



Однонаправленная
передача данных

-InfoDiode

Защита
объектов КИИ и ОПО

Экспорт
видеопотоков в
ситуационный
центр

Сегментирование
сетей АСУ ТП

28.08.2025

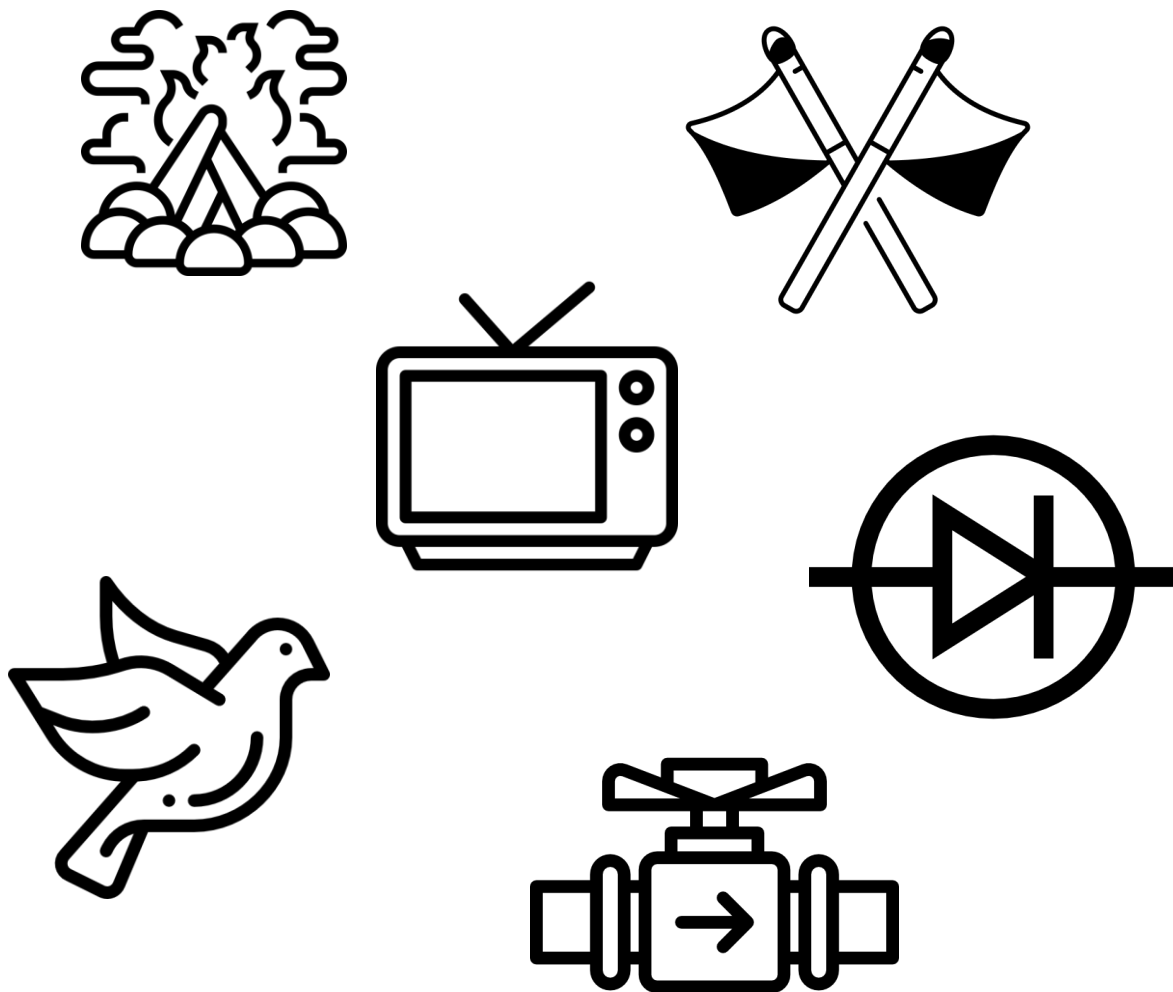
От сигнальных костров до физически однонаправленных шлюзов: как InfoDiode защищает нашу критическую инфраструктуру

Половинко Вячеслав, АМТ-ГРУП



ОДНОНАПРАВЛЕННАЯ ПЕРЕДАЧА: ФОБИИ И ЗАБЛУЖДЕНИЯ

Однонаправленный обмен – хорошо забытое старое



Системы однонаправленной передачи данных существовали и существуют для решения большого класса задач

1. Сигнализация
2. Снижение нагрузки на каналы
3. Обеспечение безопасности источника
4. Исключение компрометации информации в источнике

Сегодня в большом количестве случаев соединение (двусторонняя связь) с источником устанавливается только для того, чтобы получить данные в одном направлении из источника

Физически однонаправленный обмен - один из ключевых аспектов безопасной передачи данных

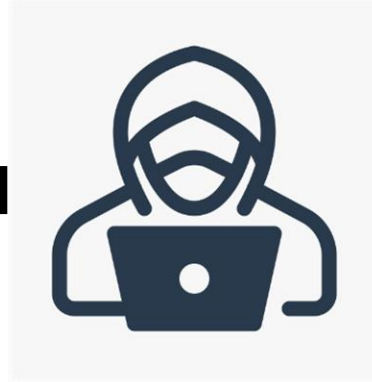
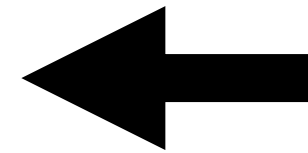
Технологическая информация

Диагностическая информация и события безопасности

Файлы и прикладные данные

SPAN

- Объекты удалены
- Объекты критичны
- Объекты автономны
- Объекты хранят значимые данные
- Объекты ограничено защищены от удаленного вектора атак
- Объекты являются частью централизованной системы контроля



- Как мы
сопрягаем сети?
Безопасно?

