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

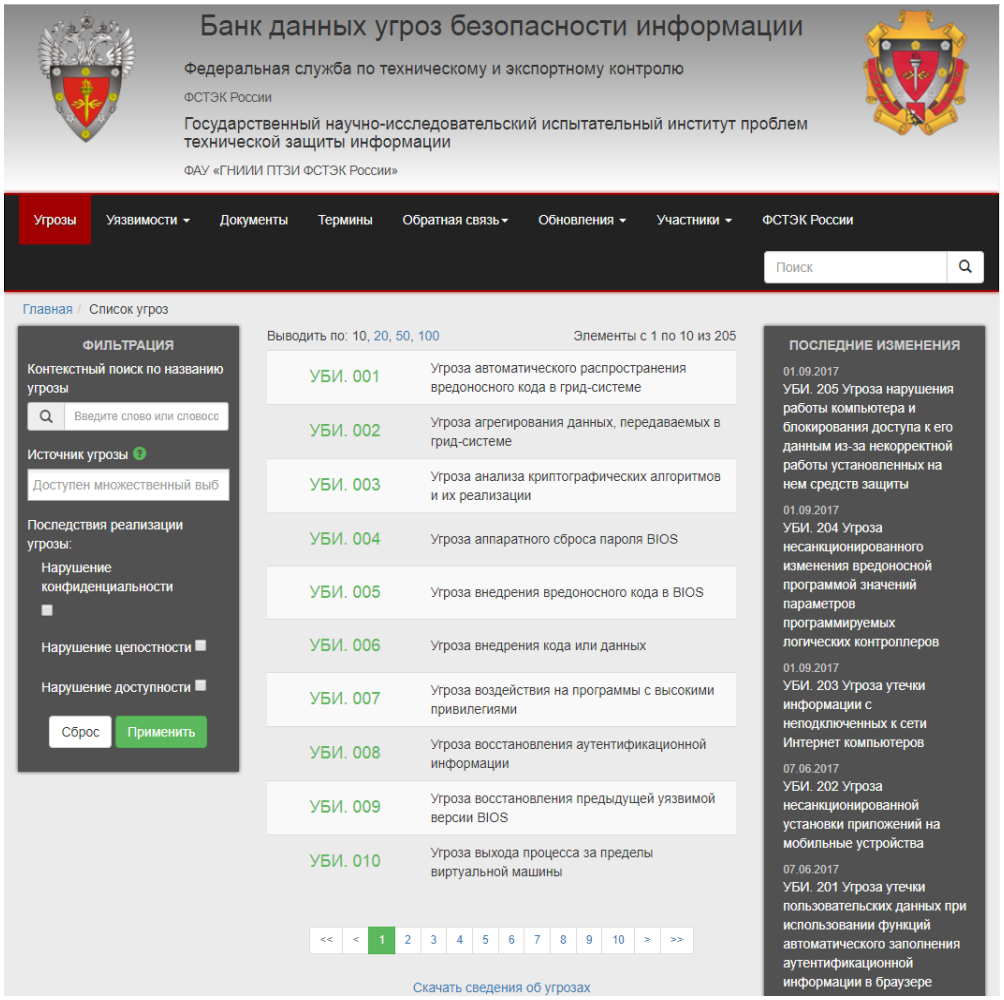
Моделирование угроз в РФ

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

