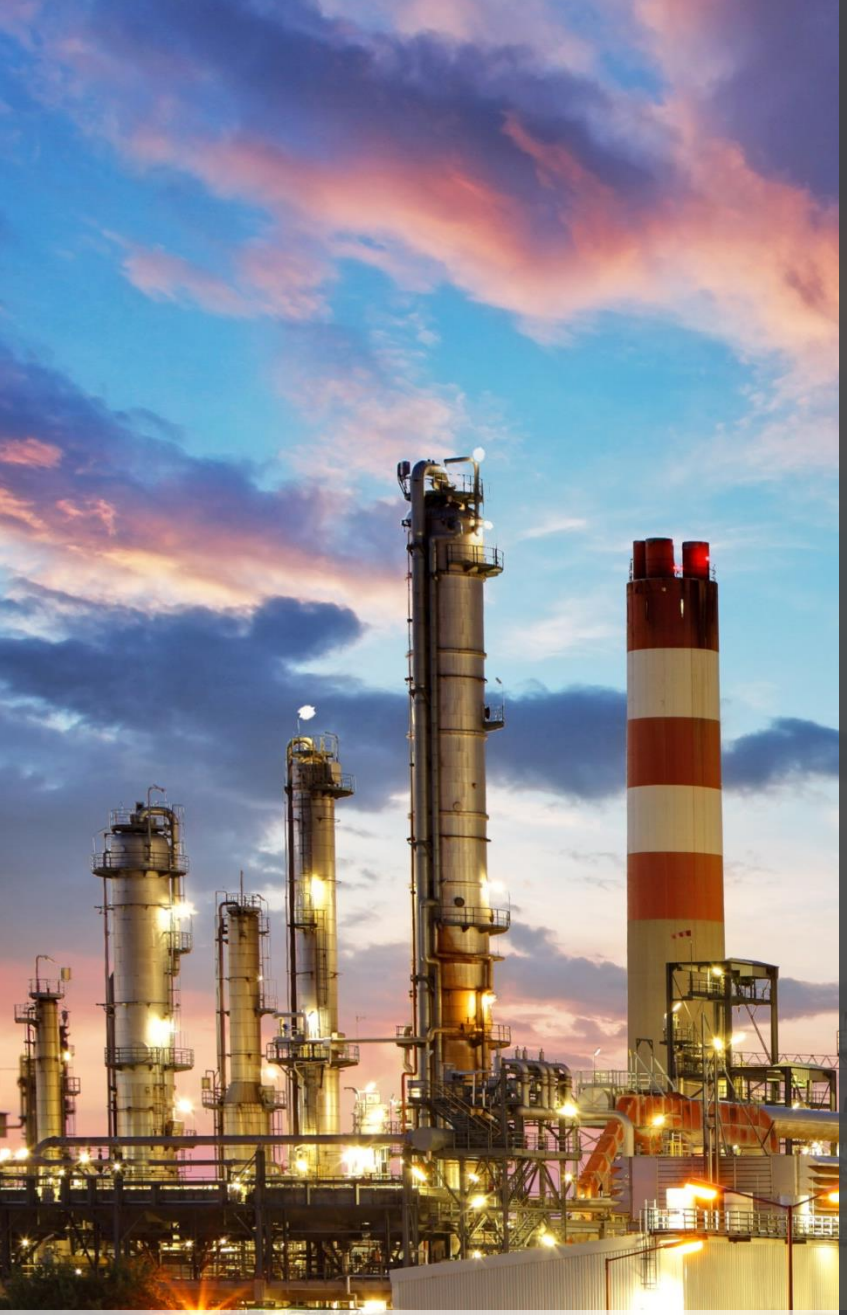


INFOWATCH®

МЫ РАБОТАЕМ,
ЧТОБЫ ЗАЩИЩАТЬ

Вопросы выбора средств защиты для АСУТП и значимых объектов КИИ

Юршев Андрей Юрьевич

INFOWATCH®

Требования законодательства РФ по обеспечению безопасности АСУТП и значимых объектов критической информационной инфраструктуры

INFOWATCH®

АСУТП - значимый объект КИИ

Необходимость создания системы **безопасности значимого объекта КИИ** определена Федеральным законом от 26 июля 2017 г. **№187-ФЗ**

Требования к созданию систем безопасности **значимых объектов КИИ** определены Приказом ФСТЭК России от 21 декабря 2017 г. **№235**

АСУТП объекта ТЭК, КВО, не значимый объект КИИ

Необходимость создания системы защиты информации и информационно-телекоммуникационных сетей объектов ТЭК определена Федеральным законом от 21 июля 2011 г. **№ 256-ФЗ**

Требования к обеспечению защиты информации в АСУТП определены Приказом ФСТЭК России от 14 марта 2014 г. **№31**

Ответственность проектировщиков КИИ/КВО

Если воздействие на объект КИИ/АСУТП повлекло причинение крупного ущерба (особо крупного, тяжкого вреда здоровью, смерть)

