



Информзащита
Системный интегратор



АСПЕКТЫ БЕЗОПАСНОСТИ АСУ ТП В ОТДЕЛЬНЫХ ОТРАСЛЯХ ПРОМЫШЛЕННОСТИ

Даренский Дмитрий
Начальник отдела промышленных систем
Департамента комплексных решений
ЗАО НИП «Информзащита»
d.darensky@infosec.ru
+7 495 980 2345 доб. 172

«ИНФОРМЗАЩИТА» СЕГОДНЯ



ЭКОНОМИЧЕСКИЕ АСПЕКТЫ

ОБЪЕМЫ И КАЧЕСТВО ПРОДУКЦИИ НАПРЯМУЮ ЗАВИСЯТ ОТ
ФУНКЦИОНАЛЬНОСТИ И НАДЕЖНОСТИ СИСТЕМ УПРАВЛЕНИЯ



ПРОСТОИ, АВАРИИ, ИЗМЕНЕНИЕ КАЧЕСТВА ПРОДУКЦИИ
НАПРЯМУЮ ВЛИЯЮТ НА ЭКОНОМИЧЕСКИЕ ПОКАЗАТЕЛИ



НИЗКИЙ УРОВЕНЬ ЗАЩИЩЕННОСТИ СИСТЕМ УПРАВЛЕНИЯ
СТАВИТ ПОД УДАР ОБЪЕМЫ И КАЧЕСТВО ПРОДУКЦИИ, А
ЗНАЧИТ И ЭКОНОМИЧЕСКИЕ ПОКАЗАТЕЛИ



Информзашита
Системный интегратор



ЭКОНОМИЧЕСКИЕ АСПЕКТЫ ВЛИЯНИЕ ЗАЩИЩЕННОСТИ

Отношения с регуляторами и контрагентами

- Сокращение объемов штрафов
- Снижение выплат по неустойкам
- Снижение количества административных взысканий

Текущие производственные показатели

- Поддержка и улучшение показателей непрерывности
- Обеспечение исполнения производственных планов на заданном уровне
- Снижение объемов воровства

Возврат инвестиций

- Снижение затрат на техобслуживание основных мощностей
- Снижение времени простоев
- Защита от появления контрафакта и «грязной» конкуренции



Информзашита
Системный интегратор



ОРГАНИЗАЦИОННО-ПРАВОВЫЕ АСПЕКТЫ

«Бумажная» безопасность

- Прикладная нормативно-техническая база не учитывает отраслевую специфику
- Нормативно-правовые акты носят рекомендательный характер
- Ввод в действие международных стандартов идет медленно

«Реальная» безопасность

- Спрос на «реальную защиту» только формируется
- Предприятия не спешат финансировать создание систем защиты
- Распространен подход «сначала отбиться от регулятора, а защищаться потом»

ОРГАНИЗАЦИОННО-ПРАВОВЫЕ АСПЕКТЫ

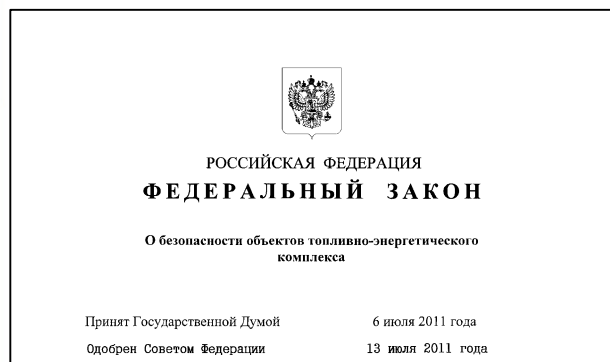
Участники рынка	«Бумажная» безопасность	«Реальная» безопасность
Владельцы АСУ ТП	Классификацию по 31 приказу и/или КСИИ не проводят, потому что никто не обязывает.	Реализуют организационные и компенсирующие меры. Внедряют только межсетевые экраны и антивирусы
Производители АСУ ТП	Не сертифицируются по требованиям безопасности, потому что никто не требует этого от них.	СЗИ от вендоров АСУ ТП либо не внедряют либо отключают.
Производители СЗИ	Решений мало, сертифицированных нет	Комплексные решения пилотируются. Поставляются только межсетевые экраны и антивирусы



Информзащита
Системный интегратор



ОРГАНИЗАЦИОННО-ПРАВОВЫЕ АСПЕКТЫ



На основании статьи 11 Федерального закона «О безопасности объектов топливно-энергетического комплекса», положений Приказа ФСТЭК №31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах производственного и технологического управления», а также пункта 42 статьи 12 части первой Федерального закона «О полиции» с 2015 года территориальные органы МВД России выполняют функции государственного контроля за обеспечением безопасности объектов ТЭК.