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

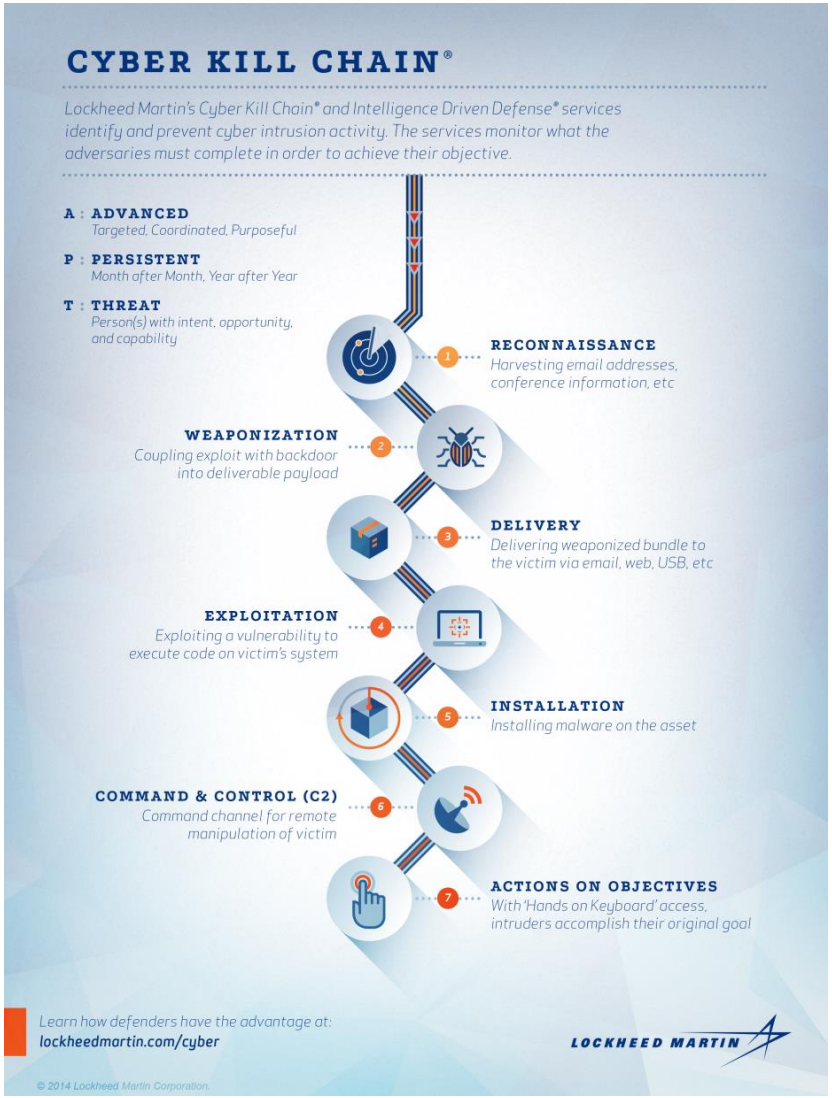
Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных

