



РЕАЛИЗАЦИЯ МЕХАНИЗМОВ БЕЗОПАСНОСТИ В СФЕРЕ
ОБЩЕСТВЕННОГО ТРАНСПОРТА КАК ПРОТИВОДЕЙСТВИЕ
АКТУАЛЬНЫМ УГРОЗАМ КИБЕРБЕЗОПАСНОСТИ

ПОЧЕМУ ТРАНСПОРТ ПОДВЕРЖЕН АРТ-АТАКАМ?

1

Государственный сектор является основной целью атак злоумышленников после 2022 г.*

*По результатам отчетности Positive Technologies и InfoWatch

2

Дестабилизация общественного транспорта оказывает деструктивное воздействие на Российскую Федерацию

КЛАССИФИКАЦИЯ КИБЕРУГРОЗ И ТЕНДЕНЦИИ ПРОТИВОДЕЙСТВИЯ

до 2022

Использование ВПО,
эксплуатация
уязвимостей*

*По результатам отчетности Positive
Technologies и InfoWatch

Выполнение требований
регуляторов как
обеспечение базиса
безопасности

2022-2024

Количественное и
качественное увеличение
числа DDoS-атак. Цель
атак-проведение самих
атак

Импортозамещение,
внедрение действительных
и рабочих практик
AppSec/DevSecOps

ПРОГНОЗ НА 2025

Рост числа APT-атак,
использование
технологий ИИ и
deepfake при
реализации атак

Использование ИИ,
технологий блокчейна,
переход к осознанному
(доверенному)
импортозамещению

КАК ПРОТИВОСТОЯТЬ НОВЫМ КИБЕРУГРОЗАМ?

ТЕХНИЧЕСКИЕ

1 внедрение принципов SSDLC

2 NGFW

3 EDR

ОРГАНИЗАЦИОННЫЕ

1 повышение осведомленности персонала

2 разработка планов и проведение учений по восстановлению работоспособности и операционной надежности систем

КАК МЫ ОБЕСПЕЧИВАЕМ БЕЗОПАСНОСТЬ ТРАНСПОРТНЫХ ПРОЕКТОВ

Полное соответствие требованиям регуляторов
(КИИ, ГИС, ПДн, PCI DSS)

Взаимодействие с Национальным
координационным центром по
компьютерным инцидентам

Отработка учений по противодействию **DDoS-**
атакам

Использование современных классов средств
защиты информации (**NGFW, endpoint-**
protection и т.д.)

Регулярное проведение анализов
защищенности и тестирований на
проникновение

Использование анти-фрод системы и
принципов безопасной разработки в
соответствии с ГОСТ Р **56939-2024**

СПАСИБО ЗА ВНИМАНИЕ!



Разоренов Степан Андреевич
Ведущий специалист Управления безопасности
Почта: Razorenov-AM@ao-rr.ru