УК РФ Статья 293. Халатность

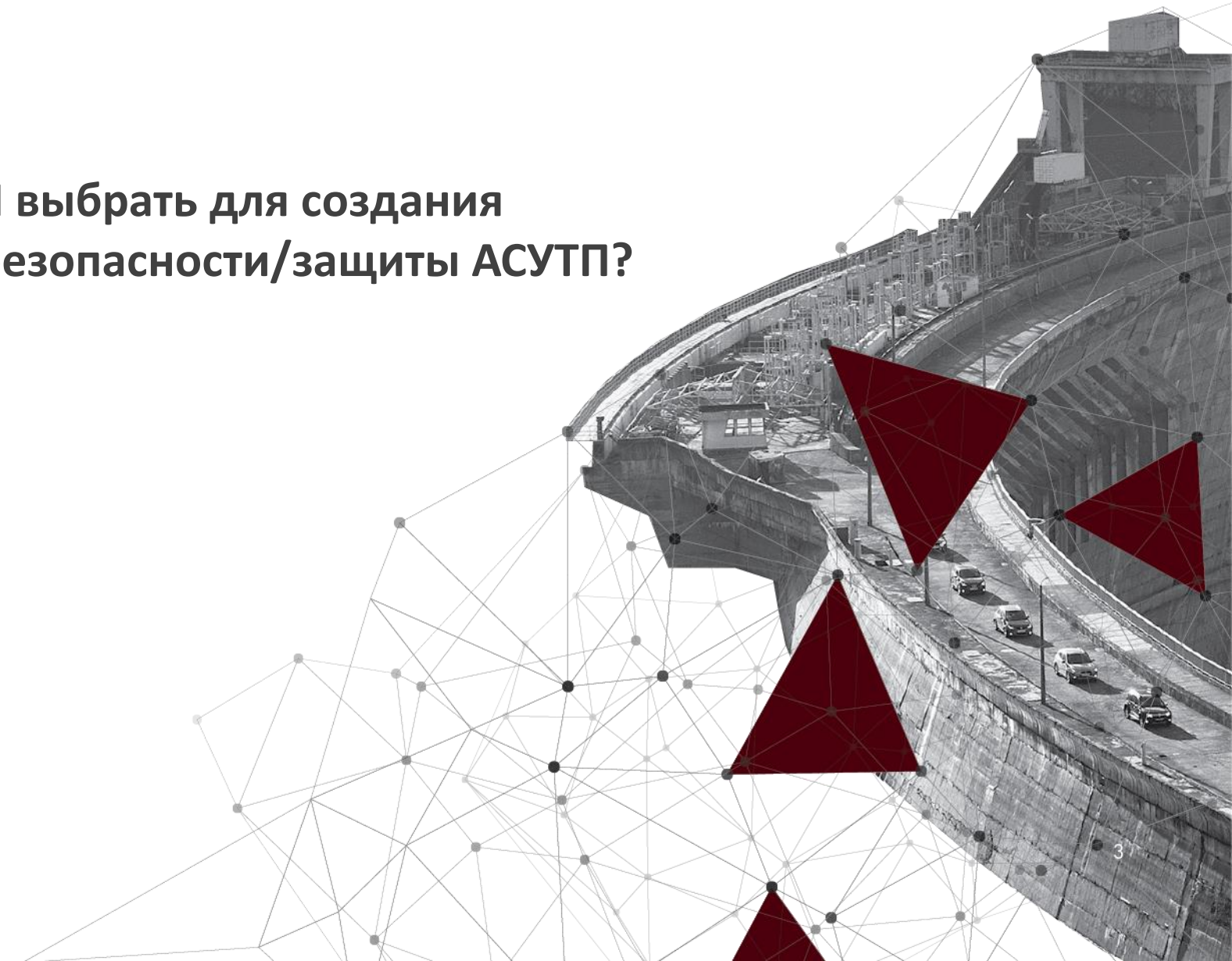
Халатность, то есть неисполнение или ненадлежащее исполнение должностным лицом своих обязанностей вследствие недобросовестного или небрежного отношения к службе либо обязанностей по должности, если это повлекло причинение крупного ущерба (особо крупного, тяжкого вреда здоровью, смерть) или существенное нарушение прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства

УК РФ Статья 217.1. Нарушение требований обеспечения безопасности и антитеррористической защищенности объектов топливно-энергетического комплекса

Как решит следствие и суд…

УК РФ Статья 274.1 Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации – для хакеров и субъектов КИИ/КВО

Какие СЗИ выбрать для создания системы безопасности/защиты АСУТП?



Приказ ФСТЭК России от 22.12.2017 № 235

Выбираем:

- **Сертифицированные** на соответствие требованиям по безопасности
- Прошедшие **оценку соответствия** в форме **испытаний** или **приёмки требованиям по безопасности**
- **С учетом возможных ограничений** со стороны производителей СЗИ на их применение на объектах КИИ

Есть возможность привлечения лицензиата к оценке соответствия

Приказ ФСТЭК России от 25.12.2017 № 239

Выбираем:

- **Сертифицированные** на соответствие требованиям по безопасности
- Прошедшие **оценку соответствия требованиям по безопасности** в форме **испытаний** или **приёмки**
- **Совместимые** с объектом КИИ
- **Не оказывающие негативного влияния** на создание и функционирование значимого объекта КИИ

Есть возможность привлечения лицензиата к оценке соответствия

Требования по созданию систем безопасности / защиты АСУТП

Приказ ФСТЭК России от 14.03.2014 № 31

Выбираем:

- **Сертифицированные** по требованиям безопасности информации
- **Прошедшие оценку соответствия**
- **Совместимые** с АСУТП
- **Не оказывающие отрицательного влияния** на штатный режим функционирования АСУ

Требования законодательства РФ по обеспечению безопасности АСУТП и значимых объектов критической информационной инфраструктуры