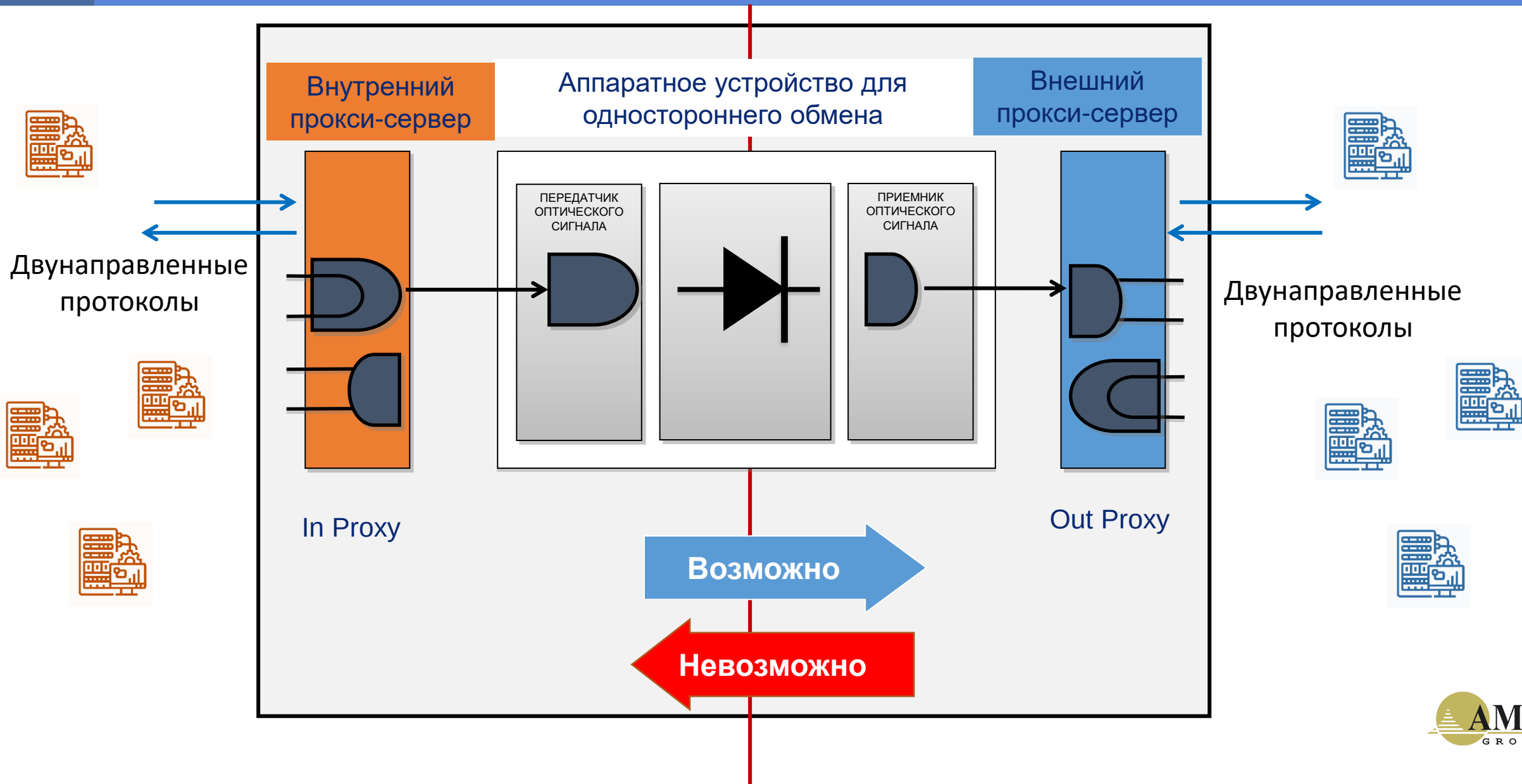


ЧТО ТАКОЕ ДИОДЫ ДАННЫХ
(INFODIODE) И КАК ОНИ ВЫГЛЯДЯТ

- **Однонаправленный шлюз (InfoDiode)** – устройство, обеспечивающее передачу файловой и потоковой информации в одном направлении и не позволяющее передачу в обратном
 - Однонаправленность передачи гарантируется **аппаратными решениями**
 - Применяется для соединения разных сегментов сети и используется в области защиты информации
 - **Ключевые признаки**
 - Однонаправленность и воздушный зазор гарантируются физическим принципом – **НЕ программным**
 - «Диоды» в двунаправленный режим **НЕ переключаются**
 - Просто открыть порты, настроить ACL в «диодах и «обмен пойдет» - НЕЛЬЗЯ
 - Современные решения этого класса позволяют передавать данные практически всех видов протоколов

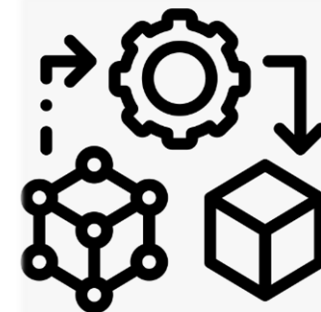


Решения InfoDiode позволяют передавать данные двунаправленных протоколов, но не пропускают сигнал к источнику



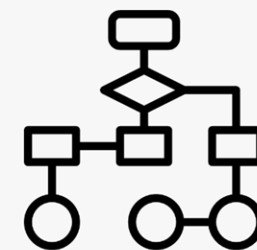
1. InfoDiode – это еще один МСЭ?

- **НЕТ**



2. Какой класс атак существует на решения «диод данных», если в нем реализована функция безопасности «на уровне физики»?

- **ОТКАЗ В ОБСЛУЖИВАНИИ,
НО ПРЕОДОЛЕТЬ ФИЗИЧЕСКИЙ ДИОД НЕВОЗМОЖНО**



3. InfoDiode может передавать двунаправленные протоколы, если связь симплексная?

- **СОЕДИНЕНИЕ ПО ПРОТОКОЛАМ НЕ УСТАНОВЛИВАЕТСЯ
ЧЕРЕЗ ДИОД, НО ДАННЫЕ ПРОТОКОЛОВ ПЕРЕДАЮТСЯ**



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

АК INFODIODE



Характеристики

Базовое аппаратное решение для монтажа на DIN-рейку или Desktop вариант.

MINI



Характеристики

Базовое аппаратное решение для монтажа в стойку.

RACK single



Характеристики

Аппаратное решение для монтажа в стойку (два «диода» в одном).

RACK - double

АПК InfoDiode позволяет соответствовать лучшим практикам по защите периметра КИИ, передавать файловый, промышленный и иной трафик