ОТРАСЛЕВЫЕ АСПЕКТЫ. НЕФТЕГАЗ

ТРАНСПОРТ

- Территориально распределенная архитектура
- Необходимость удаленного мониторинга и управления
- Необходимость мониторинга качества
- Прямая связь между защищенностью и экологичностью

ДОБЫЧА

- Нет четких границ сетей
- Частичная автоматизация
- Не обслуживаемые объекты
- Передача коммерческих данных из условно технологической в условно корпоративную сеть



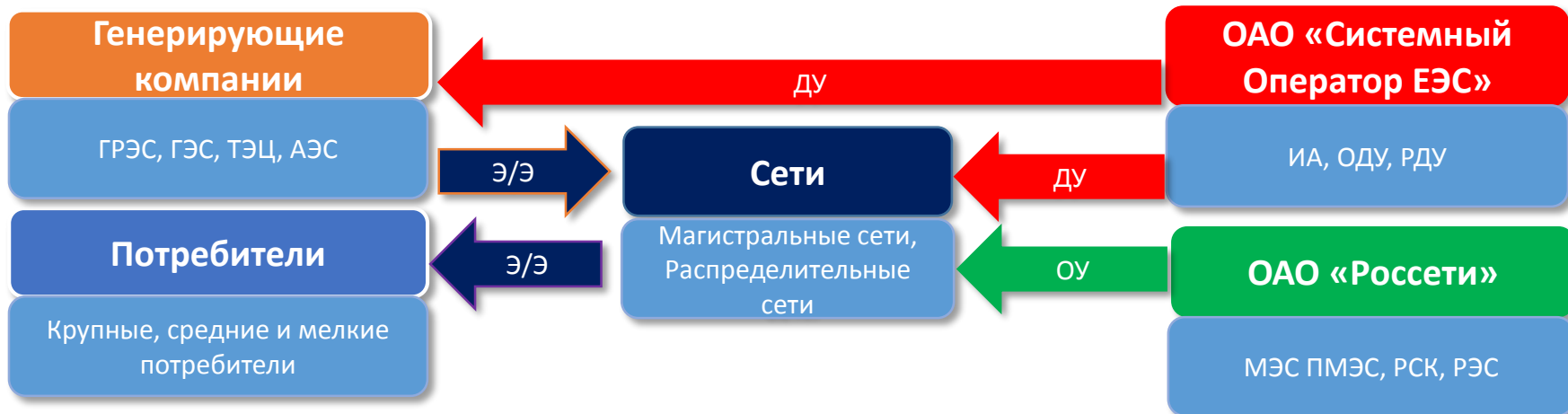
Информзащита
Системный интегратор



ОТРАСЛЕВЫЕ АСПЕКТЫ. ЭЛЕКТРОЭНЕРГЕТИКА

Системный Оператор Единой Энергетической Системы (ОАО «СО ЕЭС») осуществляет контроль за соблюдением технологических параметров системы, принимает участие в управлении сетями. ФСК и МРСК управляют магистральными и распределительными сетями, по которым электроэнергия поступает потребителям.

Компрометация систем диспетчерско-технологического управления на одном из субъектов ЕНЭС может привести к нарушениям режимов энергосистемы вплоть до возникновения аварийных ситуаций



ДУ – Диспетчерское управление
ОУ – Оперативное управление
Э/Э – Электрическая энергия

ОТРАСЛЕВЫЕ АСПЕКТЫ. ЭЛЕКТРОЭНЕРГЕТИКА

ГЕНЕРАЦИЯ

- Критичные, быстропротекающие технологические процессы
- Сложная структура управления, большое количество систем
- Критичный элемент государственной инфраструктуры
- Тенденция к снижению квалификации служб эксплуатации
- Уголовная ответственность руководства и персонала

СЕТИ

- ...
- Наличие необслуживаемых объектов
- Моральное и физическое устаревание
- Большинство объектов не имеют АСУ ТП, но являются уязвимыми



Информзащита
Системный интегратор



ОТРАСЛЕВЫЕ АСПЕКТЫ. ПРОИЗВОДСТВО

МАШИНОСТРОЕНИЕ

- Сложная структура систем автоматизации
- Большое количество «самописных» программ
- «Лоскутная» и частичная автоматизация
- Раздельное управление основными и вспомогательными производственными процессами
- Не защищенные MES/CAD/CAM, PLM – возможность для кражи разработок и процветания производства контрафакта



Информзашита
Системный интегратор



ТЕХНИЧЕСКИЕ АСПЕКТЫ

Компоненты систем автоматизации не способны защищаться. Это не их функция.

