25 лет

АКАДЕМИЯ АЙТИ

Современные вызовы кибербезопасности для промышленных систем и построение эффективной защиты АСУ ТП
Выявление уязвимостей в АСУ ТП и SCADA

Современные **вызовы** кибербезопасности для промышленных систем

Построение эффективной защиты АСУ ТП

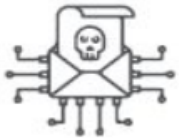
Выявление уязвимостей в АСУ ТП и SCADA

Что угрожает АСУ ТП?

Атаки на конвертеры интерфейсов и сетевые устройства не требуют понимания технологического процесса

Более 160 000
компонентов АСУ ТП
(АРМ, контроллеры и т.д.) открыты для возможных атак из Интернета

60% уязвимостей
имели самую высокую и критическую степень риска



70% от общего числа уязвимостей
приходится на такие их типы, как раскрытие информации, удаленное выполнение кода, отказ в обслуживании

78% уязвимостей обнаружены в устройствах с функциями диспетчеризации и мониторинга, в сетевых устройствах и инженерном программном обеспечении

Большинство уязвимостей
могут эксплуатироваться удаленно без необходимости получения каких-либо привилегий

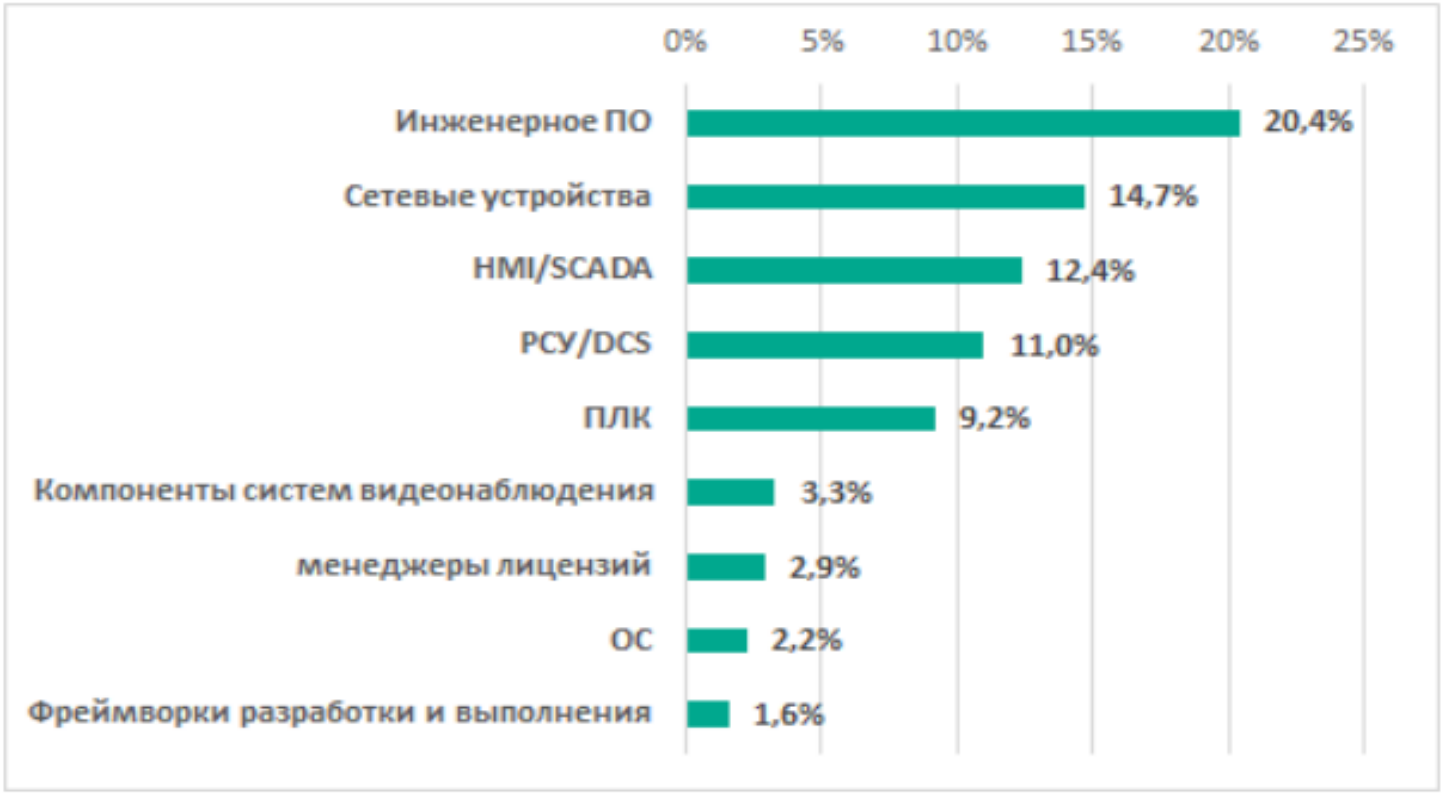
https://arinteg.ru/services/asutp.php

Уязвимые компоненты АСУ ТП

Наибольшее количество уязвимостей было выявлено в:

- инженерном ПО (103, 20%),
- сетевых устройствах промышленного назначения (78, 15%),
- SCADA/HMI-компонентах (63, 12%),
- РСУ (56, 11%)
- ПЛК (47, 9%).

Процент уязвимостей в различных компонентах АСУ ТП от общего числа уязвимостей. Уязвимости, опубликованные в 2019 году



Построение эффективной защиты АСУ ТП

на уровне операторского (диспетчерского) управления: инженерные автоматизированные рабочие места, промышленные серверы (SCADA-серверы), телекоммуникационное оборудование, каналы связи

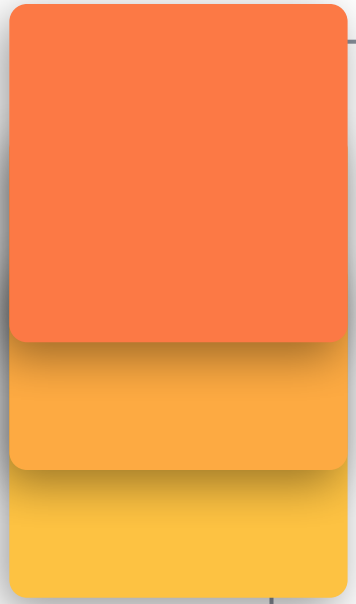
