A person in a dark suit and blue tie is holding a large, metallic gear. Several other similar gears are floating in the air around them, creating a sense of motion and complexity. The background is a blurred office setting with a window showing blinds.

Построение современных систем защиты информации с применением концепции Threat Intelligence

Тимофей Поляков

Важно не просто знать, как могут атаковать защищаемую систему

Действительно важно знать, что противопоставить атакующему на каждом его шаге

Этапы создания систем защиты информации



Моделирование угроз безопасности информации

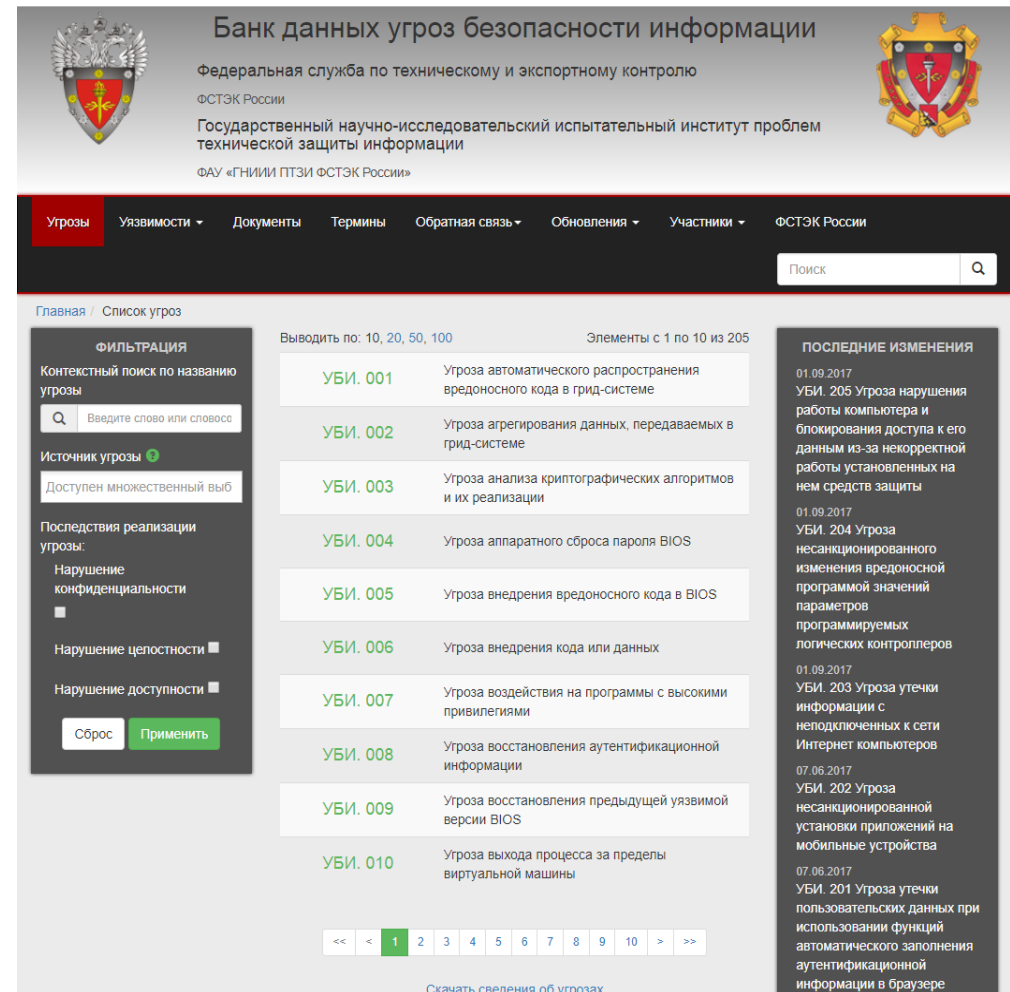
Моделирование угроз в РФ

Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных

(Утверждена Заместителем директора ФСТЭК России 15 февраля 2008 г.)

Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных

(Утверждена Заместителем директора ФСТЭК России 15 февраля 2008 г.)



Банк данных угроз безопасности информации
 Федеральная служба по техническому и экспортному контролю
 ФСТЭК России
 Государственный научно-исследовательский испытательный институт проблем технической защиты информации
 ФАУ «ГНИИИ ПТЗИ ФСТЭК России»

Угрозы | Уязвимости | Документы | Термины | Обратная связь | Обновления | Участники | ФСТЭК России

Поиск

Главная / Список угроз

Выводить по: 10, 20, 50, 100 Элементы с 1 по 10 из 205

Идентификатор	Описание угрозы
УБИ.001	Угроза автоматического распространения вредоносного кода в грид-системе
УБИ.002	Угроза агрегирования данных, передаваемых в грид-системе
УБИ.003	Угроза анализа криптографических алгоритмов и их реализации
УБИ.004	Угроза аппаратного сброса пароля BIOS
УБИ.005	Угроза внедрения вредоносного кода в BIOS
УБИ.006	Угроза внедрения кода или данных
УБИ.007	Угроза воздействия на программы с высокими привилегиями
УБИ.008	Угроза восстановления аутентификационной информации
УБИ.009	Угроза восстановления предыдущей уязвимой версии BIOS
УБИ.010	Угроза выхода процесса за пределы виртуальной машины

