Исследования в области обеспечения безопасности информации, обрабатываемой в автоматизированных системах управления технологическими процессами, являющихся объектами критической информационной инфраструктуры

Докладчик: Енютин А.Ю.
ФАУ «ГНИИИ ПТЗИ ФСТЭК России»

Вопросы доклада

1. Угрозы безопасности информации в АСУ ТП

2. Характеристика АСУ ТП как объектов защиты от угроз безопасности информации

3. Основные результаты исследований в области обеспечения безопасности АСУ ТП от реализации компьютерных атак

1. Угрозы безопасности информации в АСУ ТП

АСУ ТП как объекты КИИ

АСУ технологическими процессами

Комплекс программных и программно-аппаратных средств, предназначенных для контроля за технологическим и (или) производственным оборудованием (исполнительными устройствами) и производимыми ими процессами, а также для управления такими оборудованием и процессами

Сферы деятельности, в которых применяются АСУ ТП

Наука

Здравоохранение

Транспорт

Энергетика

ТЭК

Атомная энергия

Промышленность

Ракетно-космическая

Оборонная

Горно-добывающая

Метал-лургическая

Химическая

Основные причины, обусловливающие возможность реализации угроз безопасности информации в АСУ ТП

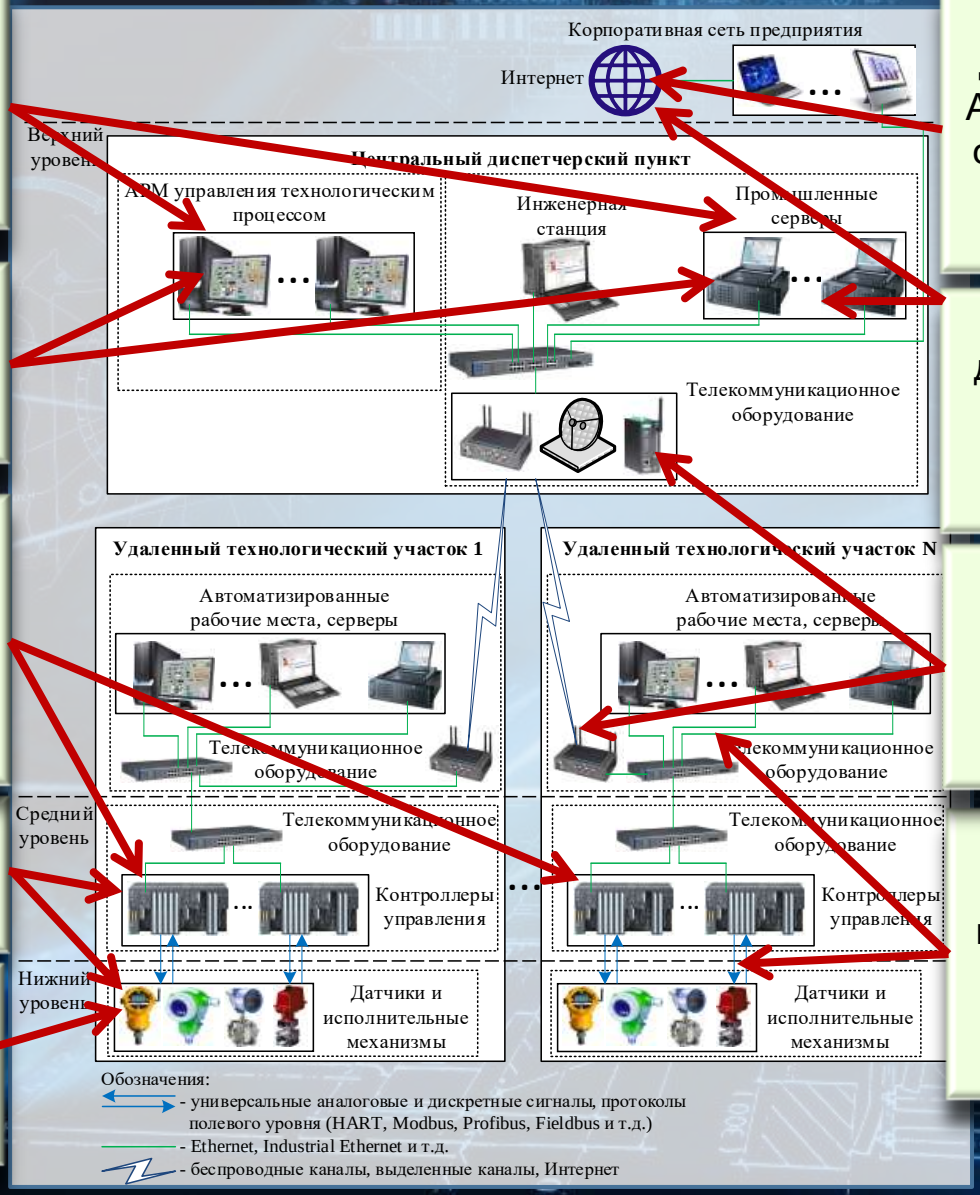
Использование программного обеспечения широкого применения, имеющего уязвимости

