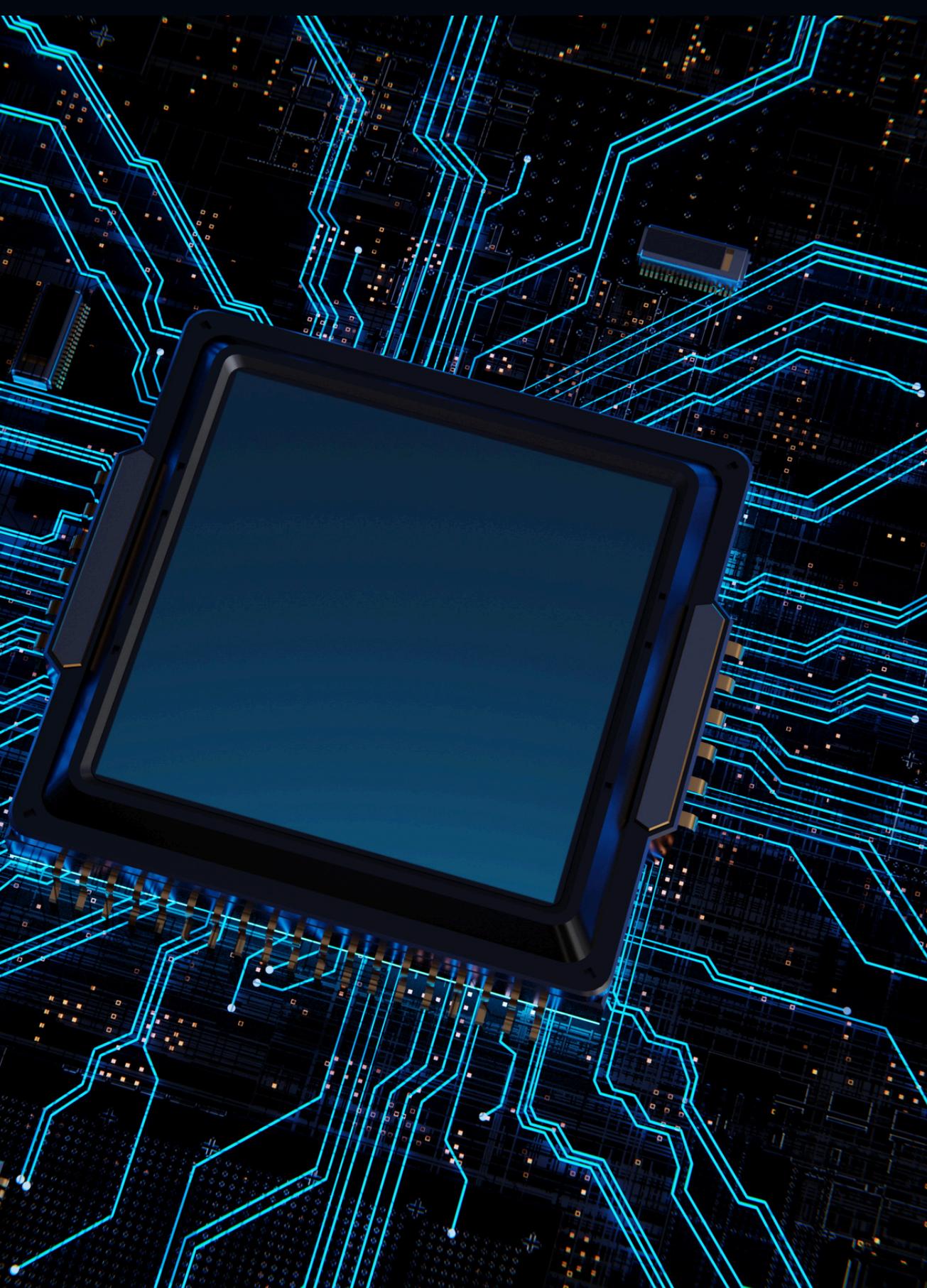


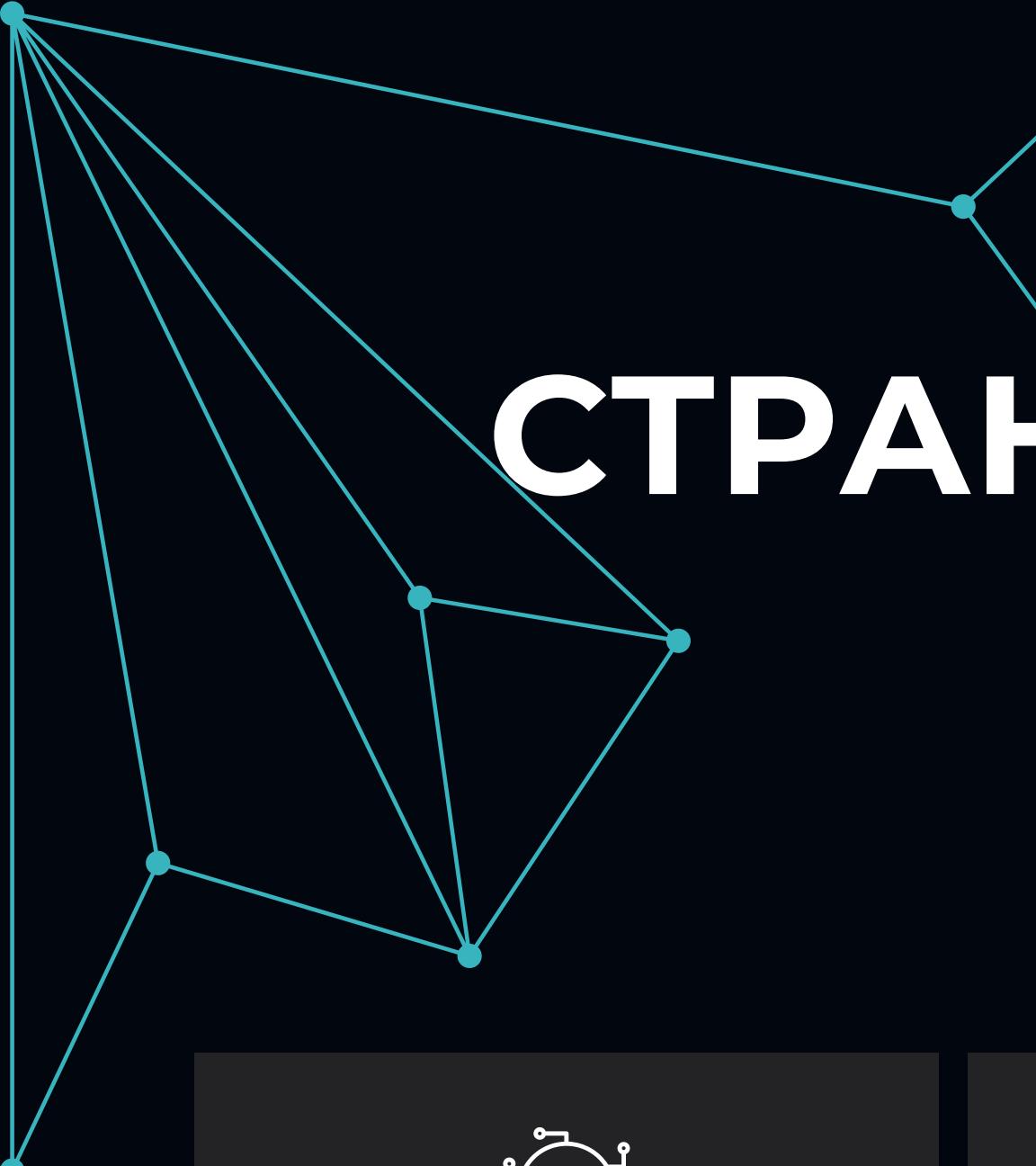
# КИБЕРВОЙНЫ: МИФ ИЛИ РЕАЛЬНОСТЬ?

KOSHONBAI KYZY MALIKA  
CS-11



# КИБЕРВОЙНЫ: МИФ ИЛИ РЕАЛЬНОСТЬ?

- Кибератаки стали инструментом геополитики
- Государства разрабатывают собственное кибероружие
- Утечки и взломы могут иметь глобальные последствия
- Ключевой кейс: *Shadow Brokers* и оружие АНБ



# СТРАННОЕ СООБЩЕНИЕ НА GITHUB

## ИСТОРИЯ №1



13 августа 2016 года на GitHub появилось странное сообщение от неизвестного пользователя.