АПК INFODIODE PRO

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

Диод снаружи

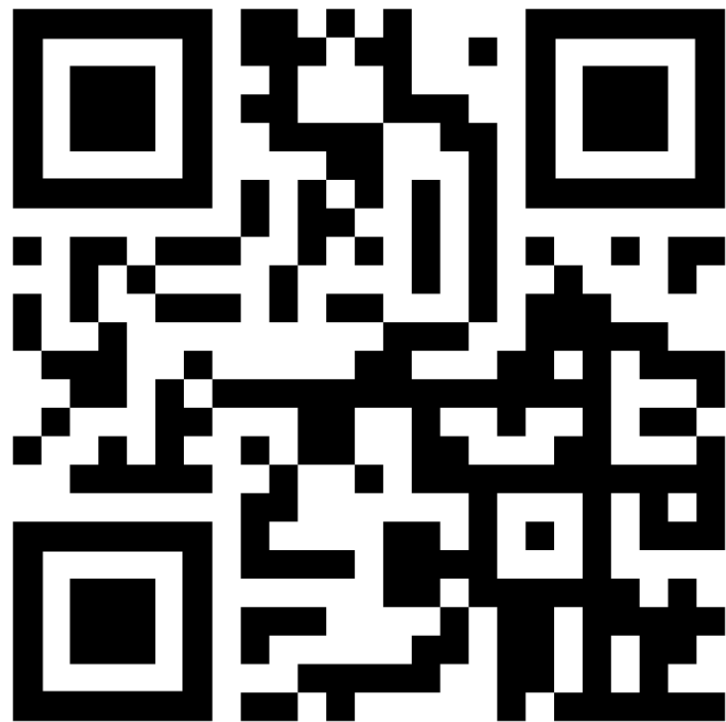


АПК INFODIODE SMART

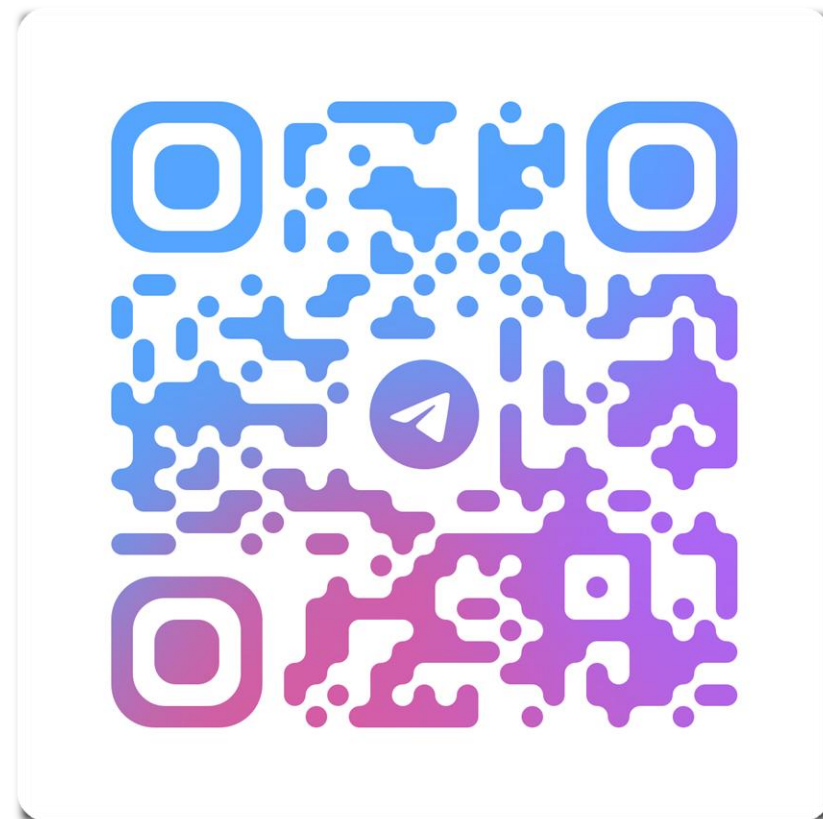
Базовый вариант
InProxy, OutProxy сервер
«диод внутри»
Форм фактор - 1U