Ограничения на обновление программного обеспечения

Ограниченные вычислительные ресурсы, исключающие возможности установки программных средств защиты информации

Слабые механизмы идентификации и аутентификации

Расположение отдельных компонентов системы за пределами контролируемых зон



Каналы обмена данными со смежными АСУ, информационными системами, в том числе через сети общего пользования

Наличие открытых для доступа общих сетевых ресурсов (в том числе из сети Интернет)

Использование беспроводных технологий передачи данных и мобильных технических средств

Использование протоколов передачи информации, в которых не предусмотрены механизмы защиты информации

Основные источники угроз безопасности информации в АСУ ТП

Источники угроз

Нарушители

Внешние

- Лица, действующие из локальной вычислительной сети предприятия;
- Лица, действующие из внешних информационных систем и сетей связи

Внутренние

- Представители обслуживающего персонала
- Сотрудники, имеющие непосредственный доступ к компонентам АСУ ТП

Закладки

Программные

- В прикладном или системном программном обеспечении
- В специальном программном обеспечении

Аппаратные

- Конструктивно встроенные
- Автономные

Вредоносные программы

«Общего назначения»

- Троянские программы
- Вирусы
- Сетевые черви и т.д.

Специализированные для АСУ ТП

- Внедряемые в АРМ и серверы
- Внедряемые в программируемые логические контроллеры

Основные способы реализации угроз безопасности информации внешними и внутренними нарушителями

Внешние нарушители

Удаленный доступ через общедоступные сетевые ресурсы

Факт:
Более 160 000 компонентов АСУ ТП доступны в сети Интернет.

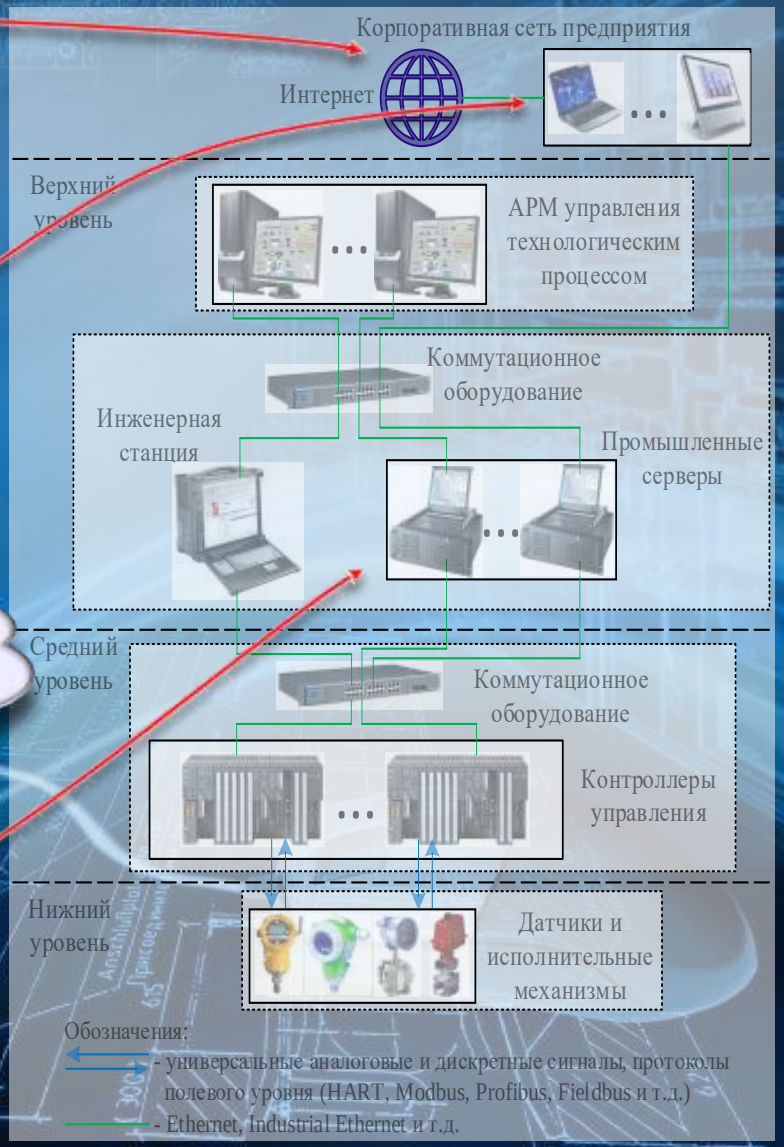
Удаленный доступ через компоненты корпоративной сети предприятия

Внутренние нарушители

Факт:
По результатам исследований в более, чем в 80% случаев может быть получен доступ из корпоративной сети

