КИБЕР БЕЗ

WWW.TEACHMESKILLS.BY

КИБЕРБЕЗОПАСНОСТЬ

С НУЛЯ

СТАНЬ ВОСТРЕБОВАННЫМ СПЕЦИАЛИСТОМ ПО КИБЕРБЕЗОПАСНОСТИ, КОТОРЫЙ ВЫЯВЛЯЕТ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И РИСКИ ПОТЕРИ ДАННЫХ.

ПАРА ПРАВИЛ

ВО ВРЕМЯ КУРСА

1. ВСЕ ВОПРОСЫ ЗАДАВАЙТЕ В ТЕЛЕГРАМ В СПЕЦИАЛЬНОМ РАЗДЕЛЕ.
2. ОБЩЕНИЕ - БЕЗ ПЕРЕХОДА НА ЛИЧНОСТИ, ПОЛИТИКИ, РЕЛИГИИ И Т.Д.
3. В ИТ-СФЕРЕ ПРИНЯТО ОБЩЕНИЕ НА "ТЫ" ВНЕ ЗАВИСИМОСТИ ОТ ВОЗРАСТА, И РАНГА.
4. ПРОСЬБА, ПО ВОЗМОЖНОСТИ, ВКЛЮЧАТЬ СВОИ КАМЕРЫ.
5. ДОМАШНИЕ ЗАДАНИЯ ПРОВЕРЯЮ В ТЕЧЕНИЕ ПАРЫ ДНЕЙ ПРИ СДАЧЕ ИХ В СРОК.
6. ЕСЛИ Д/З СДАНО НЕ В СРОК - ПРОВЕРЯЮ, КАК БУДЕТ СВОБОДНОЕ ВРЕМЯ.
7. ЕСЛИ ВО ВРЕМЯ ЛЕКЦИИ ГОВОРЮ НЕПОНЯТНОЕ СЛОВО, НЕ ОБЪЯСНИВ ЕГО - ПИШИТЕ ВОПРОС В ЧАТ)

ПРИНЯТЬ ОТКЛОНИТЬ

ПАРУ СЛОВ О СЕБЕ

1. ФИО
2. ОБРАЗОВАНИЕ
3. ПРОФЕССИЯ
4. ПОЧЕМУ ВЫБРАЛИ КИБЕРБЕЗ?
5. ЧТО ЖДЁТЕ ОТ КУРСА?
6. УРОВЕНЬ АНГЛИЙСКОГО

ПЕРВЫЕ КОМП. ВИРУСЫ

- В 1971 ГОДУ ПОЯВИЛСЯ ПЕРВЫЙ ВИРУС CREEPER, СОЗДАННЫЙ БОБОМ ТОМАСОМ, ИНЖЕНЕРОМ КОМПАНИИ BBN. "CREEPER" БЫЛ ЭКСПЕРИМЕНТАЛЬНЫМ ВИРУСОМ, РАСПРОСТРАНЯВШИМСЯ ПО СЕТИ ARPANET (ПРЕДШЕСТВЕННИЦЕ ИНТЕРНЕТА). ОН ВЫВОДИЛ СООБЩЕНИЕ: “I'M THE CREEPER: CATCH ME IF YOU CAN!”
- ПЕРВЫЙ ВИРУС ДЛЯ ПЕРСОНАЛЬНЫХ КОМПЬЮТЕРОВ БЫЛ НАПИСАН ШКОЛЬНИКОМ РИЧАРДОМ СКРЕНТА В 1982 ГОДУ И НАЗЫВАЛСЯ ELK CLONER. ОН РАСПРОСТРАНЯЛСЯ ЧЕРЕЗ ДИСКЕТЫ И ВЫВОДИЛ ШУТОЧНОЕ СТИХОТВОРЕНИЕ
- В 1986 ГОДУ БЫЛ СОЗДАН ВИРУС BRAIN — ПЕРВЫЙ СТЕЛС-ВИРУС ДЛЯ IBM PC. СОЗДАН БРАТЬЯМИ АЛВИ ИЗ ПАКИСТАНА ДЛЯ ЗАЩИТЫ СВОЕГО ПО ОТ ПИРАТСТВА, НО ВЫШЕЛ ИЗ-ПОД КОНТРОЛЯ. ЗАРАЖАЛ ЗАГРУЗОЧНЫЕ СЕКТОРЫ ДИСКЕТ И СКРЫВАЛ СВОЁ ПРИСУТСТВИЕ
- В 1987 ГОДУ ПРОИЗОШЛА ПЕРВАЯ КРУПНАЯ ЭПИДЕМИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ, КОГДА ВИРУС BRAIN ЗАРАЗИЛ БОЛЕЕ 18000 КОМПЬЮТЕРОВ В США

