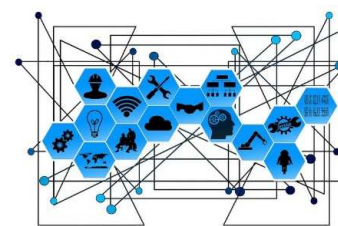
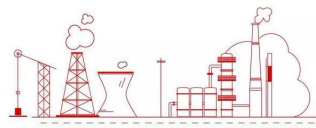


КИБЕРБЕЗОПАСНОСТЬ ПРОМЫШЛЕННЫХ СИСТЕМ. ВЗГЛЯД ВЕНДОРА АСУ ТП

Бондюгин Андрей

НОРМАТИВНАЯ БАЗА ПО ИБ АСУ ТП В РФ

STUXnet



2005

2014

2016

2017

2019

2005-2012 год

2014 год

2016 год

2017 год

2017-2019 год

Документы по
безопасности
КСИИ и КВО

Приказ ФСТЭК
России №31

Доктрина ИБ РФ

Программа
«Цифровая
экономика»

187-ФЗ
(и др. НПА по
КИИ)

ОТРАСЛЕВАЯ НОРМАТИВНАЯ БАЗА ПО ИБ АСУ ТП

Электроэнергетика

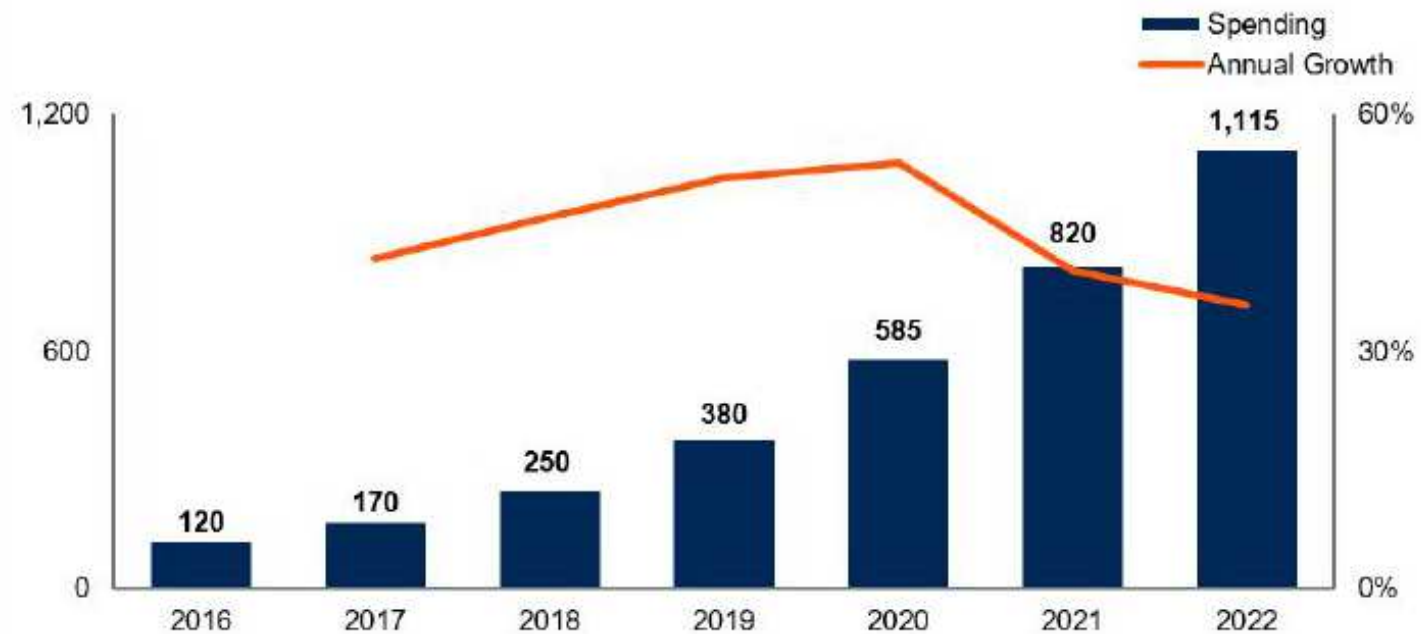
- «Концепция обеспечения информационной безопасности ОАО «Россети», утверждена и введена распоряжением ОАО «Россети» от 17.06.2014 № 249р
- Требования к встроенным средствам защиты АСТУ электросетевого комплекса, утверждены и введены распоряжением ПАО «Россети» от 30.05.2017 № 282р
- Концепция развития релейной защиты и автоматики электросетевого комплекса, утверждены распоряжением ПАО «Россети» № 356пр
- Система стандартов **СТО 56947007-29.240.01.xxx-2013** «Система обеспечения информационной безопасности ОАО «ФСК ЕЭС» и пр.

