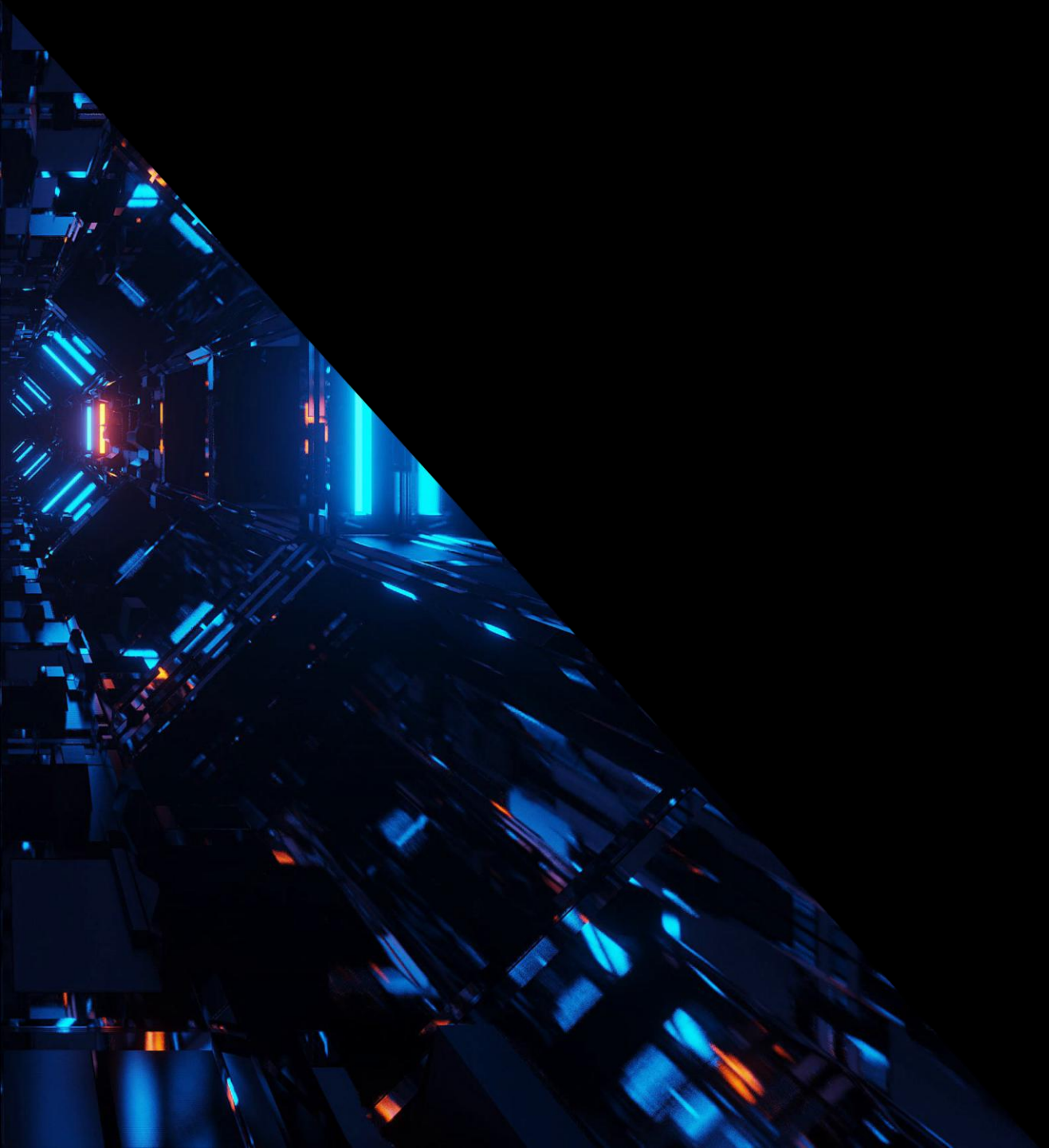


Современные технические и организацонные меры ИБ для инфраструктурных проектов

В составе холдинга

Цикада

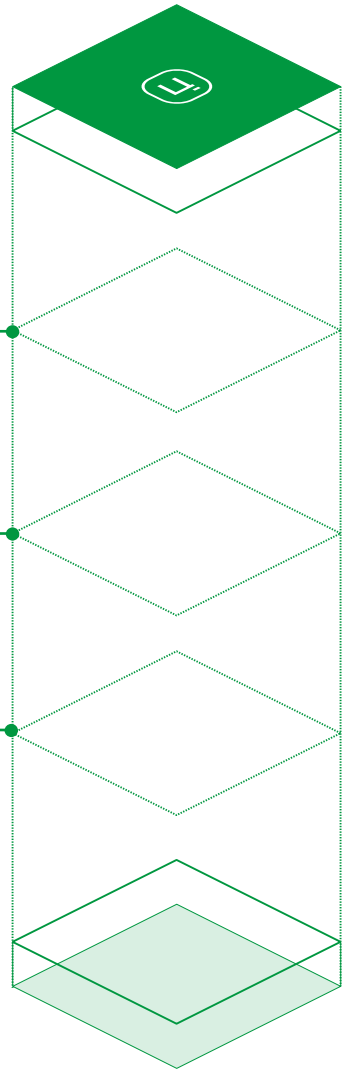
Цикада

Безопасность для новой реальности

ИНФОТАКТИКА

КИБЕР ТАКТИКА

CYREBIT



ЦИКАДА сегодня,
вертикально интегрированный холдинг, включающий компании с многолетним опытом и экспертизой в IT-бизнесе

17
лет на рынке

200+
корпоративных и государственных заказчиков

500+
комплексных проектов за год

8
направлений бизнеса

700+
квалифицированных сотрудников

ИТОГИ 2024

«Чаще всего атаки приходились
на госсектор, энергетику транспорт связь
и образование»

Замдиректор НКЦКИ

Алексей Иванов
5.02.2025 Инфофорум

Ссылка

«Целями хакеров в 2024 году чаще всего
становились компании из отраслей критической
информационной инфраструктуры — на них
пришлось около 64%»

Red Security
14.01.2025

Ссылка

ВЛИЯНИЕ НА БИЗНЕС

Нарушение критичных бизнес-процессов:

- Потеря доступности и связанности информационных систем
- Остановка работы биллинговых систем
- Потеря данных клиентов и проектов

Финансовые потери из-за потери данных:

