23.09.2021

АМТ-ГРУП

Новое поколение продуктов InfoDiode для защиты КИИ. Решения для передачи промышленных протоколов

Половинко Вячеслав – руководитель направления собственных продуктов АМТ-ГРУП

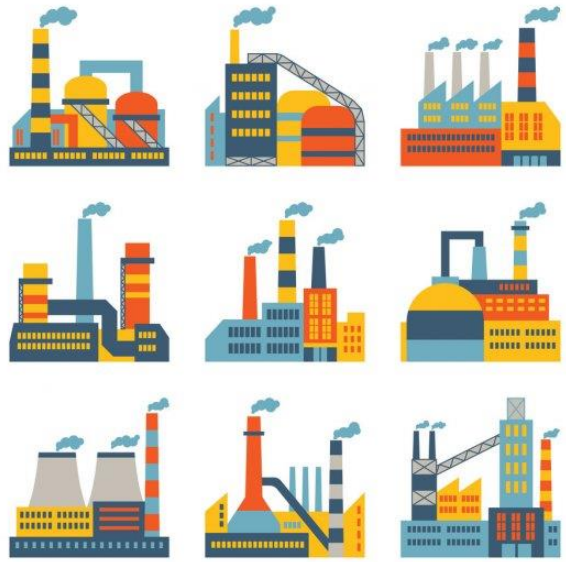
1. Актуальный взгляд на угрозы и ключевые техники атак на КИИ

2. Современные и эффективные меры защиты КИИ

Угрозы и ключевые техники атак на КИИ

Современное предприятие уже давно не изолированный сегмент

- Типовое предприятие может иметь до 500 связей с внешними организациями*
  - Облачные решения, поддержка ПО, ИТ-поддержка, системы архивирования данных, отопление, вентиляция, кондиционирование, системы безопасности (как информационной, так и общей), диспетчерские, системы поставщиков и подрядчиков
- ПО в сети OT/ICS (АСУ ТП) часто «унаследовано»
  - ПО создавалось без учета ИБ, ряд промышленных протоколов не предполагают аутентификацию
  - Аппаратные средства и сети не предполагают установки СЗИ
- 90% госорганизаций имеют от 3-х до 10-и точек сопряжения публичного и закрытого сегментов**
  - Практически каждому предприятию требуется передавать данные промышленного/закрытого сегмента наружу (телеметрия, видеонаблюдение, реплики и т.п.)



* Оценка Owl Cyber Defense
** Оценка Ростелеком Солар

Интерес киберпреступников к промышленным объектам растет!

POSITIVE TECHNOLOGIES

Специалисты связывают рост популярности использования ПО для обхода «песочниц» со смещением вектора хакерских атак от финансового сектора на предприятия, где одним из ценнейших ресурсов является коммерческая тайна.

Код за кодом: 70% вредоносного ПО используется для шпионажа

DW Made for minds.

"Самая опасная кибератака в истории Америки": что известно о Sunburst

SolarWinds была для хакеров не целью, а лишь путем доставки вредоносного софта. Хакеры разместили свой секретный код в одном из пакетов обновлений, а потом сумели через систему автоматических обновлений разослать его клиентам компании. Они могли как получить доступ к секретной информации и электронной переписке, так и осуществлять удаленный доступ и управление системами.

The disclosure makes **SonicWall** (ранее принадлежала Dell) at least the fifth large company to report in recent weeks that it was targeted by sophisticated hackers. Other companies include network management tool provider **SolarWinds, Microsoft, FireEye, and Malwarebytes**. **CrowdStrike** also reported being targeted but said the attack wasn't successful.

TADVISER
Государство. Бизнес. ИТ

Выявлена киберкампания против российских промышленных предприятий

12 октября 2020 года стало известно, что «Лаборатория Касперского» обнаружила продолжительную киберкампанию, нацеленную на российские промышленные предприятия. Характерной особенностью атак является тот факт, что операторы кампании, судя по всему, также русскоязычные.

«Лаборатория Касперского» рассказала, какими будут кибератаки на промышленные предприятия в 2021 году

