
- Требования по ЗИ в АС в защищенном исполнении … (ФСБ России)
- Требования к СЗИ ограниченного доступа, не содержащей … (ФСБ России)
- Приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»

Состав выполняемых задач

Подсистема защиты от целевых атак

- выявление целевых компьютерных атак на инфраструктуру объектов защиты

Подсистема мониторинга информационной безопасности

- мониторинг и анализ состояния информационной безопасности объектов защиты
- оперативное обнаружение и реагирование на инциденты информационной безопасности
- сбор, накопление и обработка событий, связанных с нарушением требований по защите информации
- подготовка отчетов по результатам расследований и предложений по устранению последствий выявленных инцидентов информационной безопасности, предотвращению их повторного появления
- автоматизация деятельности по мониторингу информационной безопасности, выявлению инцидентов информационной безопасности и реагированию на них
- формирование и поддержание в актуальном состоянии информации о контролируемых информационных ресурсах, в том числе средствах защиты информации

Взаимодействие со смежными ИС и ИТКС

Передаваемые данные:

- данные о событиях безопасности от средств, осуществляющих регистрацию событий безопасности
- данные о возможных уязвимостях
- данные о результатах контроля состава технических средств, ПО и СЗИ
- данные о результатах контроля соответствия параметров настроек ПО и СЗИ
- данные о работоспособности (неотключении) ПО и СЗИ
- данные о действиях пользователей и процессов, необходимых для выявления преднамеренного или непреднамеренного нарушения установленных политик безопасности, регламентов работы, фактов запрещенной деятельности, попыток совершения НСД и утечки конфиденциальной информации

