29.07.2022

АМТ-ГРУП

InfoDiode как решение по защите сетевого периметра в условиях переходного периода и ограничений на применение ранее используемых СЗИ

1. Реалии в части защиты сетевого периметра

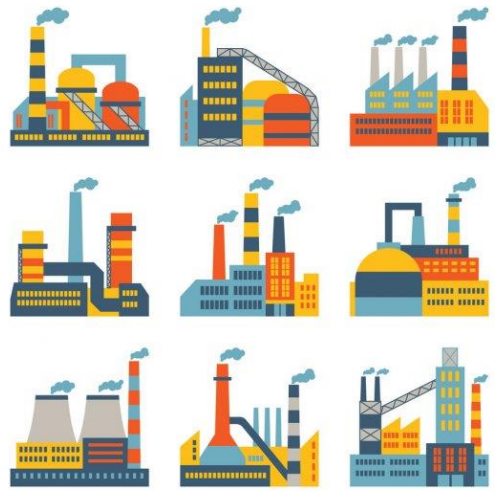
2. Что такое «диоды» и какие они бывают

3. Как «диоды» могут помочь в решении возникших проблем

Реалии сегодняшнего дня в части защиты сетевого периметра

Организации в текущих реалиях испытывают серьезные проблемы в обеспечении защиты своего сетевого периметра (7 факторов)

1. Зарубежные вендоры СЗИ уходят/ушли с рынка (Fortigate, Infoblox, Cisco, IBM и др.).
   Сетевой периметр стал менее защищен
2. Остающимся зарубежным вендорам СЗИ сложнее пройти путь сертификации (требования к более детальному документированию аппаратных платформ и т.п.).
   Аналоги организационно быстро не внедрить
3. Российские вендоры не всегда могут предложить подходящие решения. Например, промышленные файерволы или комплексные решения по безопасности.
   Выбор отечественных СЗИ ограничен
4. Поставка и поддержка программно-аппаратных и аппаратных решений в сегменте АСУТП ограничены (Siemens, GE, Honeywell, Bently Nevada и др.).
   Данные по-прежнему нужны за пределами технологического сегмента
5. Нормативная база дополнительно делает акцент на защиту КИИ в текущих условиях.
   Регулятор менее лояльно относится к сдвигу сроков реализации мер защиты
6. Срок принятия решений маленький, не учитывает потребности в бюджетировании.
   Нужны быстрые меры, гарантирующие защиту сетевого периметра
7. Угрозы и злоумышленники никуда не делись.
   Риски для КИИ только выросли



Инфраструктура СЗИ по некоторым направлениям строится фактически с нуля

Что такое «диоды» и какие они бывают

Устройство однонаправленной передачи данных функционирует на физическом уровне

- **Однонаправленный шлюз** – 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

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

InfoDiode.ru

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
АК InfoDiode, rack module	2 АК 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

InfoDiode.ru

Все решения «диод» можно условно разделить на два класса

Аппаратные «диоды»

Плюсы

- Недорого
  Решают базовые задачи изоляции
- Plug&Play
- Не требуют сопровождения службы эксплуатации

Минусы

- Не имеют IP, MAC адреса
- Требуют коммутации «порт-порт»
- Передать даже асинхронный TCP/IP трафик не получится

Аппаратно-программные «диоды»

Плюсы

- Передают асинхронный и даже синхронный TCP/IP трафик
- Несколько видов прикладного трафика одновременно
- Полноценное СЗИ (NAT, списки доступа, порты, контроль изменений конфигурации, контроль доступа)
- Интеграции: SIEM, SNMP, AD, Syslog, NTP…

Минусы

- Могут занимать 3 или более RU
- Требуют специалиста в эксплуатации с базовыми навыками
- Требуют периодического (хотя и редкого) обновления ПО

Соблюдается принцип однонаправленности **физический сигнал только в одну сторону**

АМТ-ГРУП предоставляет полную линейку решений класса «диод» для защиты КИИ и АСУ ТП и ИТ инфраструктуры

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

Количество отраслей применения InfoDiode постоянно увеличивается

InfoDiode используется в:

- ТЭК
- Платежные системы
- Финансовые организации
- Силовые ведомства
- Производство
- Транспортные компании
- Энергетика
- др.