Непосредственный физический доступ

Беспроводные сети



Основные способы внедрения программных и аппаратных закладок

Программные закладки

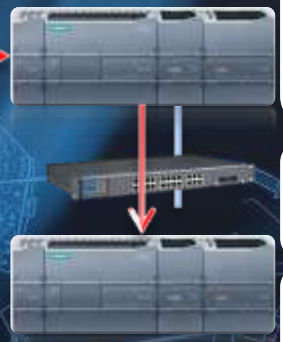
- На этапе разработки производителем программного обеспечения
- При обновлении из недоверенных (скомпрометированных) источников
- Внутренними нарушителями
- На этапе сервисного обслуживания

Аппаратные закладки

- Конструктивное встраивание на производстве компонентов АСУ ТП
- Внедрение автономных закладок (устройств) внутренними нарушителями

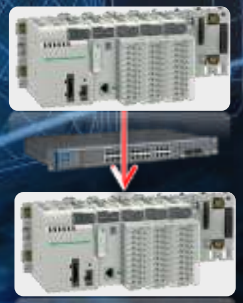
Новый вид вредоносных программ для программируемых логических контроллеров

ПЛК Siemens



PoC-код сетевого червя **PLC-Blaster**

ПЛК Schneider Electric



PoC-код сетевого червя **ClearEnergy**

ПЛК Schneider Electric

Вредоносное ПО **Triton (Trisis, HatMan)**

Заражение	• Сканирование для поиска ПЛК Siemens по 102 порту протокола TCP • Червь копирует себя в один из функциональных блоков ПЛК
Распространение	• Сканирование сети • Заражение обнаруженных ПЛК
Воздействие	• Останов ПЛК • Выдача управляющих воздействий
Заражение	• Сканирование сети с целью поиска уязвимых устройств • Получение релейных диаграмм управления
Воздействие	• Удаление релейных схем управления
Заражение	• Проникновение в системы противоаварийной защиты • Перепрограммирование системы, предназначенной для мониторинга состояния ТП
Воздействие	• Завершение производственного процесса или игнорирование тревожных признаков

Последствия реализации угроз безопасности информации в АСУ ТП

Последствия от реализации угроз безопасности информации характеризуются нарушением **целостности, доступности** и конфиденциальности защищаемой информации

Уничтожение или модификация защищаемой информации

Невозможность (затруднение) использования защищаемой информации персоналом и (или) оборудованием

Предпосылка к нарушению технологического процесса, вызванная искажением (изменением) циркулируемой в АСУ ТП защищаемой информации

Отсутствие возможности контроля и управления ходом технологического процесса вследствие блокировки выполнения функций АРМ операторов, серверов, инженерной станции, коммуникационного сервера

Возникновение аварийных ситуаций на объекте из-за выдачи неверных команд управления или несанкционированного изменения значений параметров и границ блокировок

Нарушение технологического процесса (возникновение аварийных ситуаций на объекте) из-за блокировки работы контроллера и несанкционированного выключения (уничтожения) программных или аппаратных средств

Ущерб от реализации угроз безопасности информации в АСУ ТП

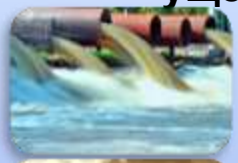
Угрозы информационной безопасности

Промышленные объекты

Аварии

Останов технологического процесса

Экологический ущерб



Загрязнение водоемов

Загрязнение атмосферы

Загрязнение земель

Социальный ущерб

Жизнь и здоровье людей

Транспортное обеспечение

Обеспечение жизнедеятельности

Экономический ущерб

Доходы бюджетов РФ

Доходы субъекта

Ущерб для обороны

Показатели гособоронзаказа

Основные зарегистрированные инциденты безопасности информации в АСУ ТП

Отрасль	Инцидент
Нефтепереработка Иран (2012 г.) 	Вирусная атака на компьютерные системы нефтяной компании Saudi Aramco
Металлургия Германия (2014 г.) 	Несанкционированный доступ к системе управления заводом
Водоочистка США (2016 г.) 	Атака на систему управления водоочистной станции
Атомная энергетика Южная Корея (2016 г.) 	Атака с применением компьютерного вируса
Энергетика Украина (2016 г.) 	Комбинированная атака на энергетические системы
Автомобильная промышленность Франция (2017 г.) 	Заражение вирусом WannaCry