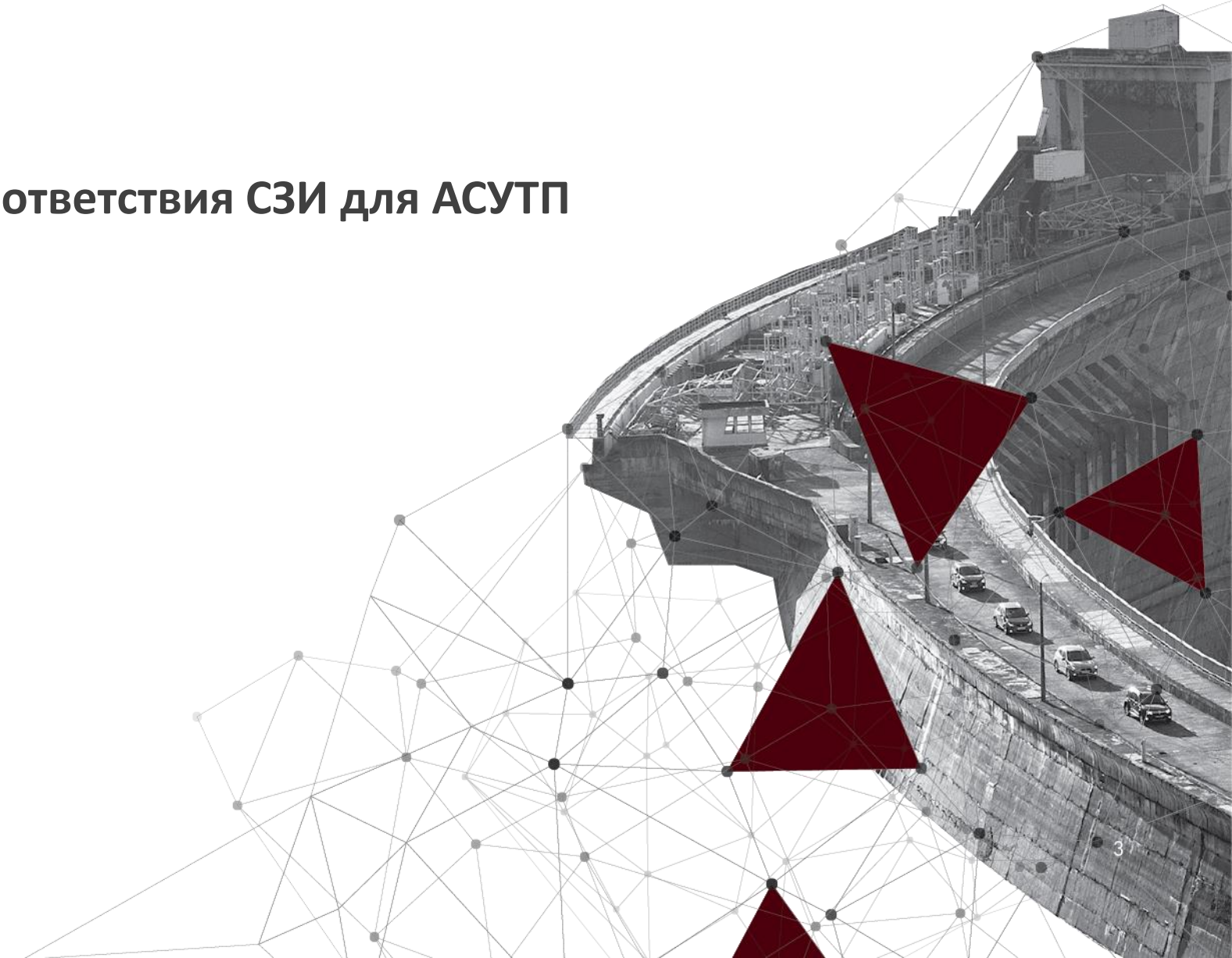
Эти СЗИ д.б. совместимы с АСУТП

В первую очередь выбираются встроенные в ПО или аппаратно-программные средства СЗИ/механизмы защиты АСУТП:

- Приказ ФСТЭК России от 14.03.2014 **№ 31, пункт 24**
- Приказ ФСТЭК России от 21.12.2017 **№235, пункт 19**
- Приказ ФСТЭК России от 25.12.2017 **№239, пункт 27**

Но есть ли в них необходимый функционал ИБ?