Банк России

Министерство обороны Российской Федерации

Росэнергоатом
Электроэнергетический дивизион Росатома

Росфинмониторинг

Транснефть

РЖД

КРЭТ

РусГидро

sollers

ЦИК

Евросибэнерго

Генеральная прокуратура РФ

ФСТЭК

Министерство здравоохранения РФ

НСПК
Национальная система платежных карт

Ростелеком

ERG

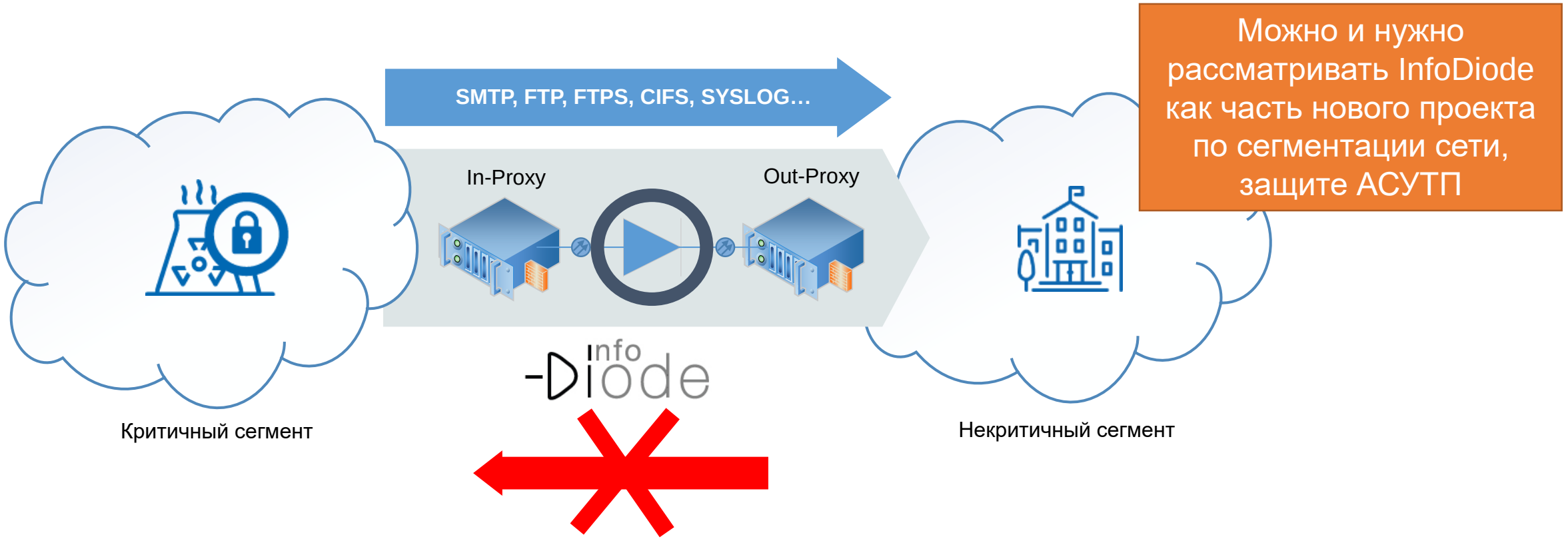
AMT GROUP

Как «диоды» могут помочь в решении возникших проблем

1. Зарубежные вендоры СЗИ уходят/ушли с рынка
Сетевой периметр стал менее защищен

Нет поддержки, нет возможности масштабировать решение по защите с применяемыми СЗИ