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



Cyber kill chain

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



Матрица ATT&CK

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

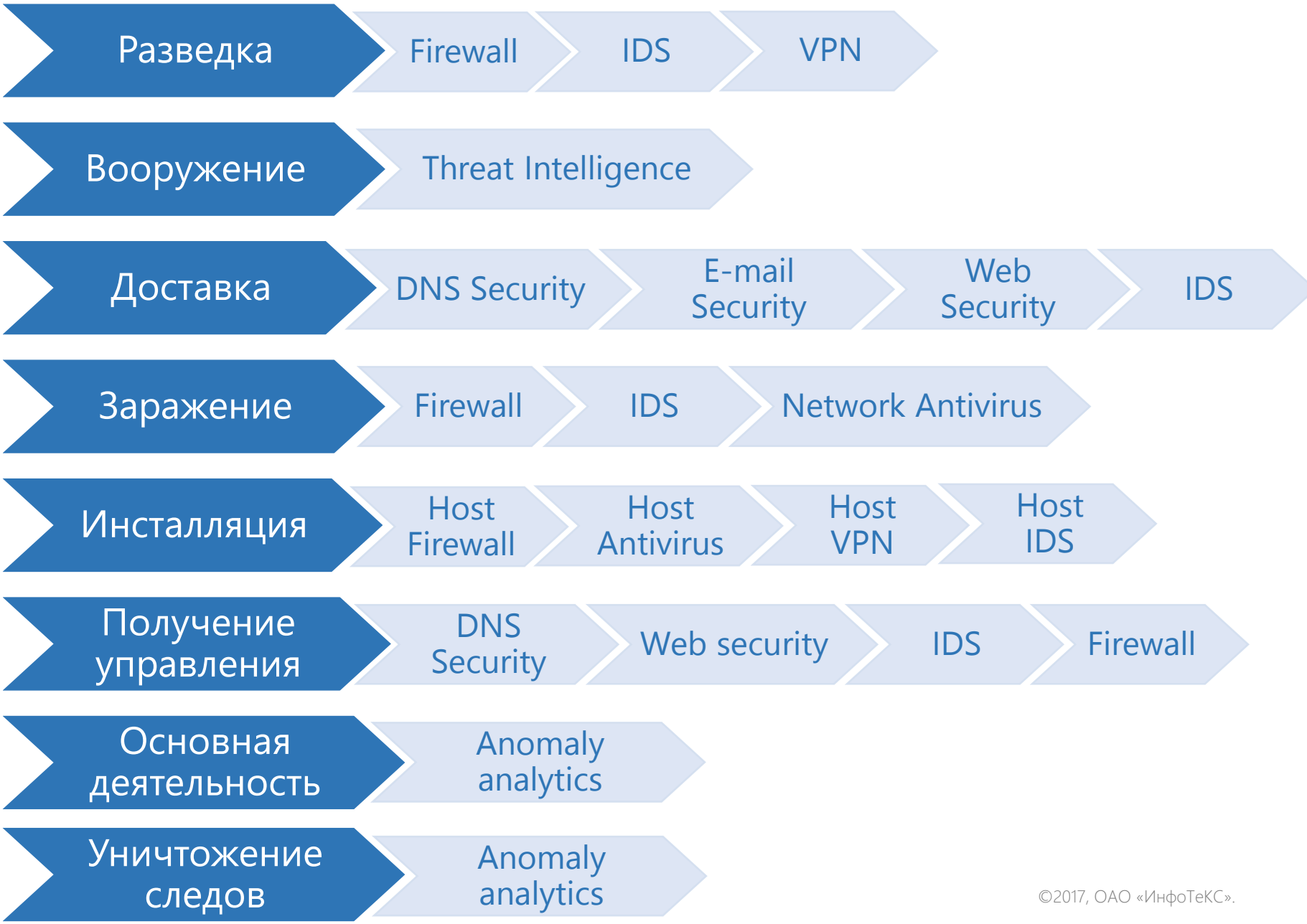
Kill Chain и ATT&CK

infotecs

Проектирование системы защиты информации

