06.04.2021

АМТ-ГРУП

Устройства класса диод как средства защиты периметра сети: мифы и реальность

Половинко Вячеслав – руководитель направления собственных продуктов АМТ-ГРУП

Современное предприятие уже давно не изолированный сегмент

- Типовое предприятие может иметь до 500 связей с внешними контрагентами, партнерами, вендорами и организациями
  - Облачные решения
  - Поддержка ПО, ИТ-поддержка
  - Системы архивирования данных
  - Отопление, вентиляция, кондиционирование (HVAC)
  - Системы безопасности (как информационной, так и общей)
  - Диспетчерские
  - Системы поставщиков и подрядчиков
- ПО в рамках сети OT/ICS (АСУ ТП), как правило, «унаследовано»
  - ПО создавалось без учета ИБ, ряд промышленных протоколов не предполагают аутентификацию

8 МИФОВ о «диодах данных»

МИФ1
«Диоды» - это обязательно дорогие устройства

Существуют самые разные классы решений в относительно недорогой ценовой категории

- Стоимость аппаратных диодов начинается от 150 т.р.

ЛИНЕЙКА 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

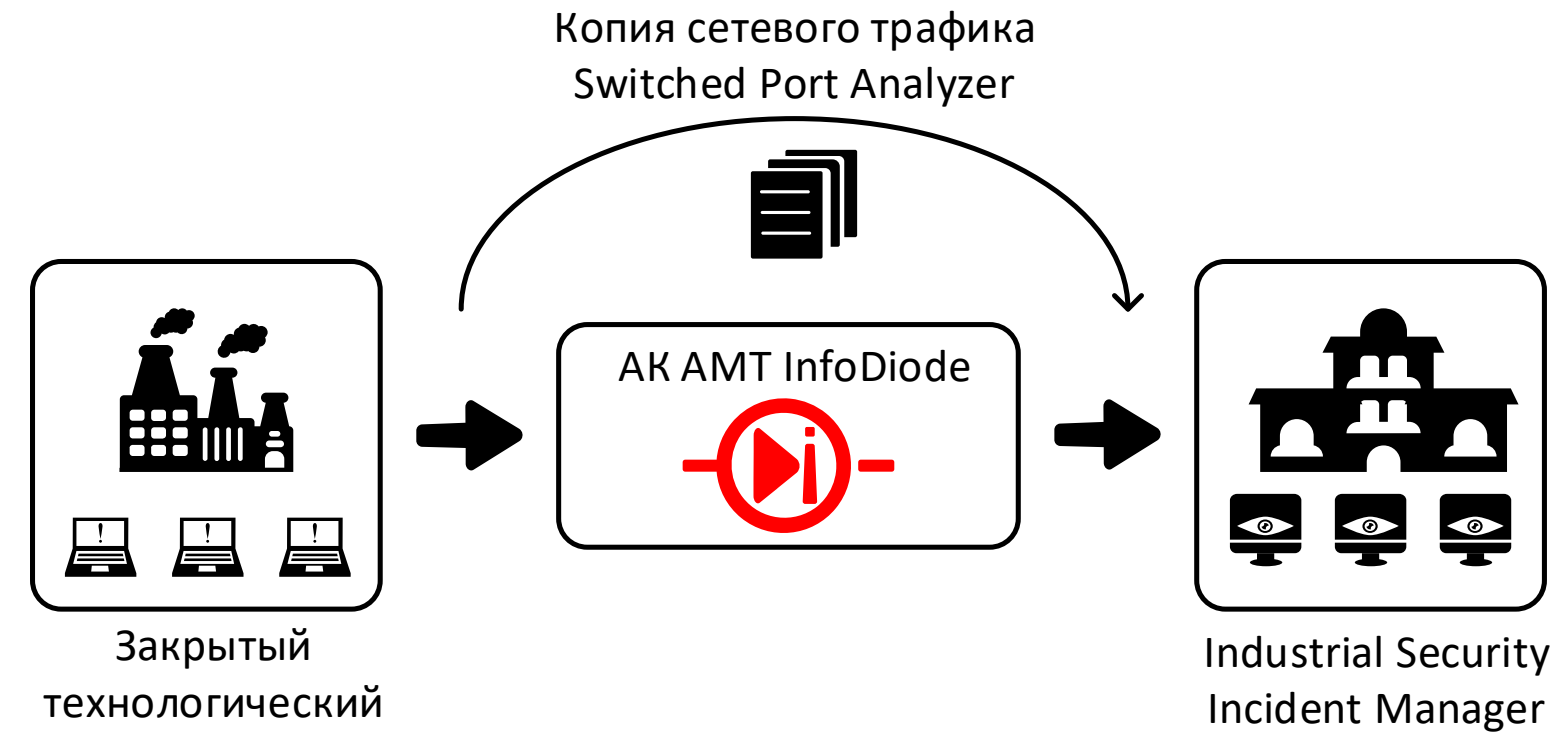
• Резервированное подключение 1+1
• Встроенные резервированные блоки питания AC для каждого из модулей
• Высота 1 RU
• Малая глубина, возможность монтажа устройств с двух сторон шкафа

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

SPAN-mirroring

Вариант 1. Передача копии технологического трафика закрытого сегмента во внешнюю систему мониторинга с использованием SPAN. Копия технологического трафика передается во внешний ПАК глубокого анализа трафика, который обеспечивает поиск следов нарушений информационной безопасности в сетях АСУ ТП, помогает на ранней стадии выявлять кибератаки, активность вредоносного ПО, неавторизованные действия персонала (в том числе злоумышленные)



