Ликбез на кибербез

Красавин Артём

IST

Компания АйЭсТи

Мы помогаем организациям определить свои критические бизнес-процессы, а также возможные события, наступление которых приведет к разрушительным или фатальным для организации последствиям.

Наши специалисты выявят информационные системы и элементы телекоммуникационной инфраструктуры, которые связаны с данными бизнес-процессами или событиями, определят уязвимости, спроектируют и внедрят систему кибербезопасности, нацеленную на невозможность наступления недопустимых событий.

IST

“

Услуги по защите цифровых активов клиентов

Сотрудничество с нами

01 **ФСБ России**

02 **ФСТЭК России**

03 **МЧС России**

Мы выполняем

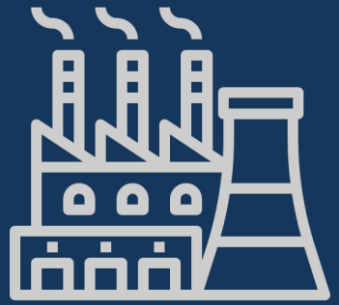
- Экспертный аудит
- Проектирование
- Поставка, внедрение и техническое сопровождение
- Построение систем кибербезопасности АСУ ТП

- Консультирование по законодательству в сфере ИБ
- Аутсорсинг ИБ
- Построение процесса безопасной разработки ПО
- Экспертное сопровождение при получении лицензий ФСТЭК и ФСБ

Корпоративные сети

Основной защищаемый ресурс:
Информация

Основная цель:
Обеспечение конфиденциальности



Промышленные сети

Основной защищаемый ресурс:
Технологический процесс

Основная цель:
Обеспечение непрерывности

Корпоративные сети

- Конфиденциальность
- Целостность
- Доступность

- Доступность
- Целостность
- Конфиденциальность

Промышленные сети

Заблуждения

1

«АСУ ТП полностью изолированы от внешнего мира»

2

«Нас никто не пытается взломать»

3

«АСУ ТП надёжно защищены разработчиком»

Украинские хакеры развернули мощную атаку на российскую промышленность. От пострадавших компаний требуют выкуп в $1-2 млн

Крупные российские промышленные компании начали атаковать новые группировки хакеров. Злоумышленники используют публичные сервисы, чтобы проникнуть в инфраструк
организаций. За расшифровку данных они требуют в
размере $1-2 млн. ИБ-эксперты сообщают, что взлам
компании стали намного быстрее: если раньше на эт

Да кому нужна эта защита?

За 2023 год хакеры-вымогатели группировки Shadow атаковали свыше 100 российских организаций

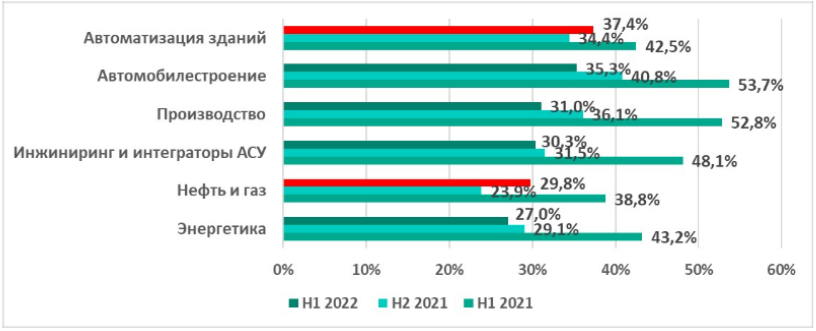
Дата: 08.03.2024. Автор: Артем П. Категории: Новости по информационной безопасности

Изображение: Plato Terentev (pexels)

Специалисты по информационной безопасности профильной компании F.A.C.C.T. провели анализ содержимого сервера, который засветился в проведении кибератак против различных российских организаций. Аналитики выяснили, что хакерская группировка Shadow начала действовать на территории РФ не весной 2023 года, как предполагалось ранее, а ещё в сентябре 2022 года.