Заражения будут становиться менее случайными или иметь неслучайные продолжения

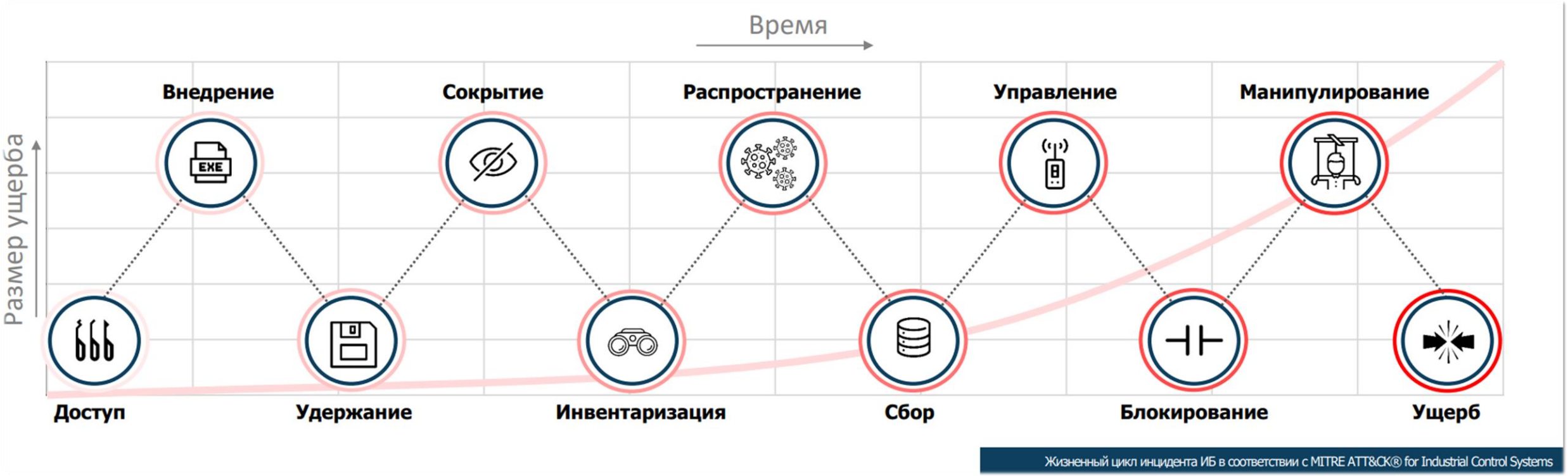
Некоторые группировки уже несколько лет специализируются на атаках на промышленные предприятия для прямой кражи денег.

Следует ожидать появления новых сценариев атак на АСУ ТП и полевые устройства, а также неожиданных схем их монетизации.

Уязвимостей больше, поверхность атаки на КИИ шире

- **Уязвимость «нулевого дня» - реальность сегодняшнего дня**
- **Скорость распространения атаки > скорости распространения защиты**
- **Канал взаимодействия с «системой-жертвой» - ключ к успешной атаке**
  - Двунаправленность важна уже на самом раннем этапе - при рекогносцировке
  - Многие техники для захвата систем реализуются на основе двустороннего взаимодействия (RAT, phishing и т.д.)
- **Длительные сценарии развития атаки являются нормой**
  - Использование вспомогательных модулей для защиты вредоносного ПО от обнаружения
- **Вектор атаки смещается на человеческий фактор**
- **Общедоступность средств атаки**
- **Зарубежный опыт с задержкой транслируется в российские реалии**
  - Регуляторы многих секторов уже включили в свои документы требования и рекомендации по применению продуктов класса «диод»