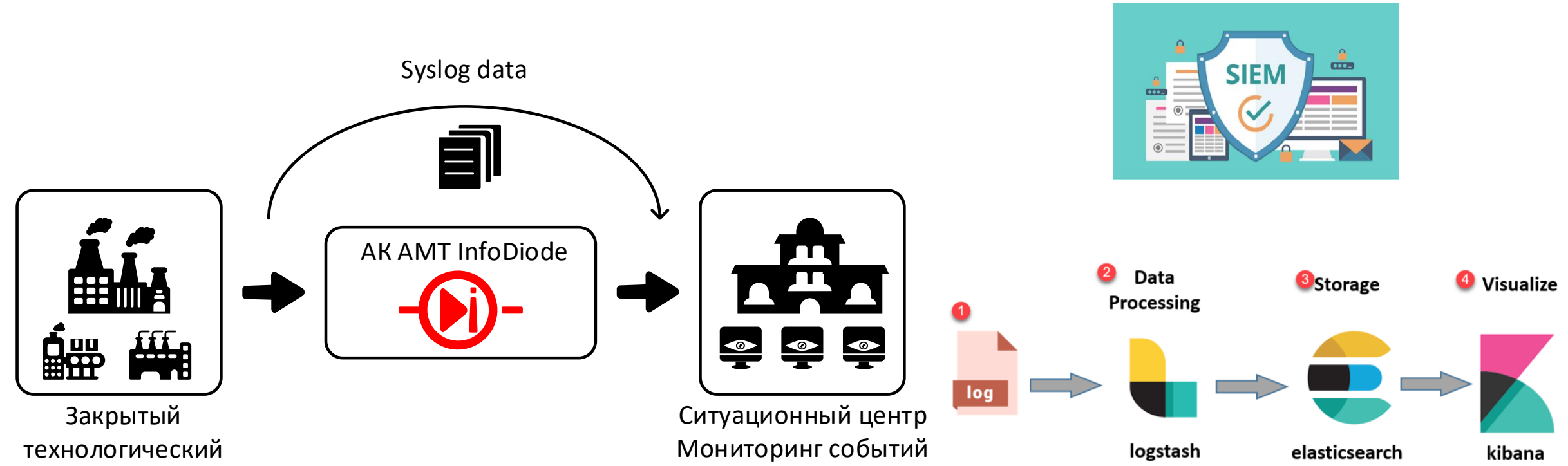
Kaspersky Industrial CyberSecurity

CyberLympha DATAPK

InfoDiode.ru

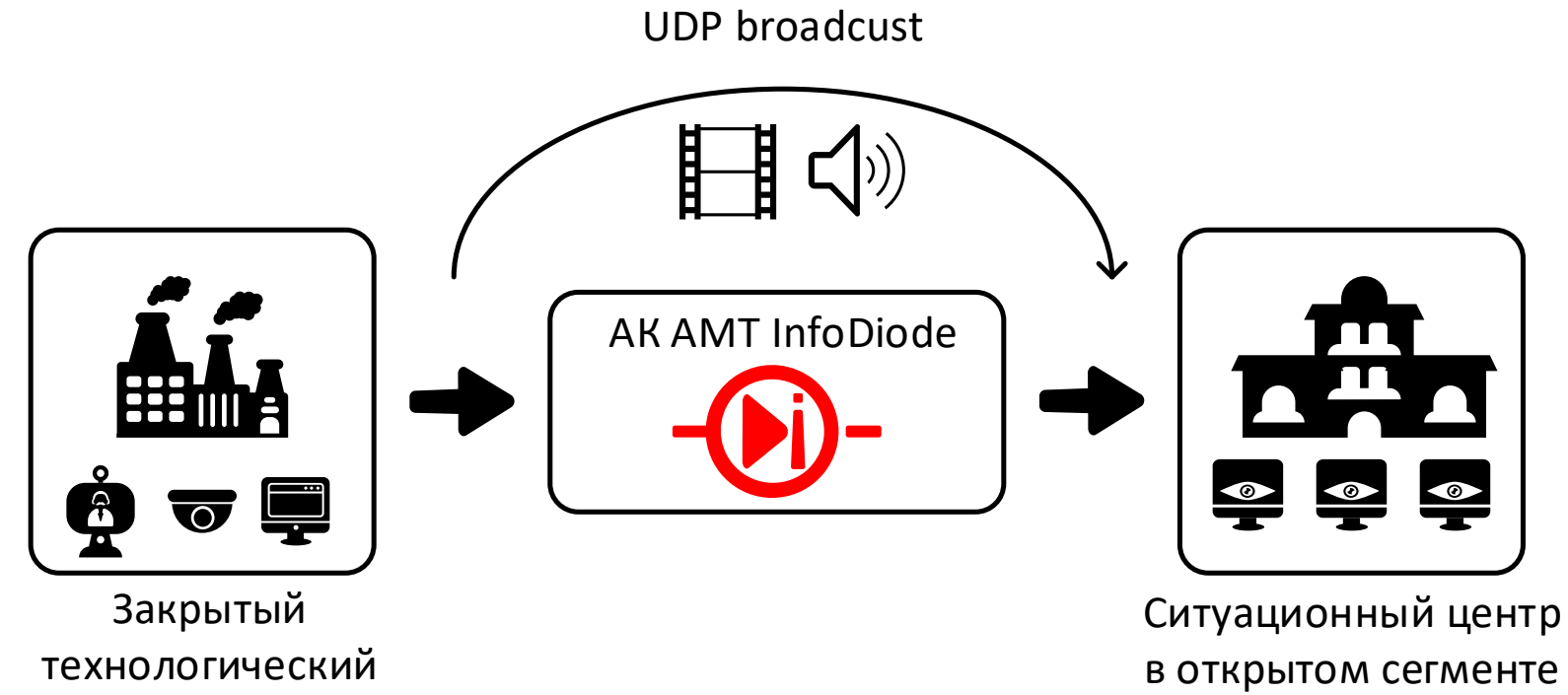
Прикладные варианты использования АК InfoDiode

Вариант 2. Передача событий технологической сети с использованием Syslog на внешнюю систему мониторинга. Логирование событий внутри технологического сегмента в централизованной системе мониторинга событий позволяет существенно снизить вероятность возникновения аварийных ситуаций и консолидировать все данные в едином ситуационном центре



Прикладные варианты использования АК InfoDiode

Вариант 3. Передача видео- и аудиотрафика из закрытого сегмента с использованием UDP, в том числе широковещательных видеопотоков. Часто бывает важно осуществлять удаленный видеомониторинг, получение сигналов от системы оповещения внутри закрытого технологического сегмента. Использование АК InfoDiode обеспечивает получение видео- и аудиопотоков, при этом гарантирует изоляцию закрытого сегмента



МИФ2
«Диоды» точно нельзя использовать для КИИ («диоды» нам не подходят)

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 промышленных предприятий для прямой кражи денег.

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

Последствия атак – существенны!