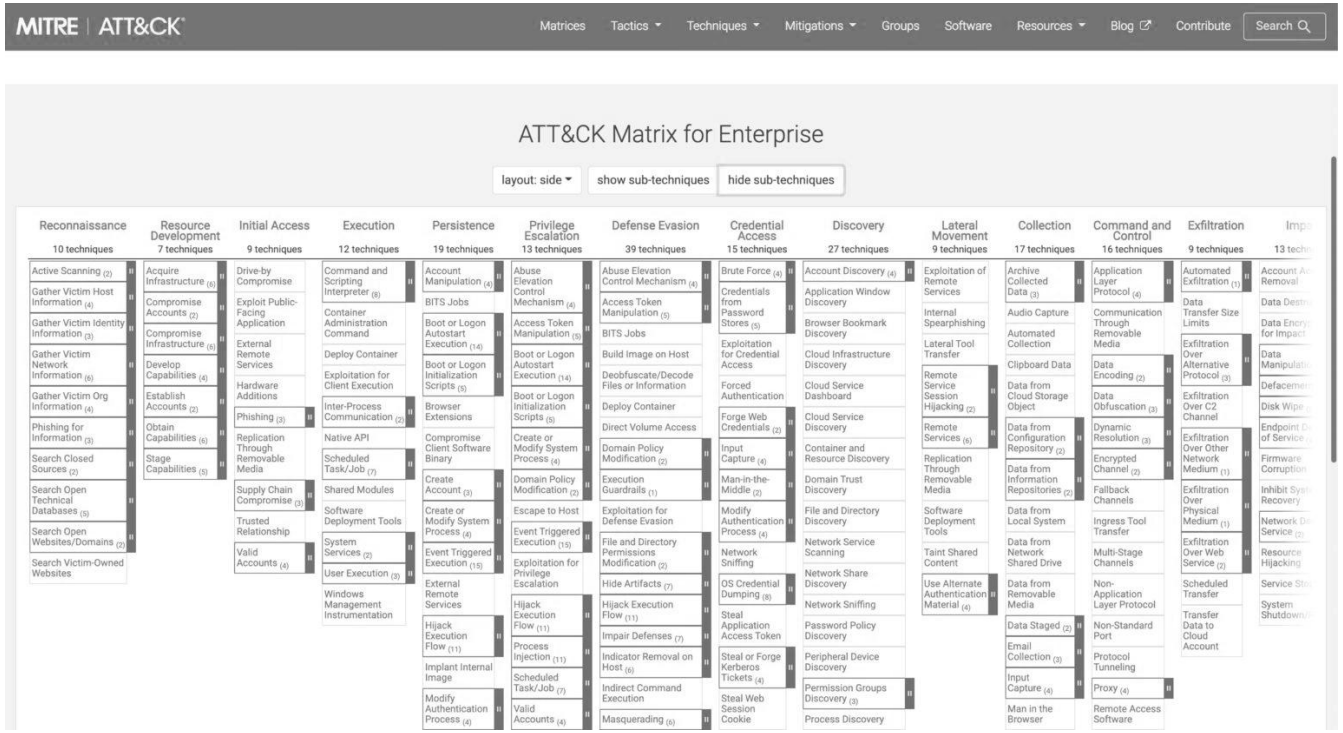
- Оборотные штрафы
- Взыскания за ущерб со стороны клиентов
- Ограничения на допуск к конкурсам и проекта