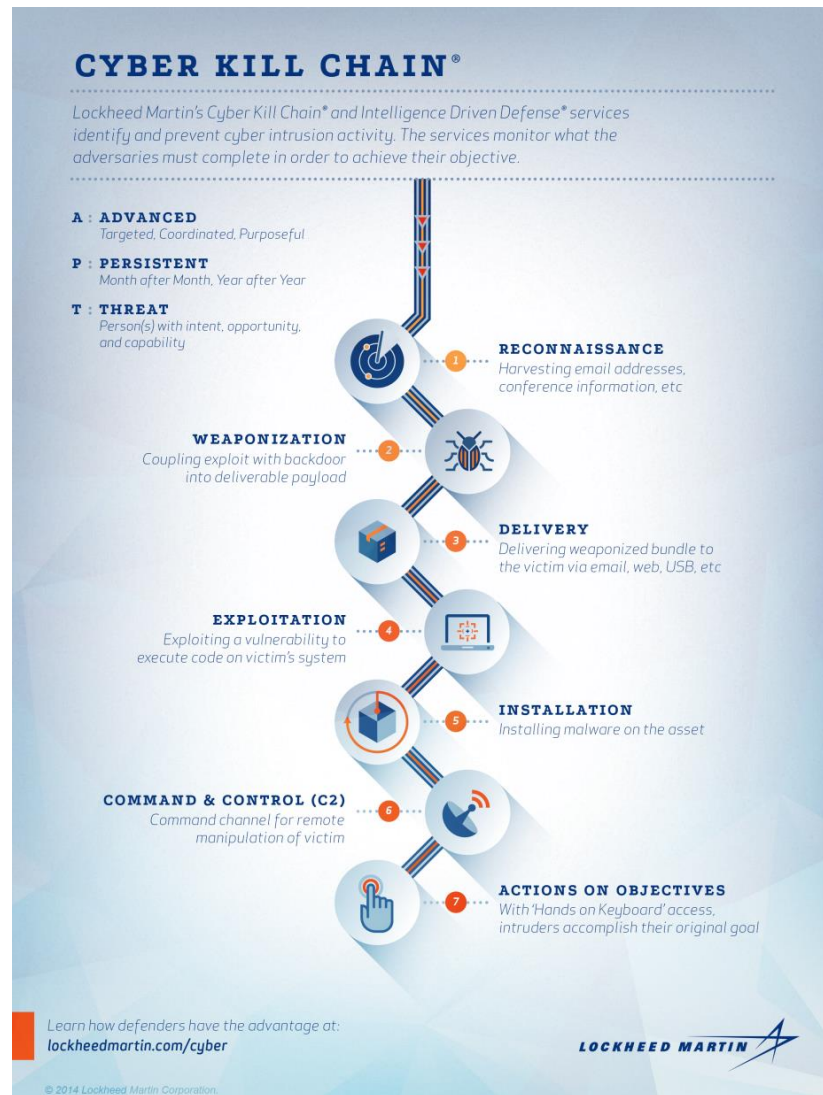
Скачать сведения об угрозах

ПОСЛЕДНИЕ ИЗМЕНЕНИЯ

- 01.09.2017 УБИ. 205 Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты
- 01.09.2017 УБИ. 204 Угроза несанкционированного изменения вредоносной программой значений параметров программируемых логических контроллеров
- 01.09.2017 УБИ. 203 Угроза утечки информации с неподключенных к сети Интернет компьютеров
- 07.06.2017 УБИ. 202 Угроза несанкционированной установки приложений на мобильные устройства
- 07.06.2017 УБИ. 201 Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере

Cyber kill chain

- Разведка
- Вооружение
- Доставка
- Заражение
- Установка
- Получение управления
- Основная деятельность
- Уничтожение следов



Матрица АТТ&СК

ATT&CK Matrix

The MITRE ATT&CK Matrix™ is an overview of the tactics and techniques described in the ATT&CK model. It visually aligns individual techniques under the tactics in which they can be applied. Some techniques span more than one tactic because they can be used for different purposes.