Диод внутри

<https://infodiode.ru/>



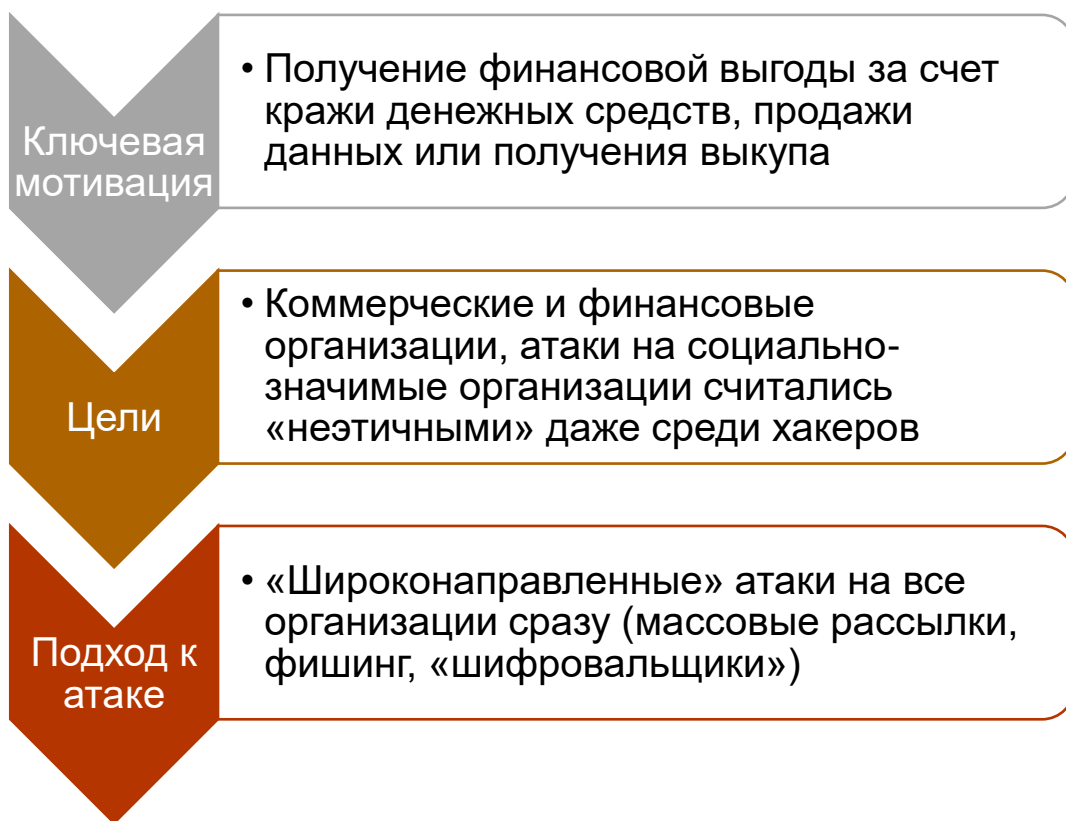
Telegram-канал InfoDiode



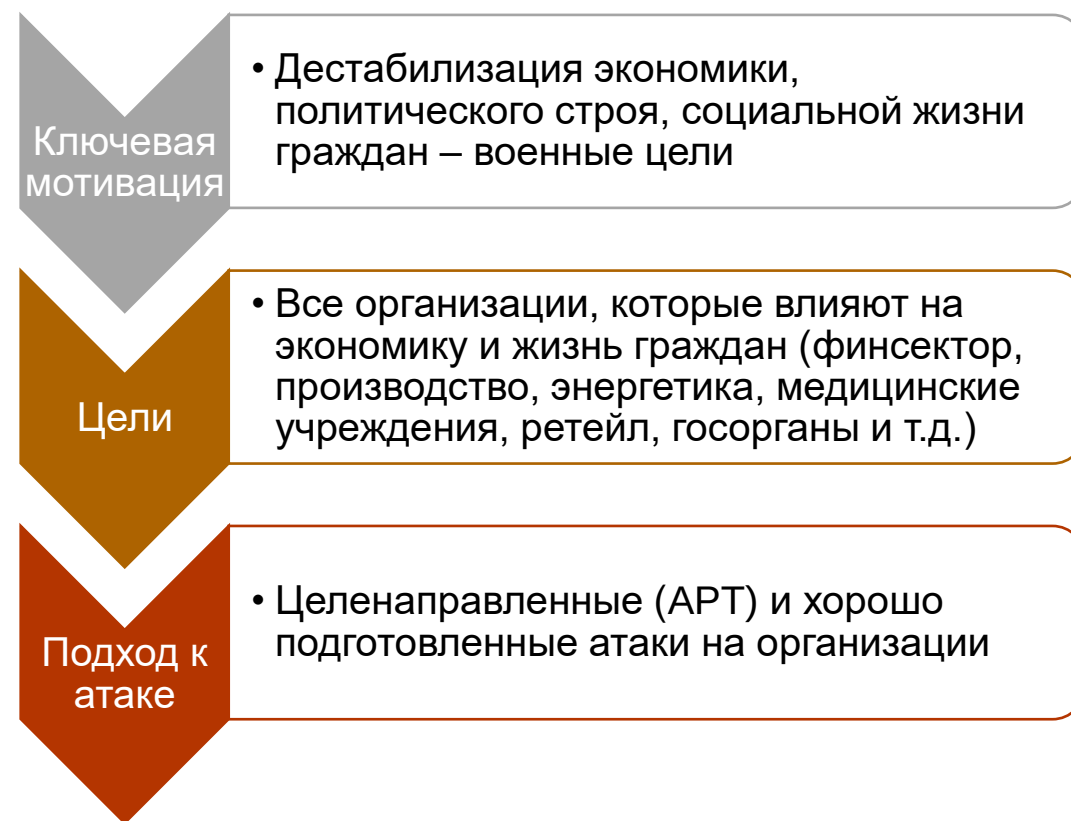


КТО НАШ НАРУШИТЕЛЬ
И КАК С НИМ БОРОТЬСЯ?

Хакеры ранее



Хакеры сегодня



Классические СЗИ не всегда обеспечивают достаточный уровень защиты





Тип нарушителя	Случайно	С умыслом	Особенности нарушителя	Особенности атаки	Сложность защиты
Внутренний	Неплохо помогают стандартные СЗИ	Требуются высоко-профессиональные команды и серьезные компенсирующие меры	Имеет идентификаторы (лицо, видео, носители, СКУД, паспорт) - оставляет хороший цифровой и физический след	Понятен объем - разные виды деструктивных воздействий (не только кибер-, но и реальный ущерб)	Помощь служб, сотрудников, граждан
Внешний	Неплохо помогают стандартные СЗИ	Требуются высоко-профессиональные команды и серьезные компенсирующие меры	Максимально анонимен, значительные ресурсы	Только кибер ущерб	Помощь очень ограничена
Внешний с внутренним	Неплохо помогают стандартные СЗИ	Требуются высоко-профессиональные команды и серьезные компенсирующие меры	"+"	"+"	"+"

Какие компетенции у нарушителя?

- **Обладают базовыми возможностями по реализации угроз**

Реализовывают только известные угрозы, направленные на известные уязвимости с использованием общедоступных инструментов.

- Авторизованные пользователи, бывшие работники, хакеры, поставщики ПО, АПК, обеспечивающих систем, обеспечивающий персонал (администрация, охрана, уборщики и т.д.).

- **Обладают базовыми повышенными возможностями по реализации угроз**

Реализовывают угрозы, в том числе направленные на неизвестные уязвимости с использованием специально созданных для этого инструментов или свободно распространяемых в сети Интернет, и не имеют возможностей реализации угроз на физически изолированные сегменты систем и сетей.

- Системные администраторы и администраторы ИБ, лица, привлекаемые для установки, настройки, испытаний, ПНР, поставщики вычислительных услуг и услуг связи, конкурирующие организации, преступные группы.

- **Обладают средними возможностями по реализации угроз**

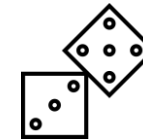
Реализовывают угрозы, в том числе на выявленные ими неизвестные уязвимости с использованием самостоятельно разработанных для этого инструментов, но не имеют возможностей реализации угроз на физически изолированные сегменты систем и сетей.

- Разработчики ПО и АПК, террористические или экстремистские группировки.

- **Обладают высокими возможностями по реализации угроз**

Имеют практически неограниченные возможности по реализации угроз, в том числе с использованием недеklarированных возможностей и программных и программно-аппаратных закладок, встроенных в компоненты систем и сетей.

- Специальные службы иностранных государств.



Случайно



Умысел



Тип нарушителя	Случайно	С умыслом	Особенности нарушителя	Особенности атаки	Сложность защиты
Внутренний	Неплохо помогают стандартные СЗИ  -Diode^{Info}	Требуются высоко-профессиональные команды и серьезные компенсирующие меры  -Diode^{Info}	Имеет идентификаторы (лицо, видео, носители, СКУД, паспорт) - оставляет хороший цифровой и физический след	Понятен объем - разные виды деструктивных воздействий (не только кибер-, но и реальный ущерб)	Помощь служб, сотрудников, граждан
Внешний	Неплохо помогают стандартные СЗИ  -Diode^{Info}	Требуются высоко-профессиональные команды и серьезные компенсирующие меры  -Diode^{Info}	Максимально анонимен, значительные ресурсы	Только киберущерб	Помощь очень ограничена
Внешний с внутренним	Неплохо помогают стандартные СЗИ  -Diode^{Info}	Требуются высоко-профессиональные команды и серьезные компенсирующие меры  -Diode^{Info}	"+"	"+"	"+"

Защита критических сетевых сегментов требует пересмотра в реалиях сегодняшнего дня

Многофункциональные межсетевые экраны уровня сети

Программное ограничение соединений по таблице правил. Возможны ошибки в конфигурации, вероятно наличие уязвимостей «нулевого дня».

Может включать в себя функции других СЗИ (антивирус, DLP, криптошлюз). Возможно взаимодействие по двусторонним протоколам.

Классические межсетевые экраны

Программное ограничение соединений по таблице правил. Возможны ошибки в конфигурации, вероятно наличие уязвимостей «нулевого дня». Требуется дополнительных СЗИ для нейтрализации иных угроз.

Возможно взаимодействие по двусторонним протоколам.

Программные «диоды данных»

Программное ограничение передачи данных в обратном направлении. Функция безопасности зависит от программной конфигурации. Уязвимости «нулевого дня» могут нарушить функцию безопасности. Передача двустороннего трафика возможна в определенных режимах.



InfoDiode (аппаратные «диоды данных»)

Гарантированное (конструктивное) ограничение передачи данных в обратном направлении. Функция безопасности не зависит от программной конфигурации. Уязвимости «нулевого дня» не позволяют нарушить функцию безопасности. Передача двустороннего трафика невозможна, только проксирование в одностороннем режиме.

«Воздушный зазор»

Гарантированная изоляция сетевого сегмента.

Невозможно никакое взаимодействие с изолированным сегментом, что может быть недопустимо для нормального функционирования предприятий и организаций. Большие накладные расходы на обмен информацией.