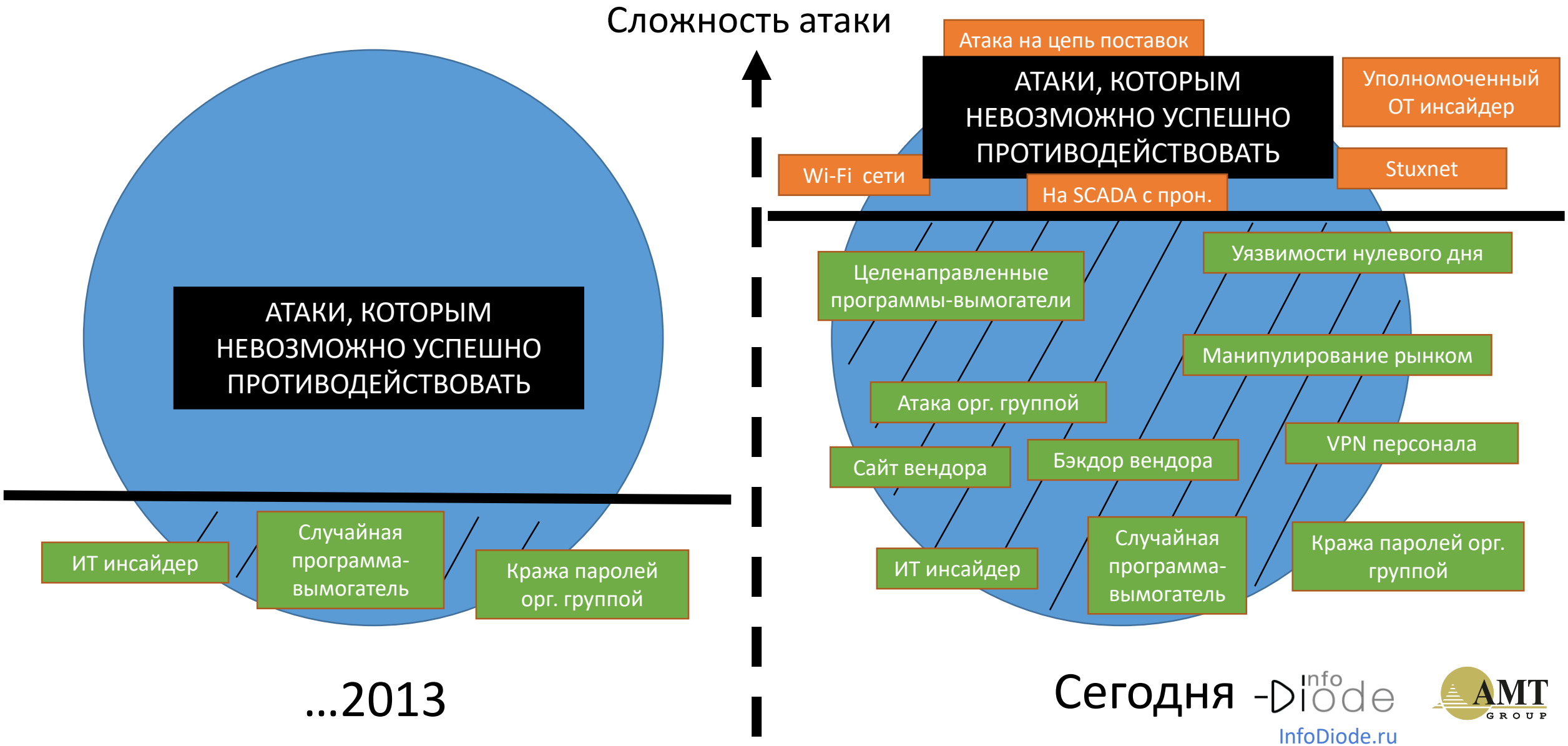
Длительные циклы развития атаки являются нормой и типовым сценарием



Атака планируется, развивается и завершается тогда, когда мы этого не видим

InfoDiode.ru

Стратегии защиты и СЗИ существенно повысили кол-во отраженных сложных атак. К сожалению, не все применяют эти стратегии и средства



InfoDiode.ru

Принципы и решения для повышения уровня защищенности периметра КИИ

Успешная стратегия – не допускать реализации самых разных классов атак

Эффективно противодействовать атаке - означает **предотвратить** конкретные этапы/последствия атаки **каждый раз**, когда такая атака осуществляется

Разные средства являются частью стратегии и имеют разную степень эффективности

- **Антивирус** – не всегда может противостоять распространению вредоносного ПО, поскольку сигнатуры такого ПО могут поступать позже, чем запустится ПО

- **Патчи ПО в части безопасности** – не всегда могут обеспечить закрытие эксплойтов известных уязвимостей. Требуется время на проверку совместимости обновления с инфраструктурой, на его получение, установку и т.п. Иногда обновления могут быть ошибочными

- **Системы обнаружения вторжений** – являются детективными, но не превентивными мерами защиты. Они способствуют оперативному выявлению проблемы, ее локализации, но требуют времени на реагирование, которое может быть использовано вредоносным ПО для реализации атаки

Фактор времени

Ряд средств защиты доказали свою эффективность за счет применения принципов асинхронности и «пространственного разделения»

- **Двухфакторная аутентификация на базе RSA** – достаточно успешно противостоит фишинговым атакам. Имея только удаленный доступ, осуществить фишинговую атаку становится невозможно

- **Аппаратное обеспечение TPM** – ключи шифрования никогда не покидают выделенные криптографические аппаратные модули и не появляются в памяти компьютера, на котором работает TPM. Без физического демонтажа оборудования похитить ключи шифрования оказывается невозможно

- **Однонаправленные шлюзы («диоды»)** – физически способны передавать информацию только в одном направлении – от критически важной ОТ сети к ИТ/корпоративной/интернет-сети, не имея возможности доставлять информацию обратно. В однонаправленно защищенных сетях ни один управляющий сигнал физически не может быть передан внутрь сегмента

Фактор пространства

Структура предложений устройств «диод» на российском рынке

Российские вендоры

Часто не рассматривают линейку таких устройств как основную. Как следствие - внимание, уделяемое этим устройствам, остаточное.
Прежде всего в части:

1. Развития
2. Технической поддержки
3. Наращивания и масштабирования
4. Сроков производства и поставки

и т.п.