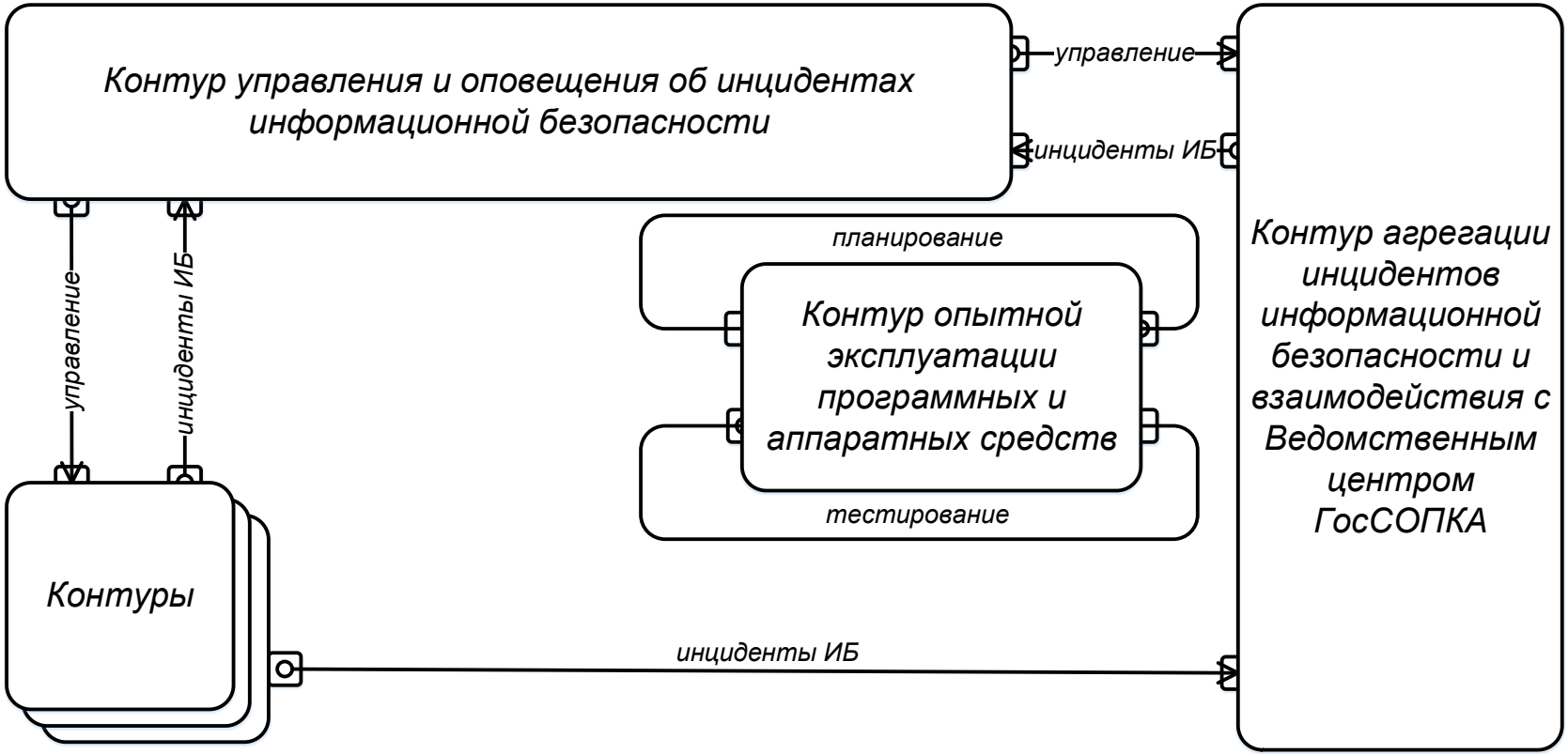
Назначение ЦМИБ

ЦМИБ предназначен для сбора и анализа событий безопасности в объектах защиты и выявления инцидентов информационной безопасности.

Архитектура ЦМИБ:

- контуры
  - независимые контуры объектов защиты
  - контур управления и оповещения об инцидентах информационной безопасности
  - контур агрегации инцидентов информационной безопасности и взаимодействия с Ведомственным центром ГосСОПКА
  - контур опытной эксплуатации программных и аппаратных средств
- подсистемы (7)

Функциональная архитектура ЦМИБ



Подсистемы ЦМИБ

- подсистема технологической инфраструктуры
- подсистема защиты информации
- подсистема защиты от целевых атак
- подсистема защиты от утечки информации
- подсистема контроля действий привилегированных учетных записей
- подсистема создания персонализированных копий документов, выводимых на печать или устройства отображения
- подсистема мониторинга информационной безопасности.

Подсистема технологической инфраструктуры

- серверное оборудование
- информационно-телекоммуникационная сеть
- автоматизированные рабочие места
- устройства хранения данных
- общесистемное программное обеспечение
- средства коллективного отображения информации
- средства резервного копирования и восстановления данных

Подсистема защиты информации

- СЗИ от НСД
- СЗИ, реализующие механизмы доверенной загрузки ОС технических средств ЦМИБ (АПМДЗ)
- САВЗ
- устройства однонаправленной передачи
- средства МЭ
- СКЗИ
- средства обнаружения компьютерных атак (СОКА)
- средства пассивной и (или) активной защиты от утечки по техническим каналам обрабатываемой в ЦМИБ информации (при необходимости), а также технические средства в защищенном исполнении и доработанные технические средства (при необходимости)

Подсистема защиты от целевых атак

- система защиты от целевых атак
- локальная репутационная база угроз

Подсистема защиты от утечки информации

- средство обнаружения утечки информации
- ПО восстановления доступа к зашифрованным данным и подбора пароля к защищённым документам
- программа поиска и гарантированного уничтожения информации на дисках

Состав подсистем

Подсистема контроля действий привилегированных учетных записей:

- средство контроля действий привилегированных пользователей

Подсистема создания персонализированных копий документов, выводимых на печать и устройства отображения:

- средство создания персонализированных копий документов

Подсистема мониторинга информационной безопасности:

- система контроля защищенности и соответствия стандартам информационной безопасности
- система мониторинга информационной безопасности

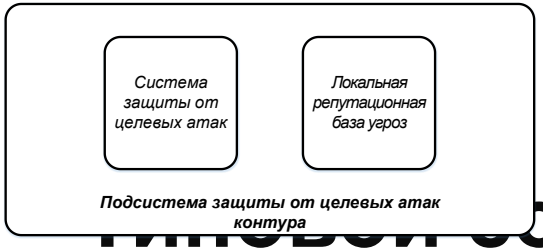
Подсистема контроля действий привилегированных учетных записей