Эксперты по кибербезопасности компании F.A.C.C.T. также указали на то, что
по август 2023 года хакерская группа вымогателей Shadow провела как минимум
вымогательского программного обеспечения против различных российских
ей профессиональной деятельности. Как минимум 10% подобных кибератак были

Специалисты «Лаборатории Касперского» подготовили отчет об угроз
промышленной автоматизации в России за первое полугодие 2023 год
выросла доля атакованных компьютеров АСУ ТП в нефтегазовой отра
источниками угроз стали интернет, съемные носители и почтовые клие



сло кибератак
енные предприятия
увеличилось на 53%

ТАСС 07 сентября 2023, 20:29 A- A+

МОСКВА, 7 сентября. /ТАСС/. Количество хакерских атак на предприятия промышленного сектора в РФ увеличилось за второй квартал текущего года на 53%, а доля атак на эту отрасль в общем объеме кибератак составила 13%, увеличившись на 5% по сравнению с первым кварталом. Об этом рассказал аналитик исследовательской группы Positive Technologies Федор Чунижеков, слова которого приводятся в аналитическом отчете компании, который имеется в распоряжении ТАСС.

Классы угроз АСУ ТП

01 Угрозы техногенного характера (аппаратные закладки)

02 Угрозы антропогенного характера (использование зараженных флешек, небезопасный Wi-Fi, USB-модемы)

03 Угрозы несанкционированного доступа (несанкционированные подключение АРМов, подключение к ПЛК)

Типовые недостатки АСУ ТП

Работа АСУ ТП на уязвимых и не поддерживающих Производителем ОС (жизненный цикл АСУ ТП 15-20 лет)

Использование неперсонифицированных УЗ на АРМ/серверах АСУ ТП и хранение паролей в незащищенном виде

Неконтролируемое удаленное подключение к АСУ ТП пользователей КСПД/подрядных организаций, имеющих возможность управления ТП

Отсутствие базовой минимально-необходимой защиты АРМ и серверов АСУ ТП (антивирусная защита, резервное копирование)

Отсутствие дублирования и/или горячего резерва серверов критичных АСУ ТП

Неуправляемые коммутаторы, «Плоские» сети, отсутствие сегментирования сети

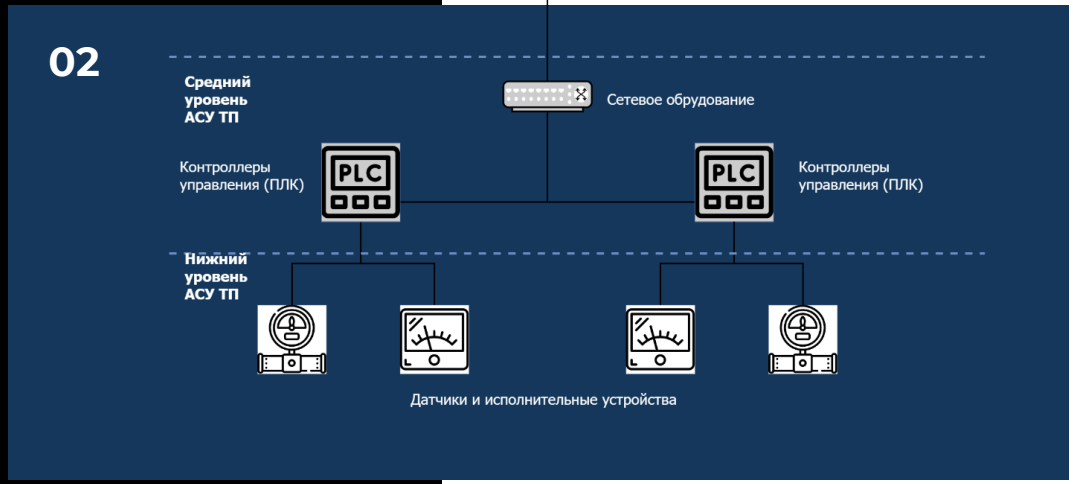
Основные вектора проникновения

Уровень SCADA/управления и КСПД

- Подключение к смежным автоматизированным системам
- Подключение к корпоративной сети через MES-систему
- Использование ПО «офисного» типа на АРМ и серверах АСУ ТП

