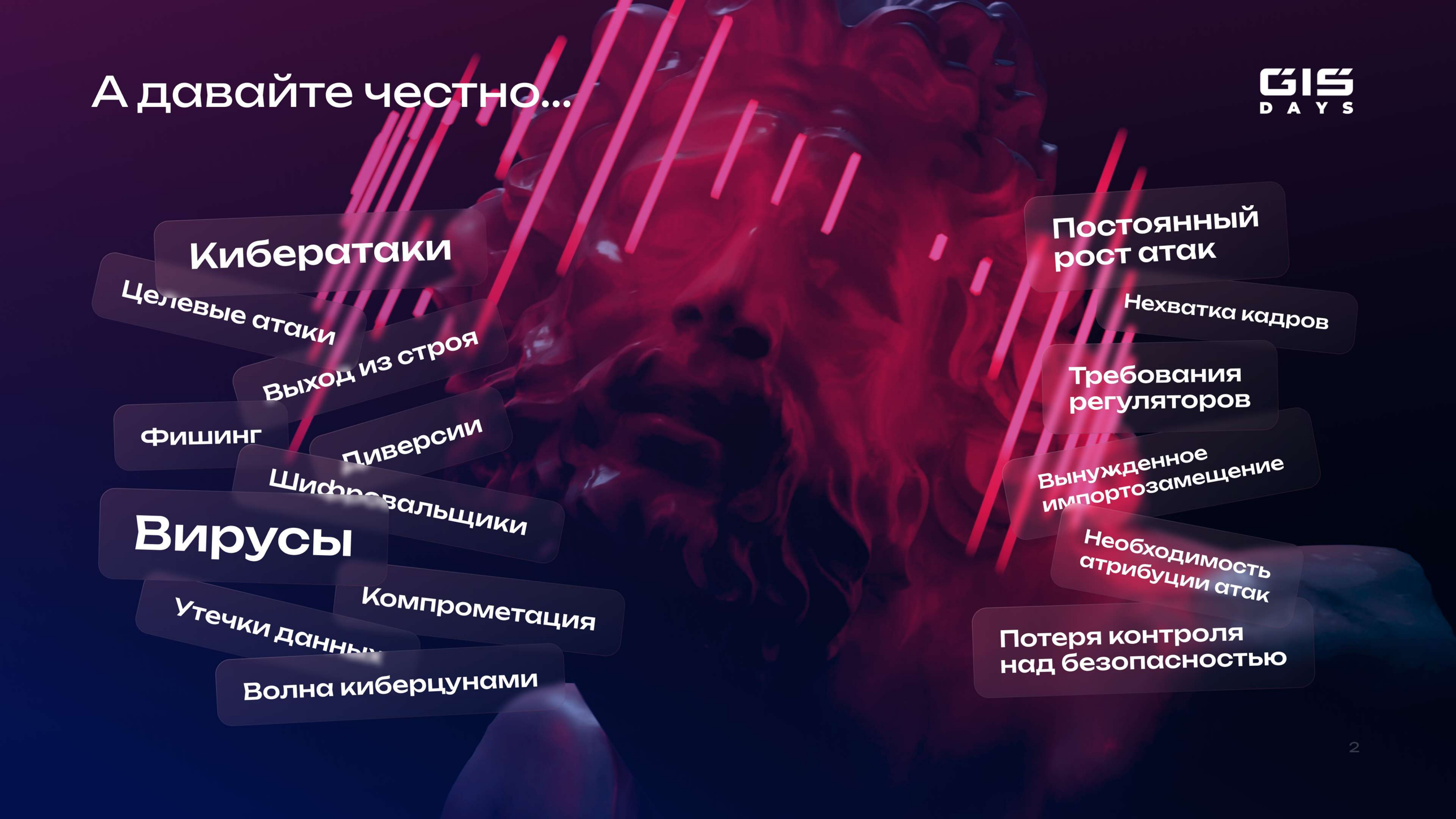
Николай Нашивочников
СТО, ООО «Газинформсервис»

Свежий взгляд на реагирование

Концепция раннего обнаружения

А давайте честно...



