BI.ZONE

Как обеспечить безопасность значимых объектов КИИ

Алексей Авдеев
Консультант по кибербезопасности

BI.ZONE

Атаки на критическую инфраструктуру

89%

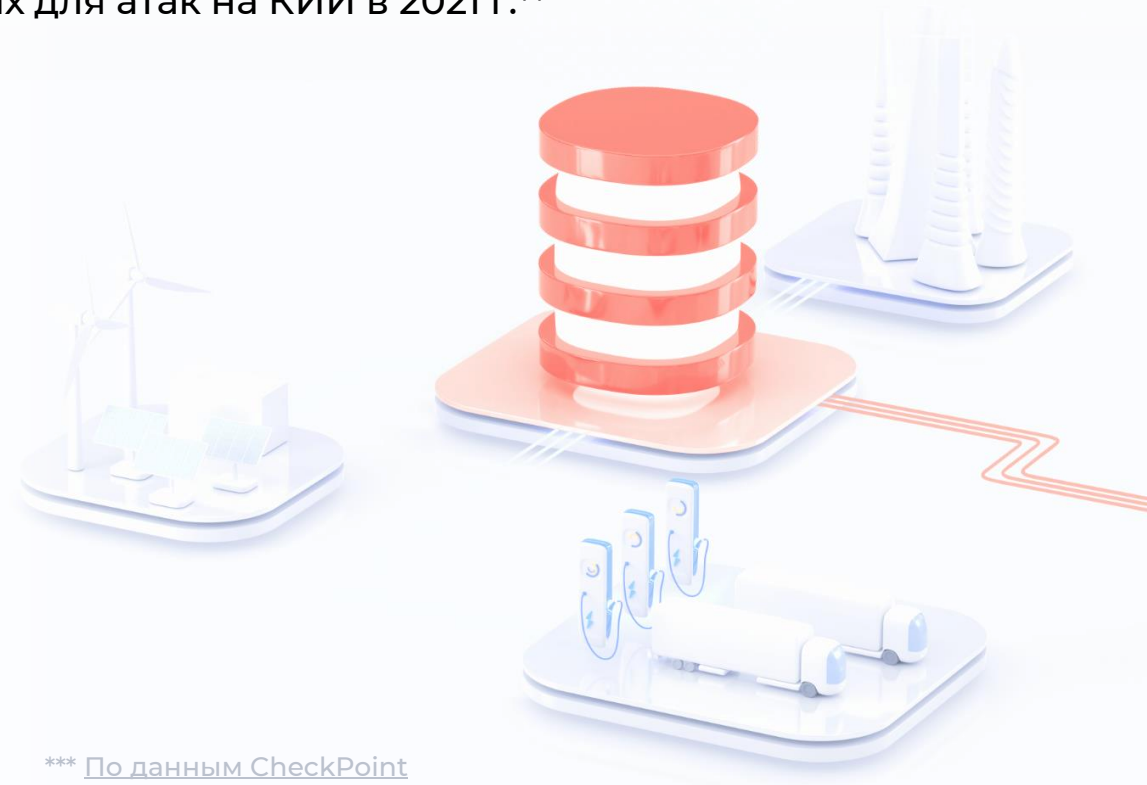
компаний критической инфраструктуры были атакованы в 2021–2022 гг.*

88%

рост числа уязвимостей в операционных технологиях, используемых для атак на КИИ в 2021 г.**

186%

рост числа атак шифровальщиков на транспортную отрасль с июня 2020 г. по июнь 2021 г.***