на уровне автоматического управления: программируемые логические контроллеры, иные технические средства с установленным программным обеспечением, промышленная сеть передачи данных

на уровне ввода (вывода) данных (исполнительных устройств): датчики, исполнительные механизмы, иные аппаратные устройства

Объекты защиты АСУ ТП

информация (данные) о параметрах (состоянии) управляемого (контролируемого) объекта или процесса (входная (выходная) информация, управляющая (командная) информация, контрольно-измерительная информация, иная критически важная (технологическая) информация)

программно-технический комплекс: технические средства (в том числе автоматизированные рабочие места, промышленные серверы, телекоммуникационное оборудование, каналы связи, программируемые логические контроллеры, исполнительные устройства), программное обеспечение (в том числе микропрограммное, общесистемное, прикладное), а также средства защиты информации



25 лет

Построение эффективной защиты АСУ ТП

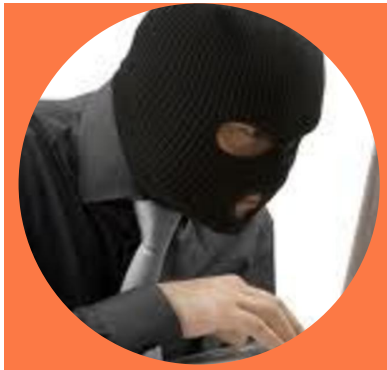
Предлагаемые решения

ОБЛАСТИ ПРАКТИЧЕСКОГО ИСПОЛЬЗОВАНИЯ

Kaspersky Industrial CyberSecurity (KICS Комплексный подход к промышленной безопасности

MaxPatrol SIEM — система мониторинга событий ИБ и выявления инцидентов

Код безопасности – Secret Net Studio Комплексное решение для защиты рабочих станций и серверов на уровне данных, приложений, сети, ос и периферийного оборудования



PT Industrial Security Incident Manager

Анализ трафика сетей АСУ ТП. Поиск следов нарушений ИБ и кибератак

Предлагаемые решения

ОБЛАСТИ ПРАКТИЧЕСКОГО ИСПОЛЬЗОВАНИЯ

InfoWatch ARMA - система для обеспечения кибербезопасности АСУ ТП

Программный комплекс «Аркан-М»
Многофункциональный межсетевой экран
Модуль обнаружения атак на всех уровнях АСУ ТП с возможностью их блокировки