Начинаются новые проекты по защите сетевого периметра



Можно и нужно рассматривать InfoDiode как часть нового проекта по сегментации сети, защите АСУТП

2. Остающимся зарубежным вендорам СЗИ сложнее пройти путь сертификации **Аналоги организационно быстро не внедрить**

Сертификация УД4 может занимать > 1 года. Иностранным вендорам требуется специфицировать и аппаратную платформу, передавать исх. коды на каждый контроллер в составе платформы

Нужны сертифицированные СЗИ, чтобы закрыть требования регулятора по защите периметра

<u>Сертификаты на соответствия ЕАЭС</u>

Соответствие требованиям:

«О безопасности низковольтного оборудования»

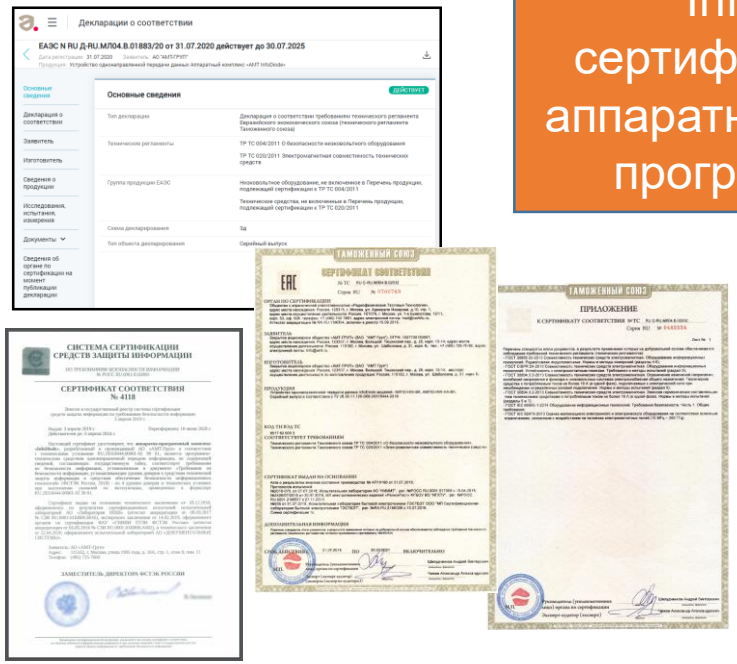
«Электромагнитная совместимость технических средств».

ЕАЭС N RU Д-RU.МЛ04.В.01883/20

<u>Сертификаты ФСТЭК УД4</u>

УД4. Сертификат № 4118

Соответствие ТУ RU.29318444.00001-02 90 01.



InfoDiode имеет сертификаты ФСТЭК и на аппаратную и на аппаратно-программную линейку

InfoDiode.ru

3. Российские вендоры не всегда могут предложить подходящие решения
Выбор отечественных СЗИ ограничен

Несмотря на то, что пока еще нет готовых решений, нужно выбирать те продукты, которые достаточно активно развиваются и могут служить основой новой экосистемы СЗИ решений

Нужны продукты, которые хорошо встроятся в текущую инфраструктуру и поддержат внедрение отечественных СЗИ

2 направления по СЗИ

InfoDiode имеет заявления о совместимости и реальные кейсы внедрений с большинством крупных решений отечественных СЗИ

Сценарии применения

- Передача БД и их инкрементов
- Обновление антивирусов
- Передача файловой информации
- Обмен близкий к синхронному (сервисы)
- Обновление WSUS
- Syslog и мониторинг
- Данные для агентов IDS\IPS
- Данные для SIEM
- Sandbox и карантины

Заявления о совместимости с вендорами СЗИ

- Kaspersky
- Positive
- Infowatch
- СайберЛимфа
- Квазар
- Др.