Компоненты систем имеют уязвимости. Контроль безопасности разработки не ведется

Проекты АСУ ТП в части ИБ выполняются формально.

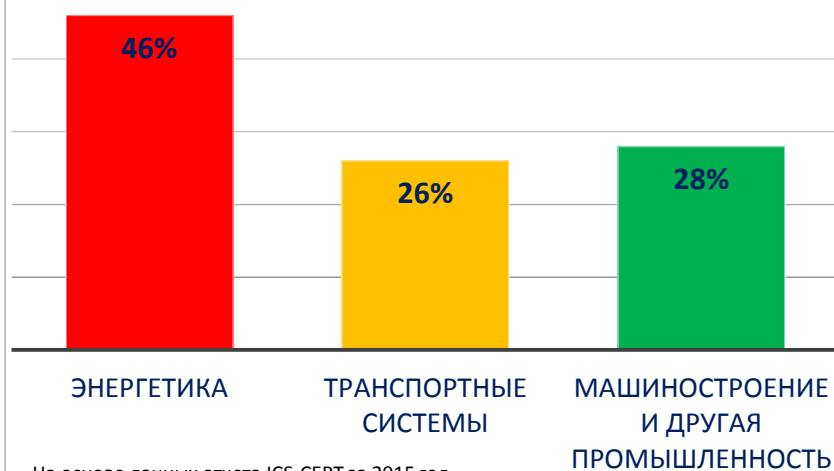
Аттестация средств измерений систем учета не показатель защищенности компонентов.

Сертификация по требованиям безопасности ФСТЭК не осуществляется.

СТАТИСТИКА

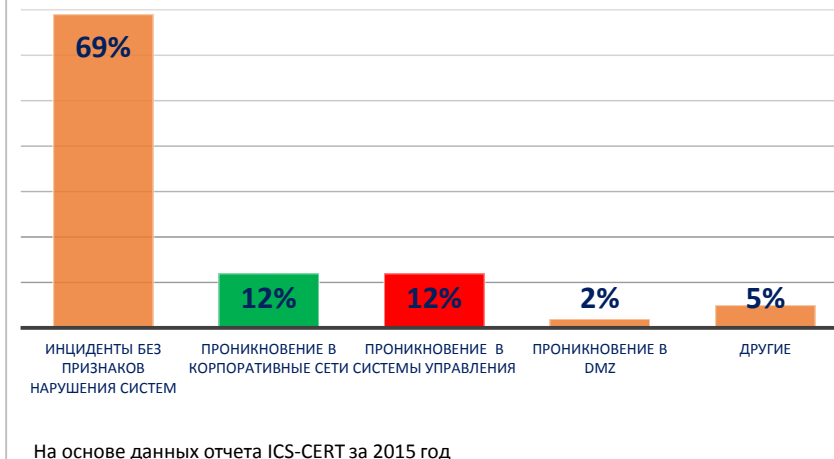
46% из 295 инцидентов ИБ АСУ ТП в 2015 году пришлось на объекты энергетики

Атаки по отраслям



В 12% из 295 инцидентов ИБ АСУ ТП подтвержден несанкционированный доступ

Глубина атак



ПРИМЕРЫ ИНЦИДЕНТОВ

ОАО, ВЫПОЛНЯЮЩЕЕ ОБОРОННЫЕ ЗАКАЗЫ

- Российские хакеры получили доступ и опубликовали документацию на гидроакустическое устройство подводной охраны, выпускаемое закрытым предприятием

НЕФТЕДОБЫВАЮЩАЯ КОМПАНИЯ

- Инициировано расследование по факту искажения отчетов по объемам добычи

ЭНЕРГОСБЫТОВАЯ КОМПАНИЯ

- Подмена данных в системе коммерческого учета позволила злоумышленникам украсть несколько десятков миллионов рублей

ЦЕМЕНТНЫЙ ЗАВОД

- Сотрудник самовольно подменял расчетные коэффициенты в системе управления отгрузкой цемента, что позволило ему в течение 6 месяцев красть продукцию

АВТОЗАВОД

- Систематическая кража управляющих программ станков с ЧПУ позволяет небольшим компаниям наладить выпуск контрафактных запчастей