* По данным Trend Micro

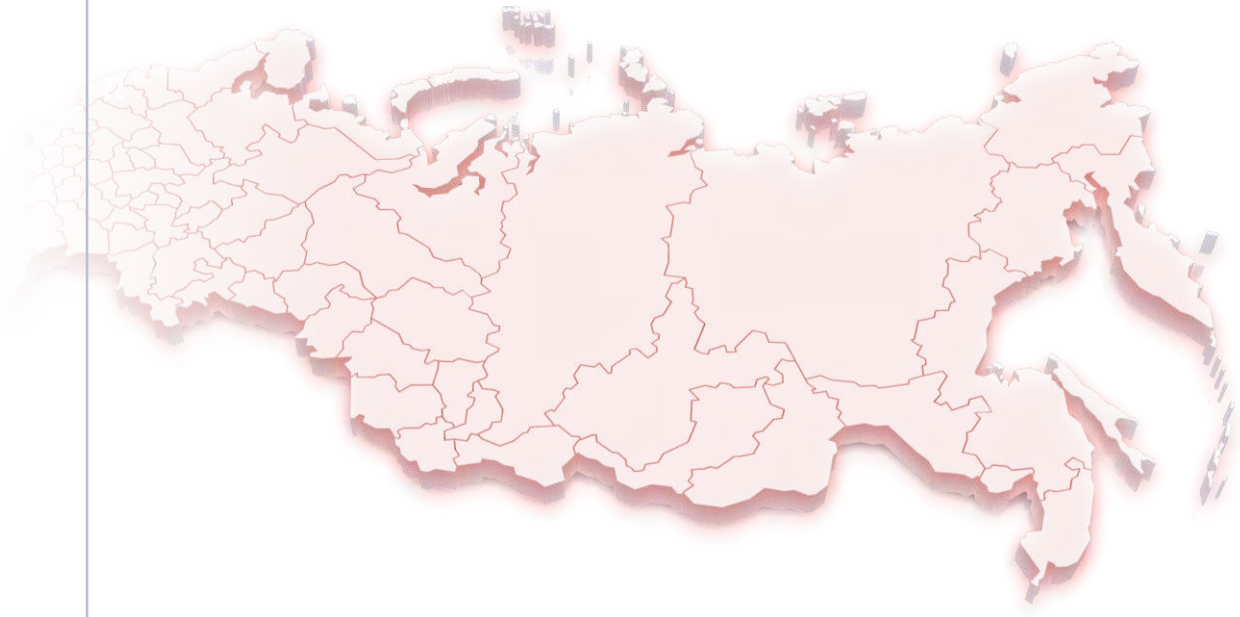
** По данным Skybox Security

*** По данным CheckPoint

BI.ZONE

Угроза национального масштаба

В условиях киберкризиса у злоумышленников появляется новый мотив: дестабилизировать и вывести из строя критическую инфраструктуру страны во всех сферах



Использование спецподразделений для кибератак на бизнес и государство

Открытое участие спецподразделений в кибервойне

Вовлечение непрофессиональных пользователей в кибератаки

Создание кибервойск под эгидой объединения военных и разведывательных возможностей с привлечением добровольного гражданского IT-сообщества

BI.ZONE

Кибератаки на объекты КИИ

Способны остановить важнейшие процессы в стране, поэтому организовывать защиту таких предприятий необходимо на высшем уровне

Во 2-м полугодии 2022 г. большинство кибератак пришлись на предприятия КИИ*

38,5%
энергетика

29,6%
производство

28,1%
нефтегазовый сектор

* Остановка процессов: что угрожает критической инфраструктуре // РБК

BI.ZONE

О чем поговорим

BI.ZONE

Нормативная документация

Федеральный закон

187-ФЗ
от 26.07.2017

Указы Президента

№ 250
от 01.05.2022

№ 166
от 30.03.2022

Приказы ФСТЭК

№ 235
от 21.12.2017

№ 239
от 25.12.2017

Приказы ФСБ

№ 367
от 24.07.2018

№ 282
от 19.06.2019

BI.ZONE

Кадровые решения

Чтобы соответствовать нормативным требованиям, организация должна:

01

Уполномочить заместителя руководителя обеспечивать кибербезопасность

02

Создать структурное подразделение по кибербезопасности

BI.ZONE

Кадровые решения

Требования к сотрудникам подразделения кибербезопасности

Для руководителя

- Высшее образование в области кибербезопасности или другое с переподготовкой
- Стаж в кибербезопасности больше 3 лет

Для сотрудников

Профессиональное образование по кибербезопасности или другое высшее образование с повышением квалификации

Для всех

Повышение квалификации по направлению «Информационная безопасность» не реже 1 раза в 3 года