Текст был на ломаном английском, с громкими заявлениями и ссылками на файлы.



Для обычных пользователей — шутка, для специалистов — **реальные инструменты кибершпионажа АНБ.**



Это стало началом крупнейшей утечки кибероружия в истории.

# КАК ДЕЙСТВОВАЛИ SHADOW BROKERS

Equation Group — кто это?

Секретное подразделение АНБ США, элитная кибергруппа, известная сложными атаками вроде Stuxnet, с технологиями недоступными обычным хакерам.

Шпионские разработки Equation Group

Инструменты для скрытого контроля устройств: Cottonmouth (USB-имплант), Dropoutjeep (iPhone-бэкдор), Ragemaster (перехват изображения с монитора). Всё строго засекречено.



**Август 2016** — Shadow Brokers заявили о взломе Equation Group



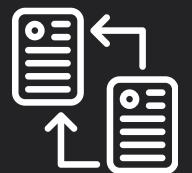
- Выложили реальные эксплойты и бэкдоры в сеть
- Предлагали «продать» данные миру, демонстрируя силу



Цель — вызвать панику и поставить под сомнение неприкосновенность АНБ



# РАССЛЕДОВАНИЕ КИБЕРИНЦИДЕНТА: КАКИЕ ВЕРСИИ?



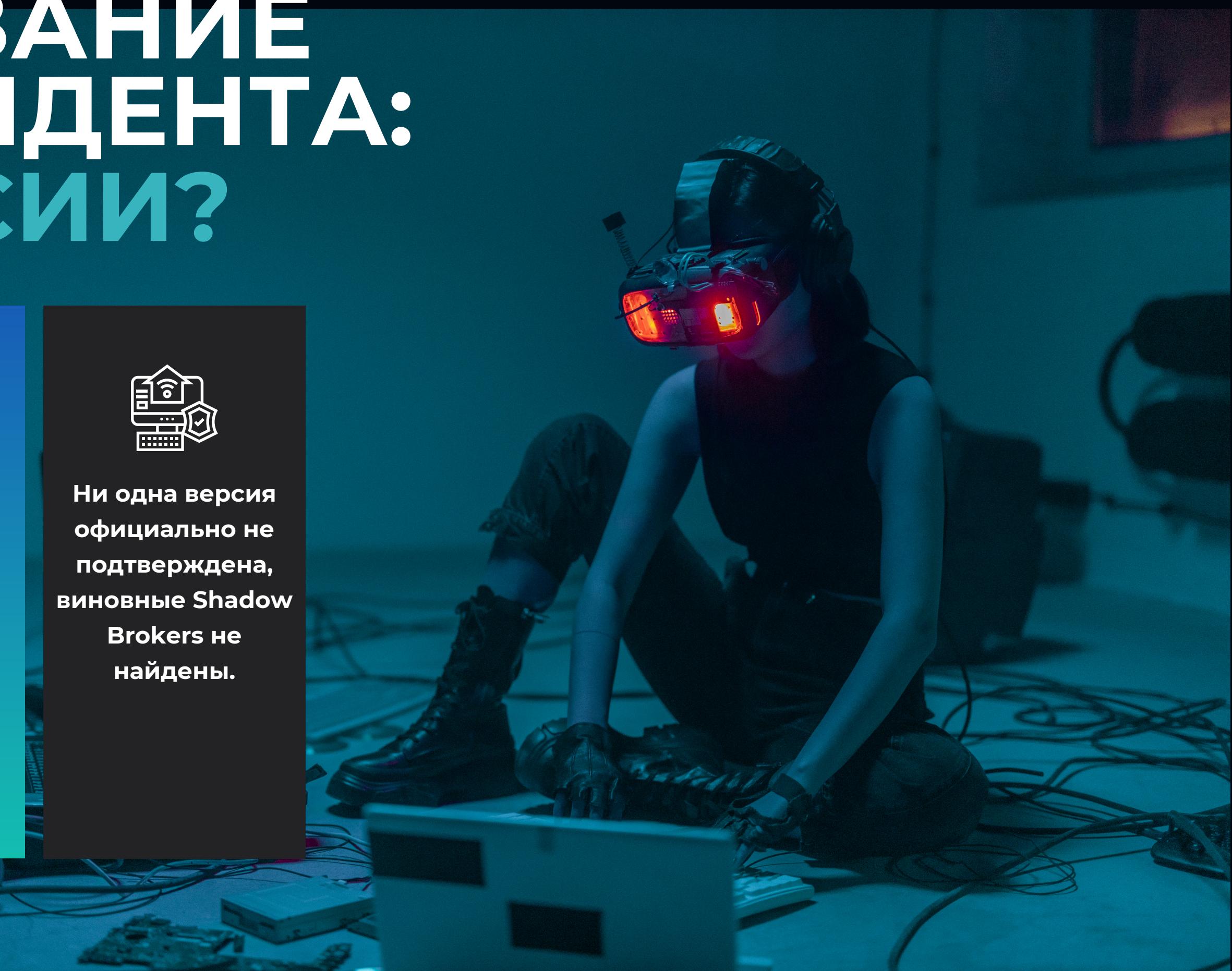
Возможный  
инсайдер  
внутри АНБ,  
подобно  
Сноудену.