Защита сетевого сегмента

- Полностью исключить внешнего злоумышленника с удаленным вектором атаки
- Сфокусироваться на мерах в отношении внутреннего нарушителя и эффективнее расследовать инциденты
- Сэкономить средства (и Capex и Opex)
- Максимально усложнить жизнь внутреннему нарушителю в части успешности кибератак, связанных с удаленным управлением, выводом данных
- Буквально и точно выполнить требования по сегментации сети ТСПД, КСПД





ПОЧЕМУ ИМЕННО ДИОДЫ ДАННЫХ (INFODIODE)

1. Физически однонаправленный канал

- Если объект изолирован «диодом» – доступа к нему нет физически
- Если «диоды» установлены в две стороны – двунаправленный канал все равно НЕ создается. В случае инцидента есть возможность сохранить канал связи для мониторинга.

2. Разрыв протоколов

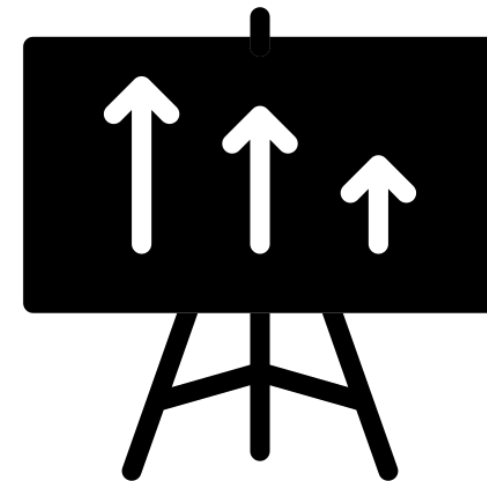
- Никакой протокол «как есть» не передается через «диод»

3. Ограниченное количество доступных для взаимодействия протоколов

- Для обмена используется только определенный набор «интерфейсных протоколов»

4. Простота администрирования и более низкая (в сравнении с иными СЗИ) стоимость владения

- Функция безопасности НЕ в программном обеспечении

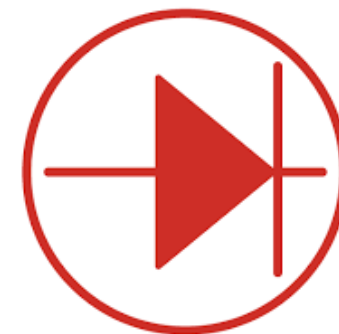


Почему именно диоды данных (InfoDiode) для промышленности и энергетики (и не только)



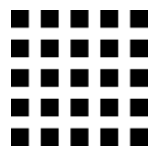
1. Особый интерес для злоумышленников

- Величина и значимость точек влияния



2. Имеют централизованную структуру сбора данных

- Потенциал атаки из централизованных структур сбора данных



3. Значительное количество объектов внутри одного объекта

- Сложность контроля за всей инфраструктурой и СЗИ



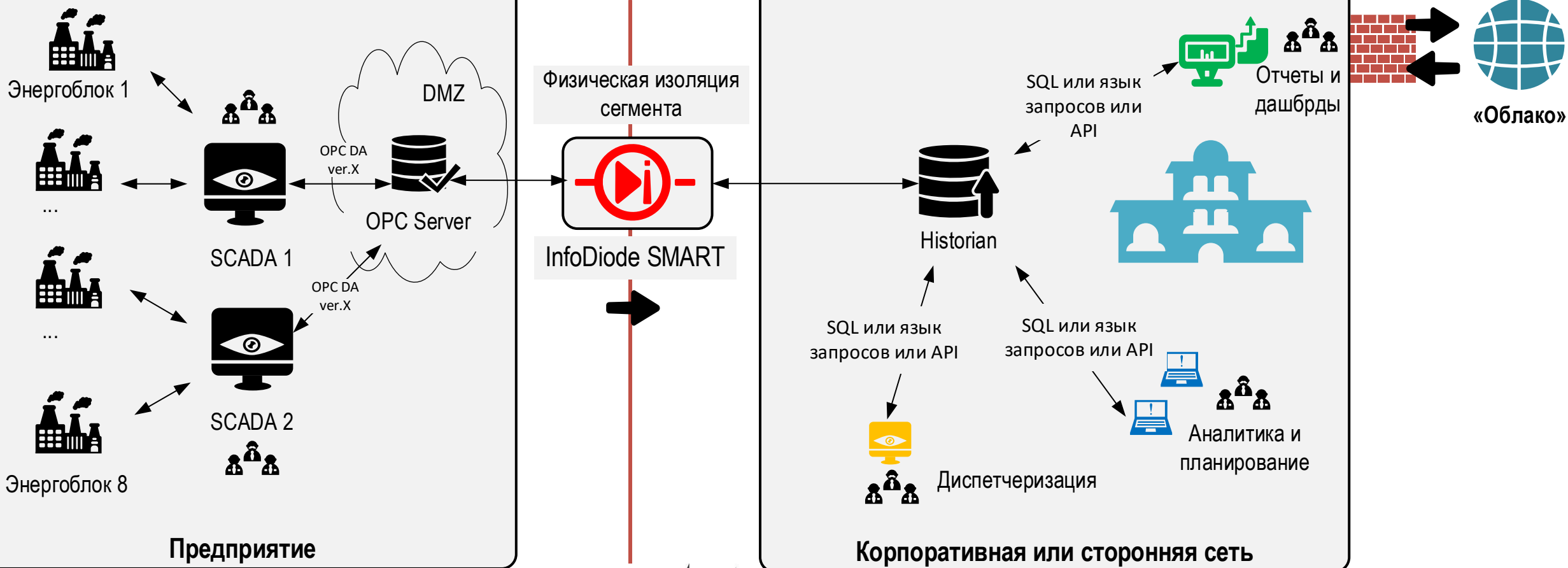
4. Высокая и возрастающая степень цифровой трансформации и модернизации

- Рост количества сервисов и систем, непосредственно завязанных на данные технологических сегментов