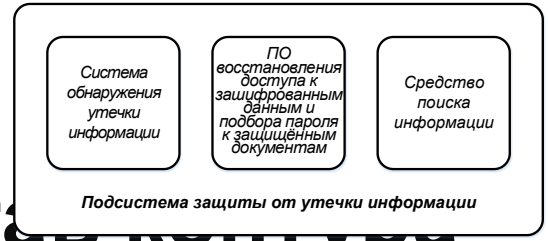
средство контроля действий привилегированных пользователей

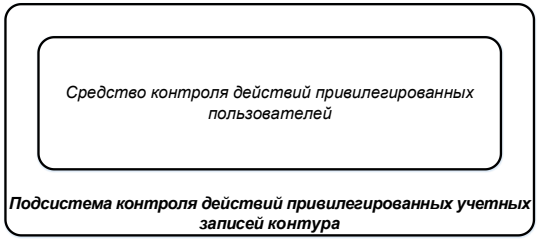
Подсистема создания персонализированных копий документов, выводимых на печать и устройства отображения

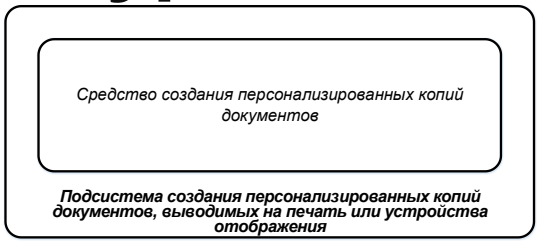
средство создания персонализированных копий документов

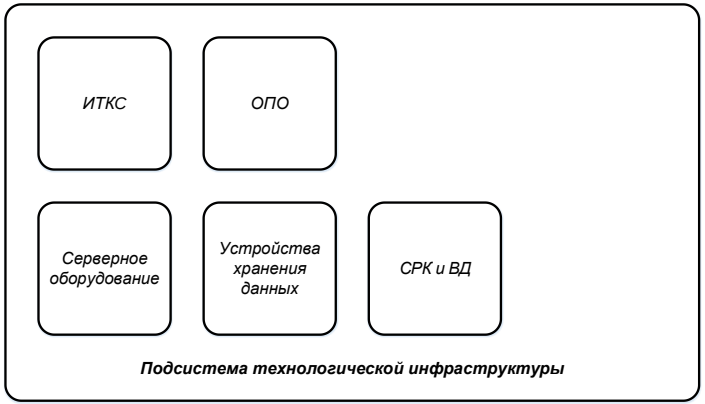
Типовой состав контура

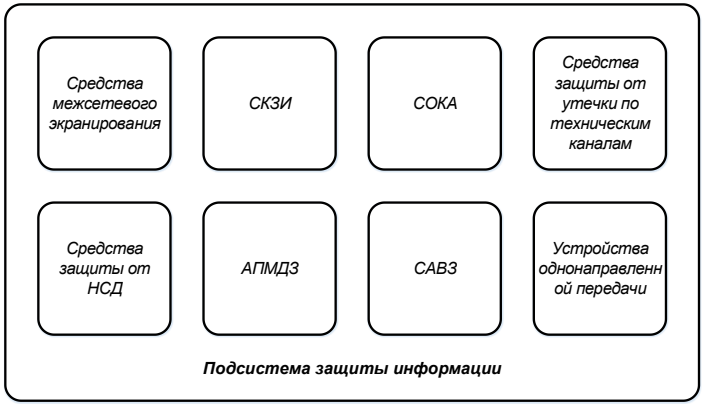












Программное обеспечение технологического контура ЦМИБ

Общесистемное ПО (ОПО):

- ОС Astra Linux Special Edition версия 1.6
- ОС Microsoft Windows 10
- ОС Microsoft Windows Server 2016;

Средства виртуализации:

- VMware vSphere 7
- ESXi
- vCenter Server

Средства резервного копирования и восстановления данных:

- Veeam Backup & Replication (для ОС Windows)
- Veeam Agent для Linux
- Veeam Agent для MS Windows

Прикладное ПО:

- Система мониторинга информационной безопасности NeuroDAT SIEM
- СУБД Postgres Pro AC Standard
- СУБД SQL Svr Standard Edtn 2019