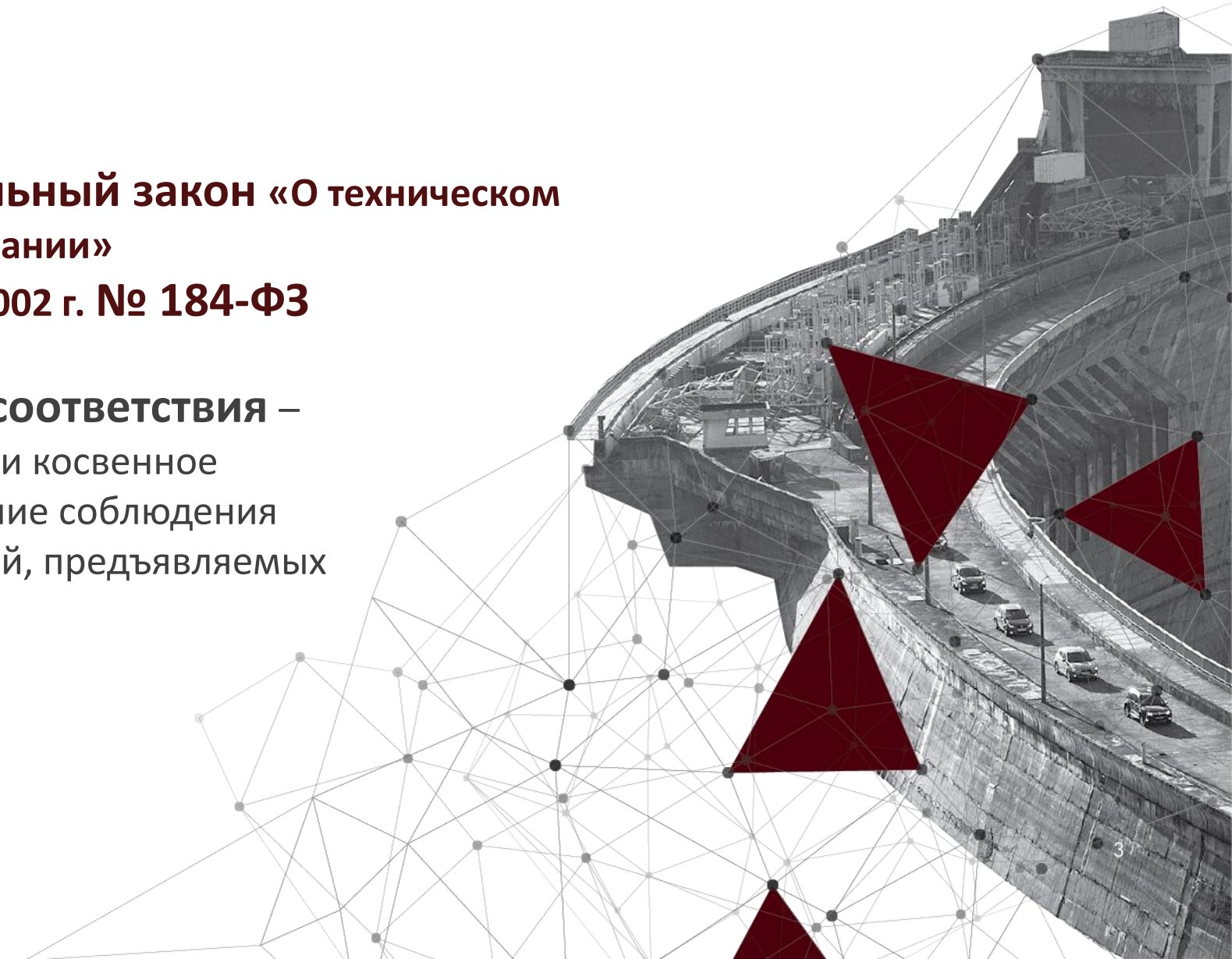
Оценка соответствия СЗИ для АСУТП



Оценка соответствия СЗИ АСУТП

Федеральный закон «О техническом регулировании»
от 27.12.2002 г. № 184-ФЗ

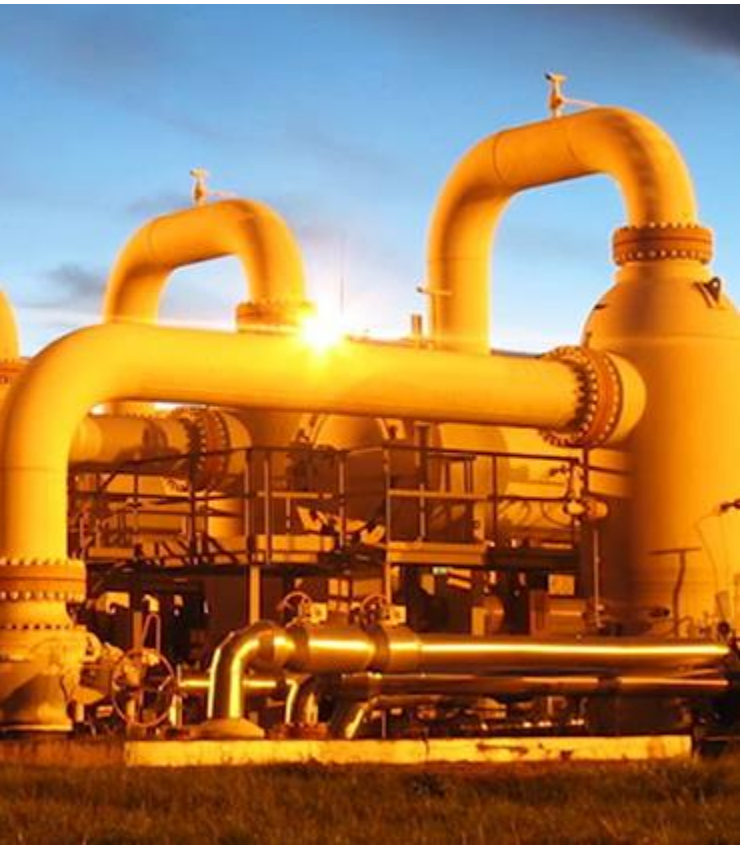
Оценка соответствия –
прямое или косвенное определение соблюдения требований, предъявляемых к объекту



Оценка соответствия СЗИ АСУТП

INFOWATCH®

Федеральный закон «О техническом регулировании» от 27.12.2002 г. № 184-ФЗ



Статья 7, пункт 3

Оценка соответствия проводится в формах:

1. государственного контроля (надзора)
2. ***испытания***
3. регистрации
4. ***подтверждения соответствия***
5. ***приемки*** *и ввода в эксплуатацию объекта,* строительство которого закончено
6. в иной форме

ОБЯЗАТЕЛЬНАЯ СЕРТИФИКАЦИЯ

INFOWATCH®

Федеральный закон «О техническом регулировании» от 27.12.2002 г. № 184-ФЗ

Статья 20

Формы подтверждения соответствия:

1. *Добровольная*
   - добровольная сертификация
2. *Обязательная*
   - декларирование соответствия
   - **обязательная сертификация**

ОБЯЗАТЕЛЬНАЯ СЕРТИФИКАЦИЯ

INFOWATCH®

Федеральный закон «О техническом регулировании» от 27.12.2002 г. № 184-ФЗ

В отношении оборонной продукции (работ, услуг), поставляемой по государственному оборонному заказу; продукции (работ, услуг), **используемой в целях защиты сведений**, составляющих **государственную тайну** или **относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа** …