Уровень датчиков исполнительных устройств и уровень сетевого оборудования

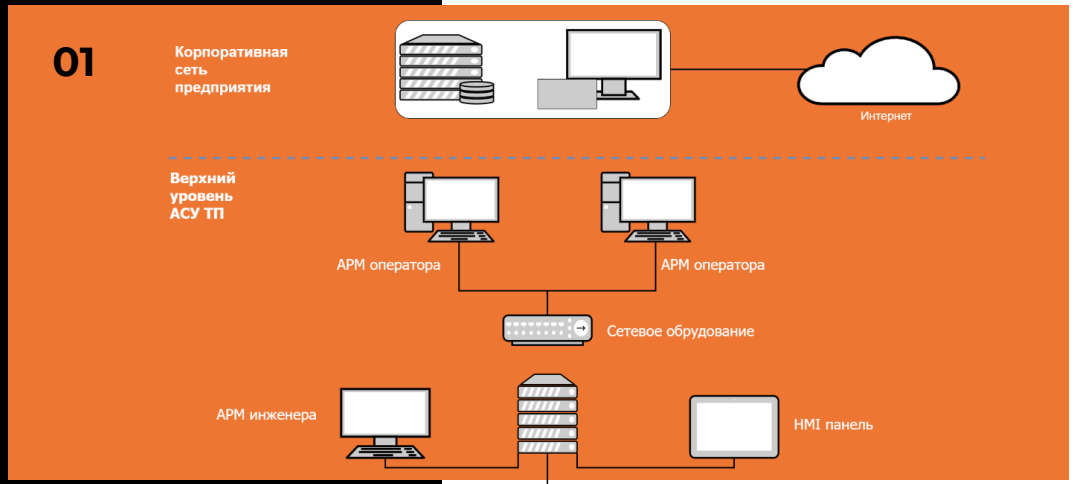
- Размещения компонентов в неохраняемых помещениях без присутствия персонала
- Территориальная распределённость, выход за контролируемую зону
- Протоколы передачи данных без механизмов защиты



Основные вектора проникновения

Уровень SCADA/управления и КСПД

- Подключение к смежным автоматизированным системам
- Подключение к корпоративной сети через MES-систему
- Использование ПО «офисного» типа на АРМ и серверах АСУ ТП