ВЕБ-АТАКИ

- **MELISSA** — МАКРОВИРУС, РАСПРОСТРАНЯВШИЙСЯ ЧЕРЕЗ EMAIL В ВИДЕ ДОКУМЕНТА WORD. ОН РАССЫЛАЛ СЕБЯ ПЕРВЫМ 50 КОНТАКТАМ В OUTLOOK, ВЫЗВАВ ПЕРЕГРУЗКУ СЕРВЕРОВ В 1999 ГОДУ
- В 2000 ГОДУ ЧЕРВЬ ILOVEYOU ЗАРАЗИЛ 45 МЛН КОМПЬЮТЕРОВ ЗА СУТКИ, УНИЧТОЖАЯ ФАЙЛЫ И КРАДЯ ПАРОЛИ. УЩЕРБ ОЦЕНИЛИ В $15 МЛРД
- ПЕРВАЯ DDOS-АТАКА ПРОИЗОШЛА В 1996 ГОДУ НА СЕРВЕР ПАНАМЫ. С ТОГО ВРЕМЕНИ DDOS-АТАКИ СТАЛИ ОДНИМ ИЗ САМЫХ ПОПУЛЯРНЫХ МЕТОДОВ АТАК

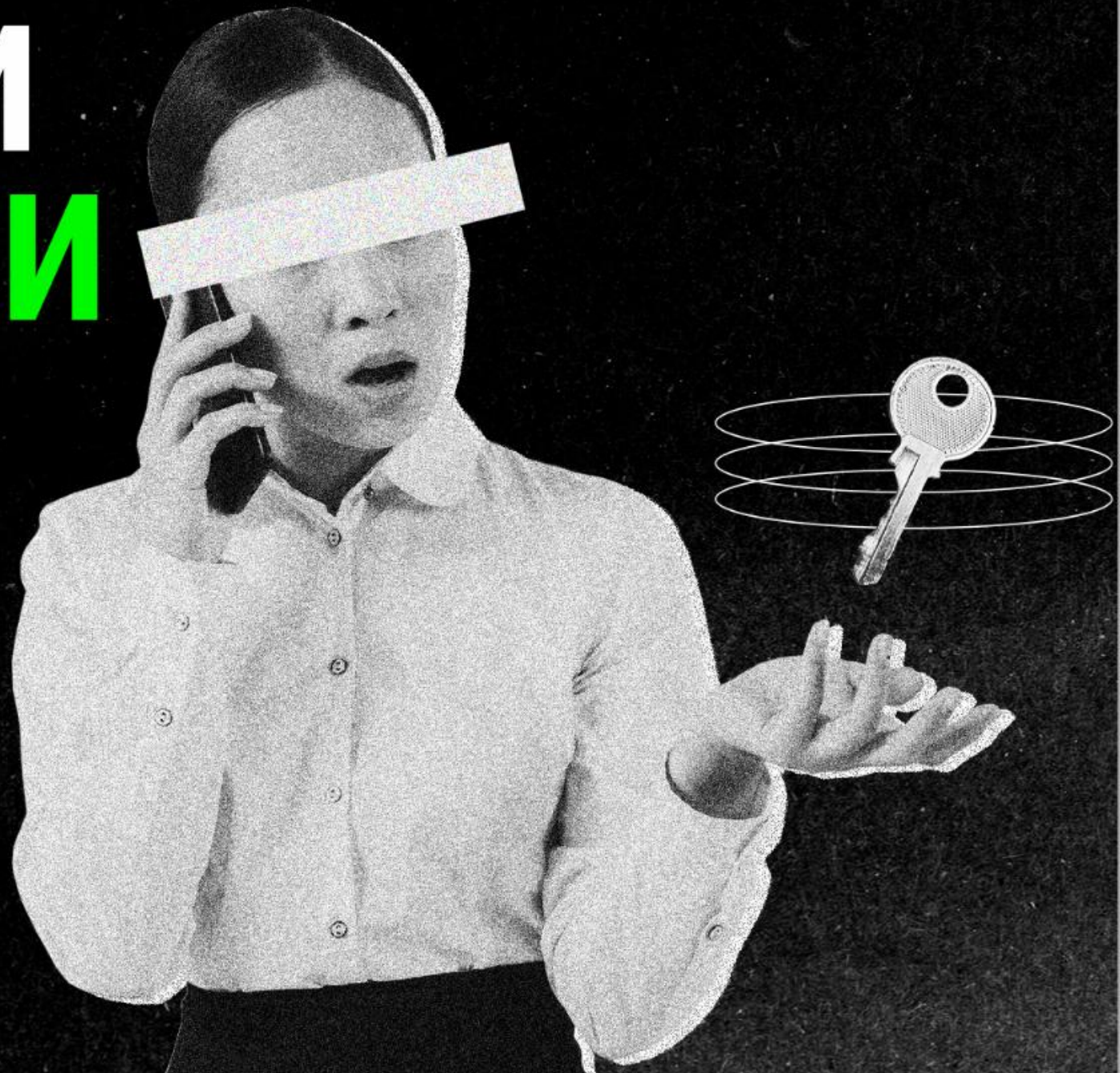
ТЕОРЕТИКИ