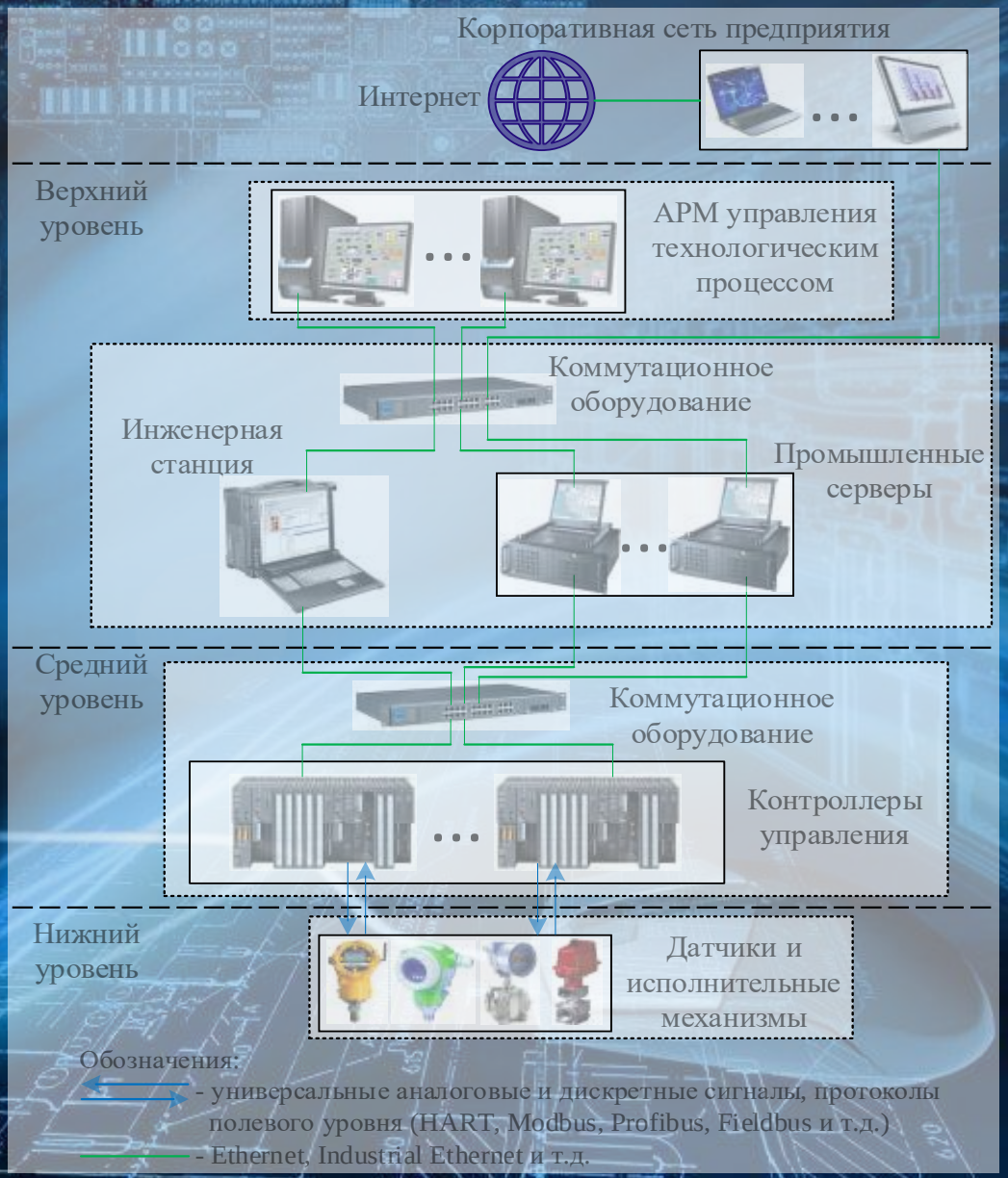
2. Характеристика АСУ ТП как объектов защиты от угроз безопасности информации

Многоуровневая архитектура АСУ ТП

Уровень операторского (диспетчерского) управления (верхний уровень)

Уровень автоматического управления (средний уровень)

Уровень контрольно-измерительных приборов и исполнительных механизмов (нижний (полевой) уровень)



Уровень операторского (диспетчерского) управления (верхний уровень)

Как объект защиты верхний уровень имеет следующие особенности:

Возможность подключения к смежным АСУ ТП и иным информационным системам

Возможность подключения к корпоративной сети предприятия

Использование широко распространенных программно-аппаратных компонентов «офисного типа»

