



Современные технические и организационные меры ИБ для инфраструктурных проектов

В составе холдинга

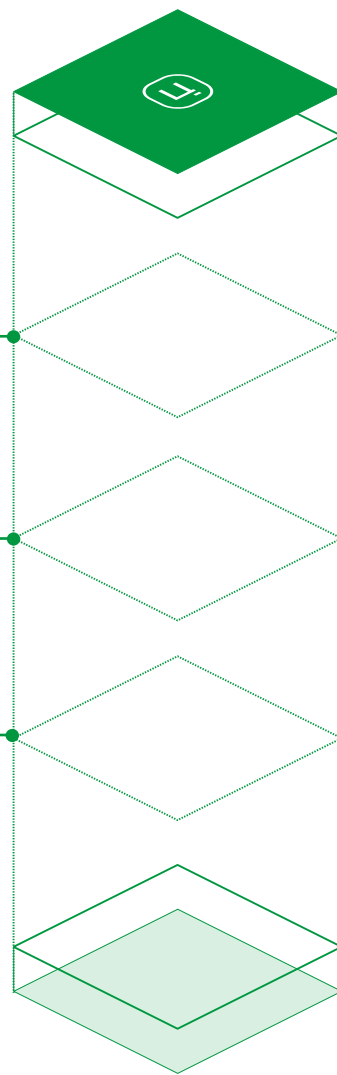
Цикада

Цикада

Безопасность для
новой реальности



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

«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](#)

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:

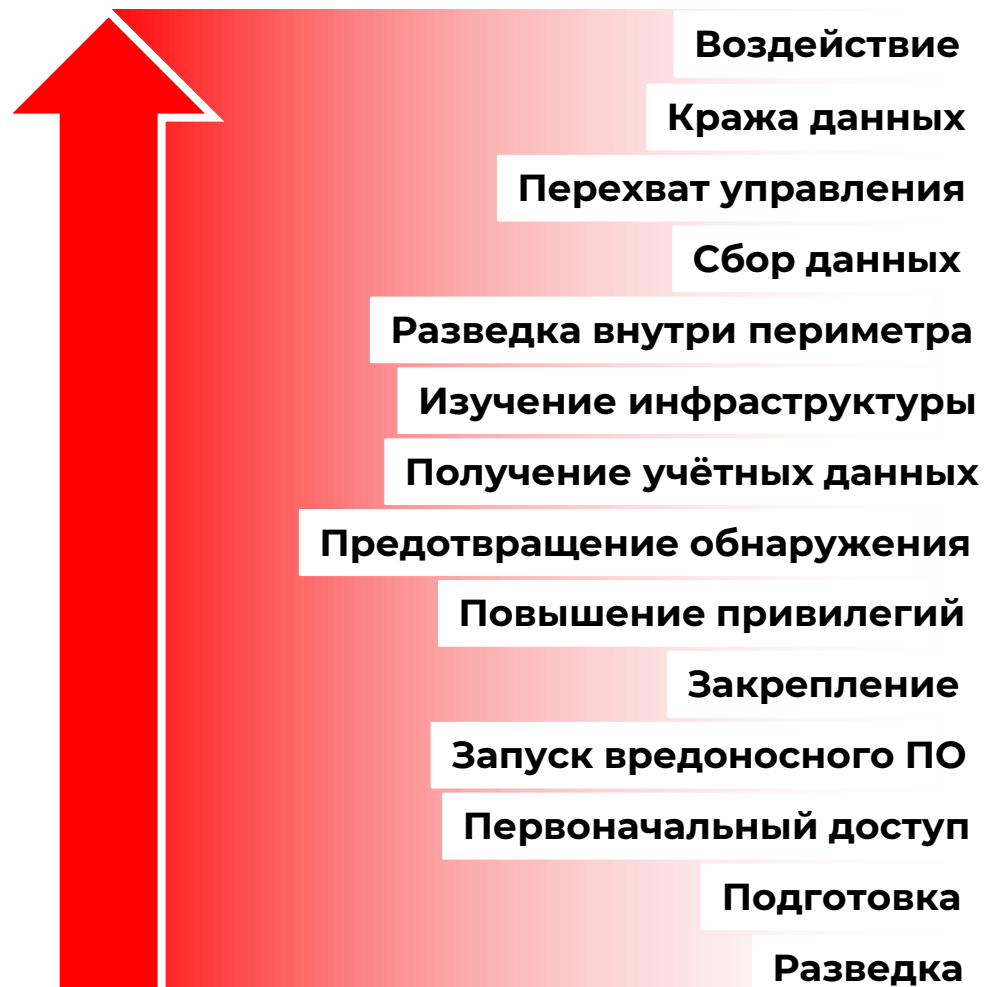
- Оборотные штрафы
- Взыскания за ущерб со стороны клиентов
- Ограничения на допуск к конкурсам и проекта