Кибератаки

Целевые атаки

Выход из строя

Фишинг

Диверсии

Шифровальщики

Вирусы

Компрометация

Утечки данны

Волна киберцунами

Постоянный рост атак

Нехватка кадров

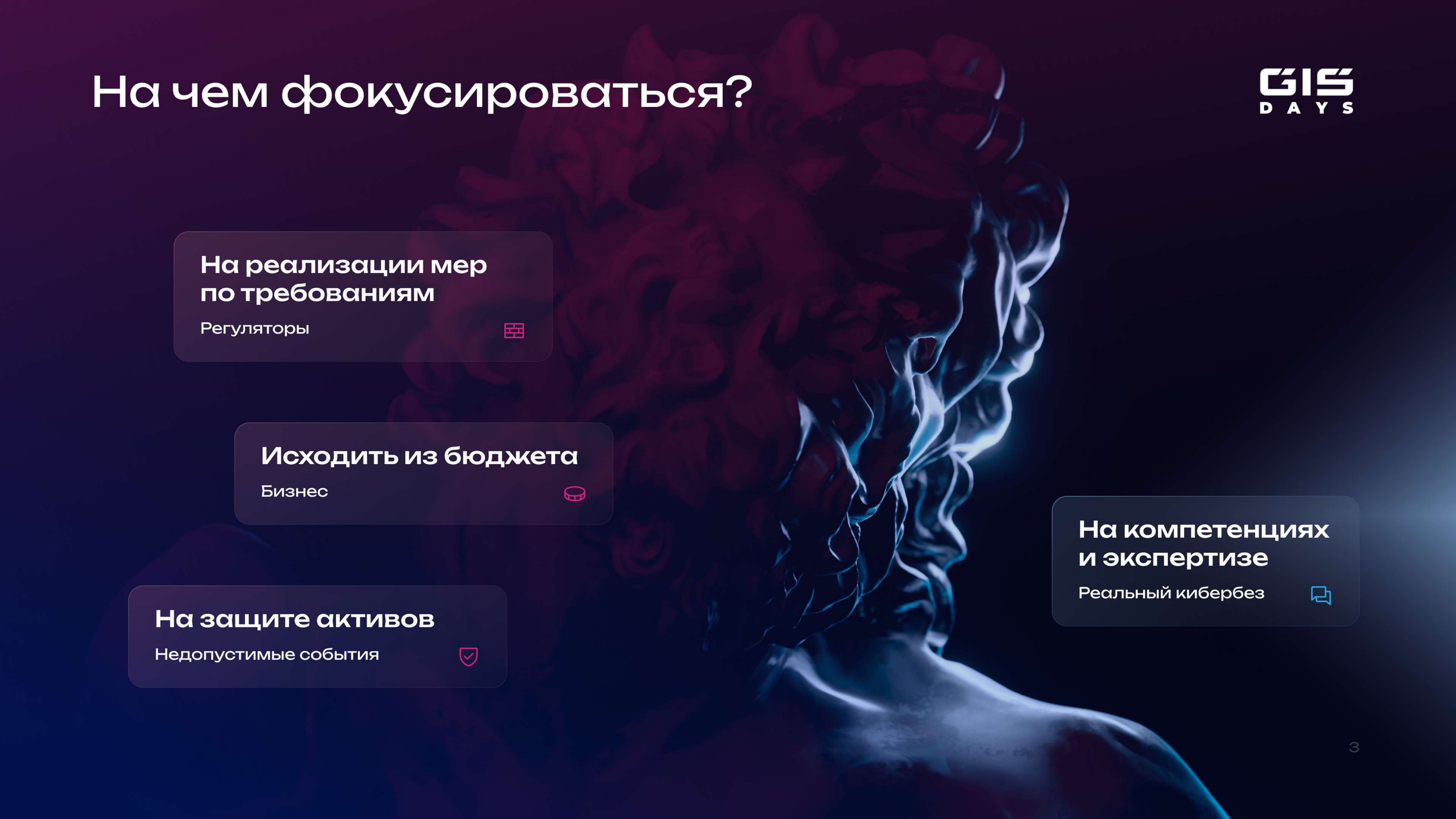
Требования регуляторов

Вынужденное импортозамещение

Необходимость атрибуции атак

Потеря контроля над безопасностью

На чем фокусироваться?