Программное обеспечение ЦМИБ

Подсистема технологической инфраструктуры:

- **Общесистемное ПО (ОПО):** ОС Astra Linux Special Edition версия 1.6, MS Windows 10, MS Windows Server 2016
- **Средства виртуализации:** VMware vSphere 7, ESXi, vCenter Server
- **Средства резервного копирования и восстановления данных:** Veeam Backup & Replication (для ОС Windows), Veeam Agent`ы для Linux и для MS Windows
- **СУБД:** Postgres Pro AC Standard, SQL Svr Standard Edtn 2019

Подсистема МИБ: Система мониторинга информационной безопасности NeuroDAT SIEM

Подсистема защиты от целевых атак: ПО KATA (3 образа на основе ОС CentOS: Sandbox, Central Node, Sensor) и KEDR (компонент в составе Kaspersky Endpoint Security)

Подсистема защиты от утечек информации: ПО «InfoWatch Traffic Monitor Enterprise Edition», «ElcomSoft Premium Forensic Bundle», «Terrier 3.0»

Подсистема контроля действий привилегированных учетных записей (СКДПУ): сервер СКДПУ, сервер СКДПУ НТ (новые технологии)

Подсистема создания персонализированных копий документов, выводимых на печать или устройства отображения: SafeCopy

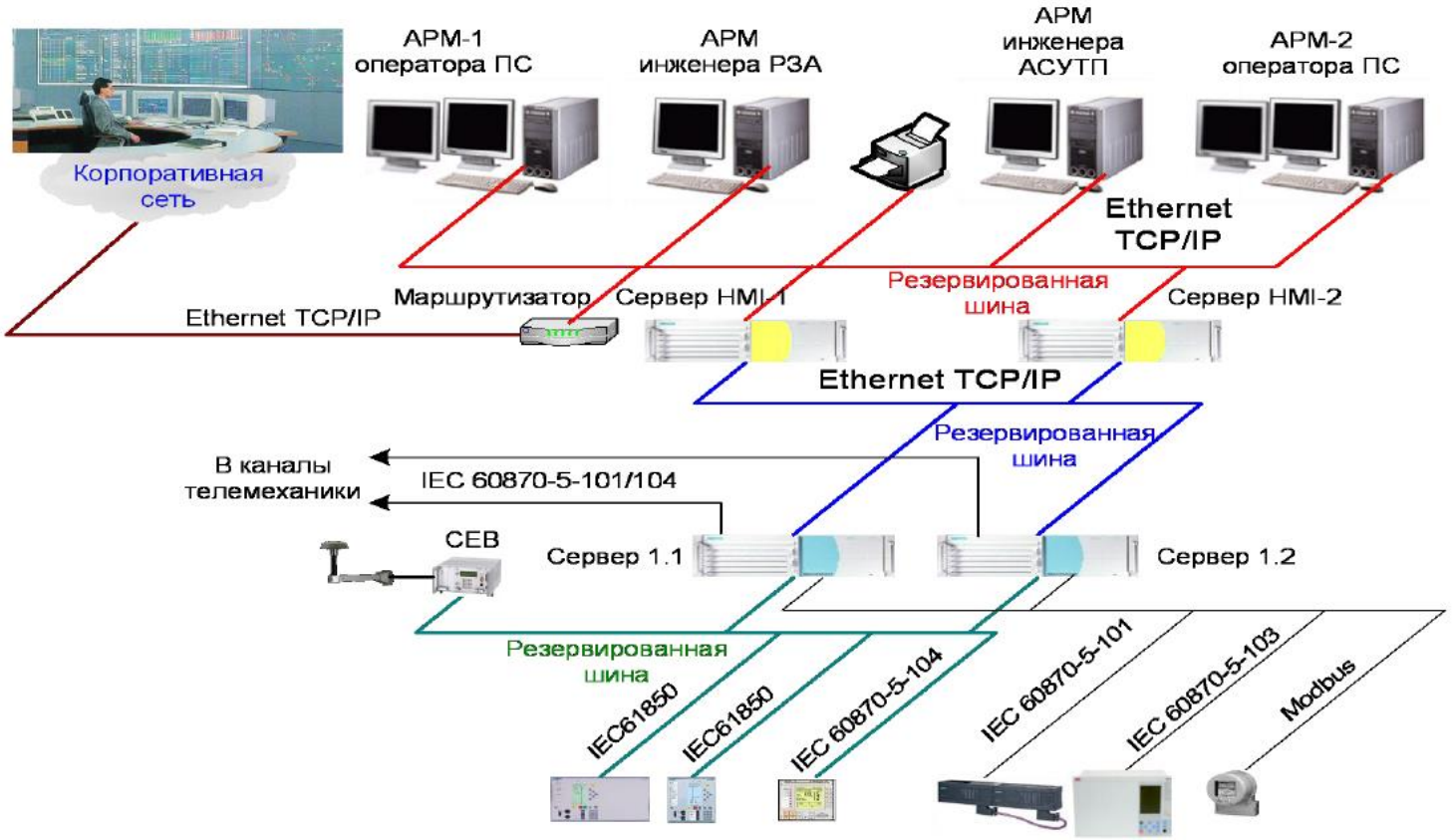
Вопрос 4

Основные понятия и определения в области АСУ ТП

Технологический процесс – (Краткое обозначение – ТП, согласно ГОСТ 3.1109-82) часть производственного процесса (или упорядоченная последовательность взаимосвязанных действий), содержащая целенаправленные действия.

Автоматизированная система управления – (Краткое обозначение – АСУ) комплекс аппаратных и программных средств, а также персонала, предназначенный для управления.

Автоматизированная система управления технологическим процессом – человеко-машинная система управления, обеспечивающая автоматизированный сбор и обработку информации, необходимой для оптимизации управления технологическим объектом в соответствии с принятым критерием.


АРМ-1 оператора ПС
АРМ инженера РЗА
АРМ инженера АСУТП
АРМ-2 оператора ПС
Корпоративная сеть
Ethernet TCP/IP
Маршрутизатор
Сервер HMI-1
Резервированная шина
Сервер HMI-2
Ethernet TCP/IP
Резервированная шина
В каналы телемеханики
IEC 60870-5-101/104
СЕВ
Сервер 1.1
Сервер 1.2
Резервированная шина
IEC61850
IEC61850
IEC 60870-5-104
IEC 60870-5-101
IEC 60870-5-103
Modbus