Промышленность, нефтегаз

- СТО Газпром 4.2-2-002 Система обеспечения информационной безопасности ОАО «Газпром». Требования к автоматизированным системам управления технологическими процессами
- Общие технические требования ОАО «АК «Транснефть». АСУ ТП и ПТС Компании. Информационная безопасность.
- Положение ПАО НК Роснефть № ПЗ-11 Р-0012 "Информационная безопасность. Автоматизированные системы управления технологическими процессами"

РОСТ РЫНКА ИБ В ПРОМЫШЛЕННОСТИ. ПРОГНОЗ GARTNER

OT Security Stand-Alone Product and Services Spend*
(in Millions of U.S. Dollars)



CAGR = 45.7%

Source: Gartner

ЭВОЛЮЦИЯ ВЗГЛЯДОВ ПРОИЗВОДИТЕЛЕЙ

Мировые вендоры:

- комплексные предложения по обеспечению ИБ поставляемых решений;
- центры компетенций в области кибербезопасности;
- инжиниринг

Российские разработчики:



РАЗВИТИЕ СЗИ В АСУ ТП

 2000-е

Парольная
защита
компонентов
АСУ ТП

Первые
адаптированные
для АСУ ТП
средства защиты
сети и
периметра,
конечных узлов

Развитие
встроенных
СЗИ у западных
вендоров АСУ

Принятие
концепции
«defence-in-
depth» в
отношении
промышленных
систем

Развитие в РФ
нормативной
базы в области
ИБ АСУ ТП

Специализированные
продукты для
защиты
промышленных
систем у
отечественных
вендоров ИБ

Встроенные СЗИ
у отечественных
производителей
АСУ ТП

 2019

ДО & ПОСЛЕ

3 года назад

- Отсутствие необходимых лицензий
- Отсутствие компетентных специалистов в штате
- Отсутствие инвестиций в разработку в части ИБ



Сегодня

- Успешно получены лицензии ФСТЭК России и ФСБ России
 - Наличие профильных специалистов в штате компании
- Постоянные инвестиции в НИОКР по разработке встроенных средств защиты информации в продуктах компании

БАЗОВЫЕ РЕШЕНИЯ. ВСТРОЕННЫЙ ФУНКЦИОНАЛ



Контроль и управление доступом (RBAC)



Идентификация и аутентификация (в т.ч. двухфакторная) **BIOSMART**



Аудит безопасности



Укрепление системы («system hardening»)