InfoDiode.ru

4. Поставка и поддержка решений в сегменте АСУТП ограничены. **Данные по-прежнему нужны за пределами технологического сегмента.**

Нет возможности приобретать промышленные Firewall от производителей, нет возможностей докупать интеграционные модули SCADA, требуется переходить на другие типы контроллеров

Задача по передаче данных остается крайне актуальной. Нужны решения которые смогут обеспечить закрытие требований ИБ и передать пром. Протоколы из АСУТП

2 направления по АСУТП

InfoDiode имеет проверенные сценарии с крупными SCADA системами, системами Historian и OPC серверами

Сценарии применения

Передача пром. протоколов:

- Modbus TCP
- S7
- Omron FINS
- Mitsubishi SLMP
- IEC 61850 MMS
- IEC 60870-5-101/103/104
- OPC DA/HDA (на Windows)
- OPC UA
- Счетчики: Меркурий, Теплоком, Энергомера и др.

Проверка совместимости с уже имеющимися вендорами и отечественными решениями

- Kepware
- WinCC
- GE Proficy (ETL)
- Wonderware (Aveva)
- System1
- MasterSCADA
- КОТМИ
- др.

InfoDiode.ru

Продукты InfoDiode совместимы со многими решениями и СЗИ и АСУТП и ИТ

Kaspersky
Private Security
Network

InfoDiode.ru

5. Нормативная база дополнительно делает акцент на защиту КИИ в текущих условиях **Регулятор менее лояльно относится к сдвигу сроков реализации мер защиты**

Требования ФСТЭК по категорированию и построению системы защиты согласно требованиям 239 приказа и др. норм. документов еще более актуальны

Следует выбирать те средства, которые не только решат вопросы в части требований регулятора, но и обеспечат реальную (не «бумажную») защиту сетевого сегмента

Приказ ФСТЭК N 239 от 25 декабря 2017 г. и N 31 от 14 марта 2014 г.

Обозначение и номер меры	Меры обеспечения безопасности значимого объекта
ЗИС.2	Защита периметра информационной (автоматизированной) системы
ЗИС.3	Эшелонированная защита информационной (автоматизированной) системы
ЗИС.4	Сегментирование информационной (автоматизированной) системы
ЗИС.6	Управление сетевыми потоками
ЗИС.8	Сокрытие архитектуры и конфигурации информационн
ЗИС.18	Блокировка доступа к сайтам или типам сайтов, запрещ
ЗИС.31	Защита от скрытых каналов передачи информации
ЗИС.34	Защита от угроз отказа в обслуживании (DOS, DDOS-ат
ЗИС.35	Управление сетевыми соединениями

Приказ ФСТЭК N 17 от 11 февраля 2013 г. и N 21 от 18.02.2013 г.

Обозначение и номер меры	Меры обеспечения безопасности значимого объекта
ЗИС.16	Выявление, анализ и блокирование в информационной системе скрытых каналов передачи информации в обход реализованных мер защиты информации или внутри разрешенных сетевых протоколов
ЗИС.17	Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы
ЗИС.22	Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы
ЗИС.23	Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами

InfoDiode позволяет уменьшить вложения в защиту АСУТП, так как он физически изолирует один сегмент от другого и упрощает применение доп. мер

InfoDiode закрывает целый ряд мер приказов ФСТЭК

InfoDiode.ru

6. Срок принятия решений маленький, не учитывает потребности в бюджетировании **Нужны быстрые меры, гарантирующие защиту сетевого периметра**

Некоторые решения требуют длительной перестройки всей системы СУИБ. Переход на нового вендора Firewall не всегда может быть быстрым и безболезненным, а защита нужна уже сейчас

Следует обеспечить оперативную и фактическую защиту периметра как можно быстрее, сохранив сетевую связность

Мы готовы помочь, если требуется сопроводить и проектирование и пилотирование

- Документ-опросник - собрать первичные требования
- Презентация\демонстрация\вебинар, необходимые документы по продукту
- «Пилот» (в лаборатории АМТ или с передачей оборудования на объект)
- Защита решения
- Подготовка технических требований