Информзашита
Системный интегратор



РИСКИ



ТЕХНОЛОГИЧЕСКИЕ РИСКИ

- Остановки
- Аварии
- Нарушение режимов
- Изменение качества продукции



ЭКОНОМИЧЕСКИЕ РИСКИ

- Мошенничество
- Фальсификация отчетности
- Фальсификация продукции



Информзащита
Системный интегратор



УГРОЗЫ БЕЗОПАСНОСТИ АСУ ТП

- Вывод из строя оборудования, объекта
- Остановка технологических процессов
- Подмена данных измерений
- Перехват управления
- Блокирование управления
- Несанкционированный доступ к оборудованию, функциям, данным

ВЛИЯНИЕ УГРОЗ АСУ ТП НА БИЗНЕС

- Нарушение нормальных режимов оборудования, производства.
- Нарушение обязательств по контрактам с клиентами и поставщиками.
- Увеличение количества/времени простоев.
- Убытки ввиду ошибочных действий персонала (или имитации таких действий).
- Снижение общего уровня безопасности производства.
- Убытки от мошенничества с использованием уязвимостей.
- Причинение вреда государственной инфраструктуре.

ТИПЫ НАРУШИТЕЛЕЙ

ВНУТРЕННИЕ

- Штатные сотрудники, имеющие легитимный доступ
- Специалисты сторонних организаций с прямым или удаленным доступом

ВНЕШНИЕ

- Спецслужбы иностранных государств
- Конкуренты
- Криминал
- «Хактивисты»

80% инцидентов происходит по вине или при участии «внутренних» нарушителей.

Поэтому изолированность АСУ ТП не является гарантией ее защищенности

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

ОТСУТСТВИЕ
ТРЕБОВАНИЙ К ЗАЩИТЕ
ПРИ ПРОЕКТИРОВАНИИ

НИЗКАЯ ЭФФЕКТИВНОСТЬ
ВСТРОЕННЫХ СРЕДСТВ
ЗАЩИТЫ

ПРАКТИКА ОТКЛЮЧЕНИЯ
ВСТРОЕННЫХ ФУНКЦИЙ
ЗАЩИТЫ

НИЗКАЯ ЭФФЕКТИВНОСТЬ
ОРГАНИЗАЦИОННЫХ МЕР

ОТСУТСТВИЕ
ТРЕБОВАНИЙ ПО
ОБЕСПЕЧЕНИЮ ИБ
ПЕРСОНАЛОМ

ОБЕСПЕЧЕНИЕ
ДОСТУПНОСТИ И
УПРАВЛЯЕМОСТИ В
УЩЕРБ ЗАЩИЩЕННОСТИ

ОТСУТСТВИЕ ПРОЦЕДУР
МОДЕЛИРОВАНИЯ АТАК И
ИНЦИДЕНТОВ ИБ

ДЛИТЕЛЬНЫЙ СРОК
ЭКСПЛУАТАЦИИ СИСТЕМ

СПЕЦИФИКА
ТЕХНОЛОГИЧЕСКИХ
СЕТЕЙ

ПОВЫШЕНИЕ
УРОВНЯ
ЗАЩИЩЕННОСТИ
АСУ ТП

ПОДХОД К РЕАЛИЗАЦИИ ПРОЕКТОВ

РАЗРАБОТКА
ТРЕБОВАНИЙ
К СИСТЕМЕ
ЗАЩИТЫ

РАЗРАБОТКА
СИСТЕМЫ
ЗАЩИТЫ

ВНЕДРЕНИЕ
СИСТЕМЫ
ЗАЩИТЫ

Подход разработан на основании
рекомендаций Приказа №31 ФСТЭК



Информзащита
Системный интегратор



ВЫПОЛНЯЕМЫЕ РАБОТЫ

РАЗРАБОТКА ТРЕБОВАНИЙ К СИСТЕМЕ ЗАЩИТЫ

- Инвентаризация активов
- Аудит и выводы по реальному уровню защищенности
- Моделирование угроз и нарушителей
- Моделирование атак и возможных схем фрода
- Разработка требований к обеспечению безопасности

РАЗРАБОТКА СИСТЕМЫ ЗАЩИТЫ

- Разработка политик и стандартов по обеспечению безопасности
- Разработка набора организационных и компенсирующих мер
- Разработка технического решения по обеспечению безопасности
- Описание процессов обеспечения безопасности
- Описание процессов управления безопасностью

ВНЕДРЕНИЕ СИСТЕМЫ ЗАЩИТЫ

- Реализация организационных и компенсирующих мер
- Реализация системы обеспечения безопасности
- Реализация системы управления безопасностью



Информзашита
Системный интегратор



ПРЕИМУЩЕСТВА ЗАО НИП «ИНФОРМЗАЩИТА»

Специализированное подразделение, сформированное из специалистов АСУ ТП (сертифицированных), имеющих компетенции не только в области ИБ, но и в области Industrial automation, Industrial networking & IT.