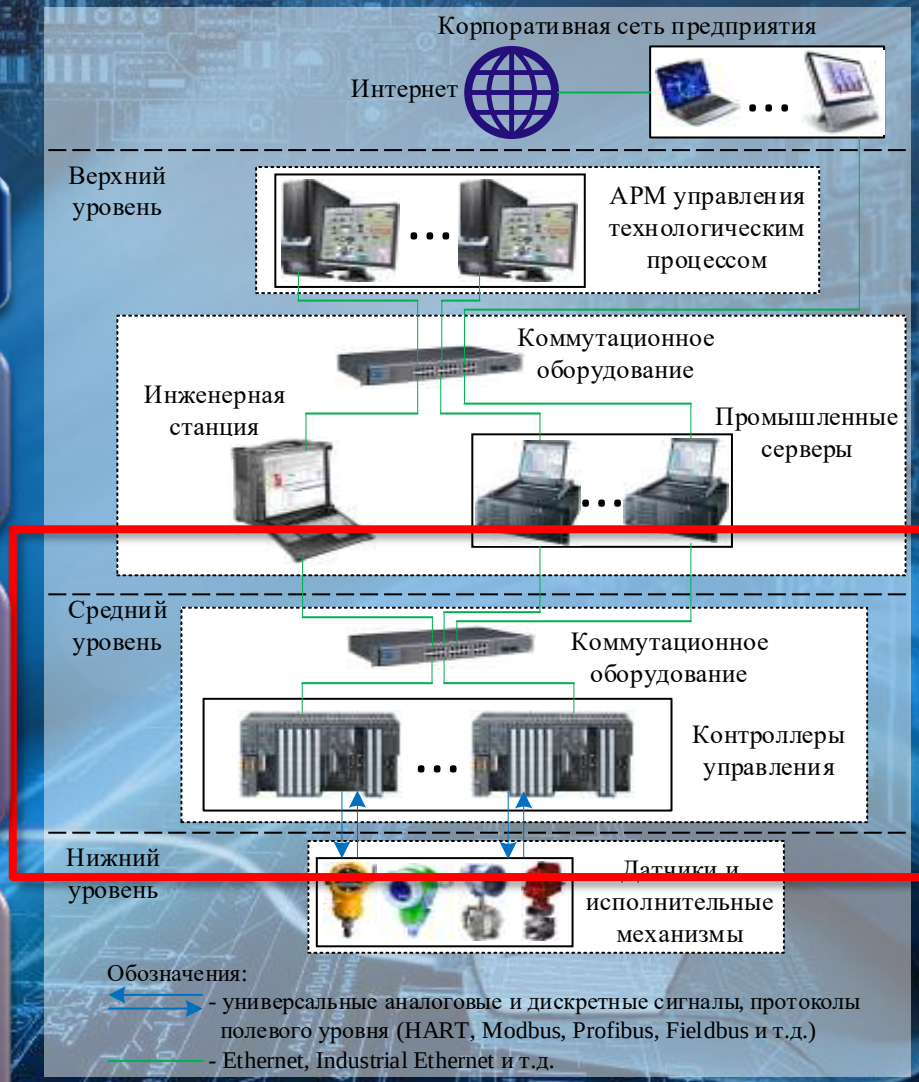
Уровень автоматического управления (средний уровень)

Как объект защиты средний уровень имеет следующие особенности:

Возможность размещения отдельных компонентов в неохраняемых помещениях

Возможность размещения отдельных компонентов на удаленных производственных площадках без постоянного присутствия персонала

Использование протоколов передачи данных, не предусматривающих механизмы защиты передаваемой информации (информация передается в открытом виде)



Уровень контрольно-измерительных приборов и исполнительных механизмов (нижний (полевой) уровень)

Как объект защиты нижний уровень имеет следующие особенности:

Возможность размещения отдельных компонентов в неохраняемых помещениях, на удаленных производственных площадках без постоянного присутствия персонала

Территориальная распределенность с возможностью выхода каналов передачи данных за пределы контролируемых зон

Использование протоколов передачи данных, не предусматривающих механизмы защиты передаваемой информации (информация передается в открытом виде)

Понятие SCADA-система

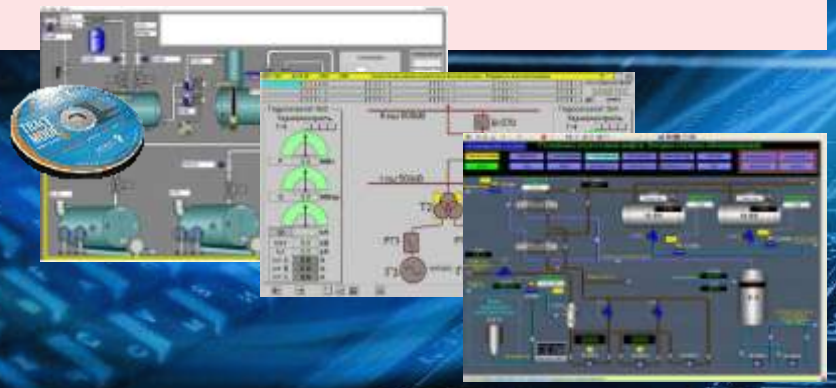
SCADA (*Supervisory Control And Data Acquisition*) - *диспетчерское управление и сбор данных*

SCADA-технология - *информационная технология, основанная на применении* ***SCADA-систем*** *для контроля и управления технологическими процессами на промышленных производственных объектах*

SCADA-система

1

Программный комплекс (программный пакет), *обеспечивающий выполнение функций контроля, сбора данных и диспетчерского управления*



2

Программно-аппаратный комплекс, *обеспечивающий связь с объектом управления, выполнение функций контроля, сбора данных, автоматического и диспетчерского управления*

Типы АСУ ТП

Локальные АСУ ТП (ПЛК-системы)

- высокая степень автономности функционирования.
- уровень операторского управления в таких системах может отсутствовать.
- как правило располагаются в одном помещении с объектом управления

Распределенные системы управления (РСУ)