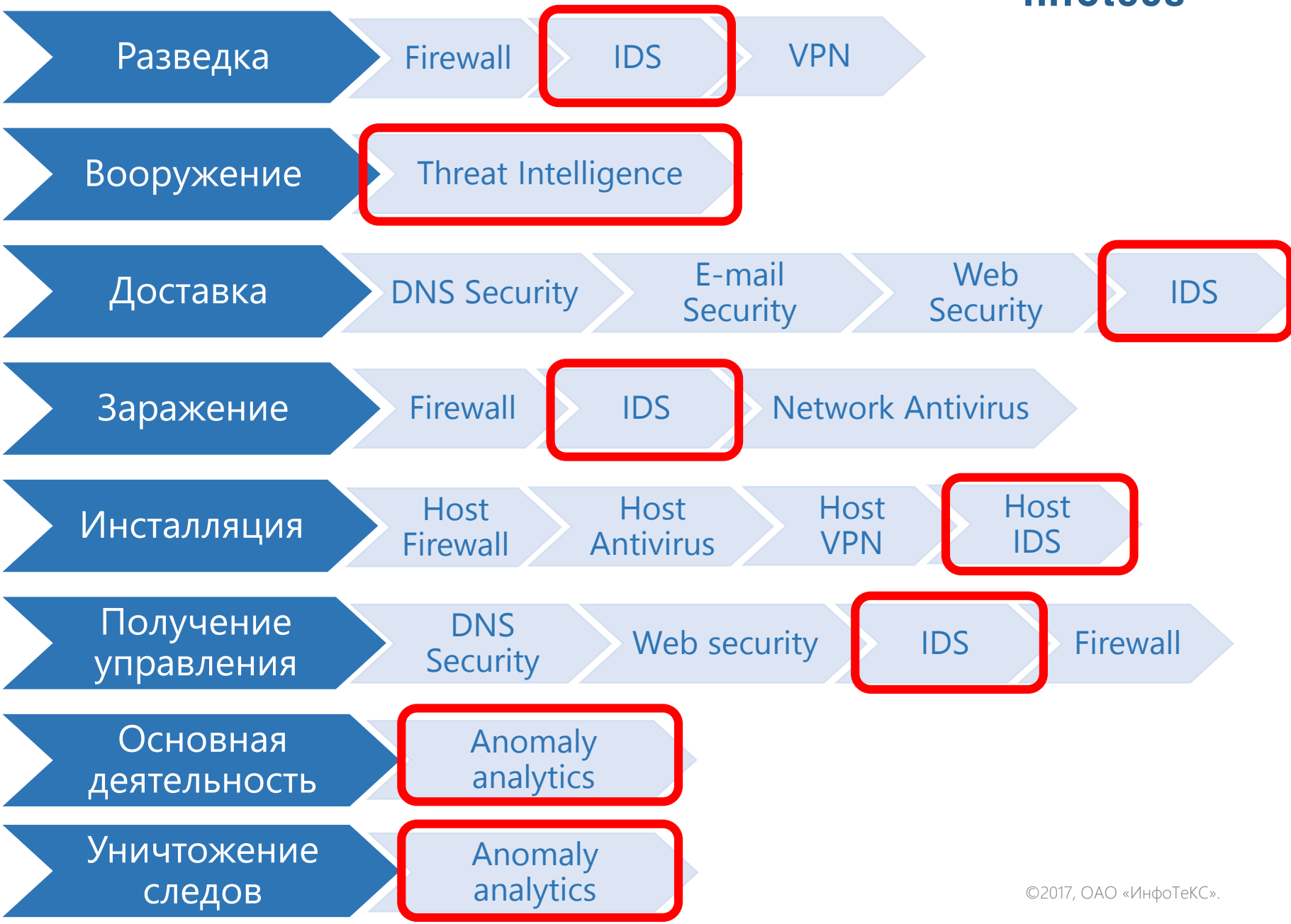
Проектирование системы защиты информации

Проектирование системы защиты информации



Проектирование системы защиты информации

infotecs



Реагирование на события ИБ

infotecs

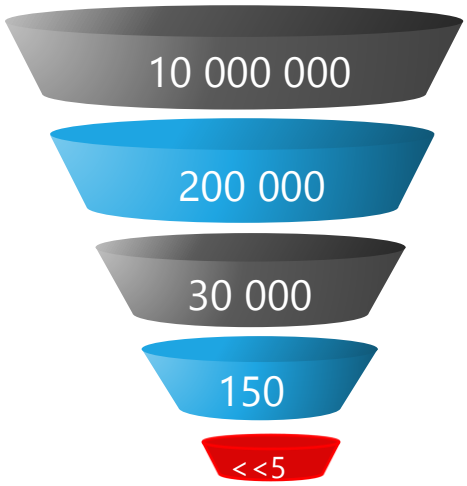
Применение концепции **Threat Intelligence**