Высокая вероятность реализации, согласно ландшафту угроз 2024 и трендам 2025



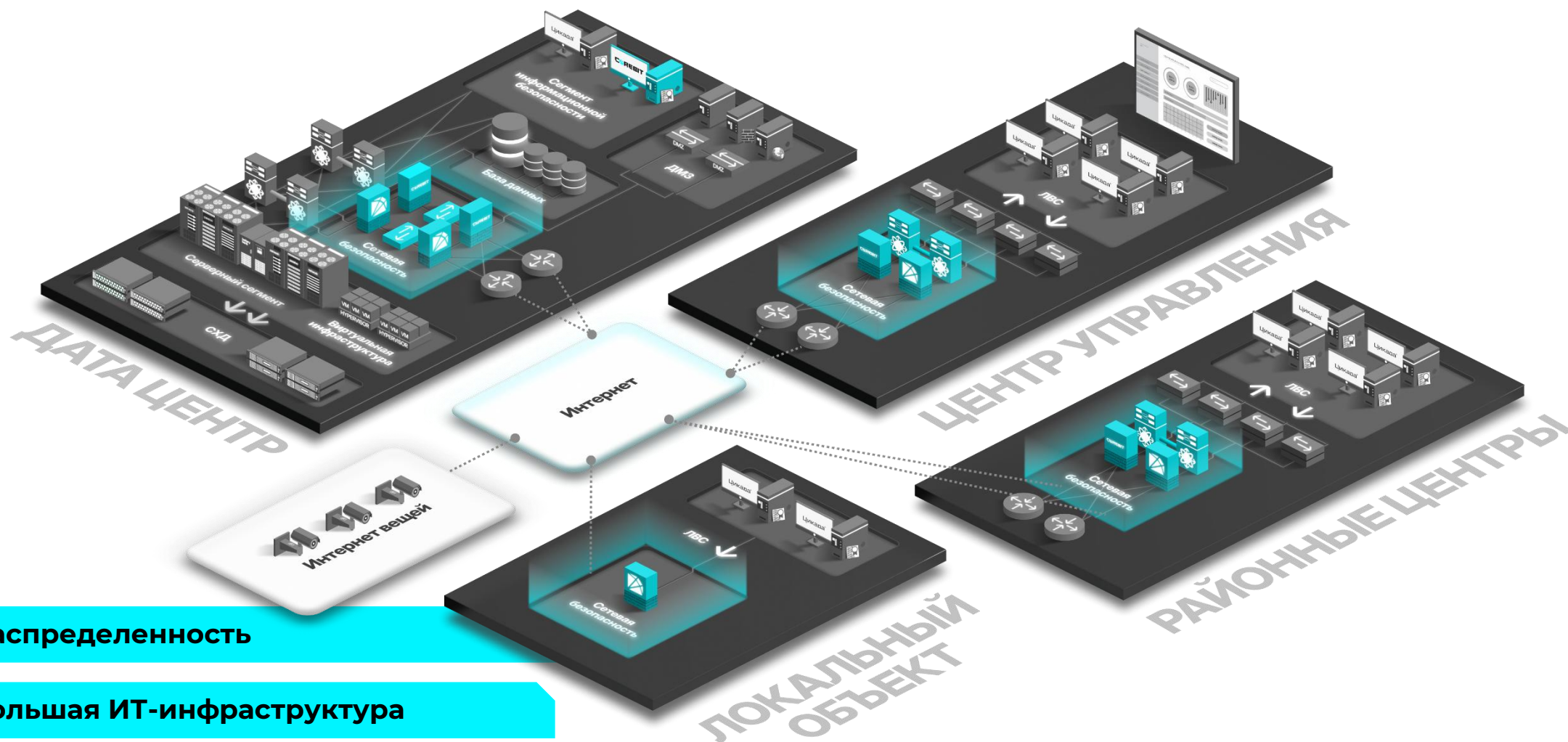
Административная и уголовная ответственность первых лиц (187 ФЗ, 152 ФЗ)