На реализации мер по требованиям

Регуляторы

Исходить из бюджета

Бизнес

На защите активов

Недопустимые события

На компетенциях и экспертизе

Реальный кибербез

Реальный кибербез

Предупреждение

Обязательно реализуйте базовый набор мер и средств защиты информации независимо от выбранного подхода:

Сегментирование сети, инвентаризация активов, разграничение доступа, принцип наименьших привилегий, расширенный аудит событий ИБ, регулярное сканирование на уязвимости ПО, анализ избыточности межсетевых правил, патч-менеджмент, обновление антивирусных баз и др.

Детектирование

- Опирайтесь на эффективные методики проактивного обнаружения
- Используйте расширенную аналитику для поиска неизвестных и сложных угроз
- Используйте преимущества модели федеративного обучения для сокращения времени обнаружения

Реагирование

- Сокращайте время реагирования за счет применения плейбуков и адаптивных шаблонов расследования
- Используйте XDR решения для комплексного реагирования на конечных точках и за их пределами
- Используйте решения Deception (приманок) для отвода угроз от корпоративного сегмента

Модели атак и классификаторы

GIS DAYS

БДУ ФСТЭК РФ

- 2015 — Создание Банка данных угроз ФСТЭК РФ
- 2020 — Насчитывает 222 угрозы безопасности информации
- 2022 — Введение в опытную эксплуатацию нового раздела угроз безопасности информации
- 2023