BI.ZONE

Установление требований по созданию системы защиты ЗОКИИ

Состав технического задания

BI.ZONE

Разработка организационных и технических мер по обеспечению безопасности ЗОКИИ

01

Разработать модель угроз безопасности информации

02

Спроектировать систему безопасности

03

Разработать эксплуатационную документацию для системы безопасности

BI.ZONE

1. Разработка модели угроз безопасности информации

Выполняется в соответствии с методическим документом ФСТЭК от 5 февраля 2021 г. «Методика оценки угроз безопасности информации»

При разработке оценивается актуальность угроз из банка данных угроз безопасности, который насчитывает 222 угрозы

BI.ZONE

2. Проектирование системы безопасности

Определить и обосновать меры безопасности

1. Определить базовый набор мер безопасности на основе категории значимости ЗОКИИ
2. Адаптировать базовый набор мер в соответствии с угрозами безопасности информации, информационными технологиями и особенностями ЗОКИИ
3. Дополнить адаптированный набор мерами, установленными иным законодательством в области безопасности КИИ и защиты информации

Выбрать СЗИ

1. Сертифицированные
2. Прошедшие оценку на соответствие требованиям по безопасности

3. Разработка эксплуатационной документации для системы безопасности

Состав документации

Описание архитектуры системы безопасности

Порядок и параметры настройки программных и программно-аппаратных средств, в том числе СЗИ

Правила эксплуатации программных и программно-аппаратных средств, в том числе СЗИ (правила безопасной эксплуатации)

BI.ZONE

Внедрение организационных и технических мер безопасности ЗОКИИ и ввод системы безопасности в действие

01

Установка и настройка СЗИ, программных и программно-аппаратных средств

02

Разработка ОРД с правилами и процедурами безопасности

03

Внедрение организационных мер

04

Предварительные испытания

05

Опытная эксплуатация

06

Анализ уязвимостей и их устранение

07

Приемочные испытания

08

Аттестация (опционально)

BI.ZONE

Анализ уязвимостей и их устранение

Способы выявления уязвимостей

- Анализ проектной, эксплуатационной документации и ОРД
- Анализ настроек программных и программно-аппаратных средств
- Выявление уязвимостей посредством анализа состава установленного ПО и обновлений безопасности с применением средств контроля защищенности или иных СЗИ
- Выявление уязвимостей программных и программно-аппаратных средств, в том числе СЗИ, сетевых служб, доступных для сетевого взаимодействия, с применением средств контроля (анализа) защищенности
- Тестирование на проникновение в условиях, соответствующих возможностям нарушителей из модели угроз

Требования к испытаниям по выявлению уязвимостей в ПО

- Статический анализ исходного кода программы
- Фаззинг-тестирование программы
- Динамический анализ кода программы (если ПО будет применяться в ЗОКИИ 1-й категории значимости)

BI.ZONE

Обеспечение безопасности в ходе эксплуатации ЗОКИИ

01
Планирование мероприятий по безопасности

02
Анализ угроз безопасности информации и последствий от их реализации

03
Администрирование системы безопасности

04
Управление конфигурацией ЗОКИИ и его системой безопасности

05
Реагирование на киберинциденты

06
Действия во внештатных ситуациях

07
Информирование и обучение персонала

08
Контроль за обеспечением безопасности

BI.ZONE

Обеспечение безопасности при выводе ЗОКИИ из эксплуатации

Архивирование информации

Уничтожение данных и остаточной информации с машинных носителей или уничтожение таких носителей

Уничтожение или архивирование данных об архитектуре и конфигурации ЗОКИИ

Уничтожение или архивирование эксплуатационной документации на ЗОКИИ и его систему безопасности, а также ОРД по безопасности ЗОКИИ

BI.ZONE

Информирование о компьютерных инцидентах

01

Если у субъекта КИИ есть ЗОКИИ:

Необходимо подключиться и обеспечивать непрерывное взаимодействие с ГосСОПКА

02

Если у субъекта КИИ нет ЗОКИИ:

Необходимо информировать НКЦКИ о компьютерных инцидентах (например, по почте или по телефону)