И ПРАКТИКИ

* * * * *

1967 ГОД. ПУБЛИКАЦИЯ СТАТЬИ "SECURITY ENGINEERING: A GUIDE TO BUILDING DEPENDABLE DISTRIBUTED SYSTEMS" ГЛЕННОМ МЭРФИ

1972 ГОД. ПУБЛИКАЦИЯ КНИГИ "THE CUCKOO'S EGG" КЕВИНОМ МИТНИКОМ

1988 ГОД. ОСНОВАНИЕ SECURITY DYNAMICS TECHNOLOGIES, INC., ПЕРВОЙ КОМПАНИИ, ПРЕДОСТАВЛЯЮЩЕЙ УСЛУГИ ПО ИБ



КОНФИДЕНЦИАЛЬНОСТЬ

ЦЕЛОСТНОСТЬ

ДОСТУПНОСТЬ

АУТЕНТИФИКАЦИЯ

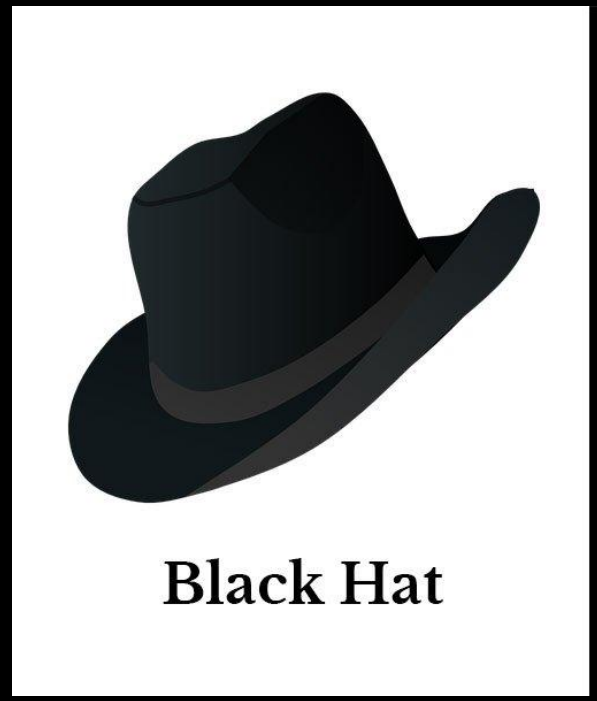
АВТОРИЗАЦИЯ

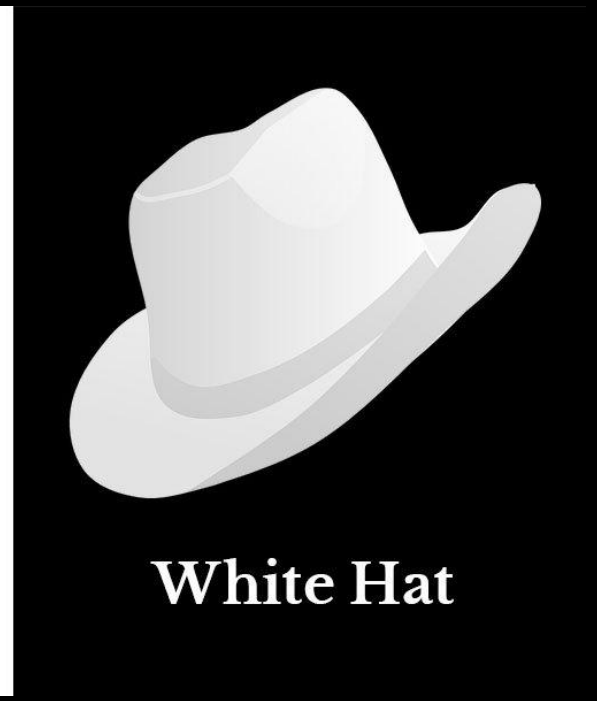
АУДИТ

Департамент информационной безопасности

- Специалист по нормативной документации (Методолог)
- Отдел внутренней безопасности
  - Начальник отдела
  - Специалист по информационной безопасности
- SOC (Security operation center)
  - Начальник отдела
  - Аналитик
  - Администратор информационных систем
- Pentest
- Application security

WHITE HAT/BLACK HAT
RED&BLUE TEAMS





RED TEAM

OFFENSIVE SECURITY

ПЕНТЕСТ ИССЛЕДОВАТЕЛИ

БЕЛЫЕ (КРАСНЫЕ) ХАКЕРЫ

BLUE TEAM

DEFENSIVE SECURITY
“КЛАССИЧЕСКАЯ ИБ”