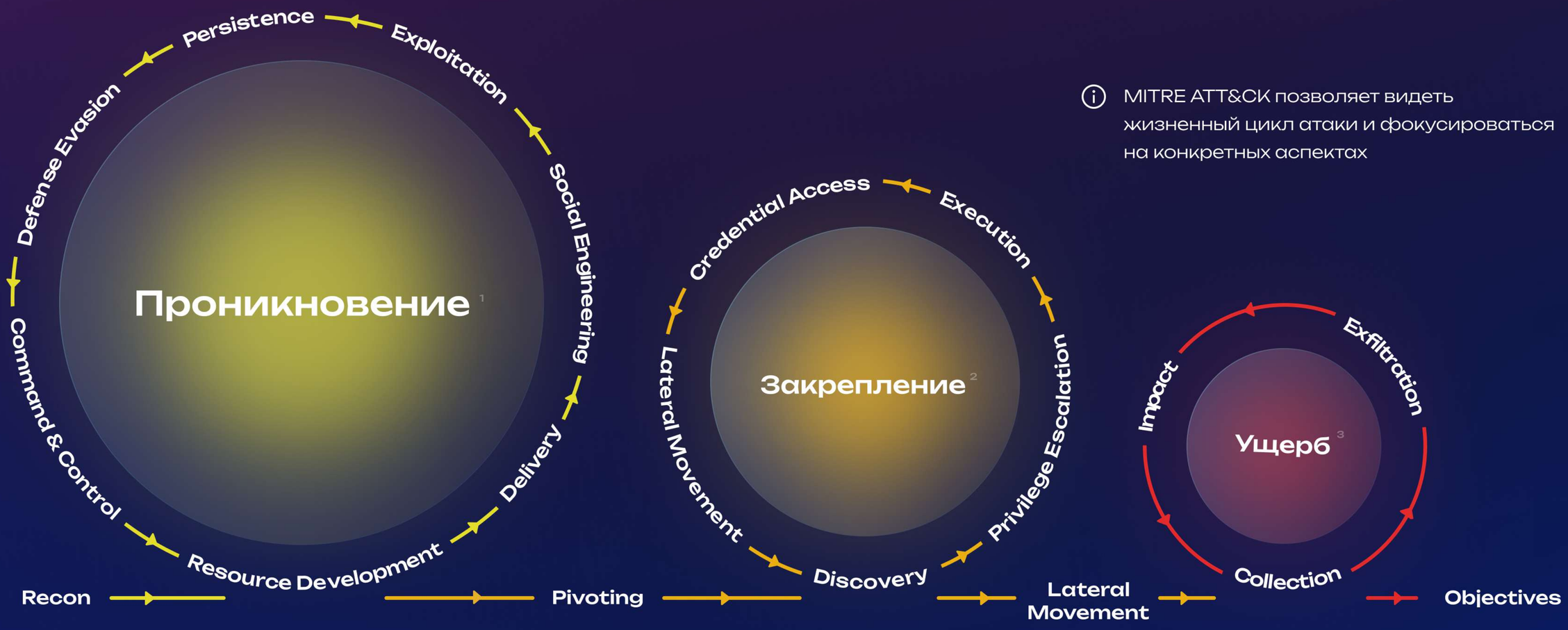
LOCKHEED MARTIN

- 2011 — Lockheed Martin Cyber Kill Chain
- 2015 — Corey Nachreiner Kill Chain 3.0 (Lateral Movement & Pivoting)
- 2016 — Sean Malone Expanded Cyber Kill Chain Model
- 2017 — Bryant Kill-Chain
- 2023

MITRE | ATT&CK

- 2013 — Эксперимент Fort Meade Experiment (FMX) MITRE ATT&CK
- 2015 — Расширение до 121 техники по сравнению с первоначальными 96
- 2017 — Paul Pols Unified Kill Chain Сочетание элемент. цепочки кибер-убийств и ATT&CK
- 2017 — API+ 169 техник для Windows, Mac и Linux
- 2018 — ATT&CK v3
- 2019 — ATT&CK v5
- 2023 — **ATT&CK v13** 14 тактик, 196 приемов, 411 подтехник, 138 групп и тд.

Жизненный цикл кибератаки



ⓘ MITRE ATT&CK позволяет видеть жизненный цикл атаки и фокусироваться на конкретных аспектах

[1] Getting In [2] Hacking Throught [3] Taking It Out

Топ векторов проникновения

Fortinet

Атаки на облачные сервисы

Replication Through Removable Media	60%
Phishing	28%
Drive-by Compromise	5%
Exploit Public-Facing Application	4%
External Remote Services	2%
Valid Accounts	1%

Kaspersky

Атаки с шифровальщиком

Exploit Public-Facing Application	42,86%
Compromised Accounts	23,81%
Phishing	11,9%
Другое	11,9%
External Remote Services	9,52%

UNICC

Атаки на объекты ООН

Phishing	29%
Valid Credentials	27%
External Remote Access Services	17%
Другое	15%
Exploit Public-Facing Application	12%

Mandiant

Начальный вектор заражения

Exploit Public-Facing Application	32%
Phishing	22%
Compromised Accounts	14%
Prior Compromise	12%
Остальное	10%
Website Compromise	7%
Brute Force	4%

CheckPoint

Доставка вредоносного ПО

Phishing	86%
Exploit Public-Facing Application	14%

* Использованы отчеты за 2022 год: Mandiant M-Trends, Kaspersky, Fortinet, CheckPoint, UNICC

Нужно ли понимать, куда пойдет хакер?