InfoDiode производится на заказ в течение 1 месяца на территории РФ

InfoDiode может быть использован как временное решение, до построения всей СУИБ и стать впоследствии ее частью

InfoDiode.ru

7. Угрозы и злоумышленники никуда не делись
Риски для КИИ только выросли

- **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**

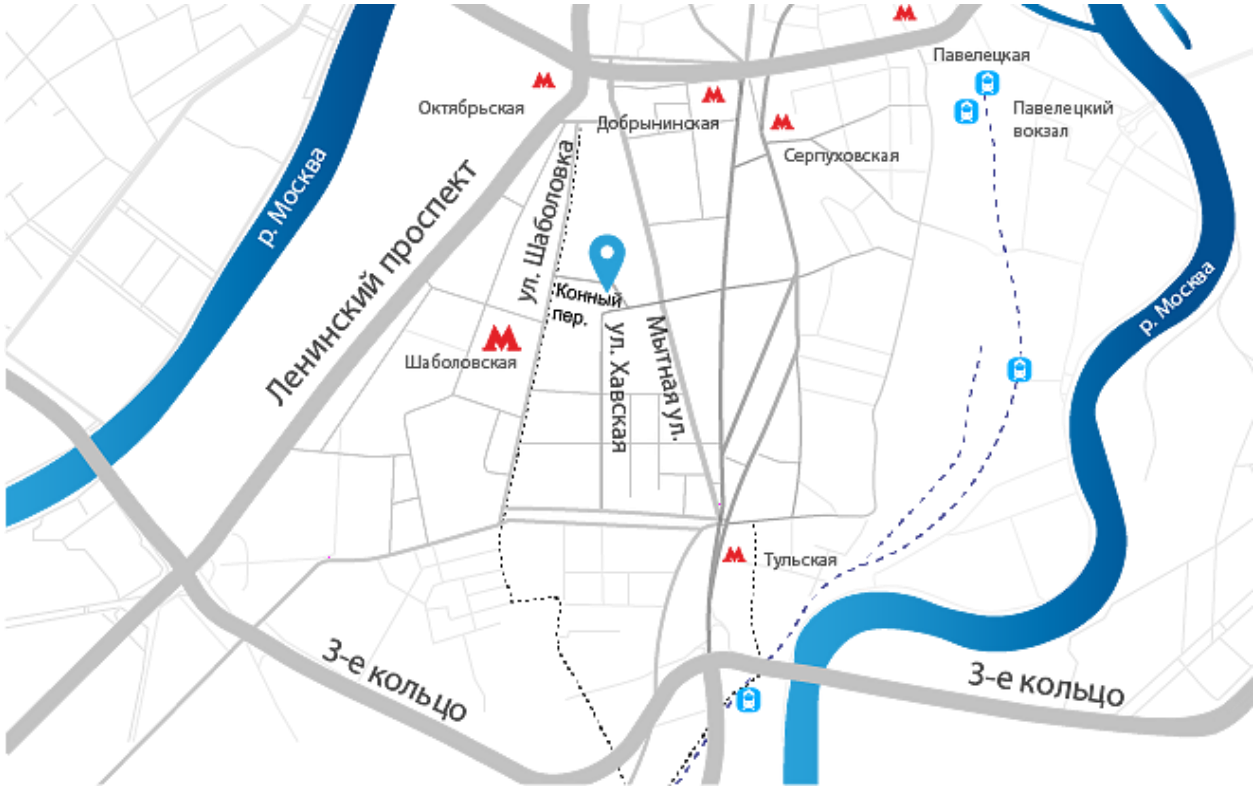
Ранее существующие факторы

- **Деятельность недружественных государств**
- **Деятельность сочувствующих групп**
- **Закладки в ПО, которые фактически делаются чуть ли не официально**

Новые факторы

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!

InfoDiode.ru