Зарубежные вендоры

Практически отсутствуют на российском рынке

1. Санкции
2. Отсутствие сертификатов соответствия от регуляторов

АМТ-ГРУП

Предлагает комплексные решения:

1. Имеет полную линейку устройств, которые поставляет на рынок уже более 6-ти лет
2. Развивает продукт (см. новые линейки, скорость выхода версий ПО, участие в конференциях и т.п.)
3. Имеет продуктовую линейку: АК и АПК

Решения АМТ-ГРУП по защите КИИ. Новая линейка продуктов InfoDiode

АК InfoDiode эффективно сочетают все лучшие практики по защите периметра КИИ в случае необходимости передачи UDP, Syslog, SPAN и др. трафика

АК INFODIODE

InfoDiode
rack module

- *Встроенные резервированные блоки питания AC*
- *Высота 1 RU*
- *Малая глубина, возможность монтажа 2 устройств с двух сторон шкафа*

InfoDiode
rack module Cluster

- *Резервированное подключение 1+1*
- *Встроенные резервированные блоки питания AC для каждого из модулей*
- *Высота 1 RU*
- *Малая глубина, возможность монтажа устройств с двух сторон шкафа*

InfoDiode
Mini

- *На DIN — рейку*
- *На монтажную пластину*
- *Напряжение питания 9-36 VDC*
- *Два ввода питания для резервирования по схеме 1+1*
- *Адаптер питания 12 V и 1,25 A для настольного размещения*

АПК InfoDiode PRO позволяет соответствовать лучшим практикам по защите периметра КИИ, организовать передачу файлового и иного трафика

АПК INFODIODE PRO

Базовый вариант	Кластерный вариант
InProxy, OutProxy сервер	2 InProxy, 2 OutProxy сервера
АК InfoDiode, rack module	2 АК InfoDiode, rack module, Cluster
Форм фактор - 3U	Форм-фактор - 6U

- Сертификация ФСТЭК НДВ4, УД4
- Сертификат соответствия требованиям тех.регламента Таможенного Союза
- Производство устройств сертифицировано

АПК InfoDiode SMART - новое решение по защите КИИ от АМТ-ГРУП

АПК INFODIODE SMART

❑ Защита и мониторинг КИИ

Обеспечивает защиту и мониторинг объекта КИИ, исключая какое-либо воздействие на него.

❑ Поддержка пром. протоколов OPC UA, Modbus, MQTT

Обеспечивает защищенное удаленное взаимодействие критичных сегментов отдельных предприятий и организаций через недоверенные сети. Передает данные за границу доверенного периметра сети по протоколам OPC UA, Modbus, MQTT, FTP(S), CIFS, SFTP, UDP, др.

❑ Основа для организации цифровых двойников

Передает реплики критических информационных ресурсов (OPC серверов, SCADA систем основных вендоров) за границы периметра АСУ ТП и КИИ для последующей обработки и анализа.

❑ Централизованные диспетчерские и ситуационные центры

Обеспечивает центры реальными онлайн данными, в том числе с видеофиксацией, в условиях гарантированной изоляции объектов наблюдения.

❑ Агрегация данных из SCADA систем в ERP, MES и «облака»

Передает данные из нескольких SCADA систем в ERP, MES системы, облачные решения, исключив какое-либо обратное влияние со стороны этих систем.

InfoDiode.ru

АПК InfoDiode SMART можно использовать в разнородной инфраструктуре КИИ

АПК INFODIODE SMART

- **Компактный – 1U rack решение.** Упрощает встраивание в разнородную инфраструктуру
  - Виртуальные среды, серверы заказчика, докеры, операционные системы
- **Поддерживает пром. протоколы** (MQTT, Modbus, OPC UA…)
- **Многофункциональный** (передает несколько видов протоколов и видов трафика одновременно: например, видео, файлы и OPC-UA)
- **Предоставляет возможность разрабатывать собственные коннекторы** под конкретные задачи и для передачи требуемых промышленных протоколов
- **Реализован на российской платформе**, российском программном обеспечении производства АМТ-ГРУП.