*Обязательными требованиями наряду с требованиями **технических регламентов** являются требования, установленные государственными заказчиками, **федеральными органами исполнительной власти, уполномоченными в области обеспечения безопасности, обороны, внешней разведки, противодействия техническим разведкам и технической защиты информации, государственного управления использованием атомной энергии,** государственного регулирования безопасности при использовании атомной энергии, и (или) государственными контрактами (договорами).*

… **особенности оценки соответствия** … устанавливаются Правительством Российской Федерации или уполномоченными им федеральными органами исполнительной власти

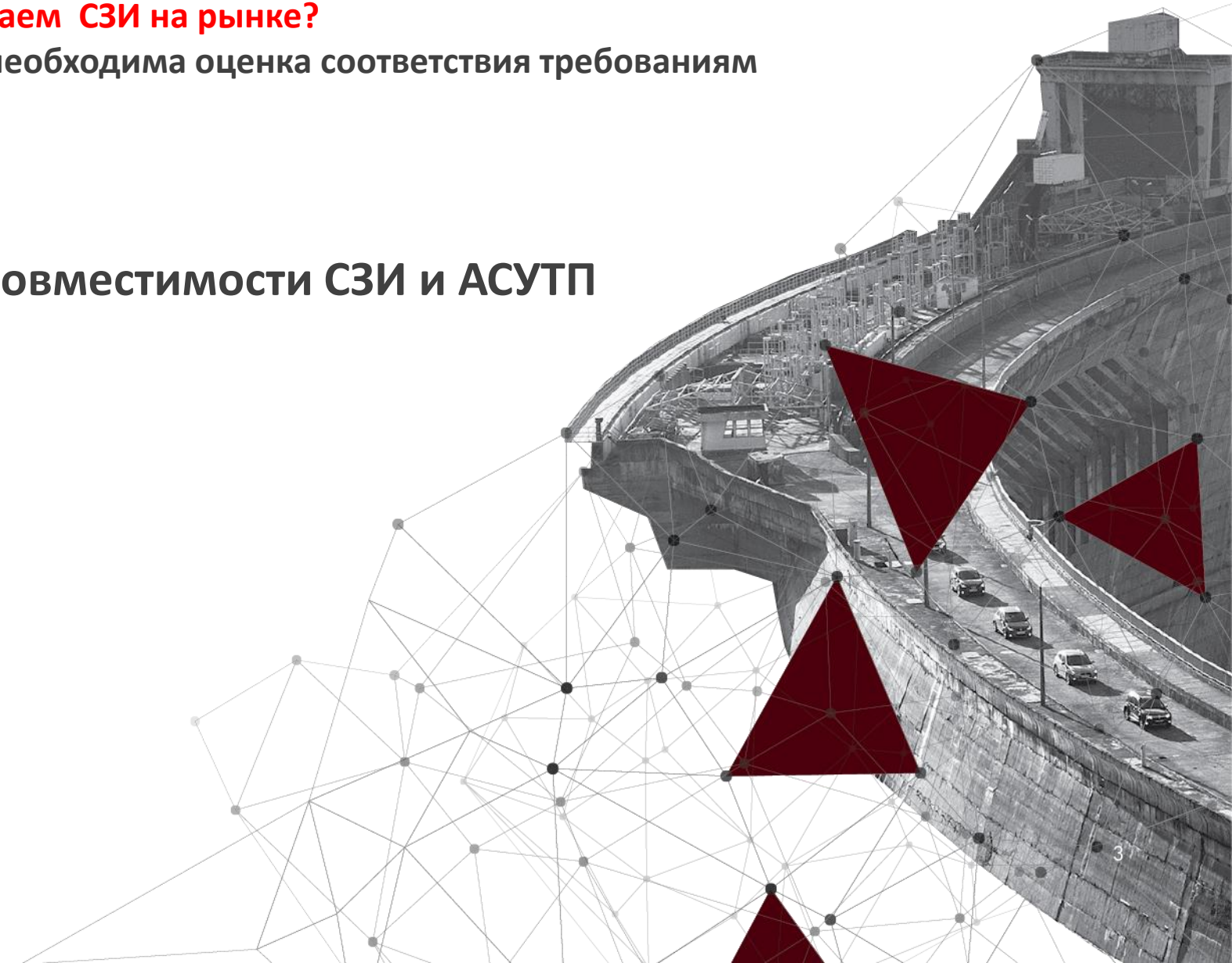
Постановление Правительства РФ о сертификации средств защиты информации **№608 1995**

Приказ ФСТЭК РФ от 03.04.2018 №55 «Об утверждении положения о системе сертификации средств защиты информации»

А если выбираем СЗИ на рынке?

Здесь также необходима оценка соответствия требованиям безопасности

Вопросы совместимости СЗИ и АСУТП



Совместимость

ГОСТ 34.003-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения.

Техническая
Программная
Информационная
Организационная
Лингвистическая
Метрологическая

Автоматизированные системы

ГОСТ 2.114-2016 Единая система конструкторской документации. Технические условия.

Функциональная
Геометрическая
Электромагнитная
Электрическая
Метрологическая
Диагностическая и пр.