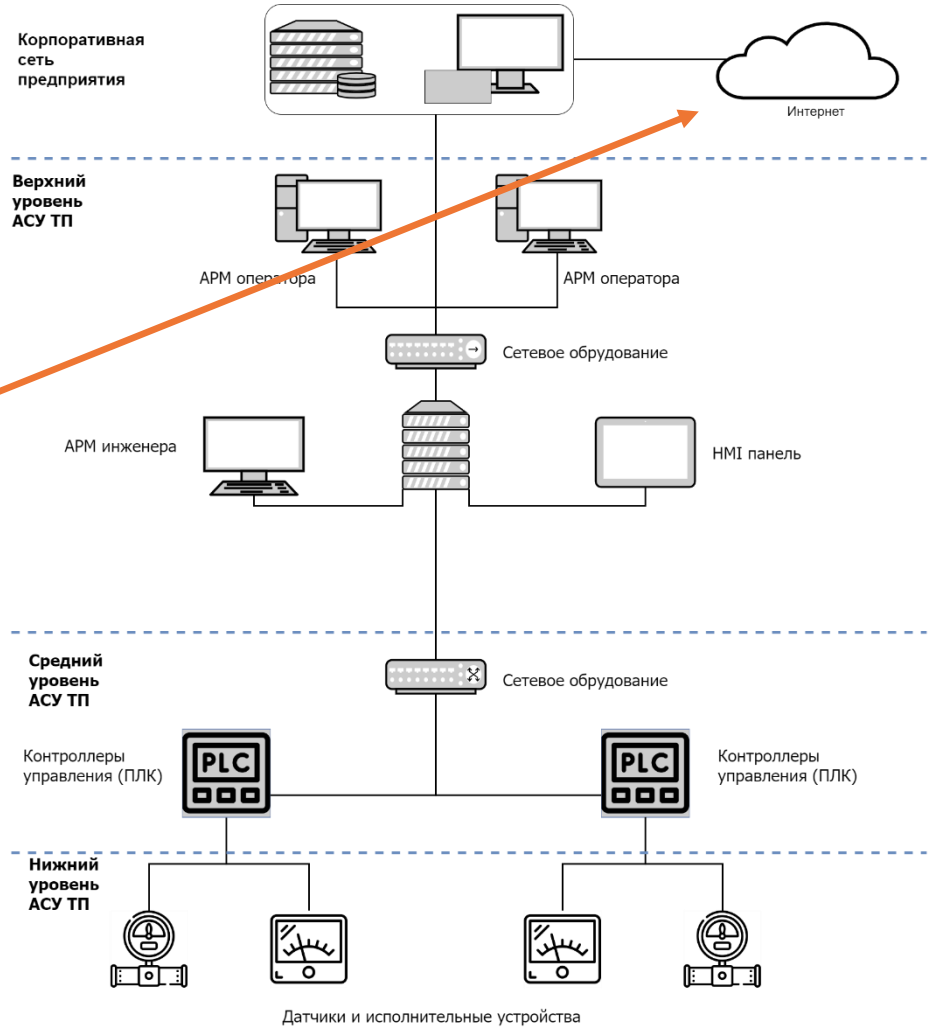
Уровень датчиков исполнительных устройств и уровень сетевого оборудования