InfoDiode.ru

Промышленные протоколы через InfoDiode SMART - уже реальность

Any
Allen-Bradley Suite
Aromat Suite
AutomationDirect Suite
Building Automation Suite
Contrex Suite
Cutler-Hammer Suite
DNP3 Suite
EFM Suite
Fanuc Focas Suite
Fisher ROC Suite
GE Suite
Honeywell Suite
IEC 60870-5 Suite
IT and Infrastructure Suite
Manufacturing Suite
Mitsubishi Suite
Modbus Suite
Oil and Gas Suite
Omron Suite
OPC Connectivity Suite
Power Suite
SattBus Suite
Siemens Plus Suite
Siemens Suite
Simatic Suite
Simulation Suite
SIXNET Suite
SNMP Suite
Thermo Westronics Suite

Modbus

Промышленные протоколы

info-Diode

Конвертеры

Удаленные АРМ

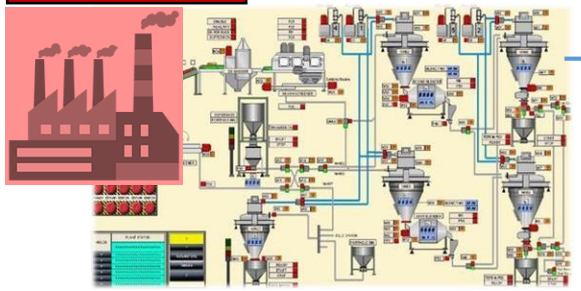
Ситуационные центры

ДОВЕРЕННЫЙ СЕГМЕНТ
Управление оборудованием