Изделия

ГОСТ 34.003-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения

INFOWATCH®

Совместимость автоматизированных систем (АС)

комплексное свойство двух или более АС, характеризуемое их способностью взаимодействовать при функционировании

Ещё раз варианты оценки соответствия КИИ, КВО

Использование **сертифицированных** СЗИ или проведение **сертификационных испытаний** если имеются требования или владельцем принято решение о применении сертифицированных СЗИ

В форме **испытаний**

В форме **приемки и ввода в эксплуатацию** объекта, строительство которого закончено

Условия создания системы безопасности/защиты

Рассмотрим вариант:

Нет требований применять в обязательном порядке сертифицированные средства защиты информации
Применяются в том числе внешние (наложенные) СЗИ

Приказ ФСТЭК России от 14.03.2014 № 31

Рассмотрим действия проектировщика при принятии решения о возможности использования выбранных СЗИ в процессе проектирования и внедрения системы безопасности/защиты объекта КИИ/АСУТП

Проектирование

Приказ ФСТЭК России от 25.12.2017 № 239

Осуществляется выбор средств защиты информации и (или) их разработка с учетом категории значимости значимого объекта, совместимости с программными и программно-аппаратными средствами, выполняемых функций безопасности и ограничений на эксплуатацию

Приказ ФСТЭК России от 14.03.2014 № 31

Осуществляется при необходимости выбор средств защиты информации с учетом их стоимости, совместимости с программным обеспечением и техническими средствами, функций безопасности этих средств и особенностей их реализации…

Осуществляется проверка, в том числе при необходимости с использованием макетов или тестовой зоны, **корректности функционирования автоматизированной системы управления с системой защиты** и **совместимости выбранных средств защиты** информации с программным обеспечением и техническими средствами автоматизированной системы управления.

Приказ ФСТЭК России от 14.03.2014 № 31

Внедрение

Установка и настройка средств защиты информации должна **обеспечивать корректность функционирования автоматизированной системы управления** и **совместимость выбранных средств защиты** информации с программным обеспечением и техническими средствами автоматизированной системы управления.

Установленные и настроенные средства защиты информации **не должны оказывать отрицательного влияния** на штатный режим функционирования автоматизированной системы управления.

Приемочные испытания – только сейчас о функционале БИ

Приемочные испытания системы защиты автоматизированной системы управления проводятся, как правило, **в рамках приемочных испытаний автоматизированной системы управления в целом** с учетом ГОСТ 34.603 и стандартов организации.

В ходе **приемочных испытаний** должен быть проведен **комплекс** организационных и технических мероприятий (**испытаний**), в результате которых **подтверждается соответствие системы защиты** автоматизированной системы управления **техническому заданию** на создание (модернизацию) автоматизированной системы управления и (или) техническому заданию (частному техническому заданию) на создание системы защиты автоматизированной системы управления, **а также настоящим Требованиям**.

Приказ ФСТЭК России от 14 марта 2014 г. №31

Подход АО «ИнфоВотч»

Подход АО «ИнфоВотч» - проведение испытаний заранее

- **испытания** для оценки **соответствия заявленного функционала** средств защиты **мерам защиты информации**
- **испытания** средств защиты **на совместимость** с АСУТП

или в процессе проектирования

Подход АО «ИнфоВотч»

Проведение испытаний СЗИ самостоятельно

- Подтверждение функционала ИБ

Проведение испытаний СЗИ с заказчиками – собственниками АСУТП

- Подтверждение функционала ИБ
- Подтверждение совместимости с АСУТП

Проведение испытаний СЗИ с вендорами АСУТП

- Подтверждение совместимости с АСУТП
- Подтверждение функционала ИБ

Оценка соответствия требованиям по ИБ

Подтверждение функционала ИБ – оценка соответствия требованиям по ИБ

Проведение испытаний по программе и методике испытаний (ПМИ)
ПМИ включает тесты на соответствие требованиям – мерам безопасности

Требования по ИБ – меры безопасности

- Приказ ФСТЭК России от 25.12.2017 года № 239
- Приказ ФСТЭК России от 14 марта 2014 года №31
- Методический документ ФСТЭК России от 11.02.2014 года «Меры защиты информации в государственных информационных системах»

Испытания на совместимость

Результат испытаний:

- АСУТП/объект КИИ работоспособен(а) при функционировании СЗИ в его составе
- СЗИ работоспособно при функционировании АСУТП/объекта КИИ, в составе которого оно находится

Что испытывали

InfoWatch Automation System Advanced Protector

InfoWatch ASAP *–*
специализированный программно-аппаратный комплекс, предназначенный для защиты АСУТП и адаптированный к использованию в технологических сетях
Сертифицирован:
МЭ – тип Д четвёртый класс
СОВ - четвёртый класс защиты

ПАК InfoWatch ASAP может функционировать в двух основных режимах:

Фоновый – выполняет мониторинг трафика, подаваемого на вход ПАК InfoWatch ASAP, и информирует оператора об инцидентах