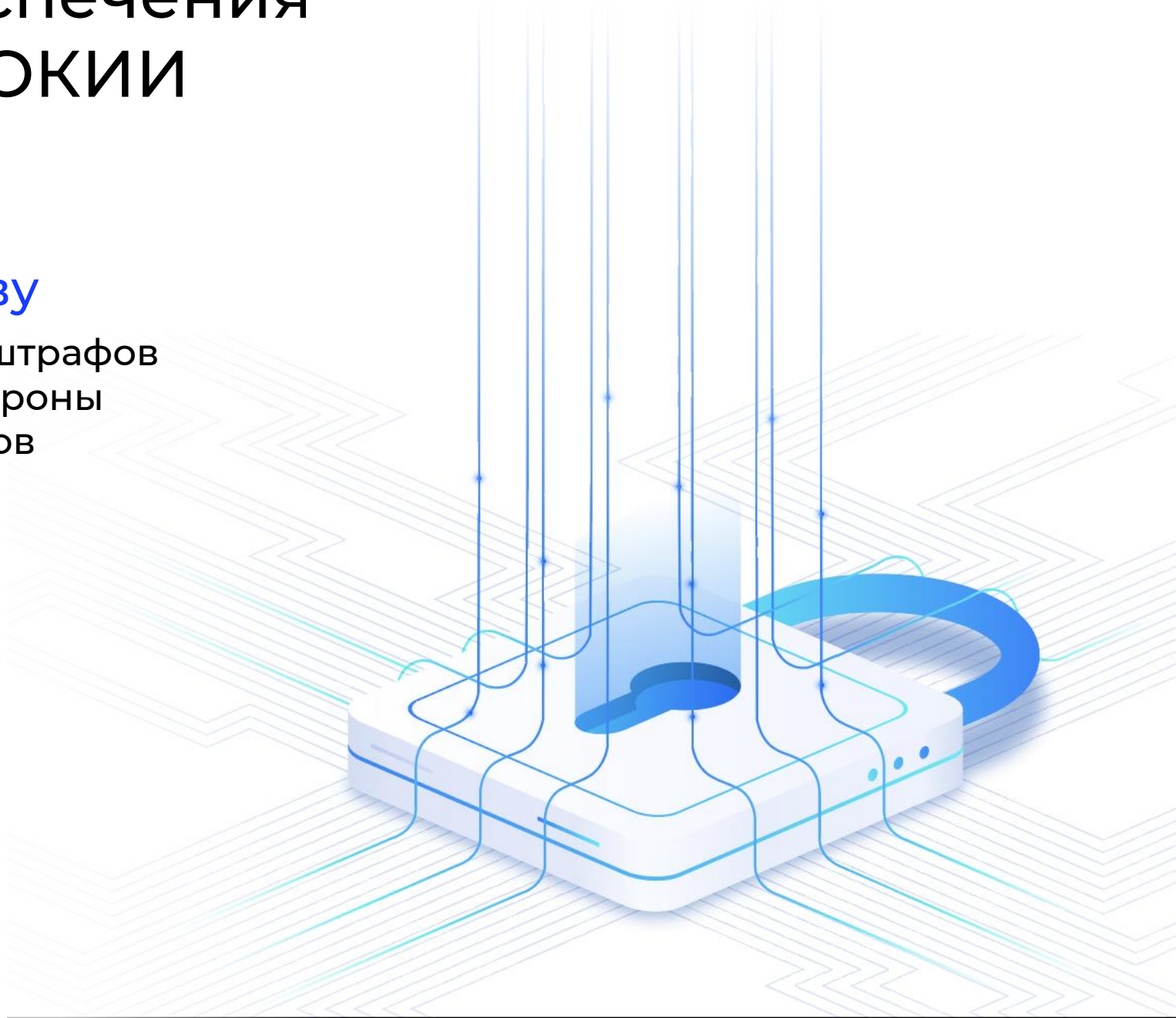
Результаты обеспечения безопасности ЗОКИИ

Соответствие законодательству

Позволяет избежать штрафов и предписаний со стороны регулирующих органов

Защищенность

Позволяет снизить риск успешных атак



Алексей Авдеев

Консультант
по кибербезопасности

a.avdeev@bi.zone

+7 (915) 335-23-54

BI.ZONE

ул. Ольховская, д. 4, корп. 2
г. Москва, 105066
+7 499 110-25-34
info@bi.zone