Системы, управляющие физическими объектами и процессами, несут бОльшие риски, чем системы сферы финансов и IT

- **Прерывание производственного процесса** (срыв контрактов, простой оборудования и сотрудников, падение биржевой стоимости акций)
- **Выход из строя дорогостоящего оборудования** (экономический ущерб, репутация)
- **Угроза жизни и здоровью людей** (заражение воды и воздуха, отключение систем жизнеобеспечения)
- **Промышленный шпионаж** (раскрытие коммерческой тайны, know-how, кража персональных данных)
- **Шантаж** (вирус-шифровальщик)

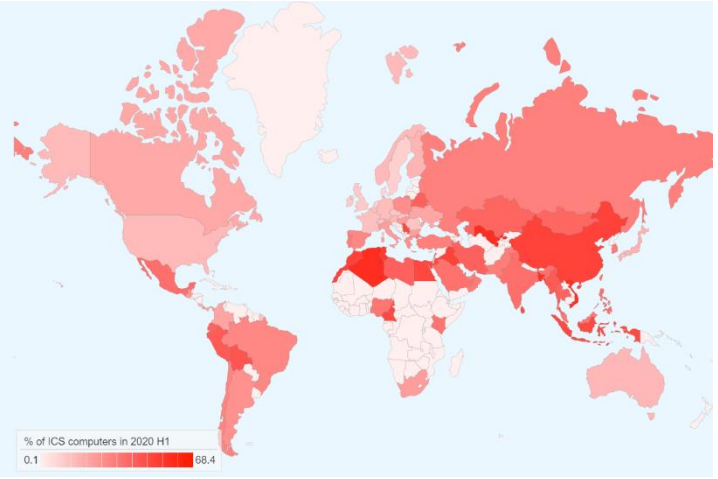
Конфиденциальность
Целостность
Доступность

Уязвимостей больше, поверхность атаки шире

- Ключевым для успеха большинства атак является установление канала взаимодействия с системой-«жертвой»
  - Уязвимость «нулевого дня»
  - Скорость распространения атаки vs скорость распространения защиты
  - Вектор атаки смещается на человеческий фактор
  - Двунаправленность важна уже на самом раннем этапе - при рекогносцировке цели. Многие техники для захвата систем также реализуются на основе двустороннего взаимодействия (RAT, phishing и т.д.)

- Общедоступность средств атаки

- Зарубежный опыт с некоторой задержкой транслируется в российские реалии
  - Регуляторы энергетического и транспортного секторов уже включили в свои документы применение продуктов класса диод



При применении устройств класса Diode

- Осуществить многие виды атак становится физически невозможным
- Вектор атаки смещается на физический периметр
- Для ряда отраслей в явном виде регламентируется их применение для разделения зон безопасности

Зарубежная нормативная база, регулирующая использование однонаправленных устройств

Международные стандарты

- Группа стандартов по управлению ИБ в системах промышленной автоматизации ANSI/ISA-62443
- Документы института SANS, в частности Tactical Data Diodes in Industrial Automation and Control Systems (https://www.sans.org/reading-room/whitepapers/firewalls/tactical-data-diodes-industrial-automation-control-systems-36057)
- Стандарт API Standard 1164. Pipeline SCADA Security

Зарубежная нормативная база, регулирующая использование однонаправленных устройств

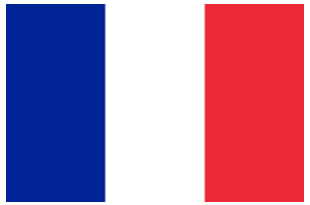
США

- «NIST SP800-82. Guide to Industrial Control Systems (ICS) Security»- NIST рекомендует использовать диоды как неотъемлемую часть защиты периметра и границ сети (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf)
- Документы NERC. NERC 1300 CIP-002 R3 Routable Protocols and Data Diode Devices (http://www.nerc.com/page.php?cid=3|22|354)
- Директива NSA and CISA Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems (Агентство национальной безопасности и Агентство кибербезопасности и защиты инфраструктуры) (https://us-cert.cisa.gov/ncas/alerts/aa20-205a)
- «Improving industrial control system cybersecurity with Defense-in-Depth strategies» - Документ The Department of Homeland Security (DHS) включил диоды и однонаправленные шлюзы в руководство «Совершенствование промышленной системы управления кибербезопасностью» (https://us-cert.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf)
- «Protecting drinking water utilities from cyber threats» - Рекомендации The Department of Energy (DOE) (https://www.osti.gov/biblio/1372266)
- «Cybersecurity programs for nuclear facilities» - Руководство Nuclear Regulatory Commission (NRC) (https://www.nrc.gov/docs/ML1703/ML17031A020.pdf)

AMT GROUP

Зарубежная нормативная база, регулирующая использование однонаправленных устройств

Франция



- «Cybersecurity for Industrial Control Systems» - Документ Национального агентства по безопасности информационных систем Франции («При подключении любой сети класса 3 (OT), такой как железнодорожные коммутационные системы, к сети более низкого класса или корпоративной сети (IT) допускаются к применению только однонаправленные шлюзы») (https://www.ssi.gouv.fr/uploads/2014/01/industrial_security_WG_Classification_Method.pdf)

Великобритания

- «Rail Cyber Security Guidance to Industry» – Документ департамента транспорта Великобритании рекомендует диоды к использованию на железнодорожном транспорте (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/732888/rail-cyber-security-guidance-to-industry.pdf)

Германия

- «Industrie 4.0. Security Guidelines» - Документ немецкой ассоциации машиностроения (VDMA) рекомендует диоды данных для защиты критических сегментов сети (https://www.vdmashop.de/refs/Leitf_I40_Security_En_LR_neu.pdf)
- «IT Security In Industrie 4.0» - документ Федерального министерство экономики… рекомендует диоды данных для защиты и изоляции «переходных» зон между критическим и сетями (OT) и ИТ-сетями (https://www.plattform-i40.de/PI40/Redaktion/EN/Downloads/Publikation/guideline-it-security-i40-action-fields.pdf?__blob=publicationFile&v=3

Зарубежная нормативная база, регулирующая использование однонаправленных устройств

Сингапур

- «Cybersecurity for Industrial Control Systems» - The Singapore Cybersecurity Agency (CSA) рекомендует использовать диоды данных и однонаправленные шлюзы в своих инструкциях для 11 секторов критической информационной инфраструктуры (CII) в целях повышения уровня их сетевой безопасности (https://www.csa.gov.sg/news/press-releases/press-statement-on-the-government-lifting-the-pause-on-new-ict-systems)
- «Annex Technology Roadmap» – Cybersecurity Infocomm Media Development Authority (IMDA) рекомендует использовать диоды данных на границе киберфизических систем на таких объектах, как атомные электростанции, производство электроэнергии/распределение электроэнергии, добыча нефти и газа, водоснабжение/сточные воды и производство (https://www.imda.gov.sg/-/media/Imda/Files/Industry-Development/Infrastructure/Technology/Technology-Roadmap/Annexes-A-3-Cyber-Security_Full-Report.pdf)

МИФ3

«Диоды» сложны в настройке и при внедрении, требуют постоянного обслуживания и сопровождения