Активный – предотвращает вредоносное воздействие

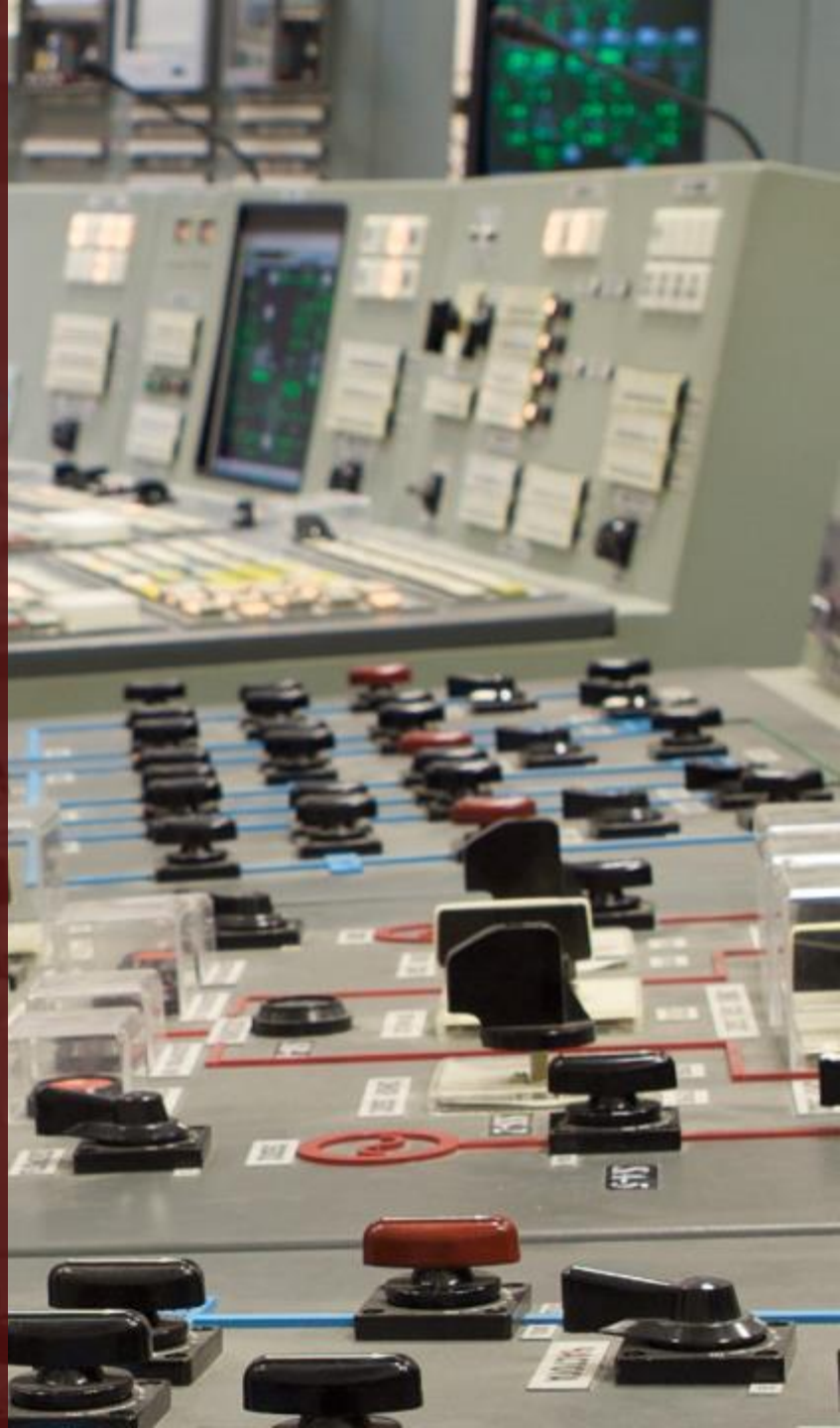
СХЕМА РАБОТЫ INFOWATCH ASAP

Получение трафика технологической сети на уровнях ПЛК и полевых устройств

Глубокий анализ пакетов (DPI)

Обнаружение/предотвращение вторжений и аномалий технологического процесса

Информирование оператора и администратора информационной безопасности



Область применения

Комплексные решения, построенные на базе платформы **InfoWatch ASAP**, позволяют **обнаруживать** (и предотвращать*) атаки на средства промышленной автоматизации, **в том числе**:

- Несанкционированная перепрошивка ПЛК
- Изменение уставок ПЛК
- Подключение устройств в технологическую сеть
- Подмена сетевого адреса
- Факт сканирования сети
- Попытки эксплуатации уязвимостей ПО и ПЛК
- Использование запрещенных функций промышленных протоколов
- Появление запрещенных информационных потоков
- Использование запрещенных протоколов прикладного уровня
- Появление пакетов промышленных протоколов с нарушением их типовых структур
- Атаки на отказ средств автоматизации в обслуживании (DoS), в том числе атаки типа «flood»

** в случае установки в разрыв каналов связи.*

Проект по тестированию (пример)

СЗИ:

ПАК InfoWatch ASAP

АСУТП:

Schneider Electric
(стенд АО «Шнейдер Электрик Системс»)

Разработаны:

- Задание на проведение пилотного проекта
- Программа и методика испытаний

Результаты испытаний оформлены:

- Протокол испытаний
- Акт

Пример: проект InfoWatch и Schneider Electric

Результат

1. Подтверждено **соответствие заявленных функций** мерам защиты информации Приказа ФСТЭК России от 14 марта 2014 г. №31
2. Подписано **заявление о совместимости ПАК IW ASAP** и оборудования **Schneider Electric**
3. Результаты могут быть использованы при:
   - принятии решения о допуске к проведению испытаний на оборудовании владельца/вендора АСУТП
   - проектировании систем защиты и АСЗИ

Результаты испытаний

В 2017-18 гг. были реализованы пилотные проекты, в ходе которых проведены испытания СЗИ разработки компаний, входящих в состав ГК ИнфоВотч: InfoWatch ASAP, InfoWatch Traffic Monitor, InfoWatch EndPoint Security на оборудовании/ПО (SCADA) вендоров: Schneider Electric, AVEVA Group / Klinkmann, Siemens, Модульные системы Торнадо, АМТ-Групп.

Важно отметить, что проводились испытания СЗИ работающих на:

- сетевом уровне (InfoWatch ASAP – МЭ, СОВ),
- уровне защиты серверов и рабочих станций (InfoWatch Traffic Monitor Enterprise (Device Monitor), InfoWatch EndPoint Security).