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
Accessibility Features	Accessibility Features	Binary Padding	Brute Force	Account Discovery	Application Deployment Software	Command-Line Interface	Automated Collection	Automated Exfiltration	Commonly Used Port
AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Application Window Discovery	Exploitation of Vulnerability	Execution through API	Clipboard Data	Data Compressed	Communication Through Removable Media
Basic Input/Output System	Bypass User Account Control	Code Signing	Credential Manipulation	File and Directory Discovery	Logon Scripts	Graphical User Interface	Data Staged	Data Encrypted	Connection Proxy
Bootkit	DLL Injection	Component Firmware	Credentials in Files	Local Network Configuration Discovery	Pass the Hash	InstallUtil	Data from Local System	Data Transfer Size Limits	Custom Command and Control Protocol
Change Default File Association	DLL Search Order Hijacking	Component Object Model Hijacking	Exploitation of Vulnerability	Local Network Connections Discovery	Pass the Ticket	PowerShell	Data from Network Shared Drive	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Component Firmware	Exploitation of Vulnerability	DLL Injection	Input Capture	Network Service Scanning	Remote Desktop Protocol	Process Hollowing	Data from Removable Media	Exfiltration Over Command and Control Channel	Data Obfuscation

Kill Chain и ATT&CK

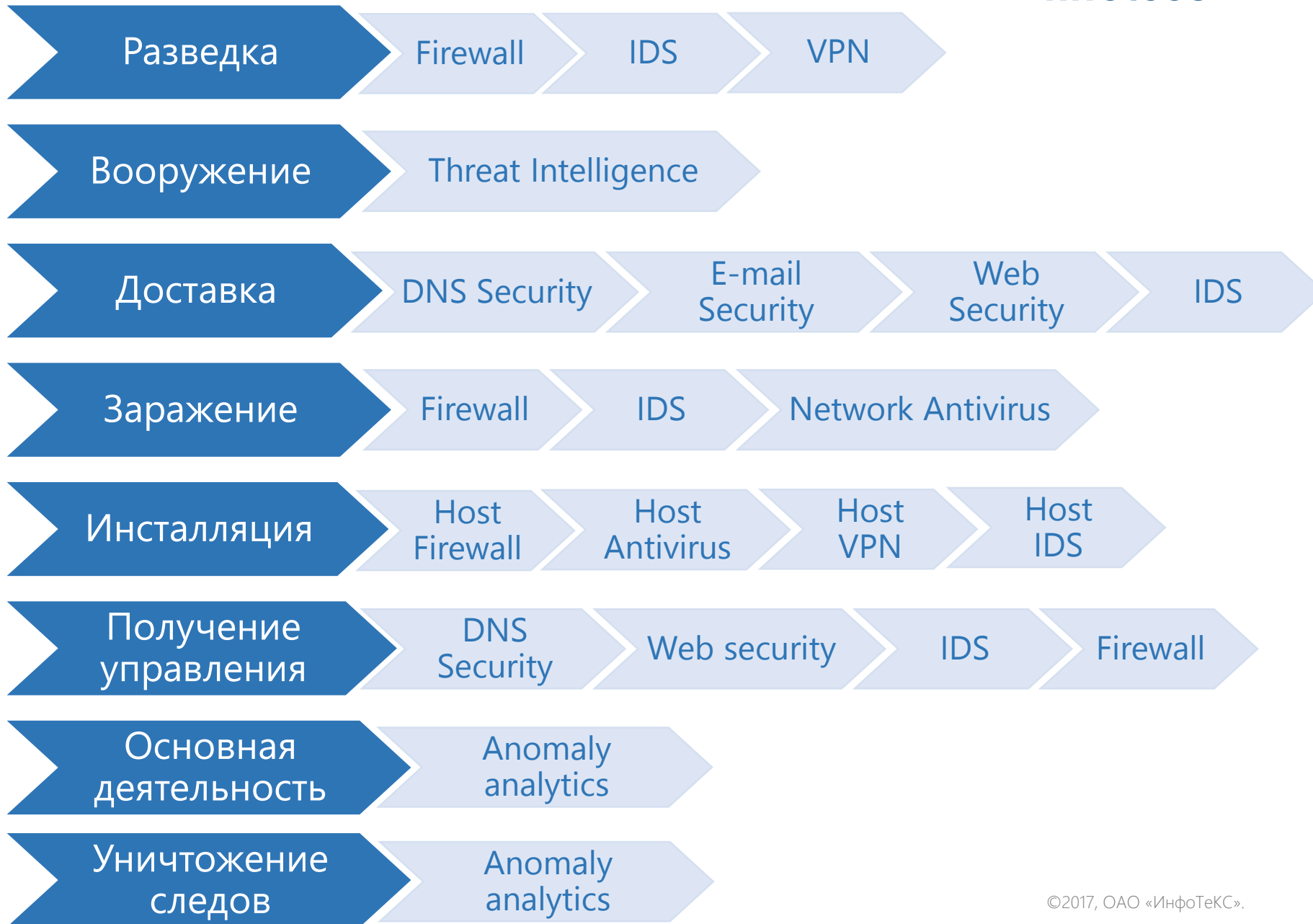


Проектирование системы защиты информации

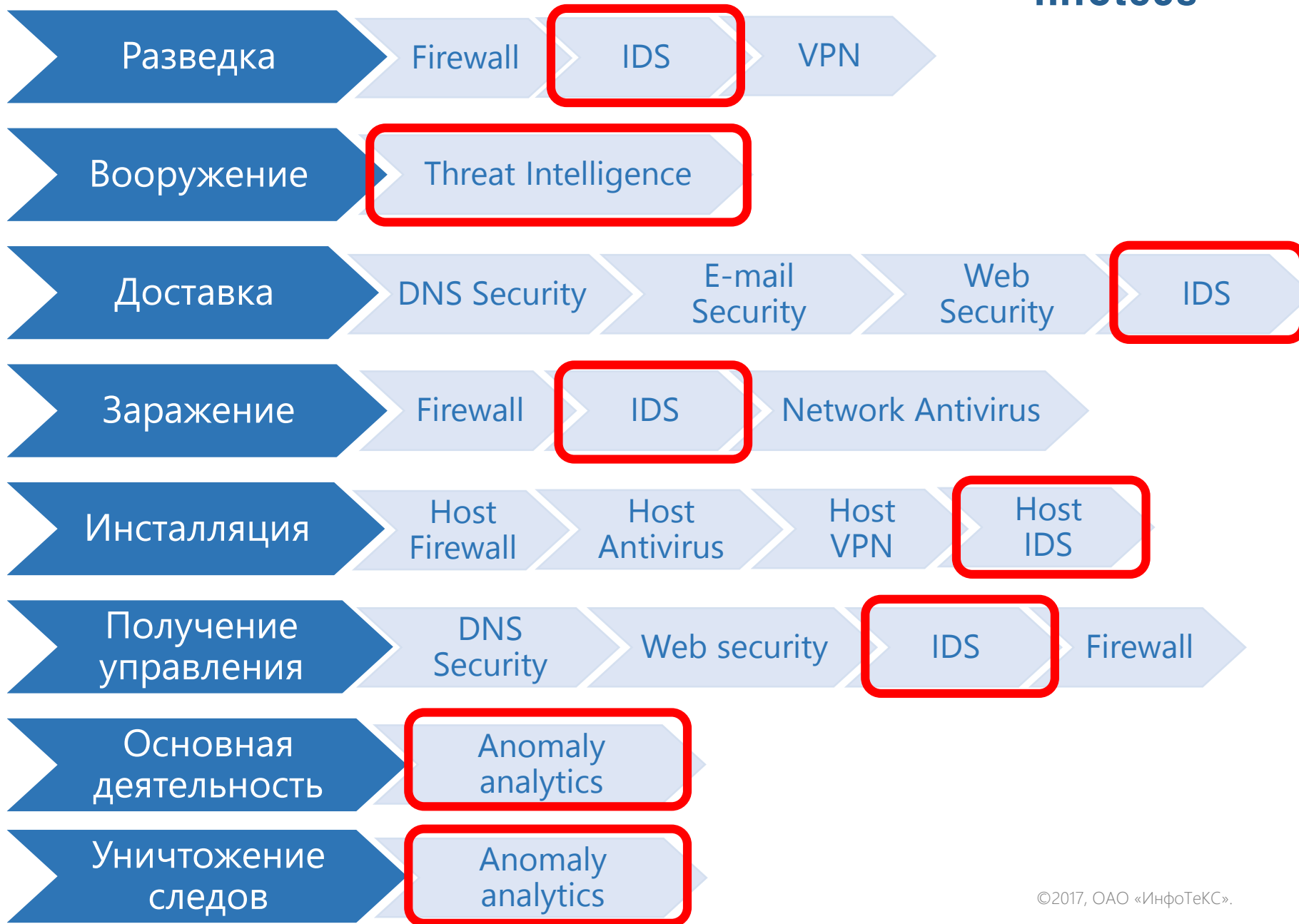
Проектирование системы защиты информации