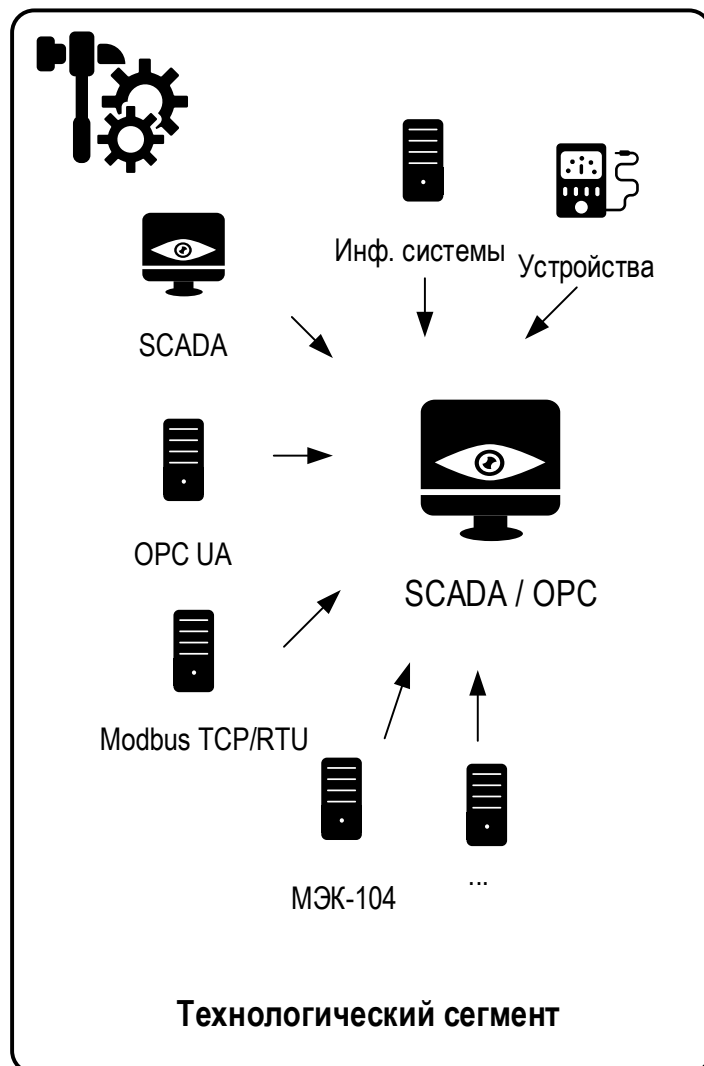
ГОТОВЫЕ РЕШЕНИЯ И КЕЙСЫ
INFODIODE

ERG первыми в СНГ реализовали проект по разделению промышленного и корпоративного сегментов с использованием решений InfoDiode SMART

**ERG****Недоверенный/внешний сегмент**

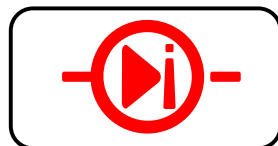
Решения для MES и Historian – InfoDiode и Indusoft (внедрение MES в условиях изоляции АСУ ТП сегмента)