Высокая вероятность реализации, согласно ландшафту угроз 2024 и трендам 2025

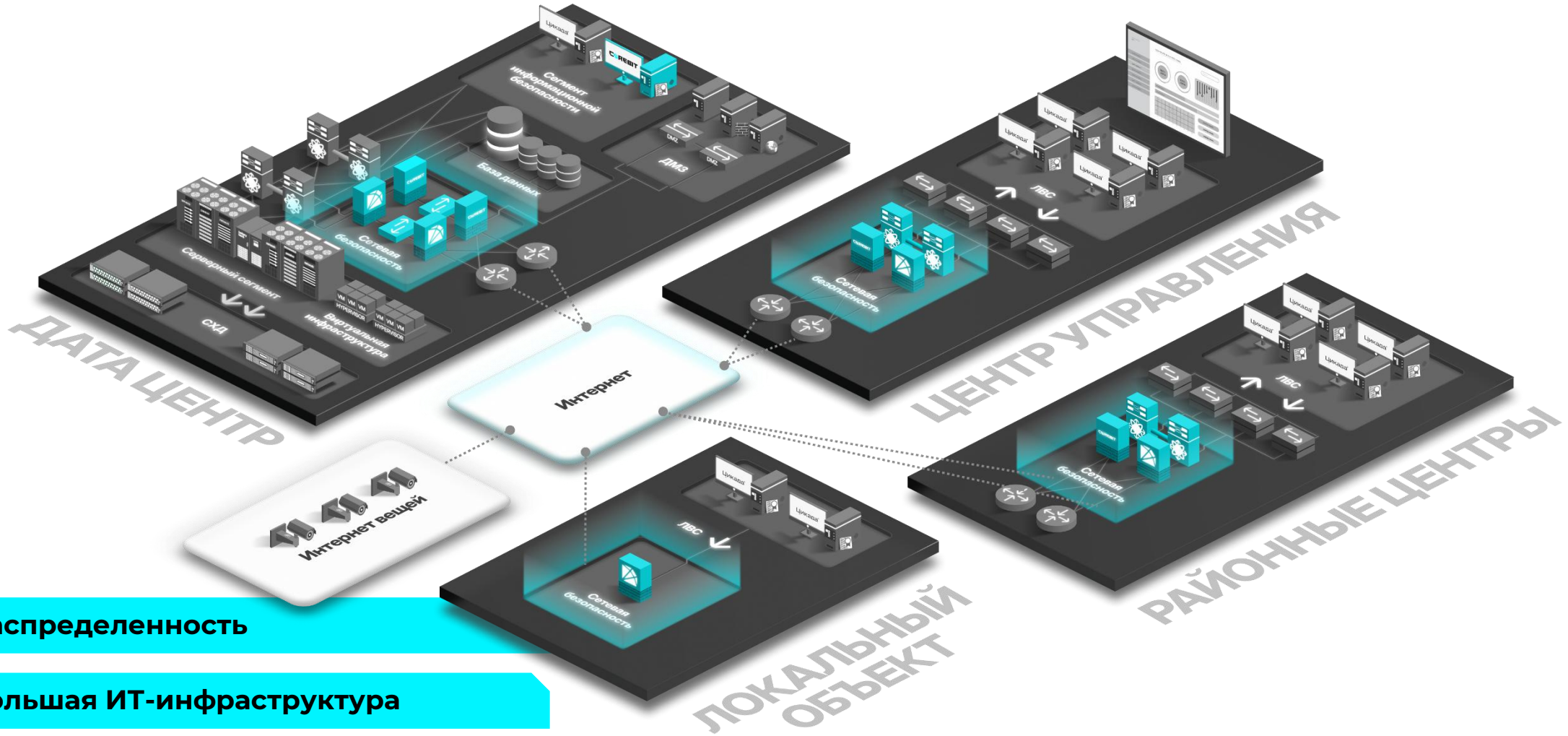
+

Административная и уголовная ответственность первых лиц (187 ФЗ, 152 ФЗ)