Линейка ИнфоТеКС ViPNet Industrial Security: шлюзы безопаснсти, криптографические средства защиты информации

Dallas Lock 8.0

сертифицированная система защиты информации накладного типа для автономных и сетевых АРМ

Требования приказа ФСТЭК 31

Задача:
выполнить требования по обеспечению безопасности АСУ ТП: приказа ФСТЭК 31

Варианты решения: применение в АСУ ТП систем:

1) «Kaspersky Industrial CyberSecurity», «Secret Net Studio», «MaxPatrol SIEM», «InfoWatch ARMA»
2) «Kaspersky Industrial CyberSecurity», «Dallas Lock 8.0», Программный комплекс «Аркан-М»
3) Kaspersky Industrial CyberSecurity», «Secret Net Studio», «MaxPatrol SIEM», «InfoWatch Automated System Advanced Protector

Требования по 187-ФЗ

Задача:
выполнить требования по подключению АСУ ТП как ЗО КИИ: ФЗ 187, п.п. 127, приказов ФСТЭК (235, 239, 75), ФСБ (366, 367, 368)

Варианты решения: применение в АСУ ТП систем:

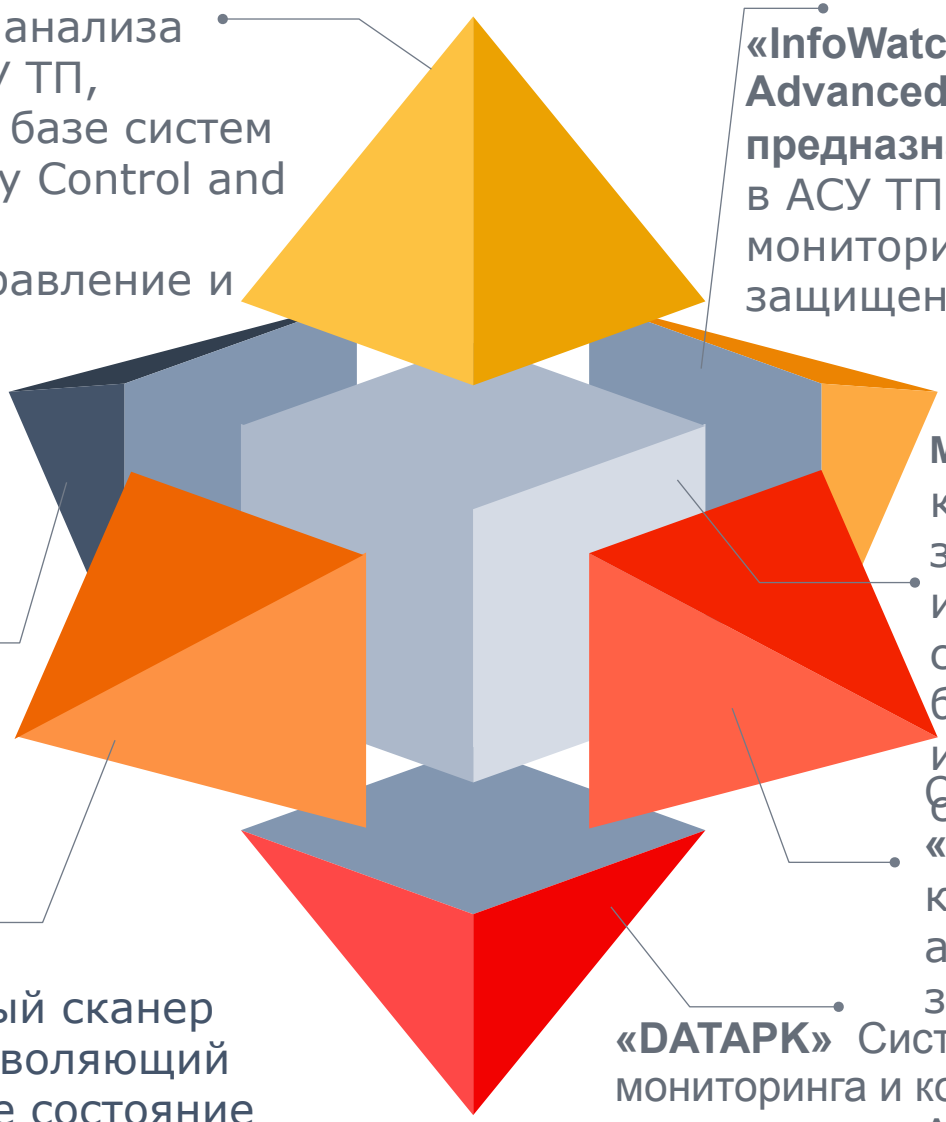
1) «Kaspersky Industrial CyberSecurity», «Secret Net Studio», «MaxPatrol SIEM», «InfoWatch ARMA», «ViPNet Industrial Security»
2) «Kaspersky Industrial CyberSecurity», «Dallas Lock 8.0», Программный комплекс «Аркан-М», «ViPNet Industrial Security»
3) Kaspersky Industrial CyberSecurity», «Secret Net Studio», «PT Platform 187», «InfoWatch Automated System Advanced Protector», «ViPNet Industrial Security»