MasterSCADA

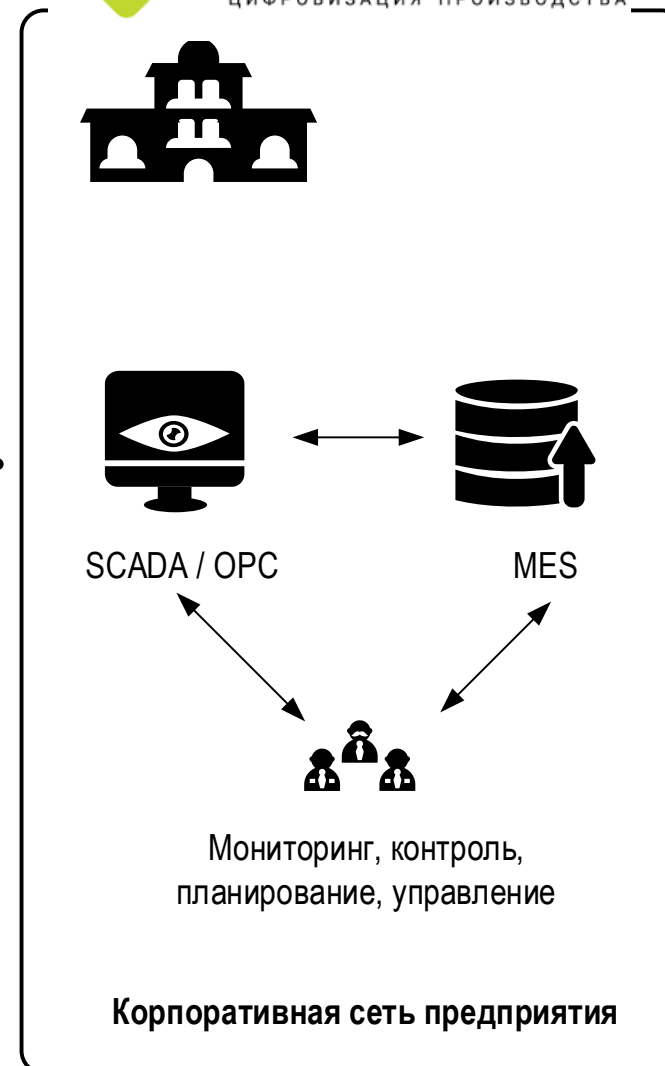


Теги/данные промышленных
протоколов

InfoDiode SMART

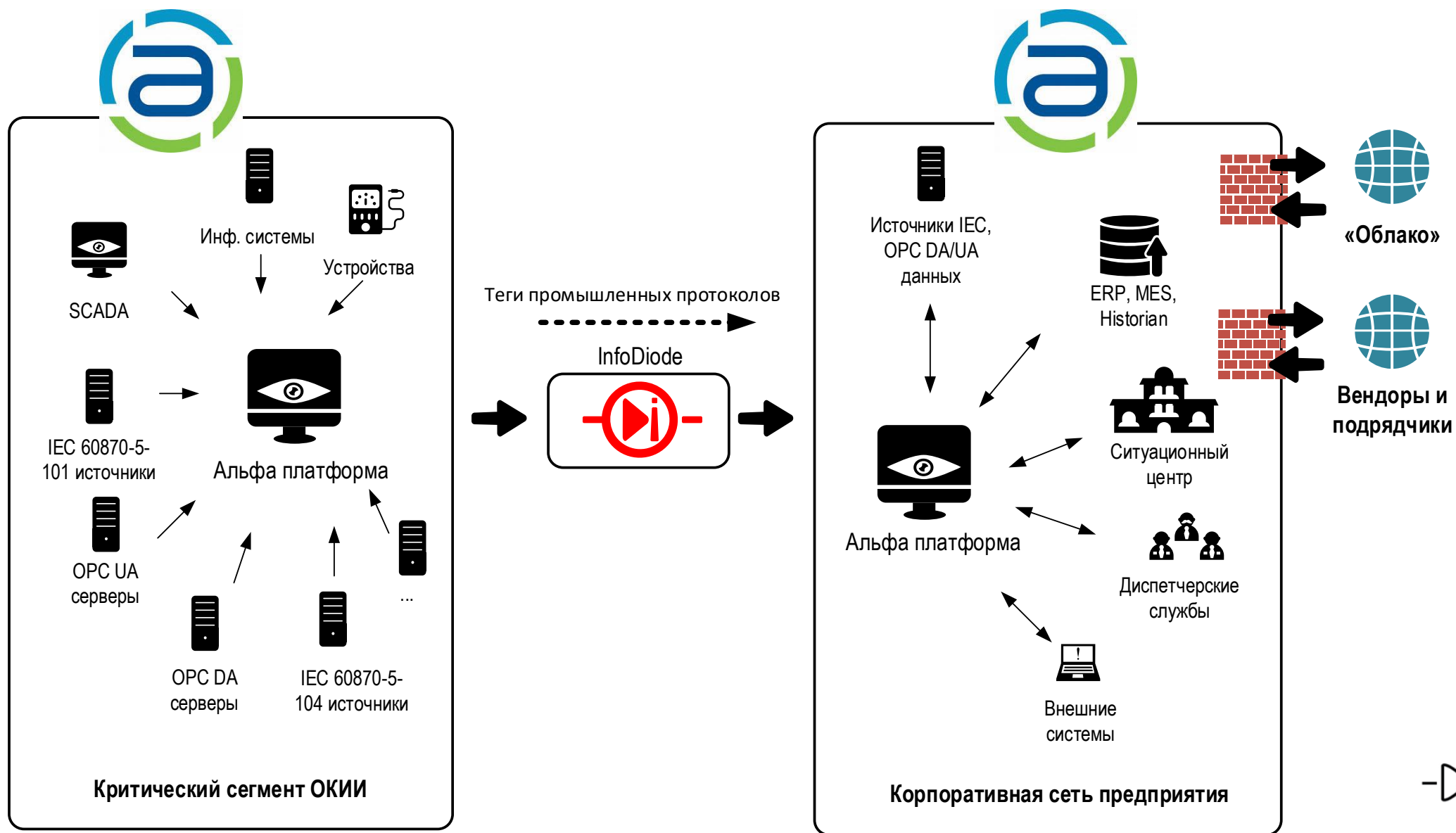


ИНДАСОФТ ЦИФРОВИЗАЦИЯ ПРОИЗВОДСТВА

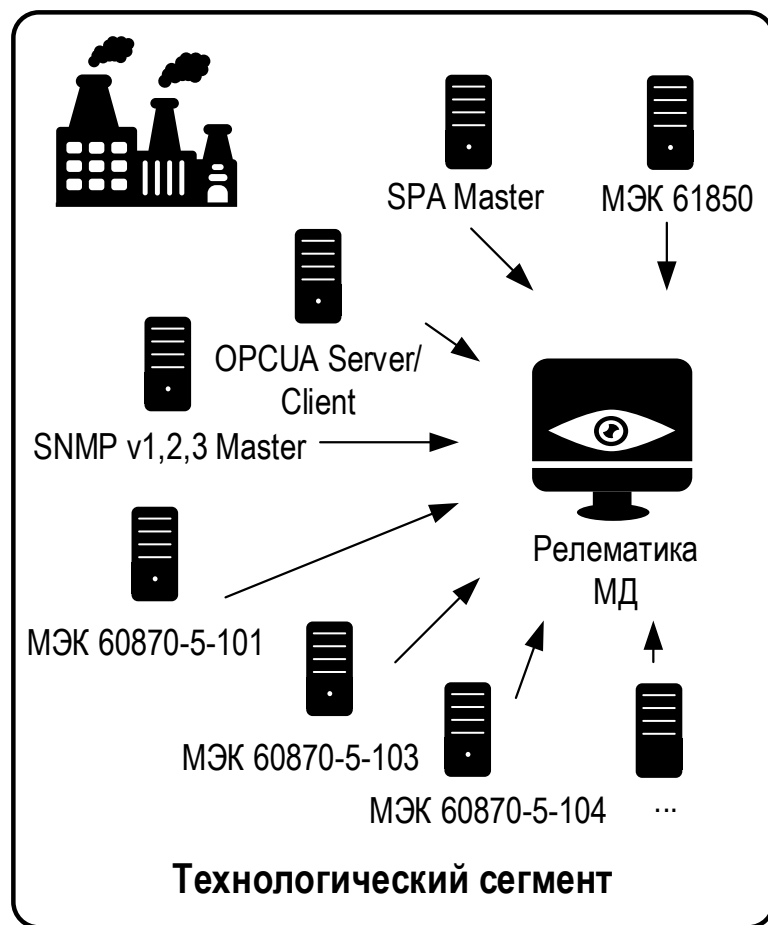




Решения для сбора данных из АСУ ТП – Альфа платформа (сбор данных с самых разных источников АСУ ТП)



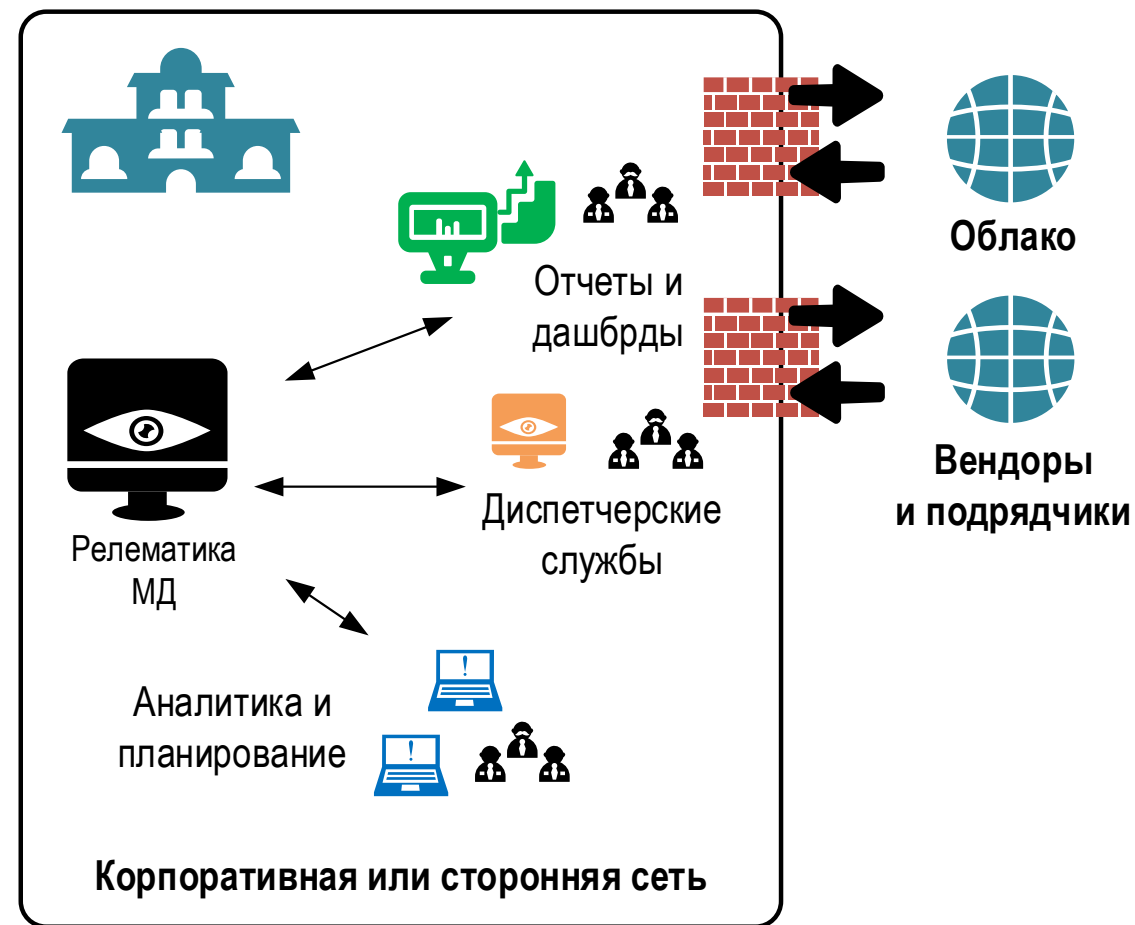
Решения для объектов энергетики – Релематика (передача данных в ЦУС)