СОСТАВ КИБЕР АТАК



MITRE ATT&CK													
Matrixes Tactics Techniques Mitigations Groups Software Resources Blog Contribute Search													
ATT&CK Matrix for Enterprise													
layout: side show sub-techniques hide sub-techniques													
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	7 techniques	9 techniques	12 techniques	19 techniques	13 techniques	39 techniques	15 techniques	27 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Active Scanning (2)	Acquire Infrastructure (3)	Drive-by Compromise	Command and Scripting Interpreter (3)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Removal
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (3)	Access Token Manipulation (3)	Credentials from Password Stores (3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (3)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	Access Token Manipulation (3)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Clipboard Data	Exfiltration Over Alternative Protocol (3)	Data Encryption for Impact
Gather Victim Network Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (4)	Boot or Logon Autostart Execution (14)	Build Image on Host	Deobfuscate/Decode Files or Information	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Data from Cloud Storage Object	Data Encoding (2)	Exfiltration Over C2 Channel	Data Manipulation
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (2)	Browser Extensions	Boot or Logon Initialization Scripts (3)	Deploy Container	Forced Authentication	Cloud Service Dashboard	Remote Services (6)	Data from Configuration Repository (2)	Data Obfuscation (3)	Exfiltration Over Other Network Medium (1)	Defacement
Phishing for Information (3)	Obtain Capabilities (3)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Create or Modify System Process (4)	Direct Volume Access	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Data from Information Repositories (2)	Dynamic Resolution (3)	Exfiltration Over Physical Channel (2)	Disk Wipe
Search Closed Sources (2)	Stage Capabilities (3)	Supply Chain Compromise (3)	Scheduled Task/Job (7)	Create Account (3)	Domain Policy Modification (2)	Execution Guardrails (2)	Input Capture (4)	Container and Resource Discovery	Software Deployment Tools	Data from Local System	Ingress Tool Transfer	Exfiltration Over Web Service (2)	Endpoint Detection and Response of Service
Search Open Technical Databases (3)	Trusted Relationship	Valid Accounts (4)	Shared Modules	Create or Modify System Process (4)	Escape to Host	Exploitation for Defense Evasion	Man-in-the-Middle (2)	Domain Trust Discovery	Taint Shared Content	Data from Network Shared Drive	Multi-Stage Channels	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains (2)	External Remote Services	Windows Management Instrumentation	Software Deployment Tools	Event Triggered Execution (15)	Event Triggered Execution (15)	File and Directory Permissions Modification (2)	Modify Authentication Process (4)	File and Directory Discovery	Use Alternate Authentication Material (4)	Network Service Discovery	Non-Application Layer Protocol	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites			System Services (2)	Event Triggered Execution (15)	Exploitation for Privilege Escalation	Hide Artifacts (7)	Network Sniffing	Network Service Scanning		Network Share Discovery	Non-Standard Port		Network Discovery
			User Execution (3)	Windows Remote Services	Hijack Execution Flow (11)	Hijack Execution Flow (11)	OS Credential Dumping (4)	Network Sniffing		Network Sniffing	Input Capture (4)		Resource Hijacking
					Process Injection (11)	Indicator Removal on Host (6)	Steal Application Access Token	OS Credential Dumping (4)		Network Sniffing	Input Capture (4)		Service Shutdown
					Scheduled Task/Job (7)	Indirect Command Execution	Steal or Forge Kerberos Tickets (4)	Peripherals Device Discovery		Network Sniffing	Input Capture (4)		System Shutdown
					Modify Authentication Process (4)	Valid Accounts (4)	Steal Web Session Cookie	Permission Groups Discovery (3)		Network Sniffing	Input Capture (4)		
							Masquerading (3)	Process Discovery		Network Sniffing	Input Capture (4)		