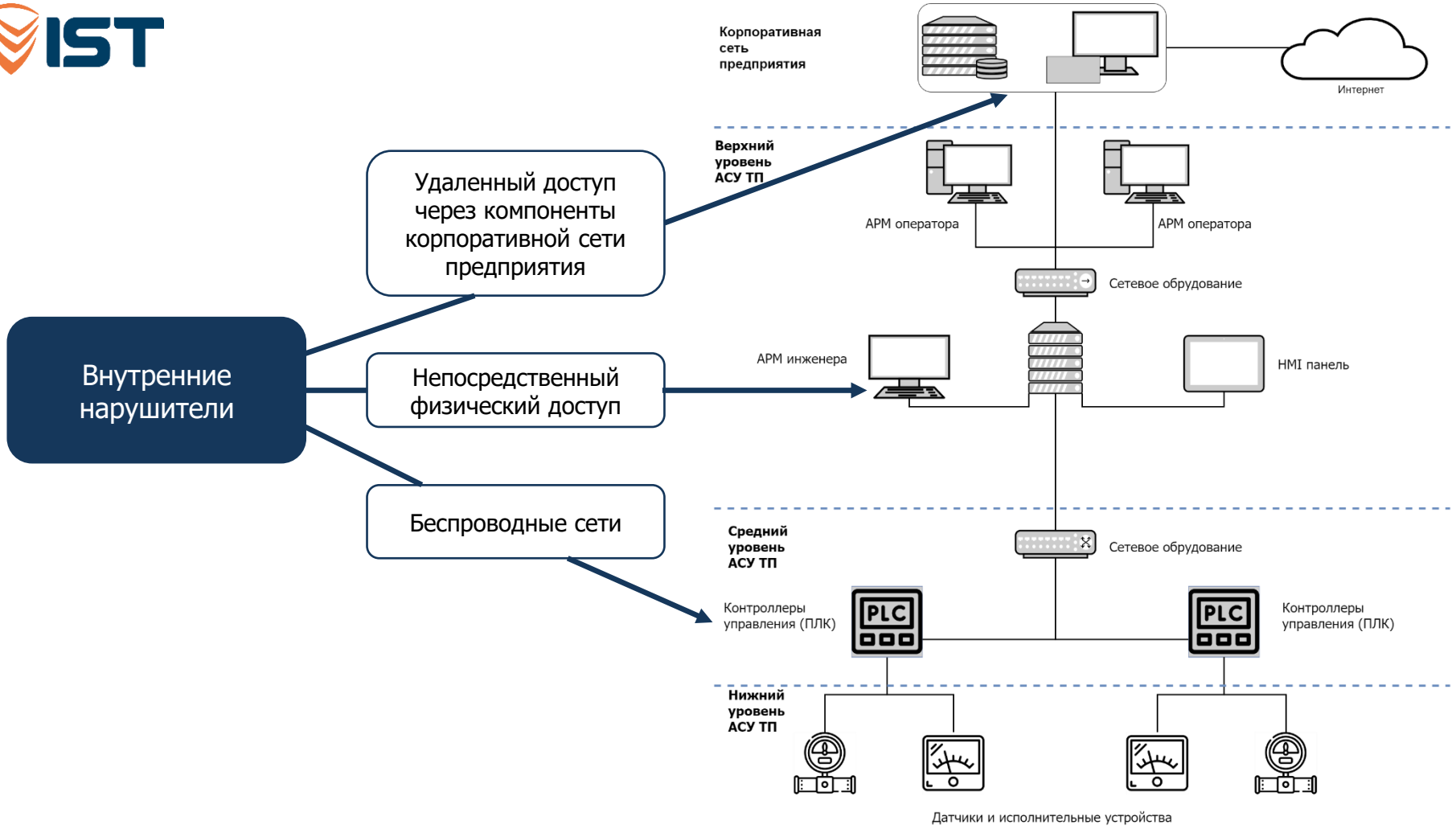
- Размещения компонентов в неохраняемых помещениях без присутствия персонала
- Территориальная распределённость, выход за контролируемую зону
- Протоколы передачи данных без механизмов защиты

Удаленный доступ через общедоступные сетевые ресурсы

Внешние нарушители

Удаленный доступ через подрядчиков имеющих доступ к АСУ ТП




Внутренние нарушители
Удаленный доступ через компоненты корпоративной сети предприятия
Непосредственный физический доступ
Беспроводные сети
Корпоративная сеть предприятия
Интернет
Верхний уровень АСУ ТП
АРМ оператора
АРМ оператора
Сетевое обрудование
АРМ инженера
HMI панель
Средний уровень АСУ ТП
Сетевое обрудование
Контроллеры управления (ПЛК)
PLC
PLC
Контроллеры управления (ПЛК)
Нижний уровень АСУ ТП
Датчики и исполнительные устройства

Как от недопустимых событий перейти к ИБ, угрозам и иным знакомым темам?