Внешняя атака  
независимых хакеров для  
шантажа или прибыли.  
Действия иностранных  
государств,  
использующих утечку в  
своих интересах.



Ни одна версия  
официально не  
подтверждена,  
виновные Shadow  
Brokers не  
найдены.



# ПОДЗРЕВАЕМЫЙ НАЙДЕН

ФБР и АНБ сосредоточились на Гарольде Томасе Мартине III, бывшем подрядчике, имевшем доступ к засекреченным материалам АНБ и других спецслужб. У него нашли 50 терабайт секретных данных. Мартин признал незаконное хранение материалов, но доказательств того, что он был Shadow Brokers, не нашли.

## Гарольд Томас Мартин III

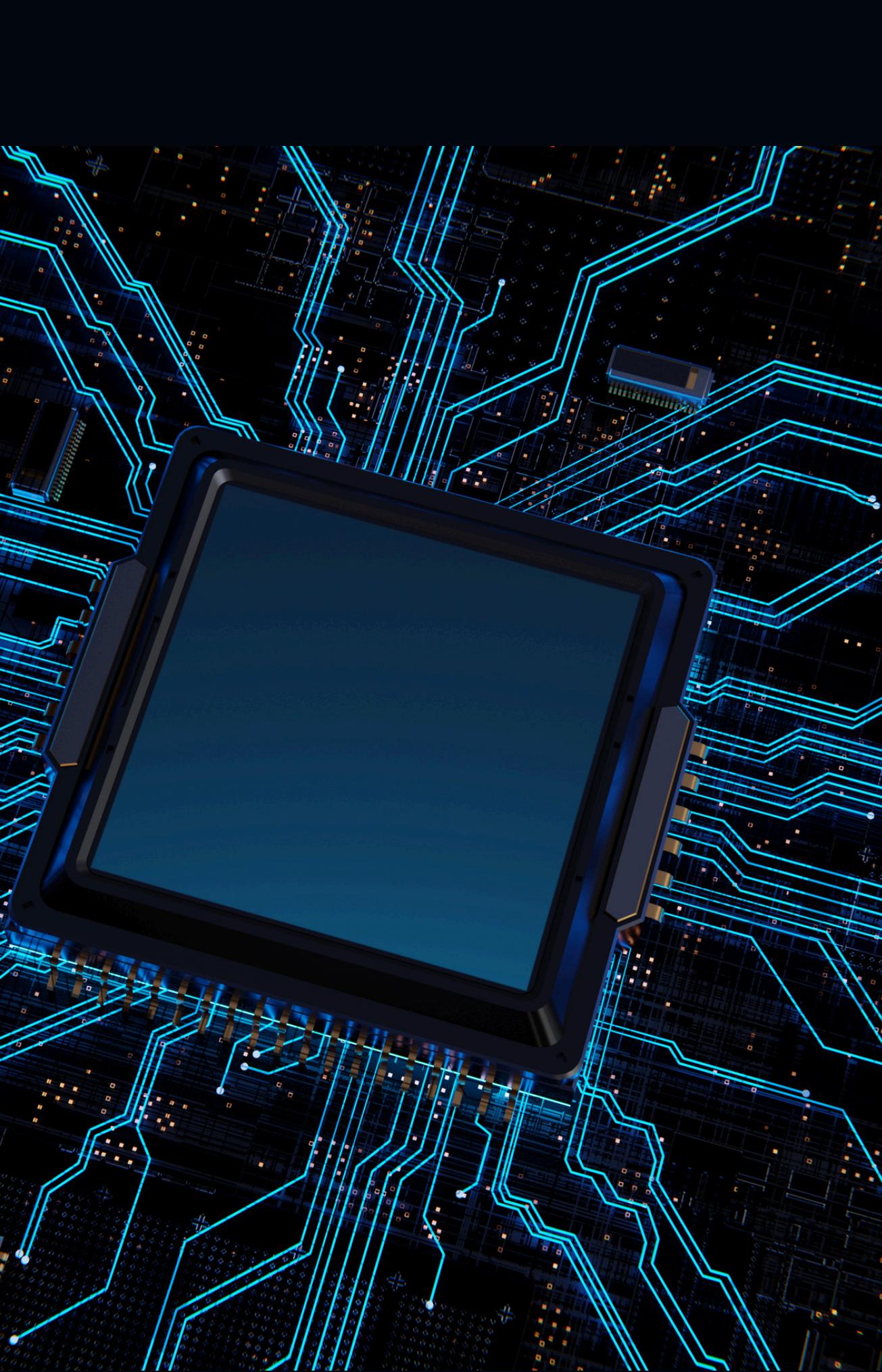
- Гарольд Томас Мартин III — бывший подрядчик АНБ
- Имеет доступ к засекреченным материалам нескольких спецслужб
- Обнаружено 50 терабайт секретных данных
- Признал незаконное хранение, но не являлся Shadow Brokers