- предназначены для автоматизированного управления и контроля отдельной производственной площадкой (технологического процесса) или совокупностью распределенных производственных площадок.
- как правило содержат несколько сегментов, которые, располагаются в различных помещениях

SCADA-системы

- как правило предназначены для управления территориально распределенными объектами.
- имеют центральный диспетчерский пункт контроля и управления

Типовая архитектура локальных систем управления (ПЛК-систем)

Особенности построения

Возможное отсутствие каналов обмена данными с другими АСУ ТП или информационными системами

Высокоскоростное управление дискретными операциями

Отказоустойчивость системы управления может быть не критична (в случае останова ТП возобновляется в короткие сроки и с минимальными потерями)

Возможное отсутствие уровня операторского управления (высокая степень автономности)

Жесткая временная синхронизация работы нескольких узлов.

Типовая архитектура РСУ

Особенности построения

Технологическая информация между компонентами РСУ передается по локальным вычислительным сетям, как правило, не выходящим из контролируемых зон

Возможно подключение к компонентам корпоративной сети предприятия

В ряде случаев для управления ТП необходимым является непосредственное участие оператора (диспетчера)

Резервирование основных компонентов системы

Возможность использования систем реального времени

Возможность использования интегрированных систем управления (компоненты всех уровней построены на базе одной программной платформы)

Типовая архитектура SCADA-системы

Особенности построения

Включение в состав системы множества взаимодействующих компонентов, находящихся на значительном удалении друг от друга, и имеющих различные программно-аппаратные платформы

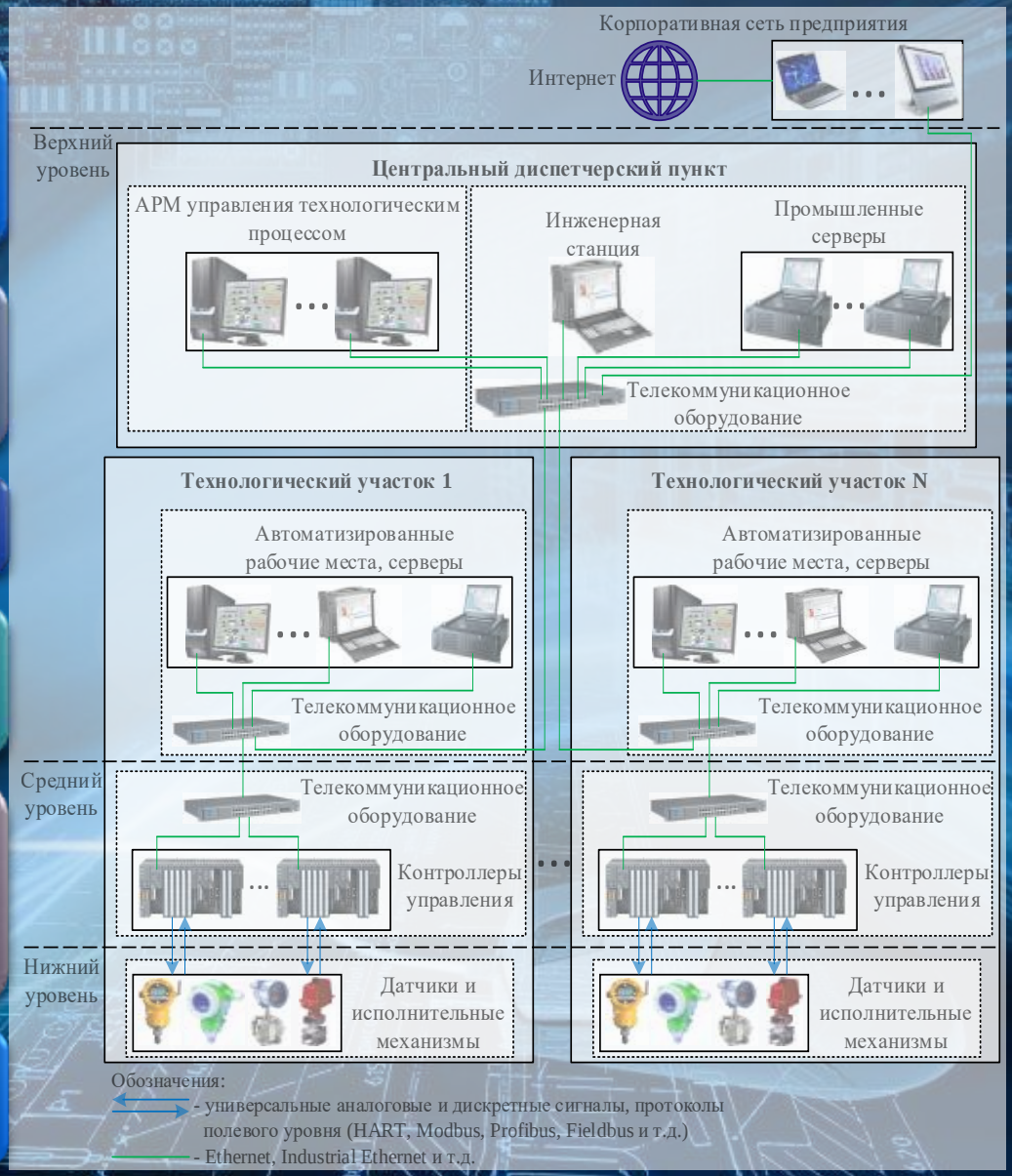
В ряде случаев для управления ТП непосредственное участие оператора (диспетчера) не требуется (на него возлагаются только функции диспетчерского контроля)