СОСТАВ КИБЕР АТАК



ОСОБЕННОСТИ ИНФРАСТРУКТУРНЫХ ПРОЕКТОВ



Распределенность

Большая ИТ-инфраструктура

Большие потоки данных

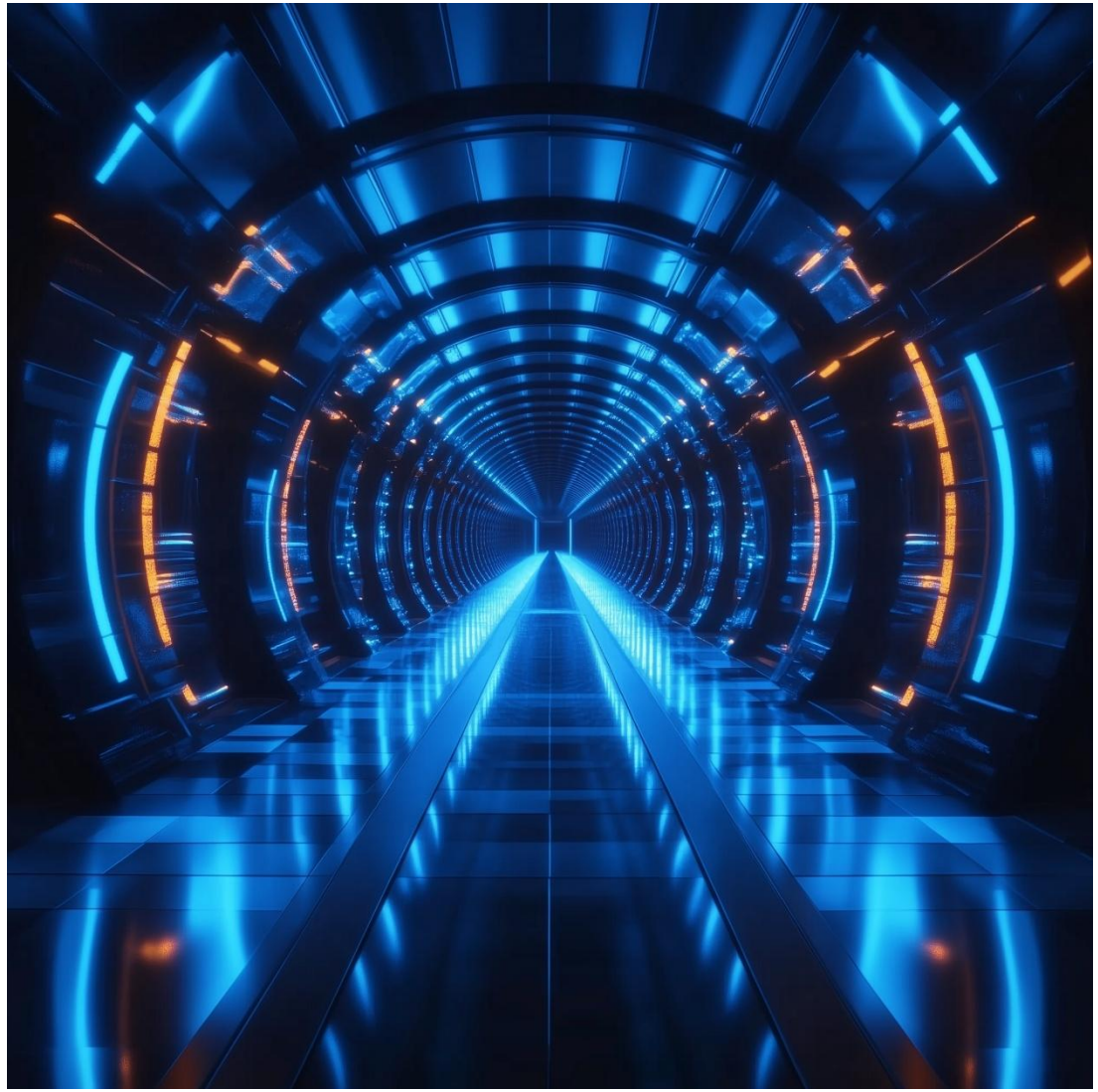
ЦИФРОВАЯ УСТОЙЧИВОСТЬ

Основные направления

- **Обучение** сотрудников компании кибергигиене, а руководителей ещё и управлению ИБ как части бизнес системы