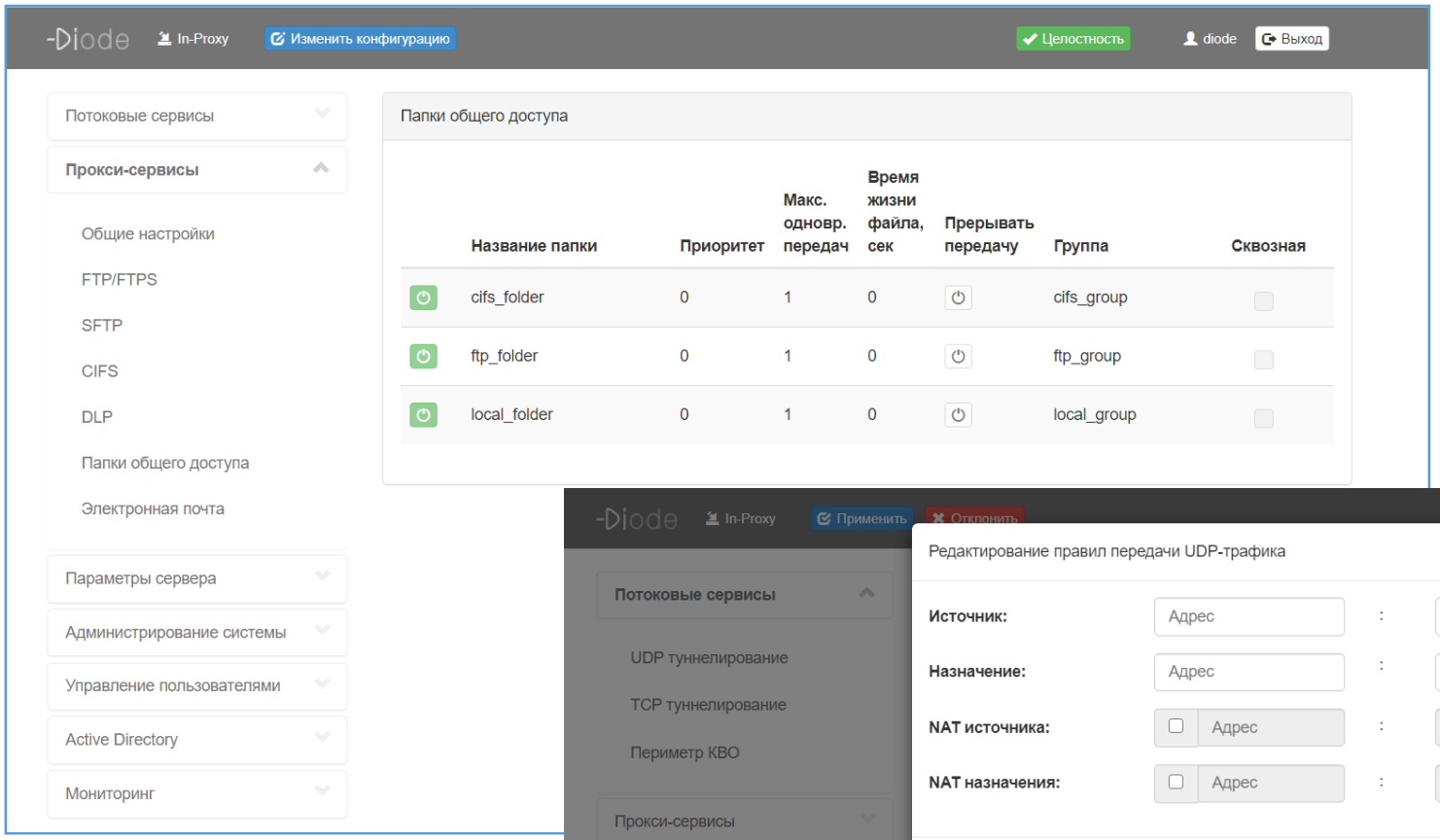
«Диод» - это устройство, практически не требующее настроек

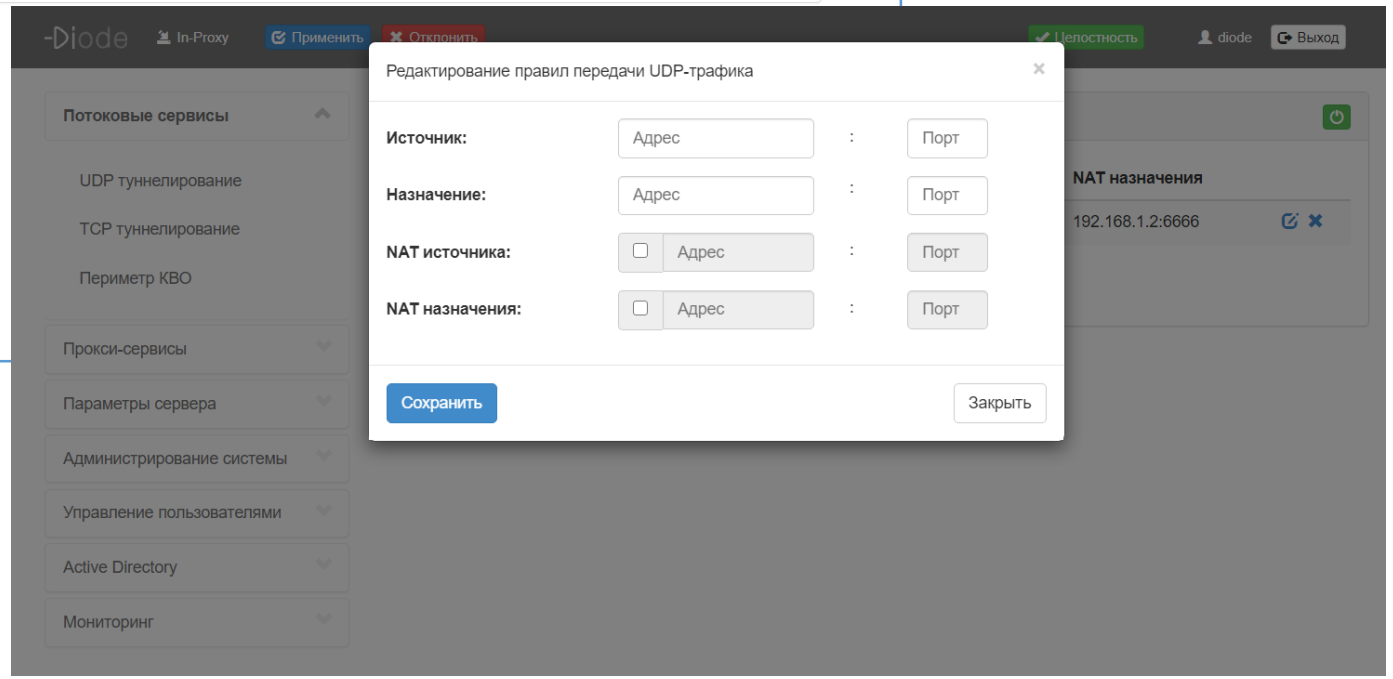
- АК InfoDiode достаточно подключить к коммутатору и настроить mirroring трафика стандартными средствами коммутатора