Концепция Threat Intelligence

ViPNet TIAS

От регистрации событий к экспертизе

Месячная статистика для организации ~500 АРМ, 10 Серверов



События информационной системы

События сенсоров ИБ

Важные ИБ-события

Критичные события ИБ

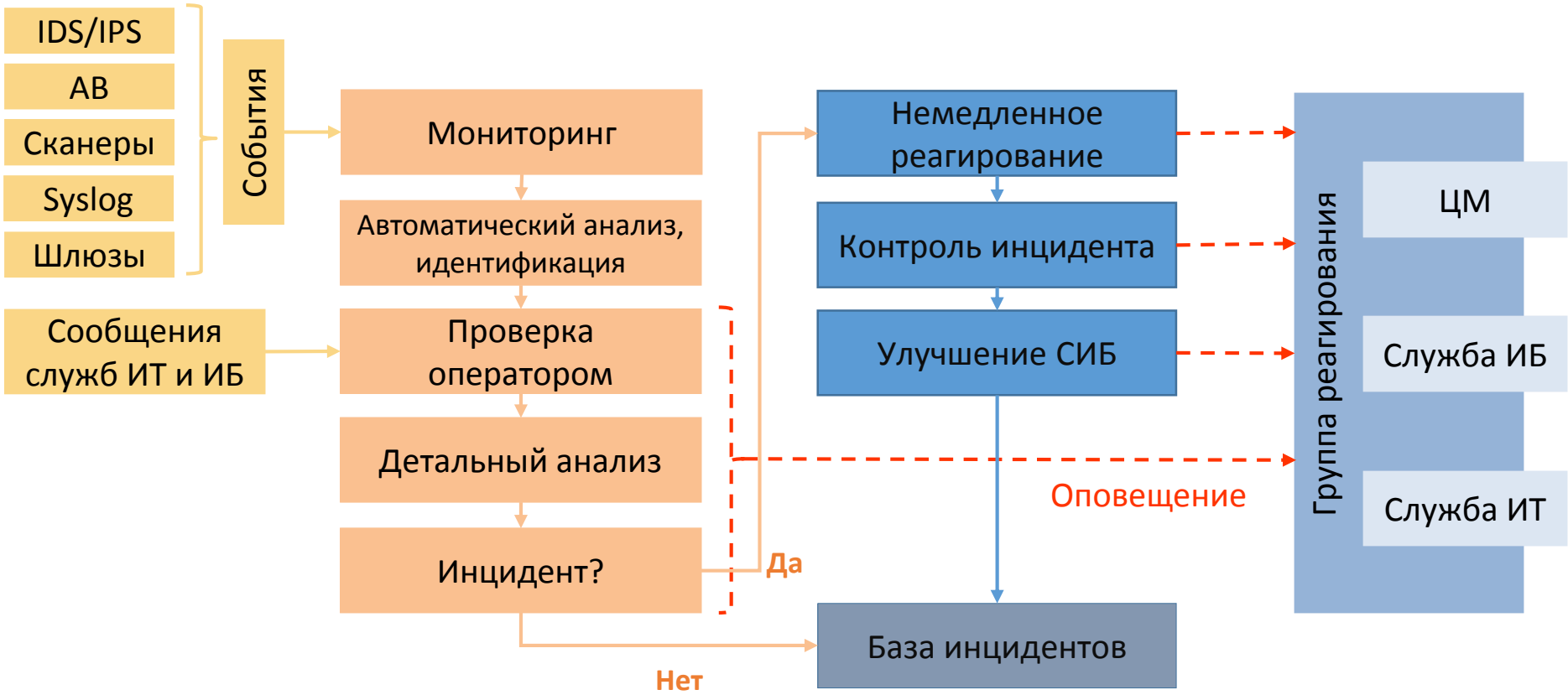
Инциденты ИБ

ViPNet IDS
Сетевые и хостовые сенсоры

ViPNet TIAS
- Обработка поступающих событий
- Выявление инцидентов безопасности
- Оповещение и отчетность