Проектирование системы защиты информации



Проектирование системы защиты информации

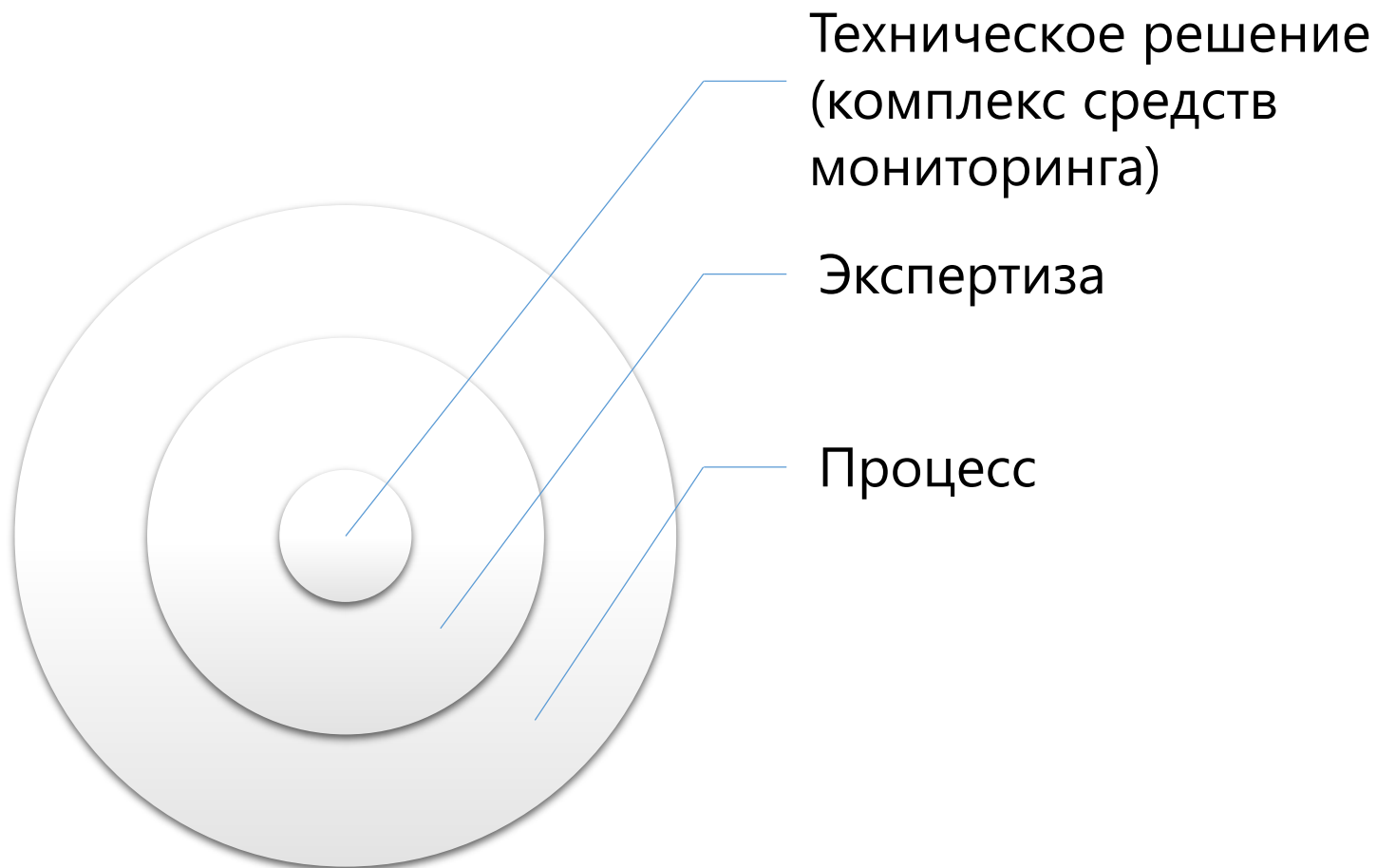


Реагирование на события ИБ

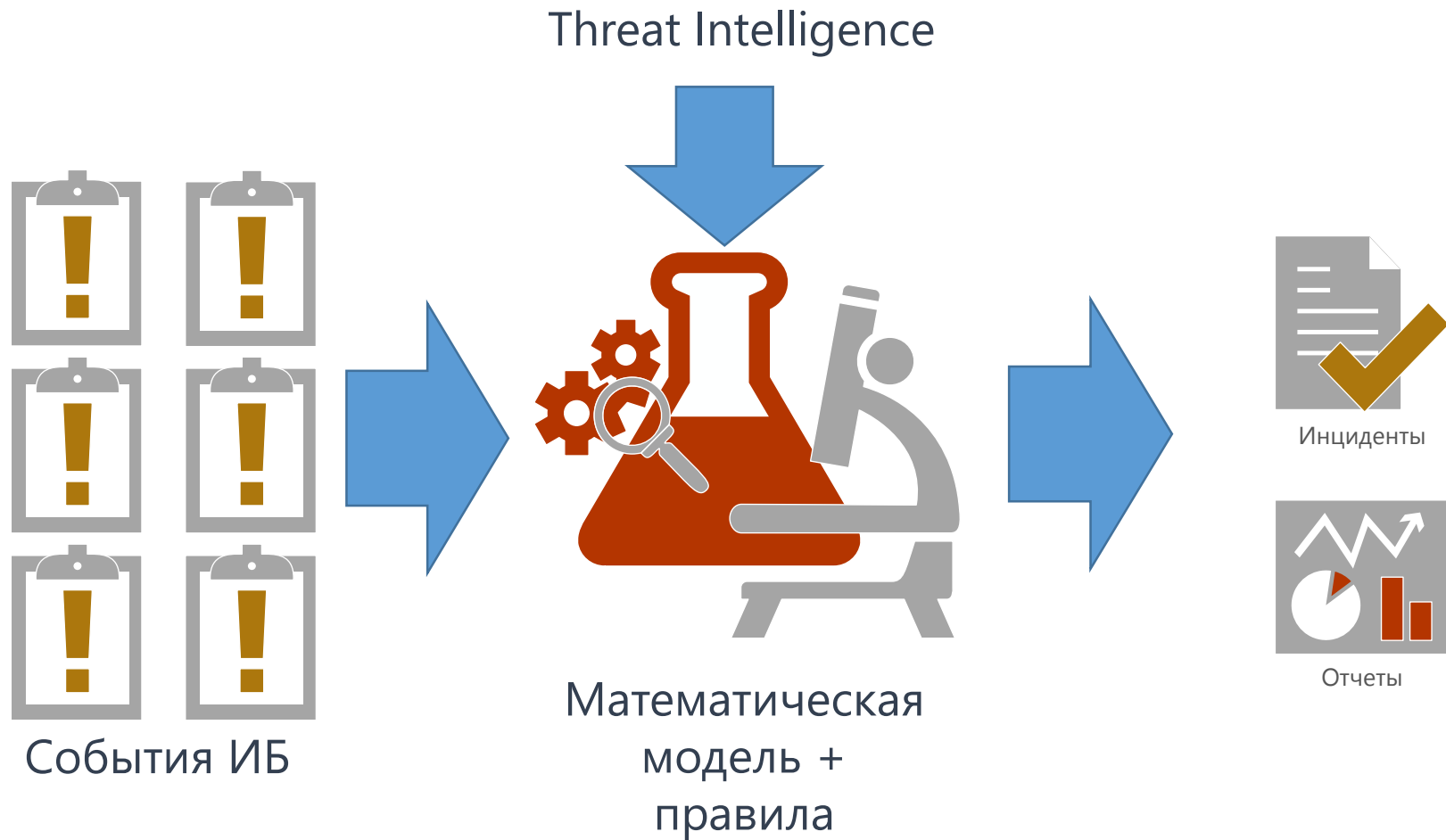


Применение концепции **Threat Intelligence**

Концепция Threat Intelligence

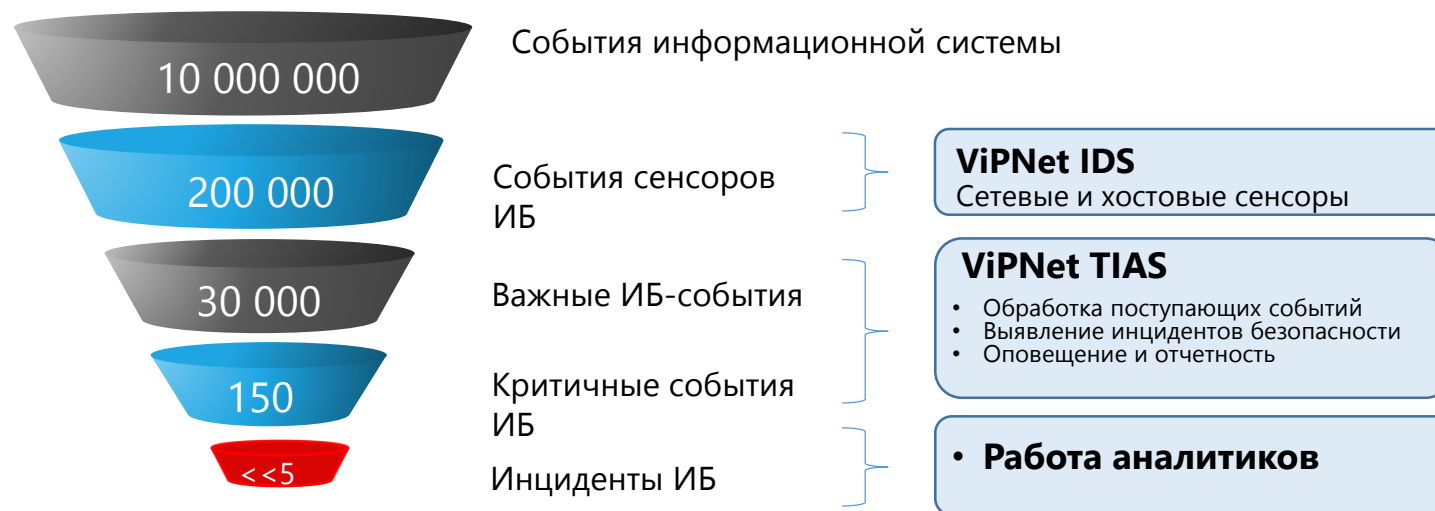


ViPNet TIAS

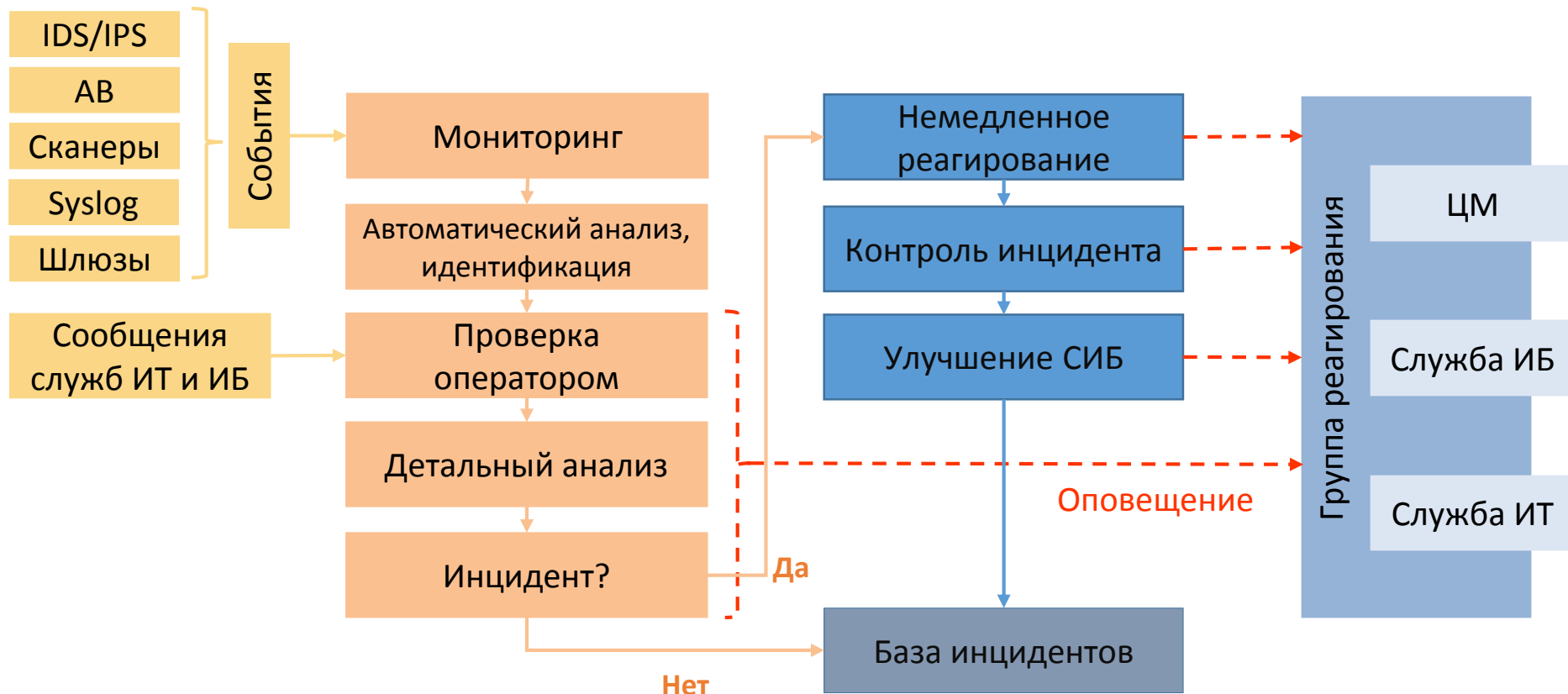


От регистрации событий к экспертизе

Месячная статистика для организации ~500 АРМ, 10 Серверов