PLUG & PLAY

- АПК InfoDiode
  1. Приходит из стейджинга готовый, с установленным ПО
  2. Plug&Play по инструкции
  3. Работа как с домашним роутером

«Диод» - это устройство, практически не требующее настроек





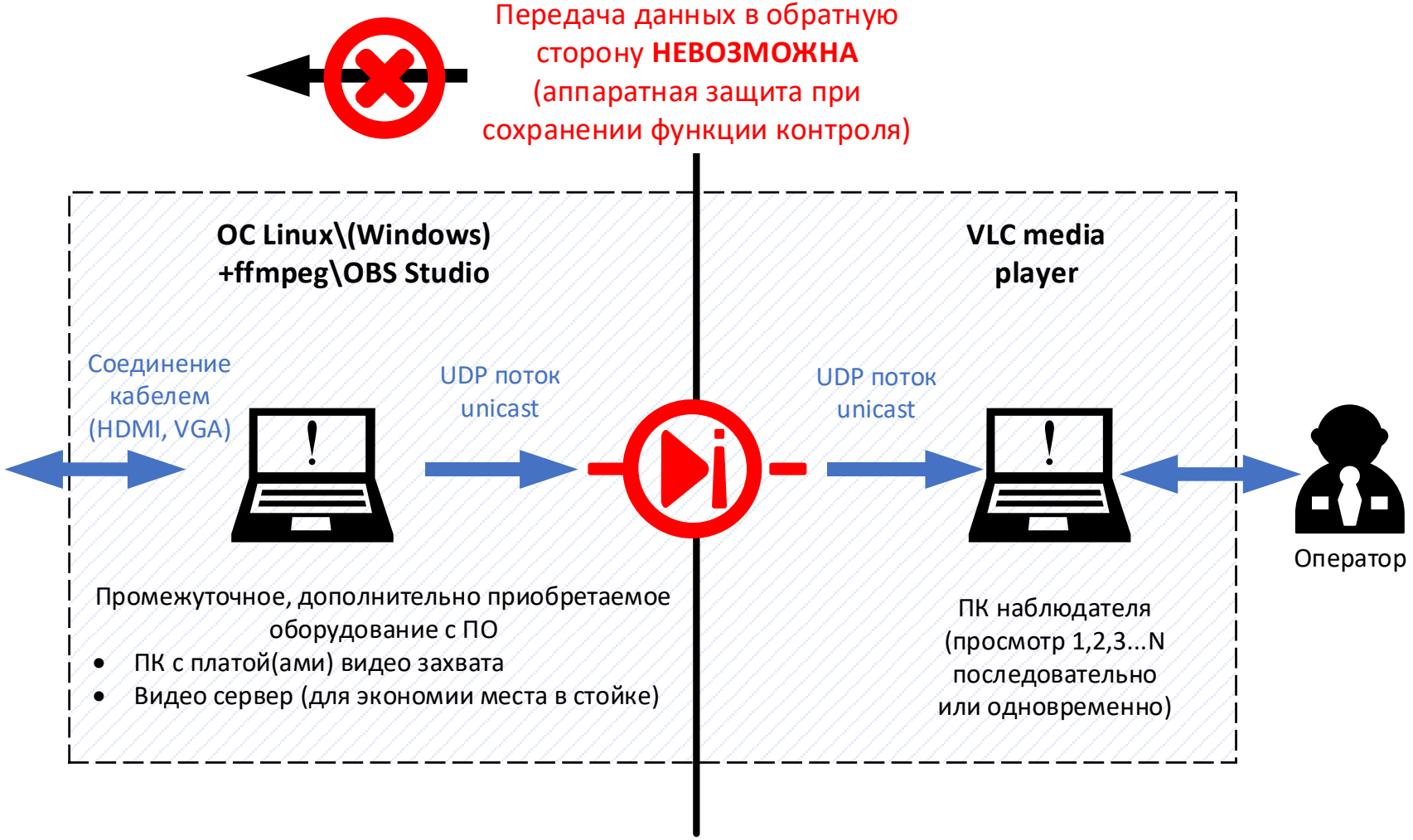
Web-консоль АПК InfoDiode

InfoDiode.ru

Стриминг рабочего стола из защищенного сегмента

ПК, для которых установка доп. ПО невозможна:

- Специфичная (нетиповая, устаревшая) ОС
- ПК категорирован



InfoDiode.ru

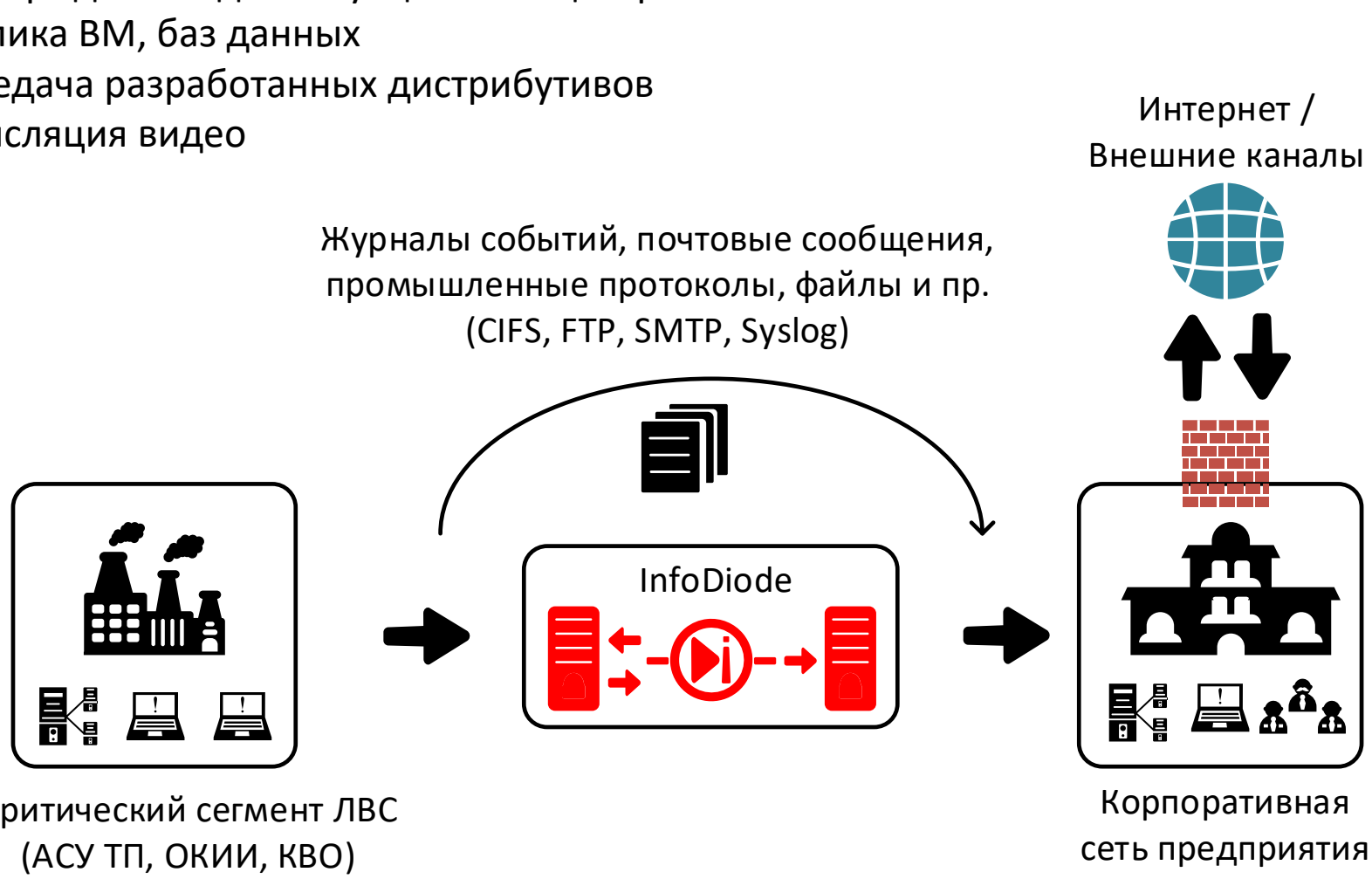
Прикладные варианты использования АПК InfoDiode