Топ-менеджмент
Знает, что действительно **недопустимо** для бизнеса

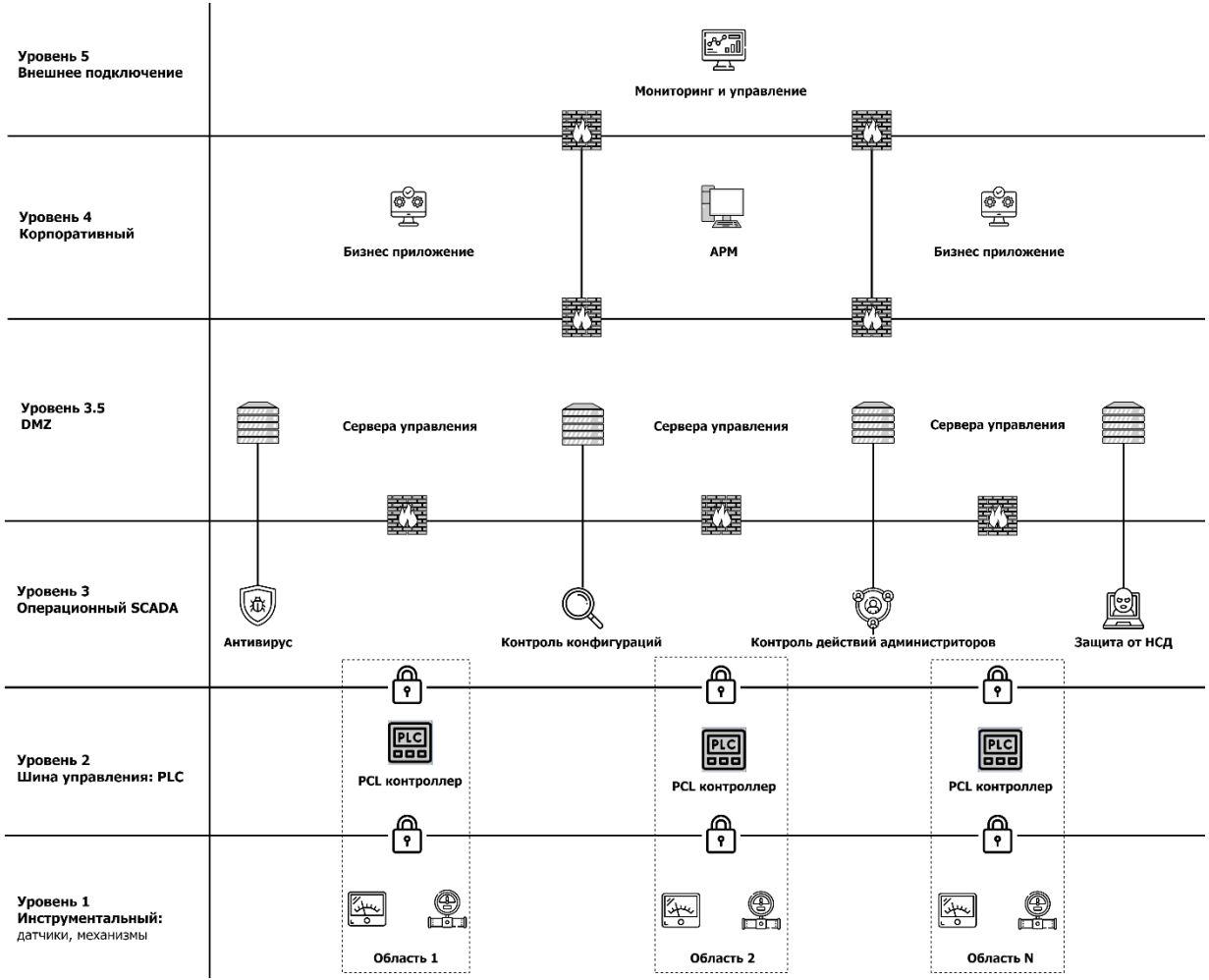
ПЕРЕЧЕНЬ
недопустимых для бизнеса событий

Операционные руководители
Помогут понять, как **недопустимое** может быть реализовано

СЦЕНАРИИ
реализации недопустимых событий

Специалисты IT и ИБ
Помогут обозначить системы, на которых **недопустимое** может быть реализовано

СИСТЕМЫ,
Взлом которых повлечёт недопустимое событие



NTA для АСУ ТП

Решения класса SIEM и SOC

Разумный баланс

Между организационными и техническими мерами защиты

Главное – это то, что кибербезопасность АСУ ТП отличается от классической информационной безопасности, и вопрос ее обеспечения на сегодняшний день весьма актуален

Красавин Артём Александрович

Ведущий пресейл-инженер

PHONE

+ 7 (964) 986-95-85

EMAIL

akrasavin@zaschita-it.ru