Безопасный удаленный доступ



Резервирование технических средств



Контроль целостности прошивки и обрабатываемых данных



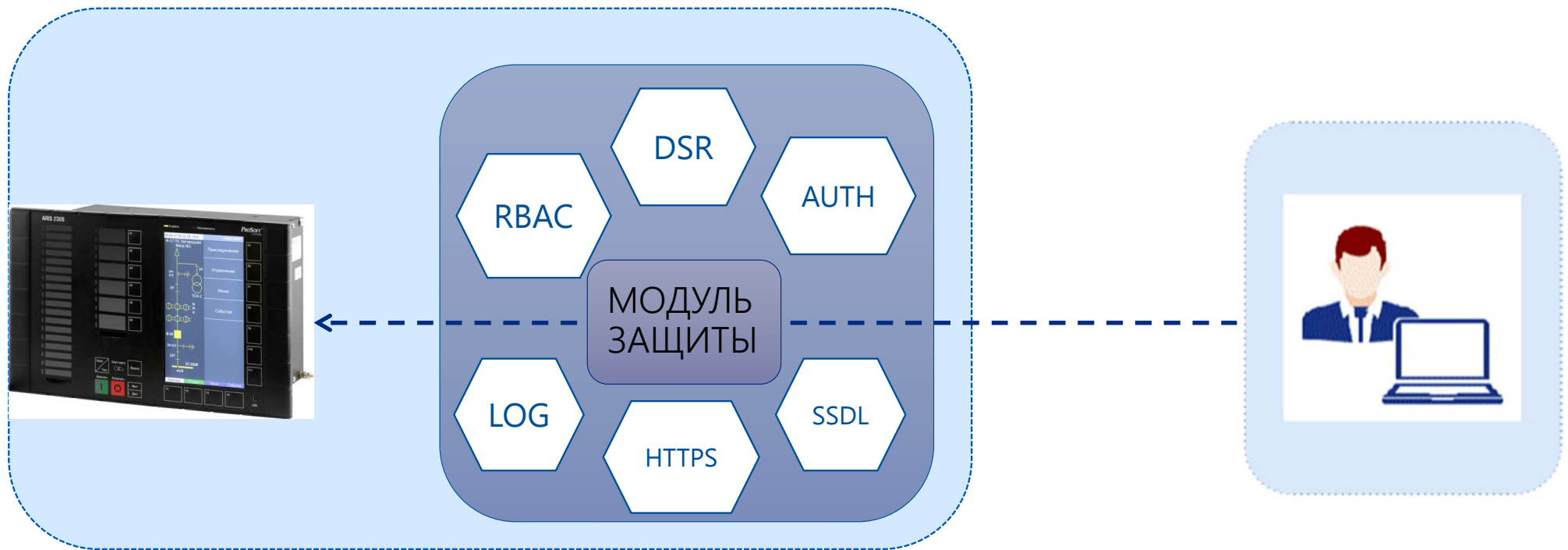
Защищенные протоколы для конфигурирования устройств



Резервное копирование и восстановление

Программно-технические средства и программные комплексы имеют встроенные механизмы защиты информации, обеспечивающие необходимый уровень защищенности обрабатываемой информации, разработанные с учетом нормативных требований

ВСТРОЕННЫЙ ФУНКЦИОНАЛ. АРХИТЕКТУРА



При реализации ВСЗИ в embedded-устройствах была переработана архитектура встроенного ПО в целях создания решения, которое бы не просто закрывало нормативные требования, но нейтрализовало актуальные угрозы безопасности.

Разработка программного обеспечения ведется с применением элементов безопасной разработки в соответствии с ГОСТ Р 56939–2016.

«ВРАГ ЗНАЕТ СИСТЕМУ» (с)

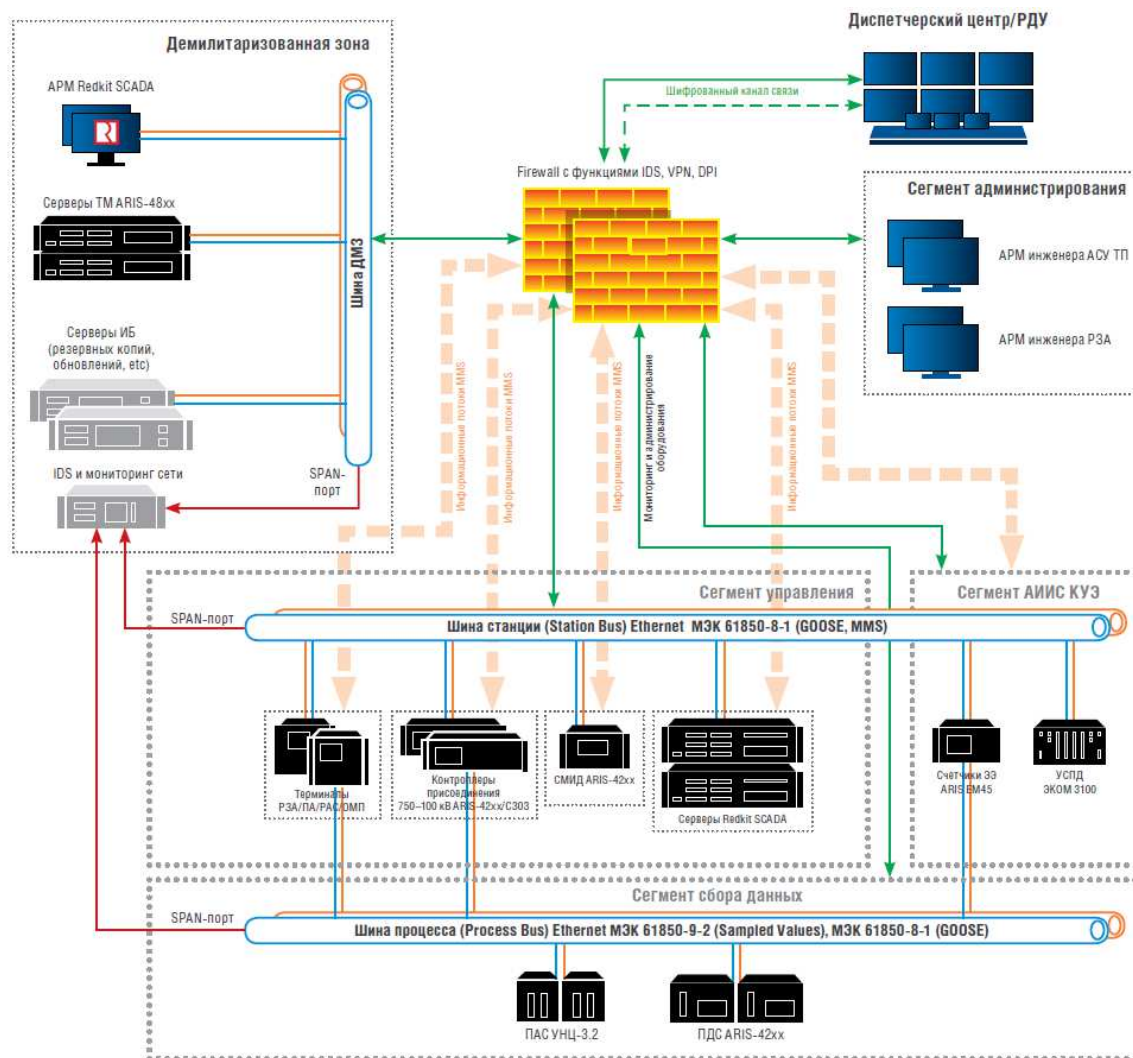
Если уязвимость может быть обнаружена, она будет обнаружена