GIS DAYS

Проникновение

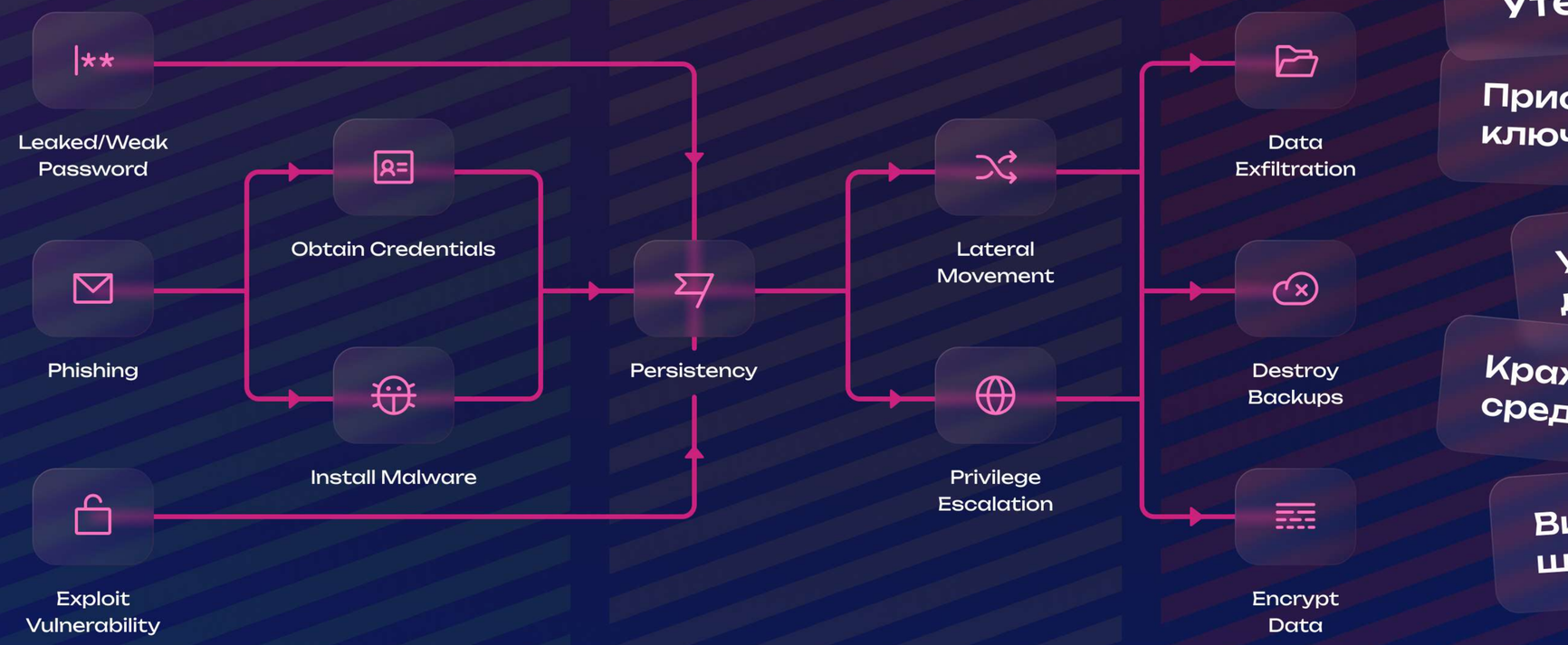
Наилучшее время для обнаружения и реагирования