Выход линий связи за пределы контролируемых зон

Возможное использование в качестве каналов связи сетей общего пользования и беспроводных каналов передачи данных

Управление различными удаленными друг от друга технологическими участками, в ряде случаев имеющими свои системы управления, в том числе построенные на различных программно-аппаратных платформах

Возможность подключения к компонентам корпоративной сети предприятия



3. Основные результаты исследований в области обеспечения безопасности АСУ ТП от реализации компьютерных атак

Лабораторно-исследовательский полигон ФАУ «ГНИИИ ПТЗИ ФСТЭК России»

Банк данных угроз безопасности информации

Открытые источники информации

Подсистема выявления уязвимостей и анализа угроз безопасности информации

Подсистема анализа защищенности

Подсистема тестовой реализации угроз

Подсистема исследования мер и средств защиты

Подсистема моделирования функционирования объектов КИИ (виртуализация, макетирование)

Подсистема моделирования критических процессов

Всего исследовано более 50 различных технологических процессов (ГЭС, транспортировка нефти, производство аммиака и др.)

Созданы макеты на базе оборудования более 5 фирм производителей (Siemens, «Текон» и др.)

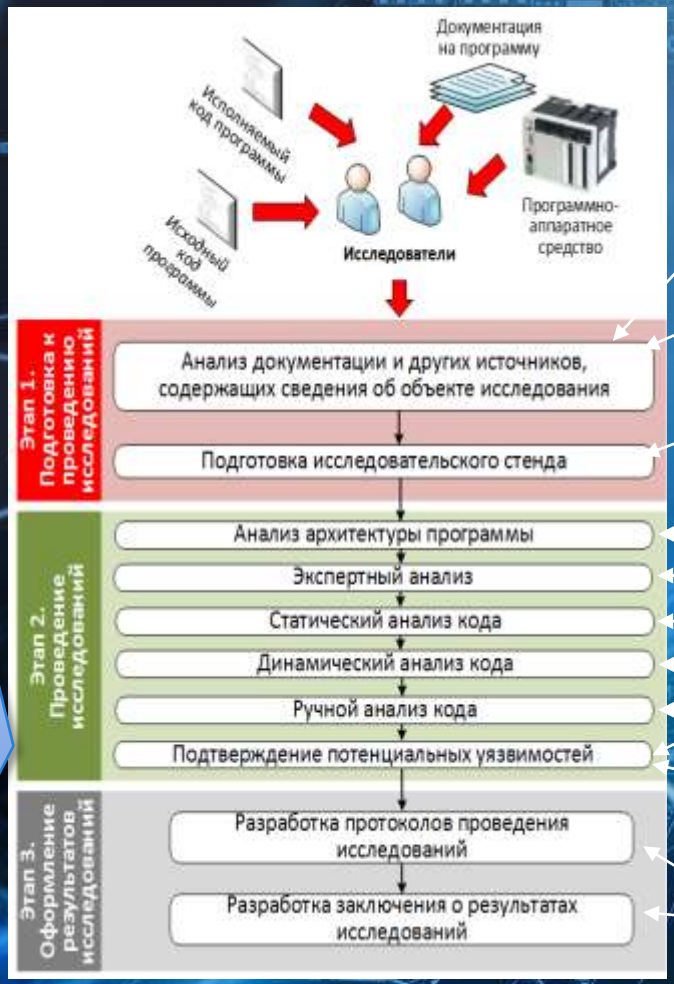
Исследования по выявлению уязвимостей

Комплекс методов по выявлению уязвимостей

- Методы экспертного анализа
- Методы динамического анализа
- Методы статического анализа
- Методы комбинированного анализа

Всего более 40 основных и вспомогательных методов

Порядок проведения исследований



Автоматизация процедур

- Специальные поисковые программы («парсеры»)
- Программы анализа данных («Data mining»)
- Программные средства виртуализации и моделирования
- Программные средства автоматизированного анализа кода
- Дизассемблеры, декомпилляторы
- Программы создания PoC-кодов уязвимостей
- Базы эксплойтов и PoC-кодов
- Программы автоматизированного анализа результатов исследования и формирования отчетов

Примечание: – Внедренные программные средства; – Перспективные (разрабатываемые) программные средства