# ВТОРОЕ ПОСЛАНИЕ SHADOW BROKERS

В сентябре 2016 года Shadow Brokers опубликовали новые данные и сделали громкие заявления, направленные на американские власти. Они снова выложили киберинструменты и продолжили насмехаться над АНБ и Белым домом. Послания носили вызывающий характер, включали политические комментарии и демонстрировали, что группа контролирует информацию о кибероружии США, ставя под сомнение неприкосновенность АНБ.

- Сентябрь 2016 — новые утечки и послания Shadow Brokers
- Громкие политические заявления против США и АНБ
- Публикация дополнительных киберинструментов
- Цель — вызвать панику и показать контроль над секретной информацией



# ЧТО СОДЕРЖАЛА НОВАЯ УТЕЧКА ОТ SHADOW BROKERS

Новая утечка включала списки IP-адресов, доменов и серверов, через которые АНБ якобы осуществляло кибератаки по всему миру. Эксперты проверяли данные и находили подтверждение в логах атак в Азии, Европе и на Ближнем Востоке. Эта информация показала, что даже самые защищённые серверы АНБ уязвимы и подвергаются контролю со стороны внешних лиц.

- Списки IP-адресов, доменов и серверов АНБ
- Подтверждение активности в логах атак по миру
- Демонстрация уязвимости даже самых защищённых систем
- Подрыв иллюзии неприкосновенности АНБ

# КАК ДЕЙСТВОВАЛИ SHADOW BROKERS

В апреле 2017 года на платформе Medium Shadow Brokers обратились к Дональду Трампу с политическим посланием, критикуя его действия. В конце поста они опубликовали пароль к ранее выложенному зашифрованному архиву, содержащему 67 эксплойтов для Windows, включая EternalBlue, инструменты для удалённого управления и вредоносные драйверы. Эта утечка дала хакерам доступ к мощному кибероружию АНБ.