Вариант 1. Экспорт данных

В данном сценарий обеспечивается гарантия целостности передаваемых данных.

- Экспорт данных для ситуационных центров
- Реплика ВМ, баз данных
- Передача разработанных дистрибутивов
- Трансляция видео

и т.п.



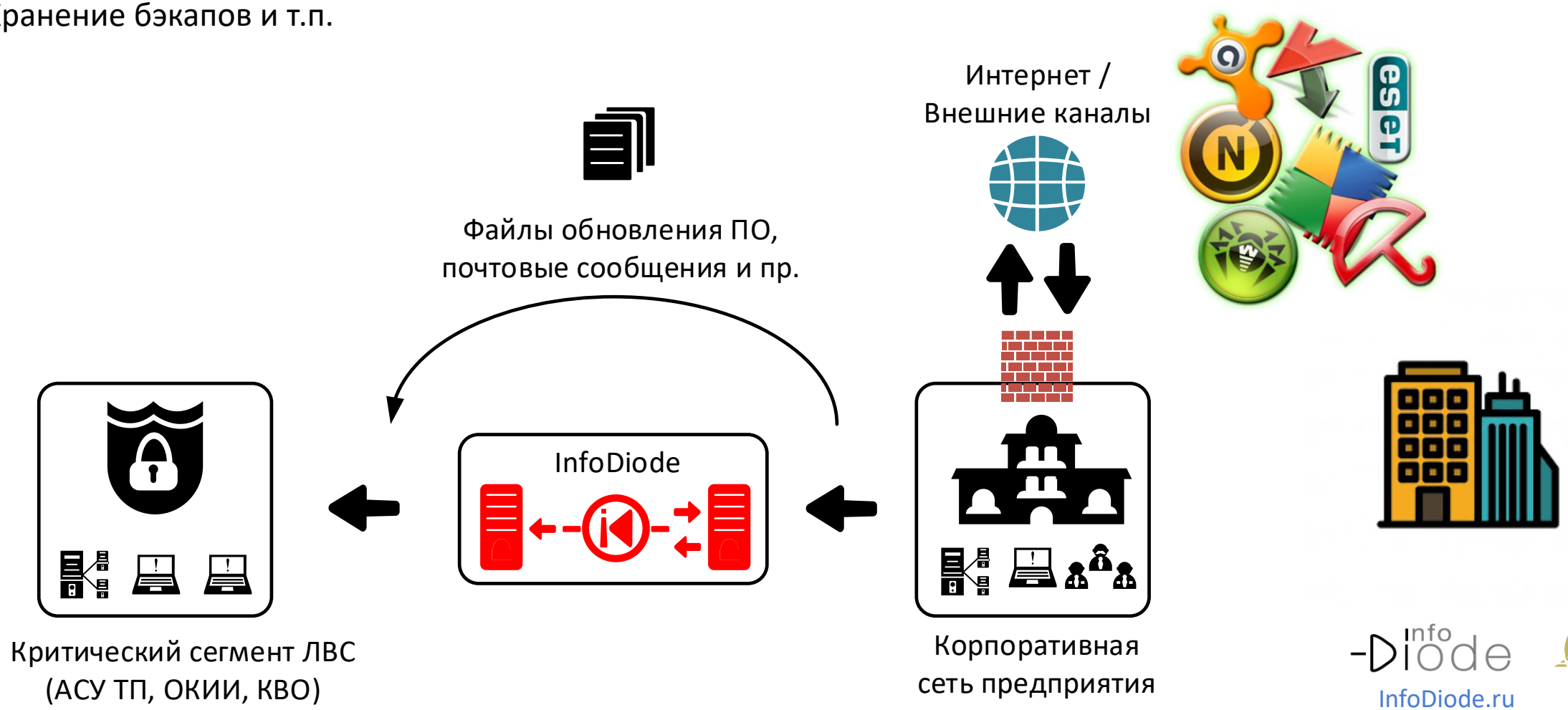
InfoDiode.ru

Прикладные варианты использования АПК InfoDiode

Вариант 2. Импорт данных

В данном сценарии обеспечивается гарантия конфиденциальности защищаемых данных.

- Загрузка обновлений
- Хранение бэкапов и т.п.