- **Работа аналитиков**

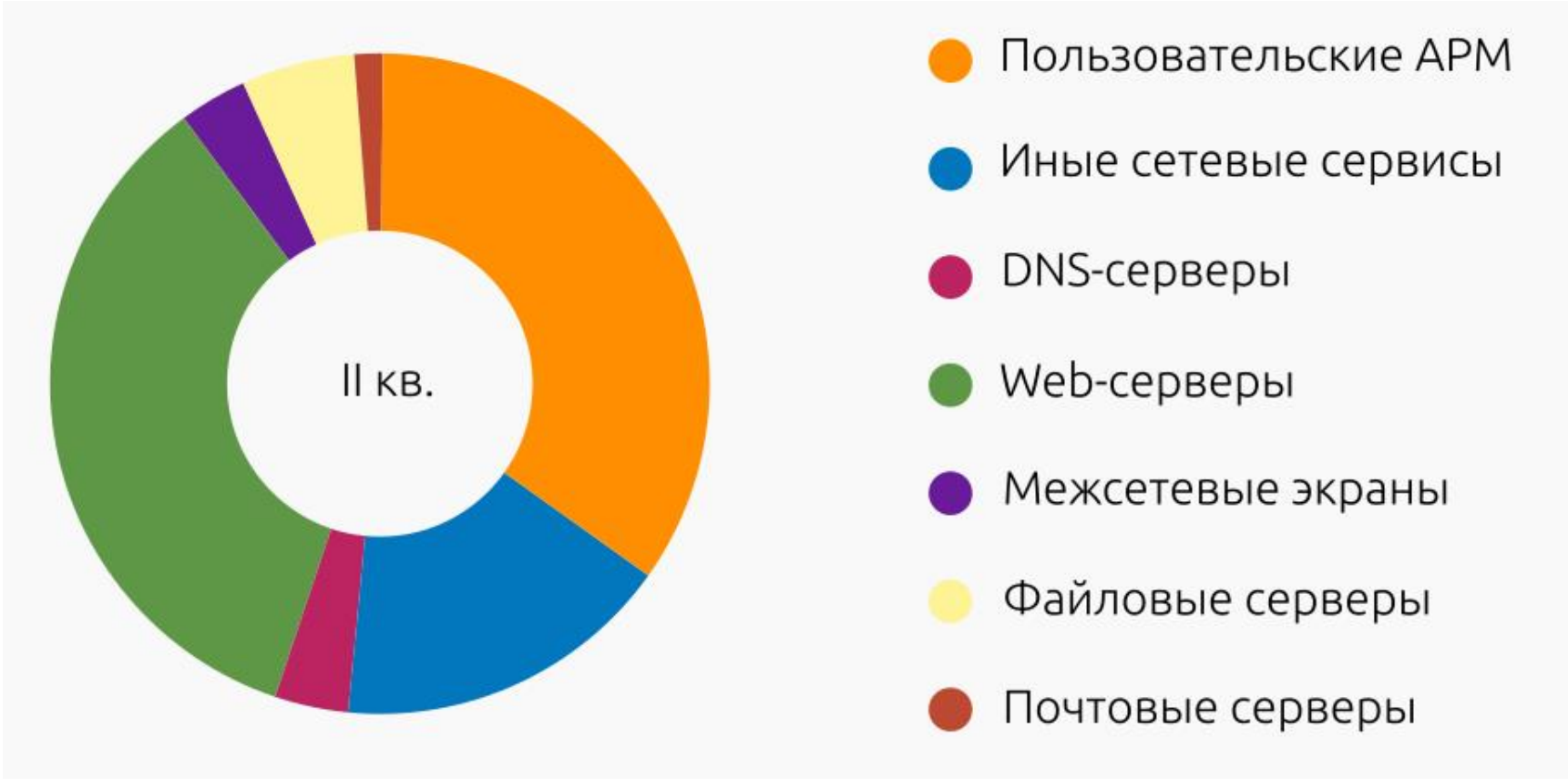
Формирование непрерывного процесса



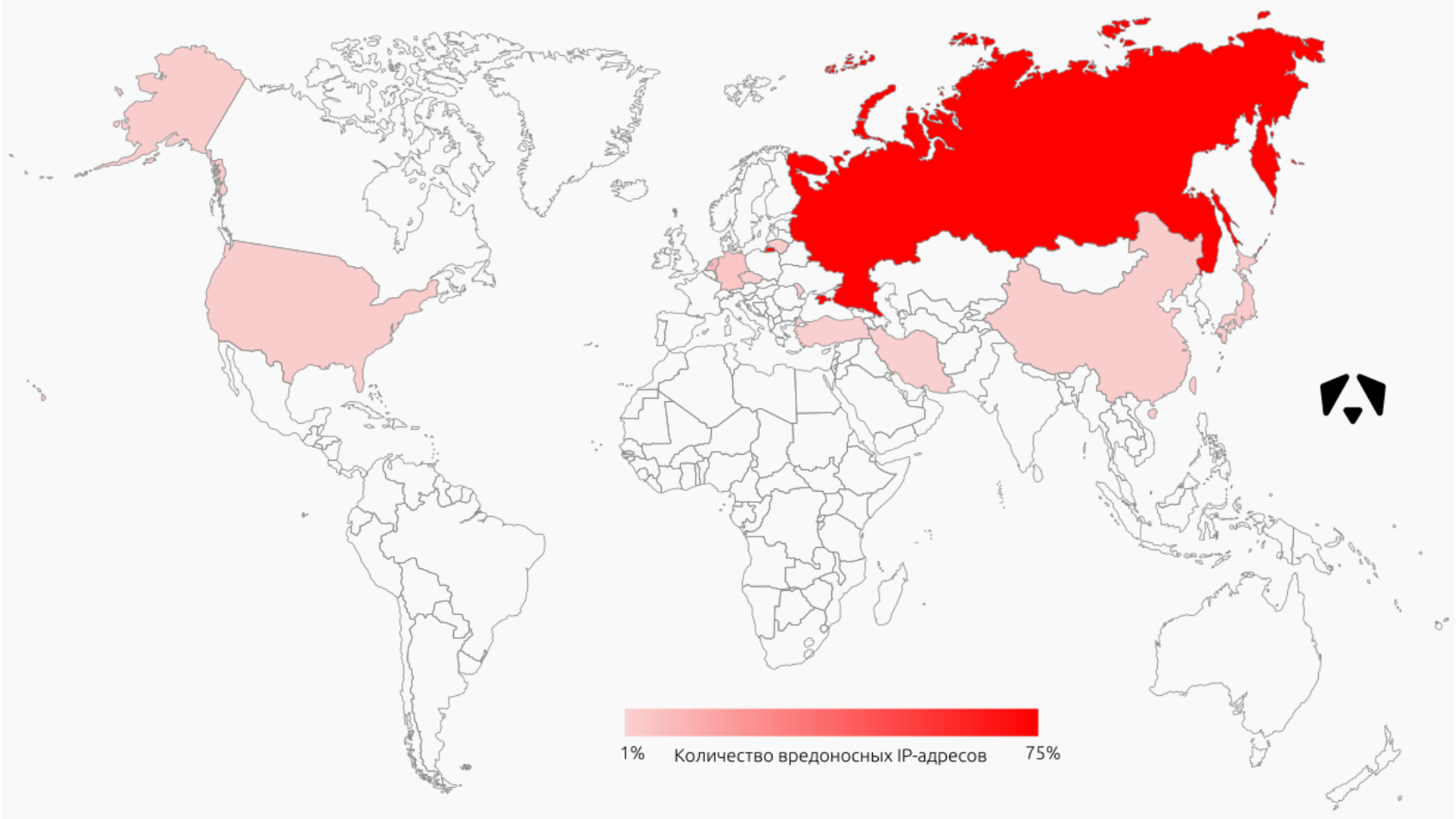
Статистика центра мониторинга

Центром мониторинга зафиксировано	
I квартал 2017	II квартал 2017
137 873 416 событий информационной безопасности	254 453 172 события информационной безопасности
98 инцидентов	144 инцидента

Распределение целей атак



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

infotecs

Вопросы?


Спасибо!