Выявление уязвимостей в АСУ ТП и SCADA

Выявление уязвимостей в АСУ ТП и SCADA

«Сканер SCADA-аудитор» предназначен для анализа защищённости АСУ ТП, реализованных на базе систем SCADA (Supervisory Control and Data Acquisition, Диспетчерское управление и сбор данных).

«InfoWatch Automated System Advanced Protector» **предназначен** для применения в АСУ ТП на КВО для мониторинга и анализа защищенности.



«RedCheck 2.6.5» - система контроля защищенности и соответствия стандартам ИБ.

MaxPatrol 8 - система контроля защищенности и соответствия стандартам безопасности информационных систем.

Сканер безопасности **«Сканер ВС» - с**истема комплексного анализа защищенности.

«Xspider 7.8» - профессиональный сканер уязвимостей, позволяющий оценить реальное состояние защищенности IT-инфраструктуры.

«DATAPK» Система оперативного мониторинга и контроля защищенности АСУ ТП.

Контроль уязвимостей ЗО КИИ

Задача: выполнить требования по контролю (выявлению) уязвимостей ЗО КИИ: ФЗ 187, постановления правительства № 127, приказов ФСТЭК 235, 239

Варианты решения: применение в АСУ ТП систем:

1. **«Сканер SCADA-аудитор»** для анализа защищённости АСУ ТП, реализованных на базе систем SCADA

2. «InfoWatch Automated System Advanced Protector» для мониторинга и анализа защищенности в АСУ ТП

3. Система анализа защищенности **MaxPatrol 8** для выявления и анализа уязвимостей