**Апрель 2017** — послание на Medium с обращением к Дональду Трампу



- Политическая критика и насмешки над США
- Публикация пароля к зашифрованному архиву



- В архиве — 67 эксплойтов, включая EternalBlue и инструменты АНБ
- Утечка дала доступ к мощному кибероружию



# ЗАКЛЮЧЕНИЕ

## **Ящик Пандоры открыт**

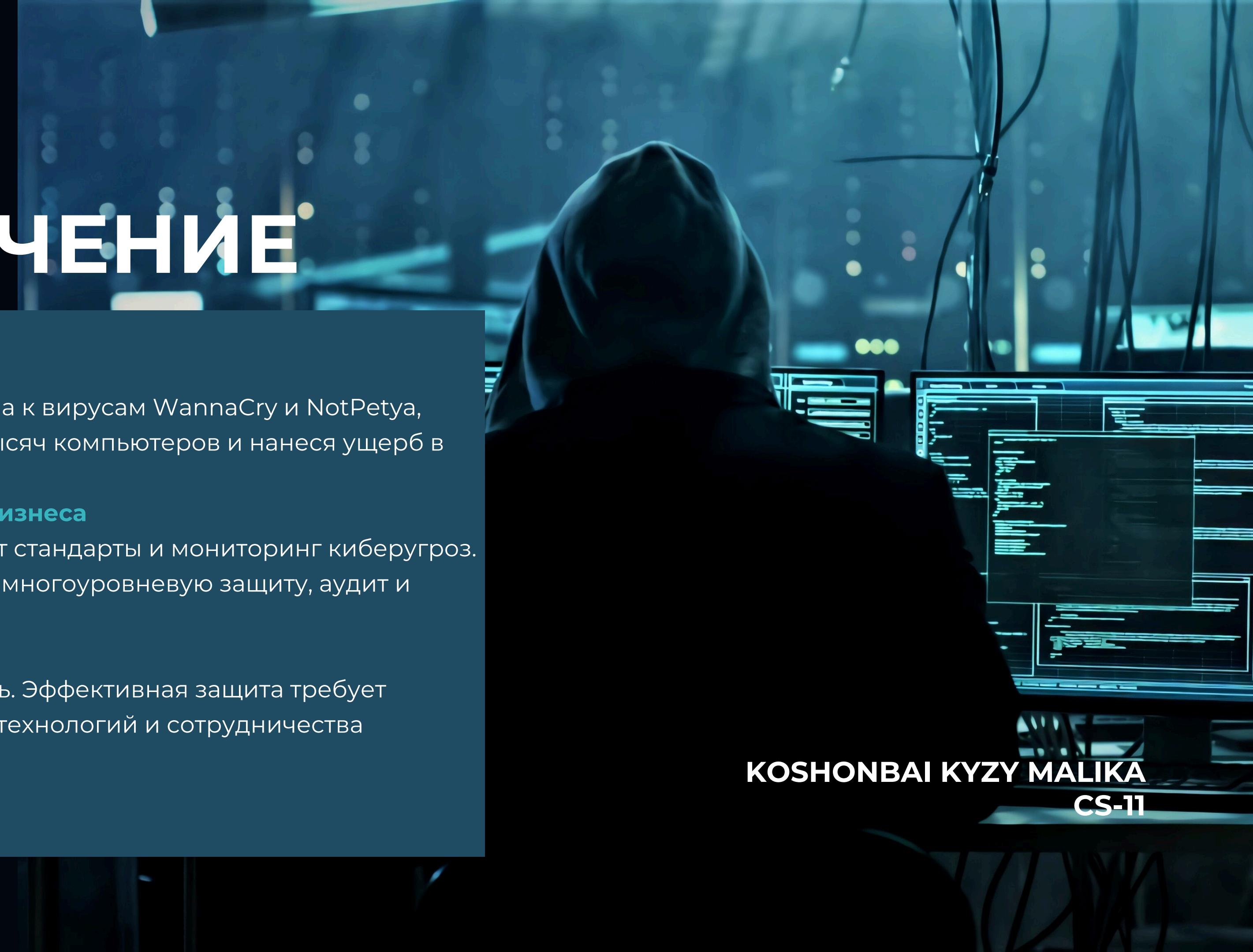
Утечка EternalBlue привела к вирусам WannaCry и NotPetya, парализовавшим сотни тысяч компьютеров и нанеся ущерб в миллиарды долларов.

## **Государство на защите бизнеса**

Государство обеспечивает стандарты и мониторинг киберугроз. Для бизнеса важно иметь многоуровневую защиту, аудит и обучение персонала.

## **Заключение**

Кибервойны — реальность. Эффективная защита требует постоянного обновления технологий и сотрудничества государства и бизнеса.



KOSHONBAI KYZY MALIKA  
CS-11