ОСОБЕННОСТИ ИНФРАСТРУКТУРНЫХ ПРОЕКТОВ



Распределенность

Большая ИТ-инфраструктура

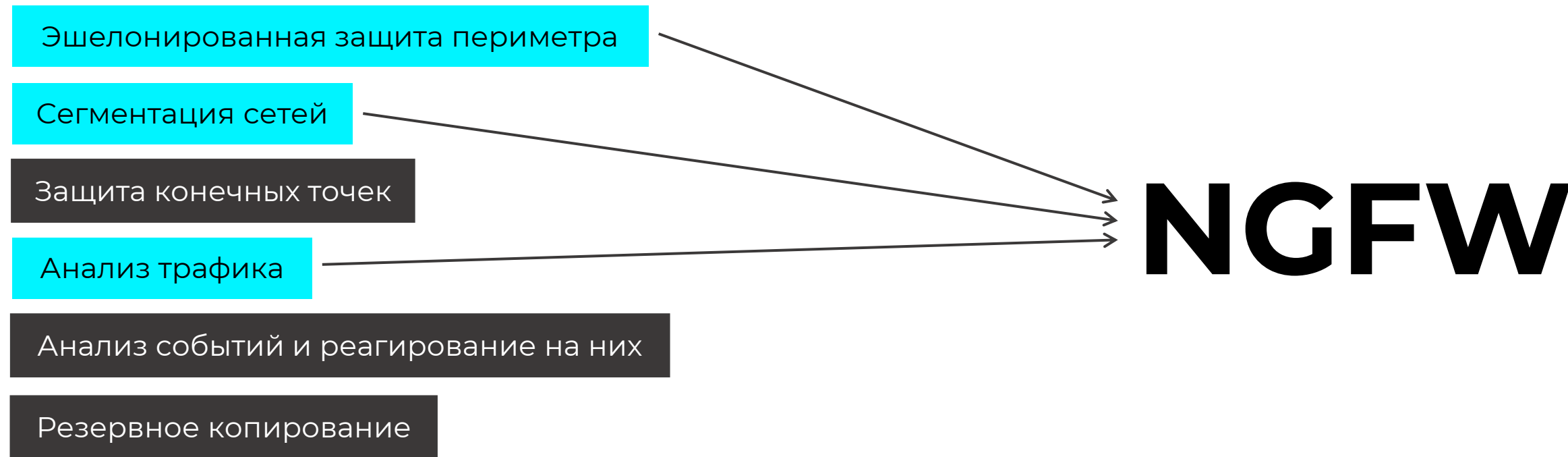
Большие потоки данных

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



Базовые меры ИБ



- 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

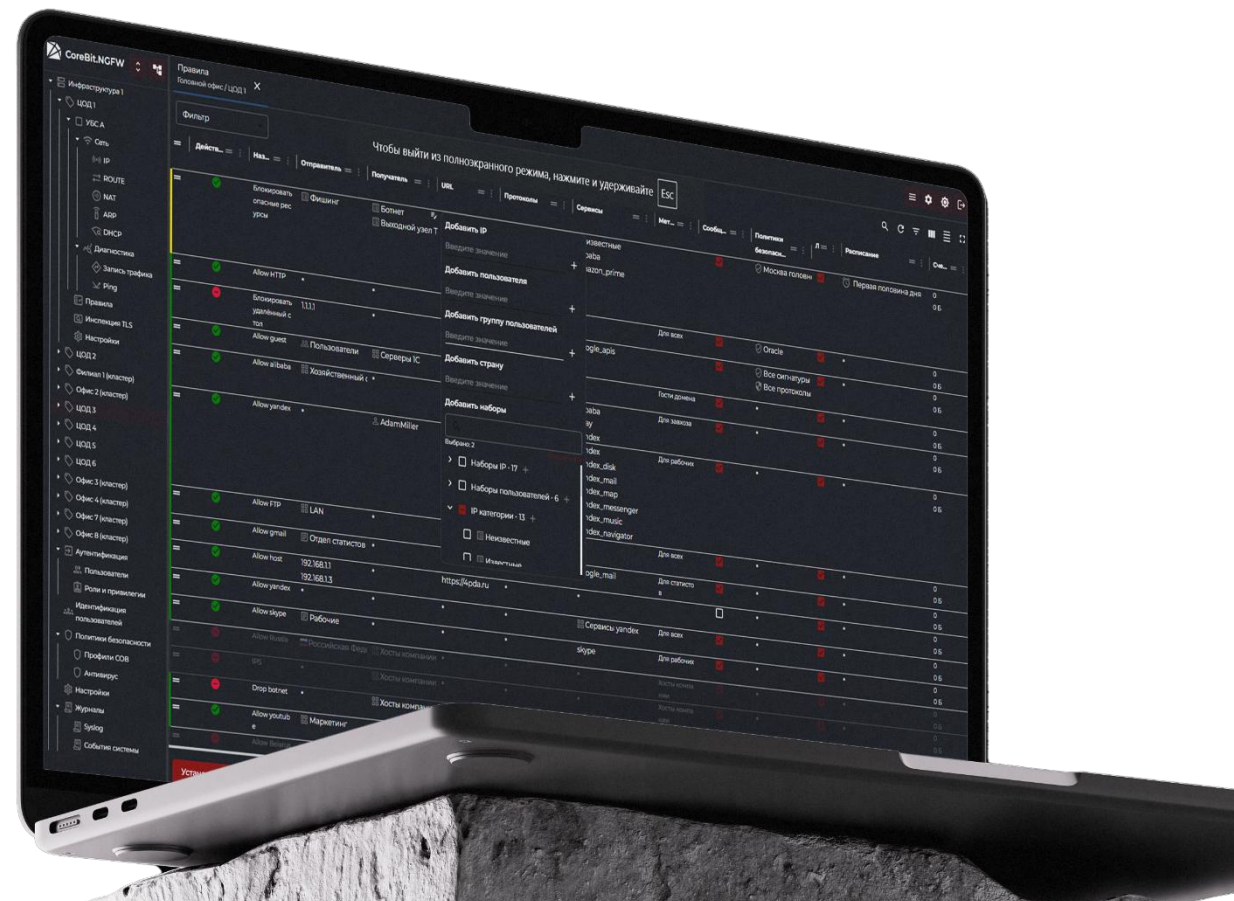
Взаимодействие с внешними системами управления по REST API

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



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



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