НЕДОВЕРЕННЫЙ СЕГМЕНТ
Ситуац. центры, диспетчерские, подрядчики, SOC, NOC

АПК InfoDiode SMART позволяет собирать данные SCADA за границами периметра

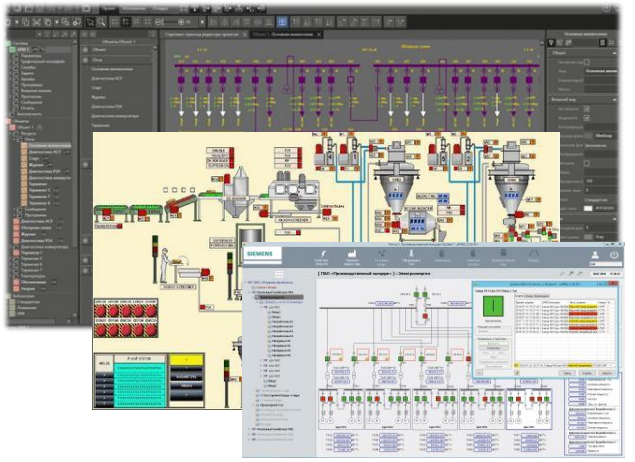
KepServer



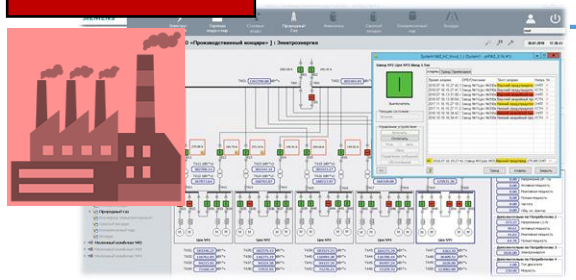
Конвертеры

info-Diode

Конвертеры
OPC UA сервер



WINCC OA

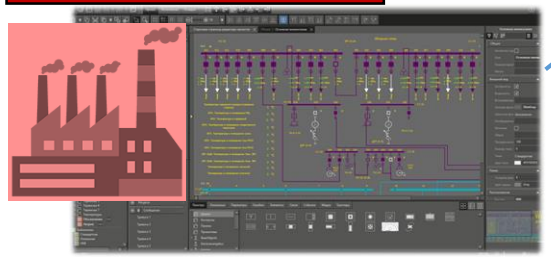


Конвертер
OPC UA

info-Diode

Централизованные
диспетчерские
Ситуационные центры

MasterSCADA 4D



Конвертер
OPC UA

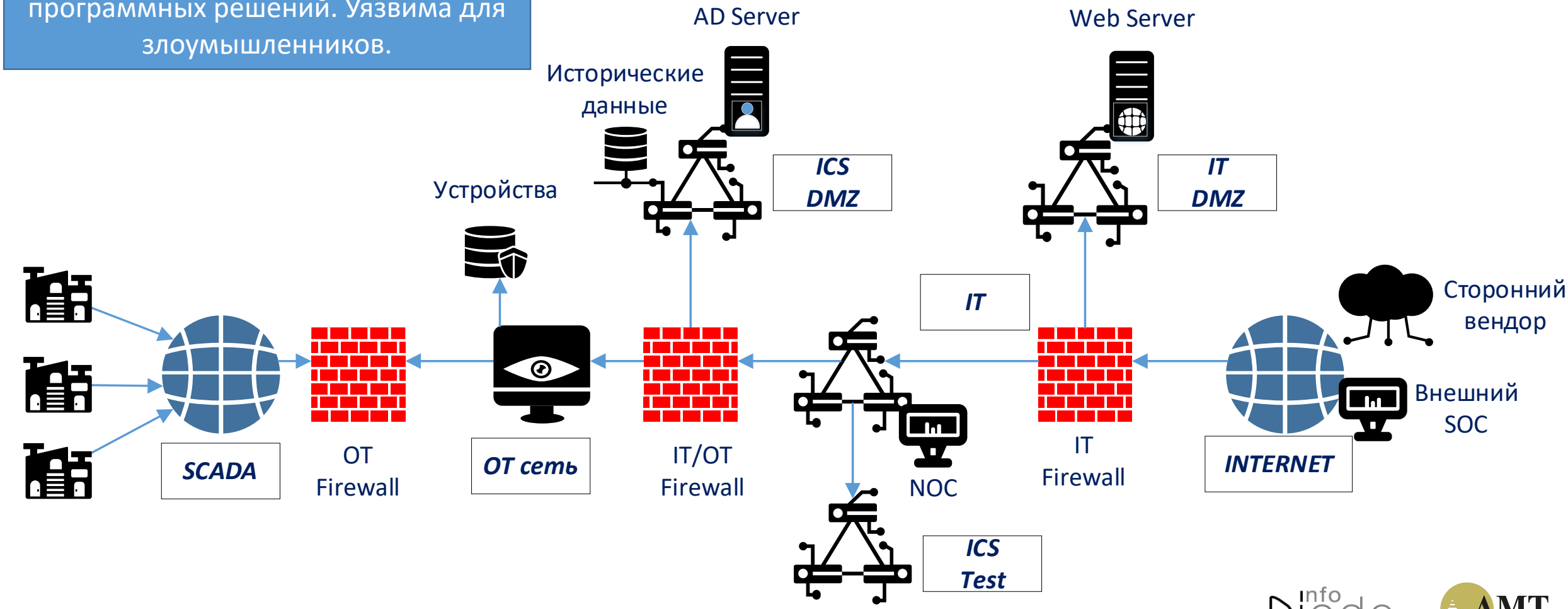
info-Diode

InfoDiode.ru

AMT GROUP

Защита КИИ только на Firewall (AS IS) – рискованная схема

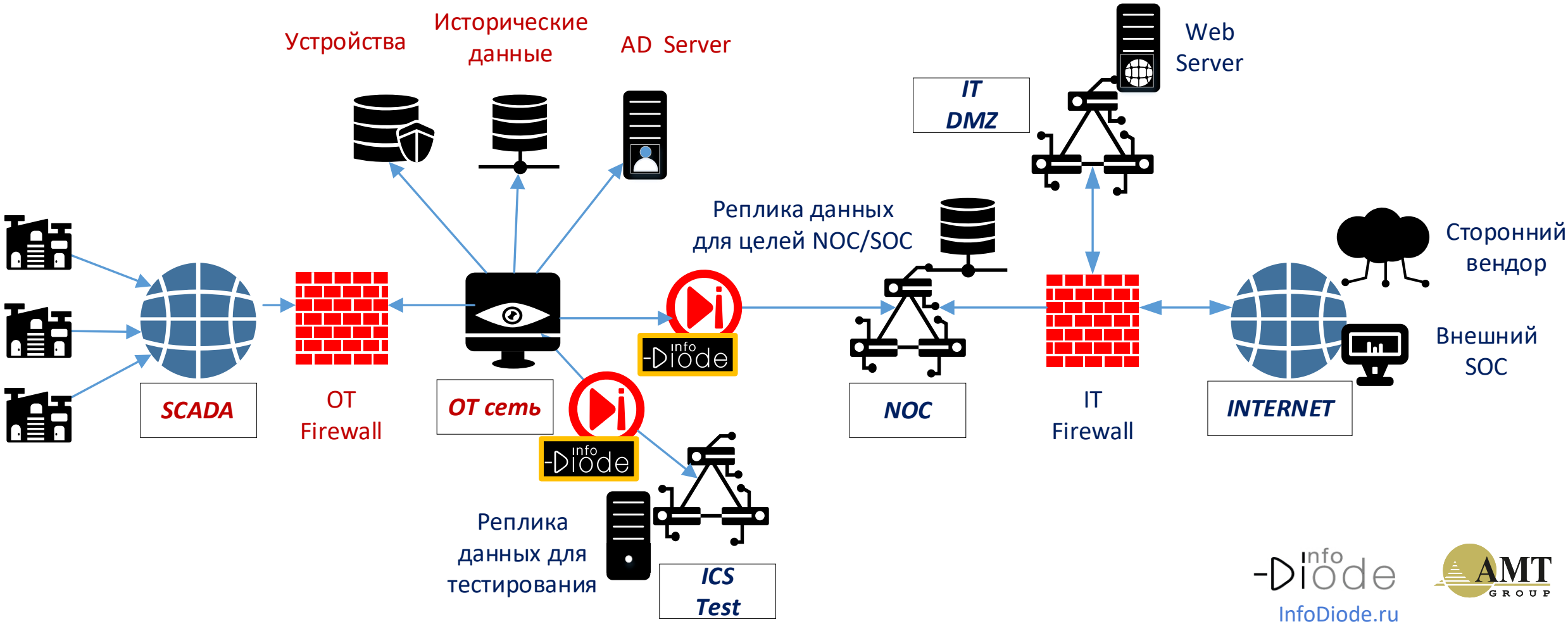
Фактически «единая сеть», сегментированная с использованием программных решений. Уязвима для злоумышленников.