В чем заключается поддержка и сопровождение «диодов»

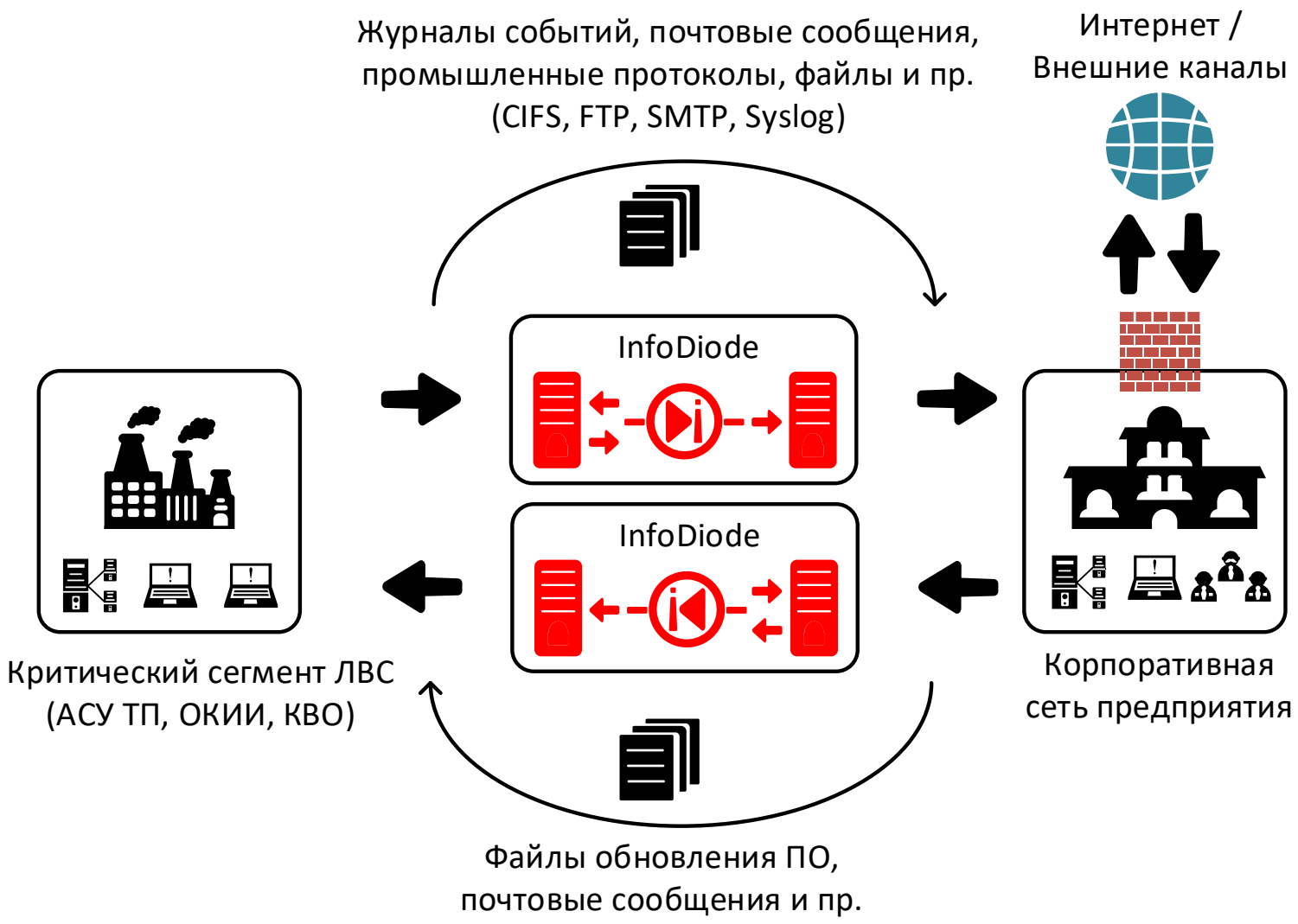
- АК InfoDiode – замена в случае выхода из строя

- АПК InfoDiode
  1. Периодические обновления прошивок (необязательно)
  2. Замена компонентов в случае выхода из строя
  3. Создание новых каналов передачи в интерфейсе web-консоли
  4. Мониторинг состояния по «модели здоровья» и контроль передачи данных

МИФ4

«Диоды» можно использовать только для организации однонаправленного взаимодействия

«Диоды» могут применяться в комплексных решениях, когда по одному контуру выполняется выгрузка данных, по второму - загрузка



- Либо изолированные, либо синхронизированные контуры
- Даже в случае TCP/IP контура через диод злоумышленнику в случае атаки тяжело изменить конфигурацию устройства и «открыть себе бэкдор»
- IPSec решения over UDP - https://tools.ietf.org/html/rfc3948

МИФ5

«Диоды» не имеют обратной связи, данные могут быть утеряны случайно, и мы об этом не узнаем

Правильнее говорить не о свойствах однонаправленной передачи, а о вероятности потери данных, а также о компенсирующих мерах

- Вероятность передать данные всегда меньше 100%, физические среды, в том числе, могут приводить к потере данных
- «Диоды» предполагают компенсирующие воздействия от потерь, характерных для однонаправленных протоколов (например, UDP)

Размер файла	Message Error Rate (MEP)	Среднее количество успешно переданных файлов до возникновения ошибки (1 / MEP)	Вероятность успешной передачи N файлов подряд, ≤		
			1	1 000	1 000 000
До 8КБ	1.2e-13	8 333 млрд	99.999999%	99.999999%	99.999987%
До 64КБ	4.4e-12	227 млрд	99.999999%	99.999999%	99.999567%
До 1МБ	2.6e-11	38 млрд	99.999999%	99.999997%	99.997407%
До 1ГБ	2.4e-8	41 млн	99.999997%	99.997640%	97.667746%
До 10ГБ	2.4e-7	4 млн	99.999976%	99.976406%	78.981053%
До 100ГБ	2.4e-6	416 тыс.	99.999764%	99.764318%	9.445838%

** Результаты рассчитаны в соответствии со статической моделью передачи данных по сети, с учетом округления.*

InfoDiode.ru

Состояние передачи можно и нужно контролировать на любом устройстве, тем более на границе сегмента КИИ

- В «диоде» реализована интеграция с SIEM, DLP, предусмотрена «модель здоровья», подготовлены OID для мониторинга средствами Zabbix

Severity (критичность)

Справочник уровней критичности основан на стандарте RFC 5424 The Syslog Protocol.

Обозначение	Числовое значение	Описание	Пример
EMERGENCY	0	Система приведена в неработоспособное состояние.	Невозможность загрузки конфигурации при старте системы.
ALERT	1	Требуется вмешательство управляющего персонала.	Недоступность интерфейса данных.
CRITICAL	2	Критическое состояние системы.	
ERROR	3	Ошибки при работе системы.	Ошибка при передаче файла на внешний сервер.
WARNING	4	Предупреждение при работе системы.	Факт начала применения новой конфигурации системы.
NOTICE	5	Важное информационное событие.	Успешная аутентификация пользователя в системе.
INFO	6	Информационное событие.	Запуск встроенного ftp-сервера.
DEBUG	7	Событие уровня отладки.	Начало передачи файла.