Технологический объект управления – (Краткое обозначение – ТОУ) это совокупность технологического оборудования и реализованного на нем по соответствующим инструкциям или регламентам технологического процесса производства.

К технологическим объектам управления относятся:

– технологические агрегаты и установки, реализующие самостоятельный технологический процесс;

– отдельные производства (цехи, участки) или производственный процесс всего промышленного предприятия, если управление этим производством носит в основном технологический характер, т. е. заключается в реализации рациональных режимов работы взаимосвязанных агрегатов (участков, производств).

Критерий управления АСУ ТП – это соотношение, характеризующее качество функционирования технологического объекта управления в целом и принимающее конкретные числовые значения в зависимости от
используемых управляющих воздействий.

Цели автоматизации управления:

- предоставление лицу, принимающему решение, релевантных данных для приятия решения;
- ускорение выполнения отдельных операций по сбору и обработке данных;
- снижение количества решений, которое требуется обрабатывать обслуживающему персоналу;
- повышение уровня контроля и исполнительской дисциплины;
- повышение степени обоснованности принимаемых решений.

Цель функционирования АСУ ТП - заключается в оптимизации работы технологического объекта управления по принятому(ым) критерию(ям) управления путем соответствующего выбора управляющих воздействий.

Такими целями, например, могут быть:

- экономия топлива, сырья, материалов и других производственных ресурсов;
- обеспечение безопасности функционирования объекта;
- повышение качества выходного продукта (изделия) или обеспечение заданных значений параметров выходных продуктов (изделий);
- снижение затрат труда человека;
- достижение оптимальной загрузки (использования) оборудования;
- оптимизация режимов работы технологического оборудования и т.д.

Автоматизированная система управления технологическим процессом предназначена для выработки и реализации управляющих воздействий на технологический объект управления.

Функция АСУ ТП – это совокупность действий системы, направленных на достижение частной цели управления.

Функции АСУ ТП подразделяются:

- Управляющие.
- Информационные.
- Вспомогательные.