Формирование непрерывного процесса



Статистика центра мониторинга

Центром мониторинга зафиксировано

I квартал 2017

137 873 416 событий
информационной
безопасности

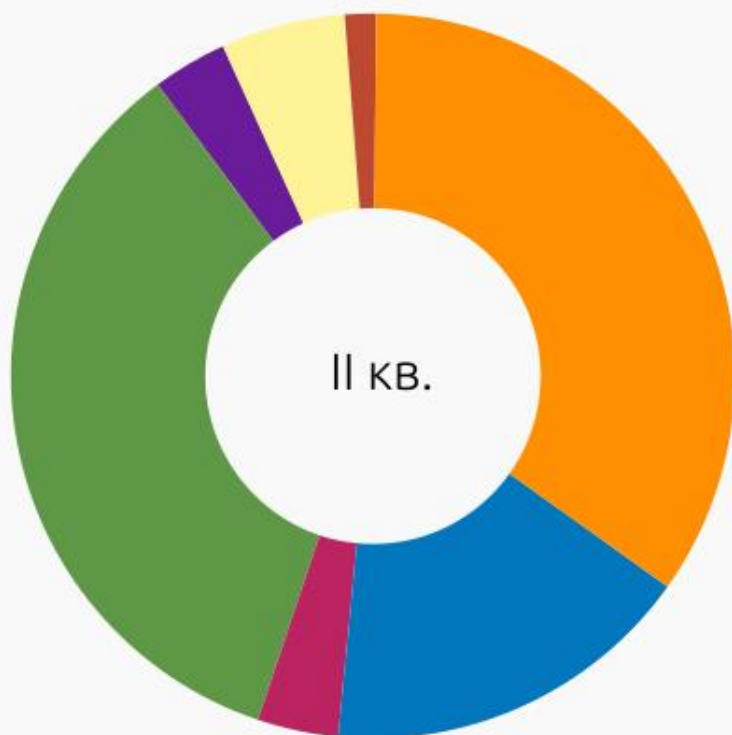
98 инцидентов

II квартал 2017

254 453 172 события
информационной
безопасности

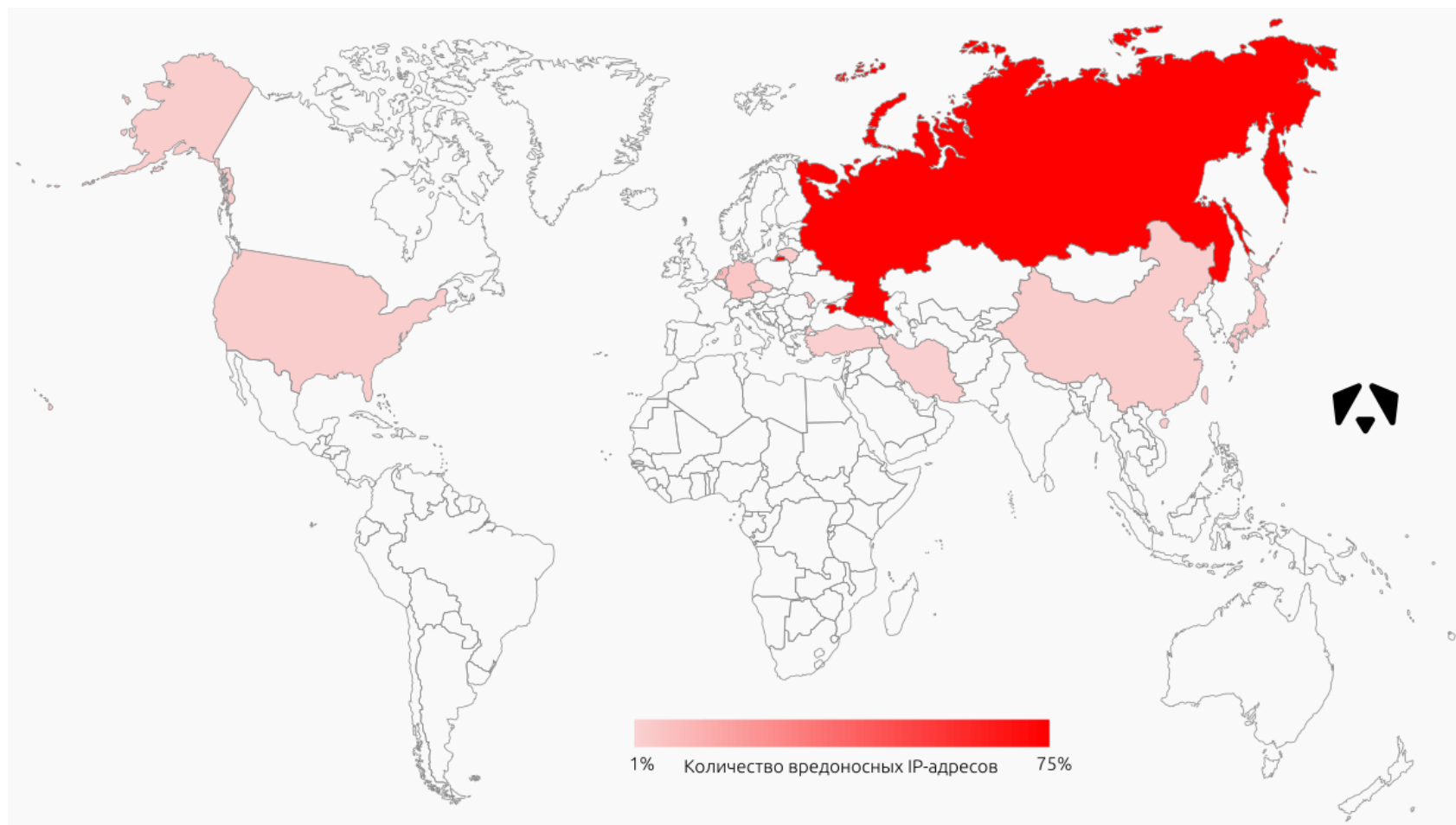
144 инцидента

Распределение целей атак



- Пользовательские АРМ
- Иные сетевые сервисы
- DNS-серверы
- Web-серверы
- Межсетевые экраны
- Файловые серверы
- Почтовые серверы

География источников атак



ИТОГИ

- Для моделирования угроз безопасности информации можно применять как методики ФСТЭК России и ФСБ России, так и другие методики
- Зная шаги атакующего, возможно построить эффективную систему защиты информации
- Применение продуктов Threat Intelligence позволит наладить процесс реагирования на события и инциденты ИБ
- Подключение к Центру мониторинга – повышение эффективности системы защиты информации

Вопросы?

A sunset scene with wind turbines and power lines. The sky is filled with orange and yellow clouds, and the sun is low on the horizon. In the foreground, several wind turbines are silhouetted against the bright sky. In the background, a series of high-voltage power lines stretch across the landscape. The overall mood is warm and serene.

Спасибо!