МИФ6
«Диоды» передают только один тип трафика

Следует рассматривать разные логические потоки. «Диод» может поддерживать несколько логических потоков

Виды трафика

- UDP - 900 Mbps (Syslog, VoIP, SNMP trap и др.)
- FTP/FTPS, CIFS, SMTP, SFTP
    - Приоритезация передачи данных и потоков
- Configuration/system backup
- Репликация виртуальных машин
- Репликация баз данных
- Передача журналов транзакций

Интеграции

- Syslog/SIEM интеграция
- NTP синхронизация
- Интеграция с AD
- Формирование файла мета-информации для его анализа средствами DLP (чтение), Syslog аудит
- SNMP v2c и v3, syslog

МИФ7
Firewall можно настроить так же, как и «диоды»

Политика нулевого доверия может быть эффективно построена именно на «диодах»

Software

- Уязвимость «нулевого дня» и др. уязвимости
- Скорость распространения атаки vs скорость распространения защиты
- Общедоступность средств атаки
- Особенности конфигурирования сами могут приводить к проблемам
- Открыто декларируются бэкдоры и workaround для многих Firewall

Hardware

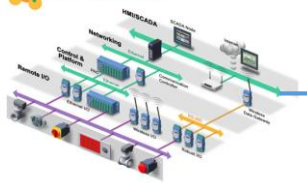
- Работают на аппаратных принципах – физически изолируют сеть
- Невозможно взломать, взлом ПО на АПК не приводит к нарушению функции безопасности
- Аппаратные решения вообще не имеют софта и неуязвимы для стороннего софта
- Удаленное конфигурирование в целях «взлома» невозможно

МИФ8
«Диоды» прежде всего ориентированы на передачу файлов

Промышленные протоколы через «диод» - уже реальность

kepware®

Modbus



kepware®

ДОВЕРЕННЫЙ СЕГМЕНТ
Управление оборудованием

НЕДОВЕРЕННЫЙ СЕГМЕНТ
Ситуационные центры, диспетчерские, подрядчики, SOC, NOC

Новые устройства АМТ-ГРУП – «пилот» на стенде

- **Компактный, упрощает встраивание в разнородную инфраструктуру – 1U**
  - Виртуальные среды, серверы заказчика, докеры, операционные системы
- **Обеспечивает поддержку промышленных протоколов (MQTT, Modbus, OPC UA…)**
- **Улучшает нефункциональные показатели текущего продукта, решение «все в одном»**
- **Потенциально предусматривает исполнение в различных форм-факторах**
- **Учитывает перспективный сегмент IoT устройств**

InfoDiode.ru

Рынок решений. Решения от АМТ-ГРУП

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. По причинам отсутствия сертификатов соответствия от регуляторов

АМТ-ГРУП

Предлагает комплексные решения:

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

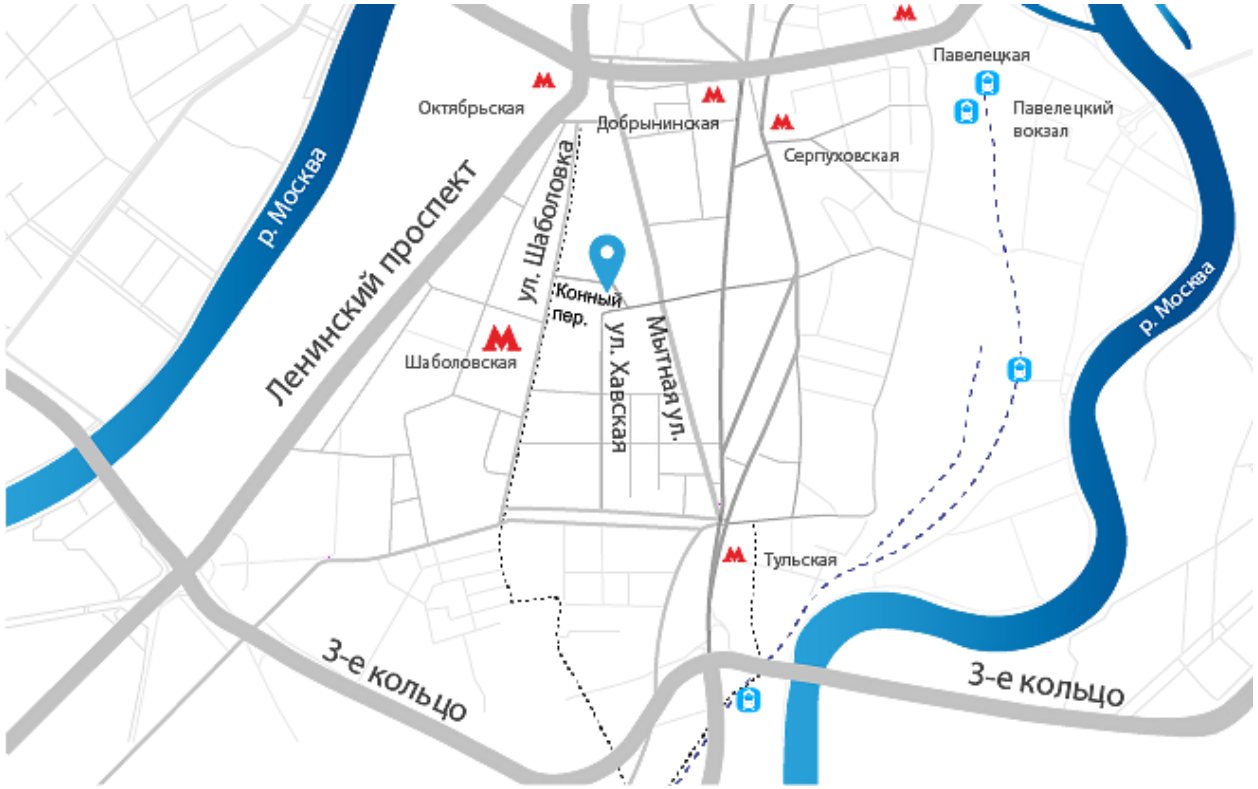
Лицензионная политика и комплексные решения АМТ-ГРУП

- **Состав спецификации**
  - Оборудование – комплект, производство АМТ-ГРУП
  - Лицензии – полнофункциональные и бессрочные
  - Техническая поддержка оборудования
  - Компоненты для формирования ЗИП
  - Работы по внедрению и интеграции

- **Техническая поддержка – варианты**
  - 8x5 или 24x7
  - Комбинация – ПО 24x7, замена оборудования 8x5
  - ЗИП для клиента или только ремонт оборудования
  - Выезд технического специалиста для ремонта

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!