Управляющая функция АСУ ТП – это функция, результатом которой являются выработка и реализация управляющих воздействий на технологический объект управления.

К управляющим функциям АСУ ТП относятся:

- регулирование (стабилизация) отдельных технологических переменных;
- однотактное логическое управление операциями или аппаратами;
- программное логическое управление группой оборудования;
- оптимальное управление установившимися или переходными технологическими режимами или отдельными участками процесса;
- адаптивное управление объектом в целом (например, самонастраивающимся комплексно-автоматизированным участком станков с числовым
- программным управлением).

Информационная функция АСУ ТП – это функция системы, содержанием которой являются сбор, обработка и представление информация о состоянии АТК оперативному персоналу или передача этой информации для последующей обработки.

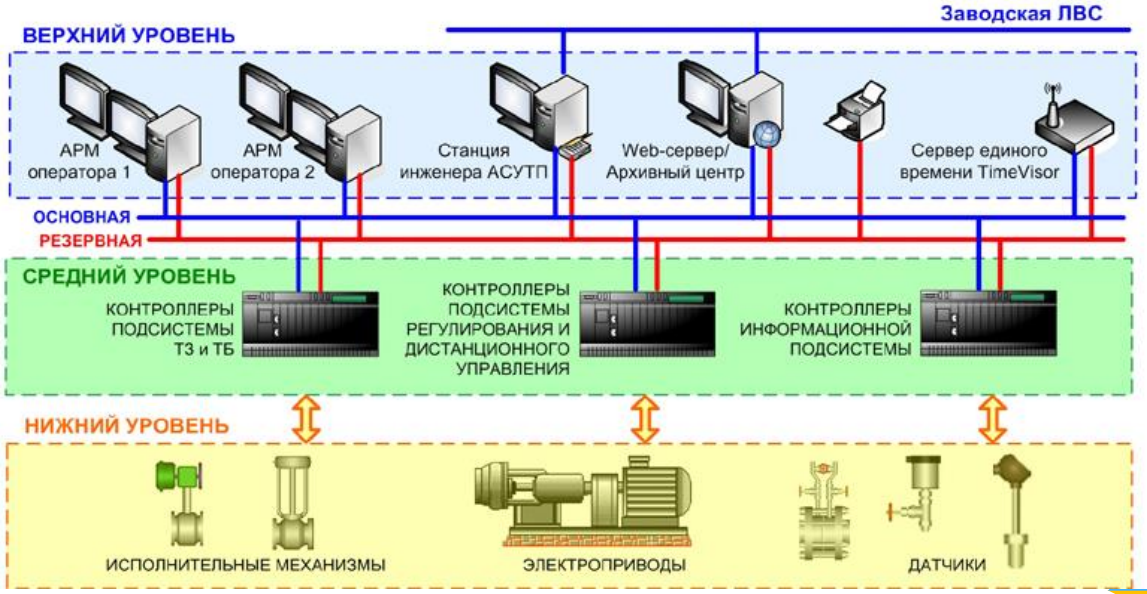
К информационным функциям АСУ ТП относятся:

- централизованный контроль и измерение технологических параметров;
- косвенное измерение (вычисление) параметров процесса (технико-экономических показателей, внутренних переменных);
- формирование и выдача данных оперативному персоналу АСУ ТП;
- подготовка и передача информации в смежные системы управления;
- обобщенная оценка и прогноз состояния ТП и его оборудования.

Вспомогательные функции АСУ ТП – это функции, обеспечивающие решение внутрисистемных задач.

Архитектура автоматизированной системы управления технологическим процессом - это наиболее абстрактное ее представление, которое включает в себя идеализированные модели компонентов системы, а также модели взаимодействий между компонентами.

верхний – диспетчерский;
средний – уровень автоматизированного управления;
нижний – полевой уровень или уровень контрольно-измерительного оборудования (КИП) и исполнительных механизмов.



В сфере промышленного производства с позиции управления можно выделить следующие основные классы структур автоматизированных систем управления технологических процессов:

- централизованную;
- децентрализованную;
- централизованную рассредоточенную;
- иерархическую.