InfoDiode.ru

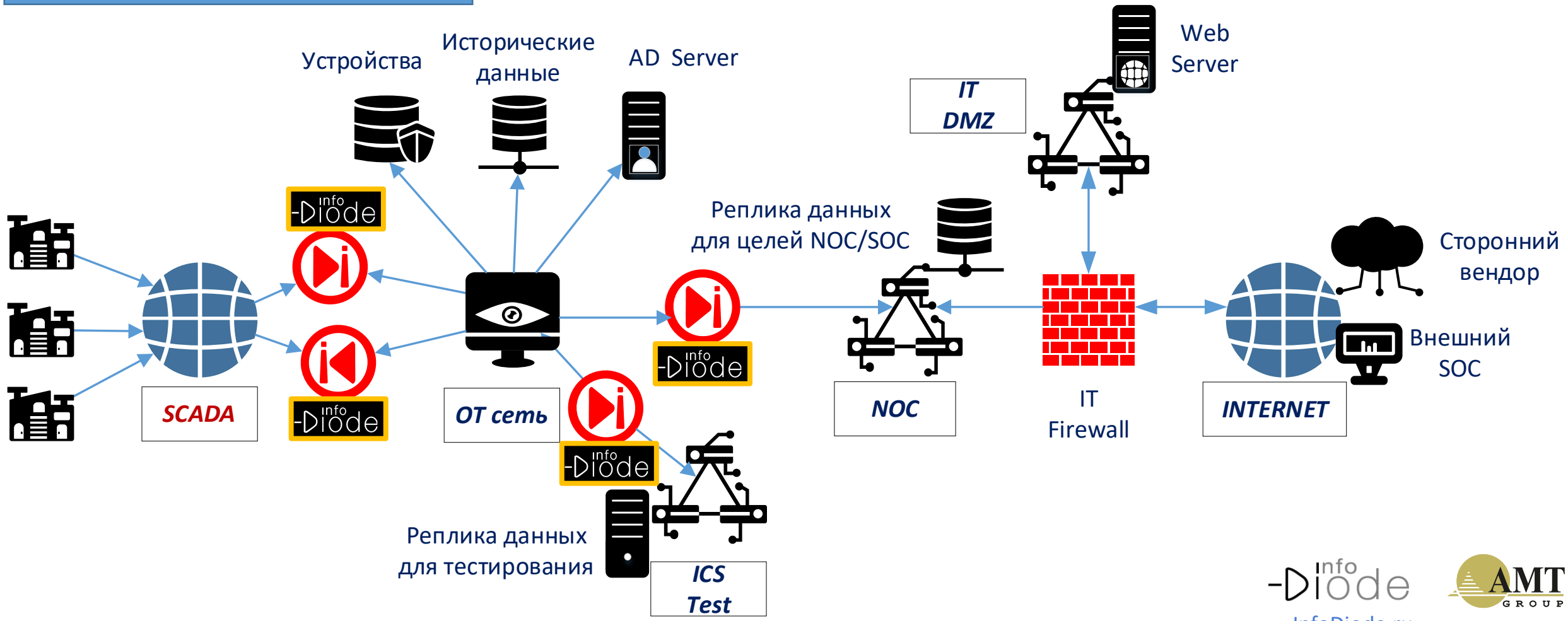
От защиты КИИ только на Firewall к защите с АПК InfoDiode SMART (ШАГ - 1)

АСУ ТП (ОТ) сеть гарантированно изолирована от КОРП (IT) сети аппаратными решениями InfoDiode



От защиты КИИ только на Firewall к защите с АПК InfoDiode SMART (ШАГ - 2)

Эшелонированная защита АСУ ТП (ОТ) сети, защита каждого сегмента с SCADA системой



АПК InfoDiode SMART дополняет линейку решений для комплексной защиты КИИ

1. **АК InfoDiode** - базовое, сертифицированное ФСТЭК УД (4), аппаратное решение, гарантирующее защиту на аппаратном уровне и эффективно решающее задачу по передаче UDP, Syslog, SPAN трафика за пределы КИИ.