Закрепление

Последняя попытка

Ущерб

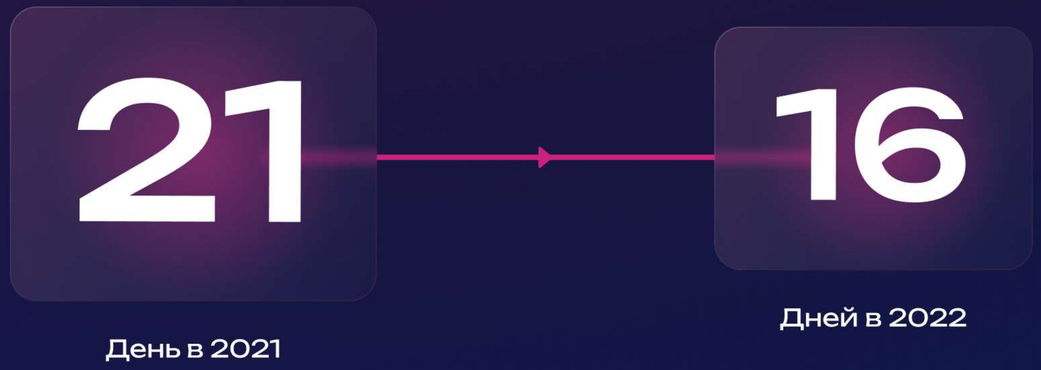
Слишком поздно

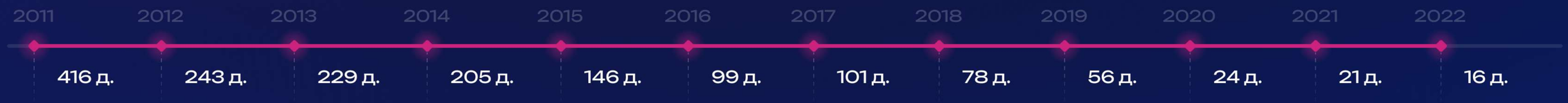


- Утечка данных
- Приостановка ключевых сервисов
- Уничтожение документов
- Кража денежных средств
- Вирус-шифровальщик

Как долго нарушитель остается незамеченным?

Среднее время по миру составляет **16 дней**, а в европейском регионе **до 22 дней**





* По данным отчета Mandiant M-Trends 2023

Огромный объем данных

XDR BI Федеративное обучение

UEBA Выявление аномалий ML TDA *

Rule-based методы

* TDA — топологический анализ данных

Изменит ли ситуацию ИИ?

Новые проблемы *	Решения
Атака протекает быстро, значит надо быстро реагировать	Федеративное обучение в агентах EDR\XDR
Большие данные, многообразие журналов - SIEM утопают в десятках тысяч EPS	Применение каскада алгоритмов ML для обработки и анализа данных
	Расширение моделей контекстными данными
	Выявление зловредных паттернов поведения, O-day атак
В атаках всё больше используются легитимные утилиты (cmd, powershell, bash и др.)	За счет предобученных классификаторов ИИ упрощает и ускоряет детектирование

* Приведена часть проблем

Наши шаги в ИИ

GIS DAYS

ПОЛИТЕХ
Санкт-Петербургский политехнический университет Петра Великого

R&D при участии Лаборатории искусственного интеллекта СПБПУ Петра Великого и исследовательского центра «Газинформсервис»

STANDOFF 365

Апробация раннего выявления атак с LolBins.
2 из 10 атак были выявлены на более ранних этапах, чем с использованием rule-based подхода

MITRE | ATT&CK®

Детектирование атак в 8 из 9 техниках Initial Access по матрице MITRE ATT&CK Enterprise

GIS ГАЗИНФОРМ СЕРВИС

Создание цифровых теней объектов инфраструктуры и выявление поведенческих аномалий

Ankey ASAP

Ankey ASAP — аналитическая платформа обработки больших данных о событиях кибербезопасности с функциями поведенческого анализа и расследования инцидентов

- Обобщение и систематизация алертов с помощью MITRE ATT&CK
- UEBA — поведенческий анализ пользователей, сущностей, атак
- Инструменты расследования инцидентов

И напоследок

Проводите своевременную инвентаризацию активов, внедряйте патч-менеджмент, менеджмент уязвимостей

Повышайте уровень базовых систем кибер-безопасности, используйте не только rule-based, но и методы расширенной аналитики, фокусируйтесь на практической безопасности и раннем реагировании

Атаки начинаются не с защищенных серверов, а с наиболее простых мишеней (обычных пользователей и их устройств)

Применение машинного обучения для анализа данных безопасности и подхода раннего обнаружения обусловлено меняющейся природой хакинга

Николай Нашивочников
СТО, ООО «Газинформсервис»

GIS DAYS

Спасибо за внимание!