Исследования по оценке защищенности

Моделирование действий внешнего нарушителя

Моделирование действий внутреннего нарушителя

Оценка потенциала нарушителей

Выявление актуальных угроз и уязвимостей

Определение последствий реализации угроз

Исследования возможных действий нарушителя на всех стадиях реализации атаки

Получение доступа → **Выполнение кода** → **Закрепление в системе** → **Повышение привилегий** → **Обход защиты** → **Получение учетных данных**

Теневая загрузка
ID: T1189 *
•УБИ.011 **

Аппаратные закладки
ID: T1200
•УБИ.023

Выполнение через API
ID: T1106
•УБИ.068

Выполнение пользователем
ID: T1204
•УБИ.006

Создание учетных записей
ID: T1136
•УБИ.198

Автозапуск в офисных приложениях
ID: T1137
•УБИ.89

Обход контроля учетных записей
ID: T1088
•УБИ.031

Эксплуатация уязвимостей для повышения привилегий
ID: T1068
•УБИ.122

Подписание кода
ID: T1116
•УБИ.162

Прошивка компонентов
ID: T1189
•УБИ.005

Манипулирование учетными записями
ID: T1189
•УБИ.197

Метод грубой силы
ID: T1189
•УБИ.008

ID:T1111 – идентификатор метода действия нарушителя *(attack.mitre.org)*
УБИ.111 – идентификатор угрозы в Банке данных угроз *(bdu.fstec.ru)*

Исследования возможных действий нарушителя на всех стадиях реализации атаки

Обзор системы

Сканирование сетевых сервисов
ID: T1046
- УБИ.098

Обнаружение информации о системе
ID: T1082
- УБИ.139

Горизонтальное продвижение

Эксплуатация удаленных служб
ID:T1210
- УБИ.167

Копирование с помощью съемных носителей
ID:T1091
- УБИ.088

Сбор данных

Сбор данных из буфера обмена
ID: T1115
- УБИ.093

Автоматизи-рованный сбор
ID: T1113
- УБИ.036

Утечка

Шифрование данных
ID: T1022
- УБИ.193

Утечка данных на физическом носителе
ID: T1052
- УБИ.071

Управление и контроль

Использование протокола прикладного уровня
ID: T1071
- УБИ.034

Маскировка данных
ID: T1001
- УБИ.111

ID:T1111 – идентификатор метода действия нарушителя *(attack.mitre.org)*
УБИ.111 – идентификатор угрозы в Банке данных угроз *(bdu.fstec.ru)*

Исследования по оценке защищенности

Перечень выявленных актуальных угроз

Угроза 1

Угроза N

Меры и средства защиты

Оценка способности различных применяемых мер и средств защиты информации противостоять угрозам

Оценка влияния технических средств защиты на штатное функционирование системы

Результаты исследований на полигоне

Более 15 фирм-производителей АСУ ТП

SIEMENS (Германия)

tecon (Россия)

Более 30 фирм-производителей программного обеспечения

CISCO

symantec.

ZyXEL

Более 50 технологических процессов

Выявлено более **500** неизвестных ранее уязвимостей программного обеспечения (из них более **100** для программного обеспечения АСУ ТП).
Всего внесено более **21 000** описаний уязвимостей программного обеспечения

БАНК ДАННЫХ УГРОЗ безопасности информации БДУ

Внесено более **200** описаний угроз безопасности информации

Разработана утилита, позволяющая автоматически определять наличие уязвимостей в информационной системе

Направления развития исследований

- Методы определения актуальных угроз.
- Автоматизация построения сценариев угроз

Подсистема выявления уязвимостей и анализа угроз безопасности информации

- Методы анализа больших объемов данных (Data mining).
- Автоматизация сбора сведений об угрозах и уязвимостях.
- Прогнозирование угроз

Подсистема анализа защищенности

Подсистема тестовой реализации угроз

Создание базы PoC-кодов и средств их реализации

- Методы оптимизации при выборе мер защиты.
- Автоматизация задания требований к защите на основе данных об угрозах

Подсистема исследования мер и средств защиты

Подсистема моделирования функционирования объектов КИИ (виртуализация, макетирование)

- Расширение номенклатуры оборудования и программного обеспечения.
- Расширение возможностей виртуализации

Подсистема моделирования критических процессов

- Создание базы моделей типовых объектов.
- Разработка методов выявления критических параметров и построения сценариев развития нештатных ситуаций

Цель развития исследовательской базы

Повышение достоверности данных об угрозах безопасности информации и уязвимостях

+

Снижение ресурсозатрат на проведение анализа

+

Исключение «человеческого фактора»

+

Повышение обоснованности принимаемых мер защиты

+

Принятие превентивных мер защиты на основе данных прогноза угроз безопасности информации

=

Увеличение полноты и достоверности сведений о существующих в системе угрозах и уязвимостях

+

Повышение эффективности принимаемых мер защиты

=

Повышение защищенности объектов критической информационной инфраструктуры

Исследования в области обеспечения безопасности информации, обрабатываемой в автоматизированных системах управления технологическими процессами, являющихся объектами критической информационной инфраструктуры