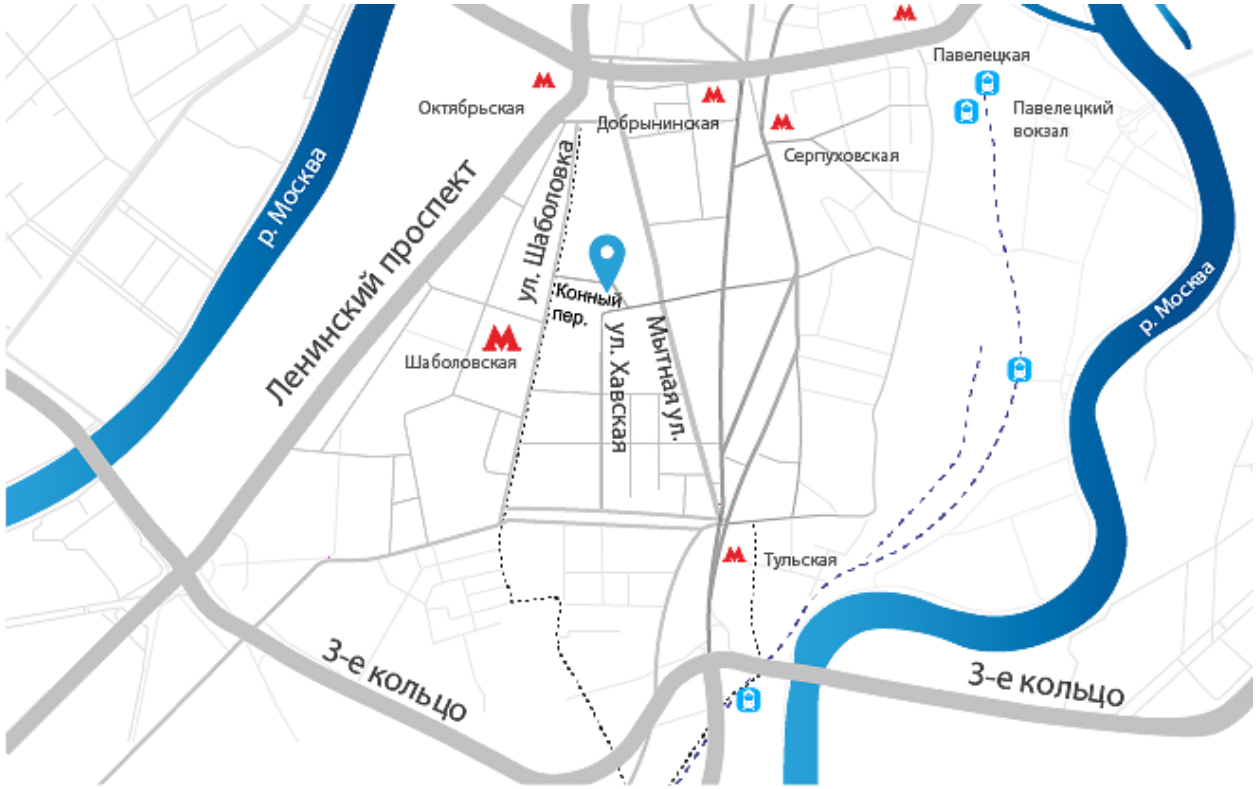
2. **АПК InfoDiode PRO** – сертифицированное ФСТЭК УД (4) решение для передачи значимых файловых потоков, дистрибутивов, реплик ВМ и баз данных, электронной почты, бэкапов и т.п. из доверенного сегмента вовне.

3. **АПК InfoDiode SMART** – новое решение для передачи за пределы периметра КИИ промышленных и специфических протоколов, в том числе видео, для интеграции SCADA систем, организации удаленных ситуационных центров за границей периметра, в условиях гарантированной изоляции КИИ

InfoDiode.ru

Как с нами связаться

- Адрес: 115162, Россия, Москва, ул. Шаболовка, д. 31, корп. Б, подъезд 3, этаж 2, вход с Конного переулка
- Телефон/Факс: +7 (495) 725-7660, +7 (495) 646-7560
- Факс: +7 (495) 725-7663
- E-mail: **InfoDiode@amt.ru**
- Сайт: **InfoDiode.ru**
- Техническая поддержка: **https://support.amt.ru**



СПАСИБО ЗА ВНИМАНИЕ!