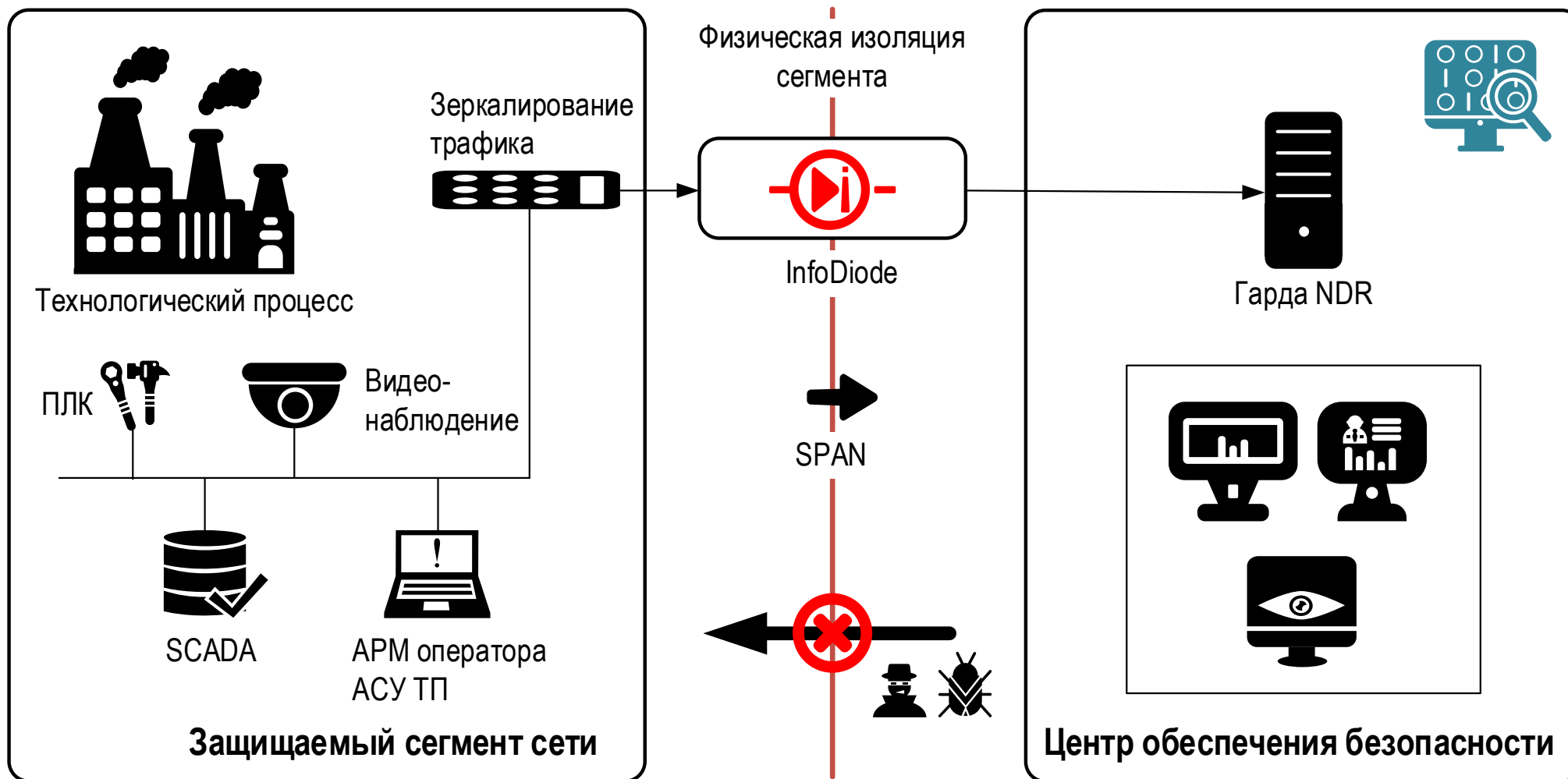
Физическая изоляция
сегмента



АПК InfoDiode SMART



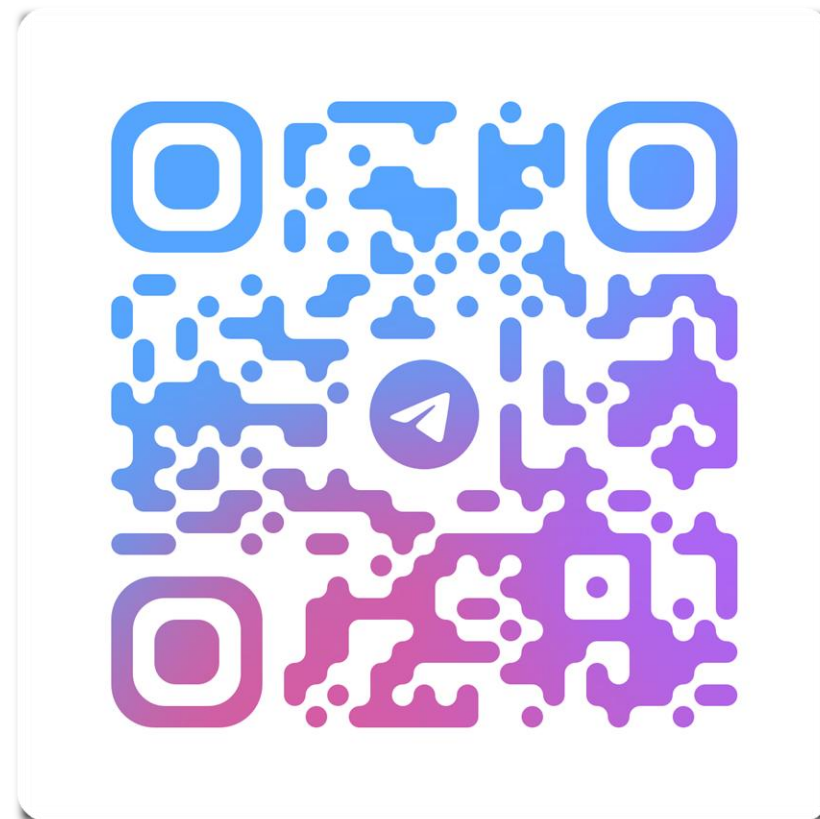
Решения класса NDR, IDS и Deception– InfoDiode (имитация инфраструктуры, обнаружение аномалий в рамках COB)



<https://infodiode.ru/>



Telegram-канал InfoDiode



СПАСИБО ЗА ВНИМАНИЕ!