Централизованная структура осуществляет реализацию всех процессов управления объектами в едином органе управления, который осуществляет сбор и обработку информации об управляемых объектах и на основе их анализа в соответствии с критериями системы вырабатывает управляющие сигналы. Появление этого класса структур связано с увеличением числа контролируемых, регулируемых и управляемых параметров и, как правило, с территориальной рассредоточенностью объекта управления.

ICS (Industrial Control System)

Достоинствами централизованной структуры являются достаточно простая реализация процессов информационного взаимодействия; принципиальная возможность оптимального управления системой в целом; достаточно легкая коррекция оперативно изменяемых входных параметров; возможность достижения максимальной эксплуатационной эффективности при минимальной избыточности технических средств управления.

Недостатки централизованной структуры следующие: необходимость высокой надежности и производительности технических средств управления для достижения приемлемого качества управления; высокая суммарная протяженность каналов связи при наличии территориальной рассредоточенности объектов управления.

Децентрализованная структура АСУ ТП

Построение системы с такой структурой эффективно при автоматизации технологически независимых объектов управления по материальным, энергетическим, информационным и другим ресурсам. Такая система представляет собой совокупность нескольких независимых систем со своей информационной и алгоритмической базой.

Для выработки управляющего воздействия на каждый объект управления необходима информация о состоянии только этого объекта.

DCS (Distributed Control System)

Иерархическая структура АСУ ТП

С ростом числа задач управления в сложных системах значительно увеличивается объем переработанной информации и повышается сложность алгоритмов управления. В результате осуществлять управление централизованно невозможно, так как имеет место несоответствие между сложностью управляемого объекта и способностью любого управляющего органа получать и перерабатывать информацию.

Кроме того, в таких системах можно выделить следующие группы задач, каждая из которых характеризуется соответствующими требованиями по времени реакции на события, происходящие в управляемом процессе:

задачи сбора данных с объекта управления и прямого цифрового управления (время реакции - секунды, доли секунды);

задачи экстремального управления, связанные с расчетами желаемых параметров управляемого процесса и требуемых значений уставок регуляторов, с логическими задачами пуска и остановки агрегатов и др. (время реакции Ч секунды, минуты);

задачи оптимизации и адаптивного управления процессами, технико-экономические задачи (время реакции - несколько секунд);

информационные задачи для административного управления, задачи диспетчеризации и координации в масштабах цеха, предприятия, задачи планирования и др. (время реакции Ч часы).

очевидно, что иерархия задач управления приводит к необходимости создания иерархической системы средств управления. такое разделение, позволяя справиться с информационными трудностями для каждого местного органа управления, порождает необходимость согласования принимаемых этими органами решений, то есть создания над ними нового управляющего органа. На каждом уровне должно быть обеспечено максимальное соответствие характеристик технических средств заданному классу задач.

Для выполнения функций АСУ ТП необходимо взаимодействие следующих ее составных частей:

- технического обеспечения (ТО);
- программного обеспечения (ПО);
- информационного обеспечения (ИО);
- организационного обеспечения (ОО);
- оперативного персонала (ОП).

Техническое обеспечение АСУ ТП представляет собой полную совокупность технических средств, достаточную для функционирования АСУ ТП и реализации системой всех ее функций.

Программное обеспечение АСУ ТП – совокупность программ, необходимых для реализации функций АСУ ТП, заданного функционирования комплекса технических средств АСУ ТП и предполагаемого развития системы.

Информационное обеспечение АСУ ТП включает:

– информацию, характеризующую состояние автоматизированного технологического комплекса;

– системы классификации и кодирования технологической и технико-экономической информации;

– массивы данных и документов, необходимых для выполнения всех функций АСУ ТП, в том числе нормативно-справочную информацию.

Организационное обеспечение АСУ ТП представляет собой совокупность описаний функциональной, технической и организационной структур, инструкций и регламентов для оперативного персонала АСУ ТП, обеспечивающее заданное функционирование оперативного персонала в составе АТК.

В состав оперативного персонала АСУ ТП входят:

– технологи-операторы, осуществляющие контроль за работой и управление технологическим объектом управления с использованием информации и рекомендаций по рациональному управлению, выработанных комплексом технических средств АСУ ТП;

– эксплуатационный персонал АСУ ТП, обеспечивающий правильность функционирования комплекса технических средств АСУ ТП.