DLP: 17 приказ ФСТЭК России - ОЦЛ.5, 239 приказ - ЗИС.17.

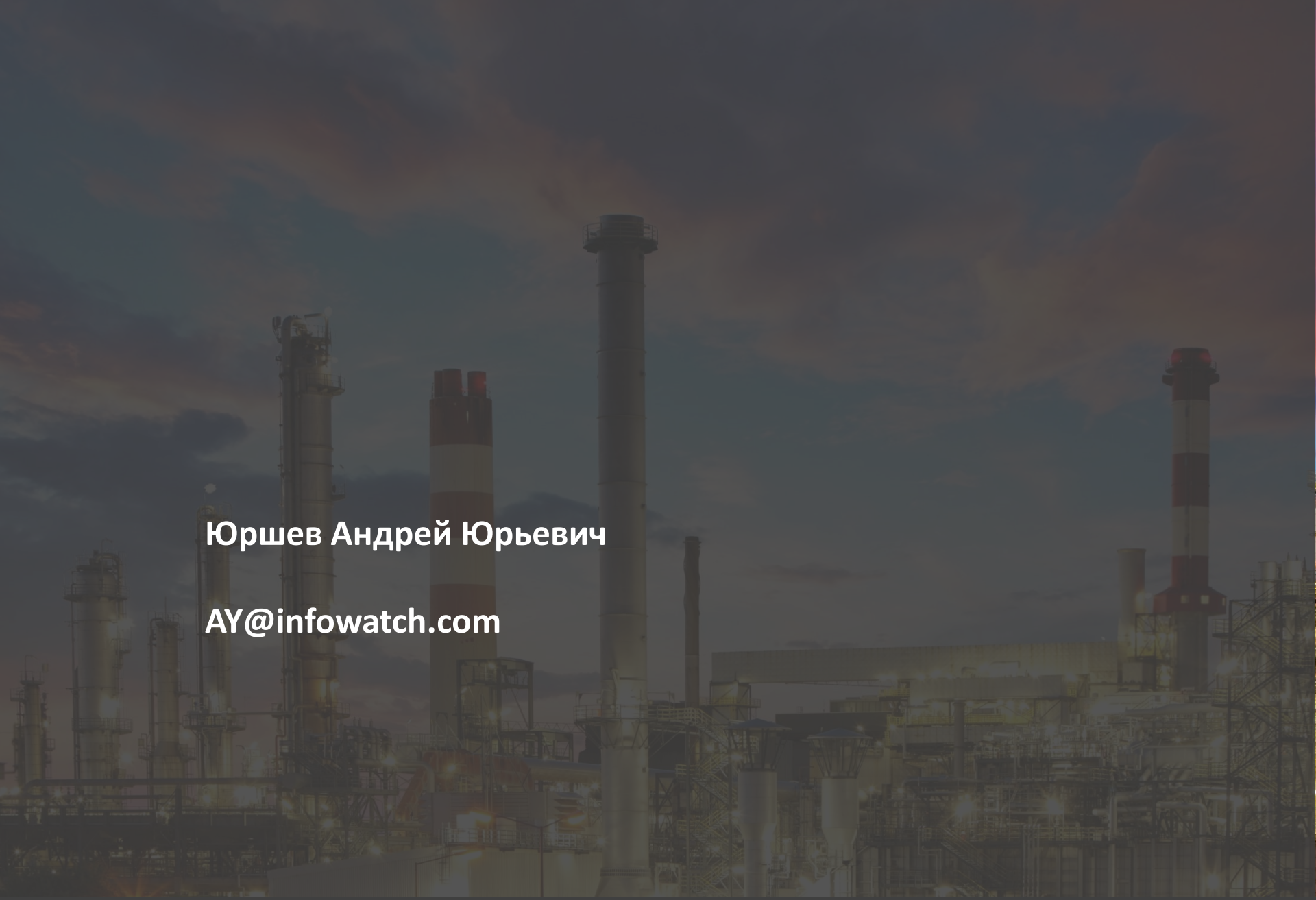
Результаты испытаний

Компания ИнфоВотч разработала методику и провела испытания для оценки соответствия СЗИ собственного производства требованиям безопасности информации и подтверждения их совместимости с оборудованием и ПО ряда производителей АСУТП.

Подтверждено соответствие ряду мер безопасности информации средств защиты информации разработки ГК ИнфоВотч для рабочих станций (серверов) и сетевого уровня.

Где испытывали

Отрасль	Предприятие	Производитель оборудования АСУТП
Внедрение		
Топливно-энергетический комплекс	Электростанция собственных нужд, нефтедобыча	Siemens PLC, Siemens SCADA
Пилотные проекты		
Нефтехимическая промышленность	Комбинат «Нефтеоргсинтез»	Siemens PLC, Siemens SCADA, Siemens simatic scalance
Металлургическая промышленность	Крупный металлургический комбинат	Siemens PLC, Siemens SCADA
Топливно-энергетический комплекс	ТЭЦ	ООО «Модульные Системы Торнадо»
Горно-обогатительная	Крупный горно-обогатительный комбинат	Siemens PLC, Siemens SCADA, Moxa
Стендовые испытания		
Нефтяная промышленность	Нефтяная промышленность (транспортировка)	Виртуальная среда с протоколами Modbus, IEC 101/104, OPC UA
Нефтяная промышленность	АО «Шнейдер Электрик Системз» для предприятий отрасли (добыча)	Schneider Electric PLC Schneider Electric SCADA Семейство SCADA Wonderware
Топливно-энергетический комплекс	ТЭЦ	АО «АМТ-групп»



Юршев Андрей Юрьевич

AY@infowatch.com

INFOWATCH®