4. «DATAPK» для оперативного мониторинга и контроля защищенности АСУ ТП

5. «RedCheck 2.6.5» - для контроля защищенности и соответствия стандартам ИБ

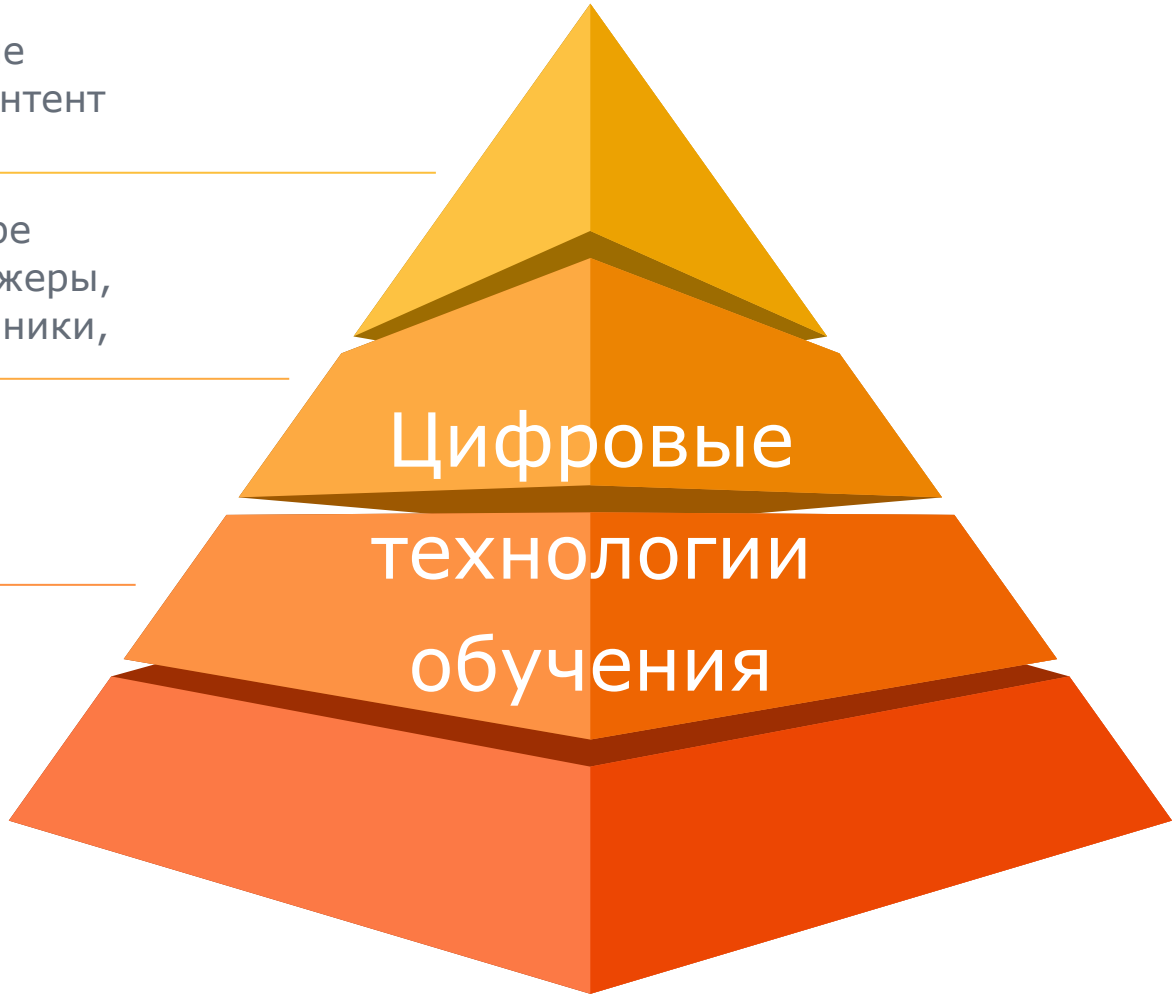
Академия АйТи – партнер конференции Кибербезопасность цифрового предприятия

Переподготовка, повышение квалификации, учебный контент

Цифровые продукты в сфере образования: курсы, тренажеры, симуляции, цифровые двойники, платформы

Создание образовательных экосистем вендоров

Методология организации и построения процесса обучения



Академия АйТи сегодня

25 лет

АПЛАНА
ГРУППА КОМПАНИЙ

Входит в ГК Аплана

АКАДЕМИЯ АЙТИ

Основана в 1995 г.

E-learning и очное обучение

Направления обучения:

Информационные технологии
Информационная безопасность
ИТ-менеджмент и управление проектами
Разработка и тестирование ПО
Гос. и муниципальное управление

Филиалы:
Санкт-Петербург, Казань, Уфа, Челябинск, Хабаровск, Красноярск, Тюмень, Нижний Новгород, Краснодар, Волгоград, Ростов-на-Дону

Головной офис в Москве

Ресурсы более 400 высококлассных экспертов и преподавателей

Разработка программного обеспечения и информационных систем

Ежегодные награды Microsoft, Huawei, Cisco и другие

Программы по импортозамещению

Сеть региональных учебных центров по всей России

Крупные заказчики

СБЕР
РЖД
Билайн
TATNEFT
НОРНИКЕЛЬ

100+
сотрудников

25 лет

АКАДЕМИЯ АЙТИ

Спасибо за внимание!

Вадим Ерышов к.т.н.
Руководитель кафедры
«Информационная
безопасность»

Центральный офис:
Москва, Варшавское шоссе 47, корп.4, 10 эт
Тел: +7 (495) 662-7894, 662-7895
Факс: +7(495) 974-7990
e-mail: academy@it.ru

АКАДЕМИЯ АЙТИ

лидер корпоративного обучения

www.academy.it.ru