- **Внедрение организационных и технических мер** по обеспечению информационной безопасности на всех этапах жизненного цикла бизнес процессов и систем

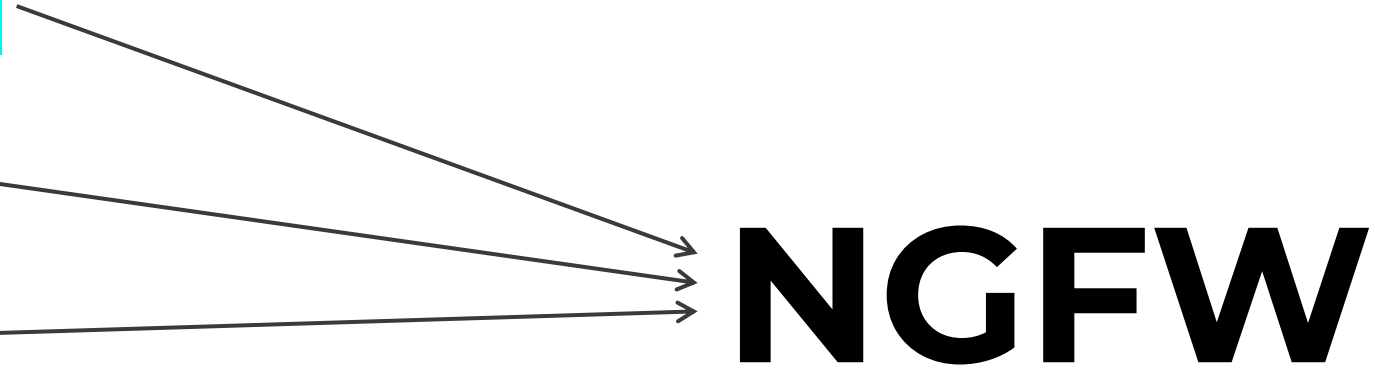
- **Внедрение процессов безопасной разработки** и корректировку трудовой, управленческой деятельности компании в части встраивания в них инструментов информационной безопасности для решения повседневных и управленческих задач