Специалисты компании имеют опыт создания систем автоматизации и защиты информации в атомной отрасли, электроэнергетике, пищевой промышленности, а также автоматизированных систем для нужд Минобороны.

Большой опыт проведения аудитов АСУ ТП с анализом защищенности и отнесением к КСИИ (с 2011 года) в таких отраслях, как нефтегаз и электроэнергетика, критические объекты государственной и социальной инфраструктуры.

Опыт проведения инструментального анализа АСУ ТП.

Наличие специалистов и опыта работ по проведению исследований и анализа программного обеспечения и исходного кода приложений.

Опыт исследования встроенных механизмов защиты компонентов АСУ ТП (software, hardware).

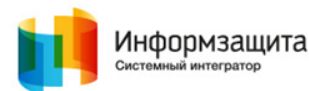
Возможность проводить анализ не только уровня защищенности, но и функциональной надежности систем, уязвимости архитектур.

«Информзащита» участвовала в разработке Приказа №31 ФСТЭК.

«Информзащита» входит в состав технического комитета «Защита информации» ТК 362 Росстандарта.

«Информзащита» принимает участие в рабочих группах крупных компаний, а также в Минэнерго и национального комитета СИГРЭ по теме безопасности АСУ ТП.

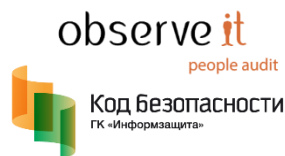
Наличие собственного стенда АСУ ТП для проведения исследований систем и отдельных компонентов, тестирования вендорских и проектных решений.



ОПЫТ ПРОЕКТОВ ЗАО НИП «ИНФОРМЗАЩИТА»

ОАО «АК «Транснефть»	2011	• Разработка стандарта безопасности АСУ ТП
ОАО «ТНК-ВР»	2011	• Обследование и анализ рисков мошенничества на АЗС
ОАО «Тюменьэнерго»	2012	• Аудит АСУ ТП
ОАО «Тюменьэнерго»	2012	• Разработка стандарта безопасности АСУ ТП
ОАО «Тюменьэнерго»	2012	• Разработка модели угроз и плана защиты АСУ ТП
ФСК ЕЭС	2012	• Разработка шаблонов стандартов по ИБ, включая АСУ ТП
ОАО «Лукойл» (2 завода)	2012	• Аудит АСУ ТП
ОАО «МТК»	2012	• Аудит АСУ ТП
ОАО «МТК»	2012	• Разработка стандарта безопасности АСУ ТП
ОАО «МТК»	2012	• Разработка модели угроз и плана защиты АСУ ТП
ООО «Лукойл-Информ»	2013	• Разработка стандарта безопасности АСУ ТП (Сеть)
ФСТЭК	2013	• Разработка требований по защите АСУ ТП
ОАО «Тюменьэнерго»	2014	• Дополнительное обследование АСУ ТП
ОАО «Тюменьэнерго»	2014	• Анализ угроз безопасности АСУ ТП
ОАО «Тюменьэнерго»	2014	• Проектирование системы защиты АСУ ТП
ОАО «НК «Роснефть»	2014	• Обследование и аудит АСУ ТП НПЗ
ОАО «НК «Роснефть»	2014	• Типовые технические решения по защите
ОАО «Мосводоканал»	2014	• Обследование АСУ ТП
ОАО «Мосводоканал»	2014	• Анализ системы управления информационной безопасностью АСУ ТП
ОАО «Мосводоканал»	2014	• Оценка рисков безопасности АСУ ТП
• ОАО «НК Роснефть»	2015	• Аудит АСУ ТП на 4-х предприятиях
• ОАО «НК Роснефть»	2015	• Аудит компонентов СИКН
• ООО «Лукойл-Информ»	2015	• Аудит АСУ ТП с отнесением к КСИИ

Ключевые партнеры в области ИБ



Взаимодействие с вендорами АСУ ТП





Информзащита
Системный интегратор



Даренский Дмитрий
Начальник отдела промышленных систем
Департамента комплексных решений
ЗАО НИП «Информзащита»
d.darensky@infosec.ru
+7 495 980 2345 доб. 172