Если уязвимость может быть проэксплуатирована, она будет проэксплуатирована

При эксплуатации уязвимости будет нанесен максимально возможный ущерб



ЗАЩИЩЕННАЯ ЦИФРОВАЯ ПОДСТАНЦИЯ



КОМПЛЕКСНЫЕ РЕШЕНИЯ. СОТРУДНИЧЕСТВО

- Создание полноценных комплексных решений по построению АСУ ТП с учетом требований ИБ требует совместной работы вендора АСУ ТП и вендора (интегратора) ИБ
- Актуальными вопросами сотрудничества являются:
 - ✓ *Участие в создании совместных комплексных решений*
 - ✓ *Отработка и тестирование решений в области защиты АСУ ТП*
 - ✓ *Предоставление сервисов в области ИБ Заказчикам*
 - ✓ *Анализ защищенности*



ПРЕИМУЩЕСТВА КОМПЛЕКСНЫХ РЕШЕНИЙ



Соответствие требованиям российского законодательства (Федеральный закон №187-ФЗ, Приказы ФСТЭК России №239, №31)



Отработанные и протестированные решения наиболее эффективны для оказания сервиса по выявлению и реагированию на компьютерные атаки



Партнерство с ведущими производителями средств защиты информации и интеграторами, позволяющее гибко подходить к выбору применяемых решений и учитывать все пожелания и потребности Заказчика



Применяемые средства защиты информации имеют заключение о совместимости с оборудованием и программными комплексами, входящими в состав ПТК АСУ ТП



Разработанные решения проходят процедуру оценки соответствия в независимых аккредитованных лабораториях

ТЕНДЕНЦИИ И ПРОГНОЗЫ НА БУДУЩЕЕ

- Неизбежный рост рынка OT Security, как в мире, так и в России.
- Развитие сервисов по мониторингу состояния ИБ, обнаружению и предотвращению компьютерных атак в промышленных системах.
- Следование лучшим мировым практикам и международным стандартам в области ИБ АСУ ТП.
- Реализация концепций security-by-design, built-in-security.
- Формирование комплексных предложений по обеспечению ИБ от вендоров АСУ ТП для российского рынка.



БЛАГОДАРЮ ЗА ВНИМАНИЕ!



**ПРОСОФТ
СИСТЕМЫ**

ООО «Прософт-Системы»
Россия, г. Екатеринбург,
ул. Волгоградская, 194 а
Тел.: (343) 356-51-11

prosoftsystems.ru



Бондюгин Андрей Андреевич
Специалист по информационной безопасности
моб. +79221567512
a.bondiugin@prosoftsystems.ru