ОСНОВНЫЕ СОВРЕМЕННЫЕ РЕШЕНИЯ

Базовые меры ИБ

- Эшелонированная защита периметра
- Сегментация сетей
- Защита конечных точек
- Анализ трафика
- Анализ событий и реагирование на них
- Резервное копирование



NGFW

- Обнаружение и предотвращение вторжений
- Защита сети от MITM
- Защита от DoS-атак
- Защита DHCP-snooping
- DNS proxy
- NAT, PAT
- Защита от ARP-poisoning, защита ICMP
- DPI (Deep Packet Inspection)
- Инспекции SSL/TLS-сессий
- Анализатор сетевого трафика
- Фильтрации сессий по атрибутам протоколов уровня L2-L7
- Морфологический анализ запросов
- …

ОСОБЕННОСТИ УПРАВЛЕНИЯ

Интегрируемость

Взаимодействие с внешними системами управления по REST API

Масштабность

Возможности по созданию в веб-интерфейсе центра управления сетью сложной иерархии вложенности элементов на уровне филиалов, федеральных и локальных кластеров с гибкой настройкой ролевой модели доступа пользователей к конфигурациям функций безопасности

Широкие возможности настройки

- Удобное редактирование всех атрибутов правил фильтрации без необходимости перехода в другие вкладки веб-интерфейса
- Возможности по созданию пользовательских наборов данных
- Возможности по поиску, фильтрации и сортировки правил межсетевого экрана

ПРИМЕР РЕШЕНИЙ

Средние и малые объекты	**CoreBit.NGFW 150** МЭ (Application Control) – до 500 Мбит/с Пропускная способность в режиме защиты от угроз (NGFW) – до 200 Мбит/с	**CoreBit.NGFW 250** МЭ (Application Control) – до 8 Гбит/с Пропускная способность в режиме защиты от угроз (NGFW) – до 300 Мбит/с	**CoreBit.NGFW 500** МЭ (Application Control) – до 16 Гбит/с Пропускная способность в режиме защиты от угроз (NGFW) – до 500 Мбит/с
Центры управления и крупные объекты	**CoreBit.NGFW 1000** МЭ (Application Control) – до 45 Гбит/с Пропускная способность в режиме защиты от угроз (NGFW) – до 3,5 Гбит/с	**CoreBit.NGFW 2000** МЭ (Application Control) – до 100 Гбит/с Пропускная способность в режиме защиты от угроз (NGFW) – до 15 Гбит/с	**CoreBit.NGFW 5000** МЭ (Application Control) – до 120 Гбит/с Пропускная способность в режиме защиты от угроз (NGFW) – до 20 Гбит/с
ЦОД	**CoreBit.NGFW 6000** МЭ (Application Control) – до 160 Гбит/с Пропускная способность в режиме защиты от угроз (NGFW) – до 25 Гбит/с	**CoreBit.NGFW 7000** МЭ (Application Control) – до 180 Гбит/с Пропускная способность в режиме защиты от угроз (NGFW) – до 30 Гбит/с	


COREBIT
Наши технологии
Ваша безопасность

Наши технологии – ваша безопасность

ООО «Корбит»
+7 495 133 26 89
info@corebit.ru
www.corebit.ru

В составе холдинга
Цикада