ИНФРАСТРУКТУРА
АУДИТ
РИСК-МЕНЕДЖМЕНТ
ИНЦИДЕНТЫ
ОБУЧЕНИЕ
ЗАКОНОДАТЕЛЬСТВО
APPSEC
АНАЛИТИКА

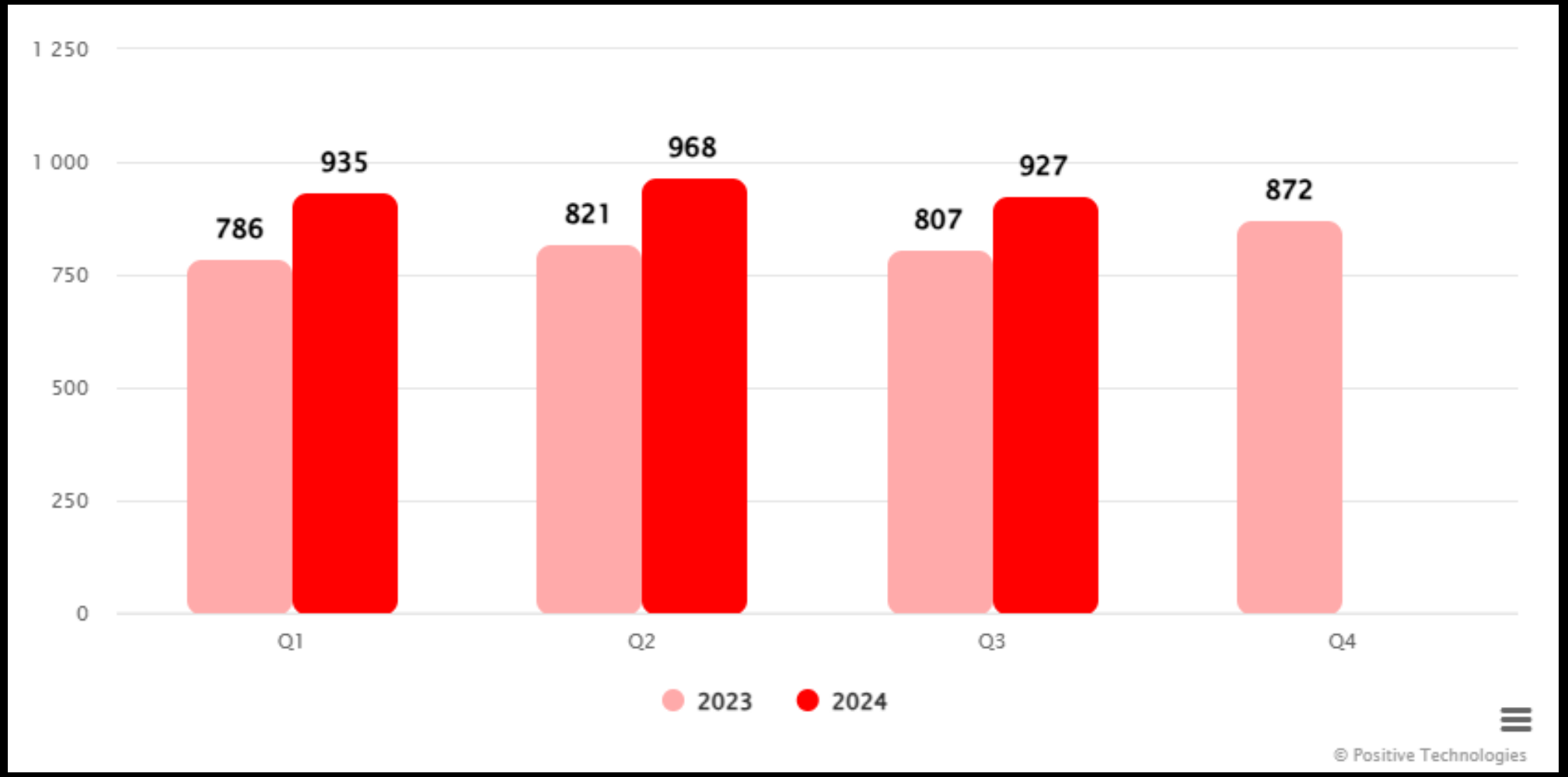
АКТИВ - ЭТО ВСЕ, ЧТО ИМЕЕТ ЦЕННОСТЬ ДЛЯ ОРГАНИЗАЦИИ. АКТИВЫ МОГУТ БЫТЬ МАТЕРИАЛЬНЫМИ ИЛИ НЕМАТЕРИАЛЬНЫМИ, И ОНИ МОГУТ БЫТЬ СВЯЗАНЫ С ИНФОРМАЦИЕЙ, СИСТЕМАМИ ИЛИ ЛЮДЬМИ.

УГРОЗА - ЭТО ПОТЕНЦИАЛЬНЫЙ ИСТОЧНИК УЩЕРБА ДЛЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ ИЛИ АКТИВА.

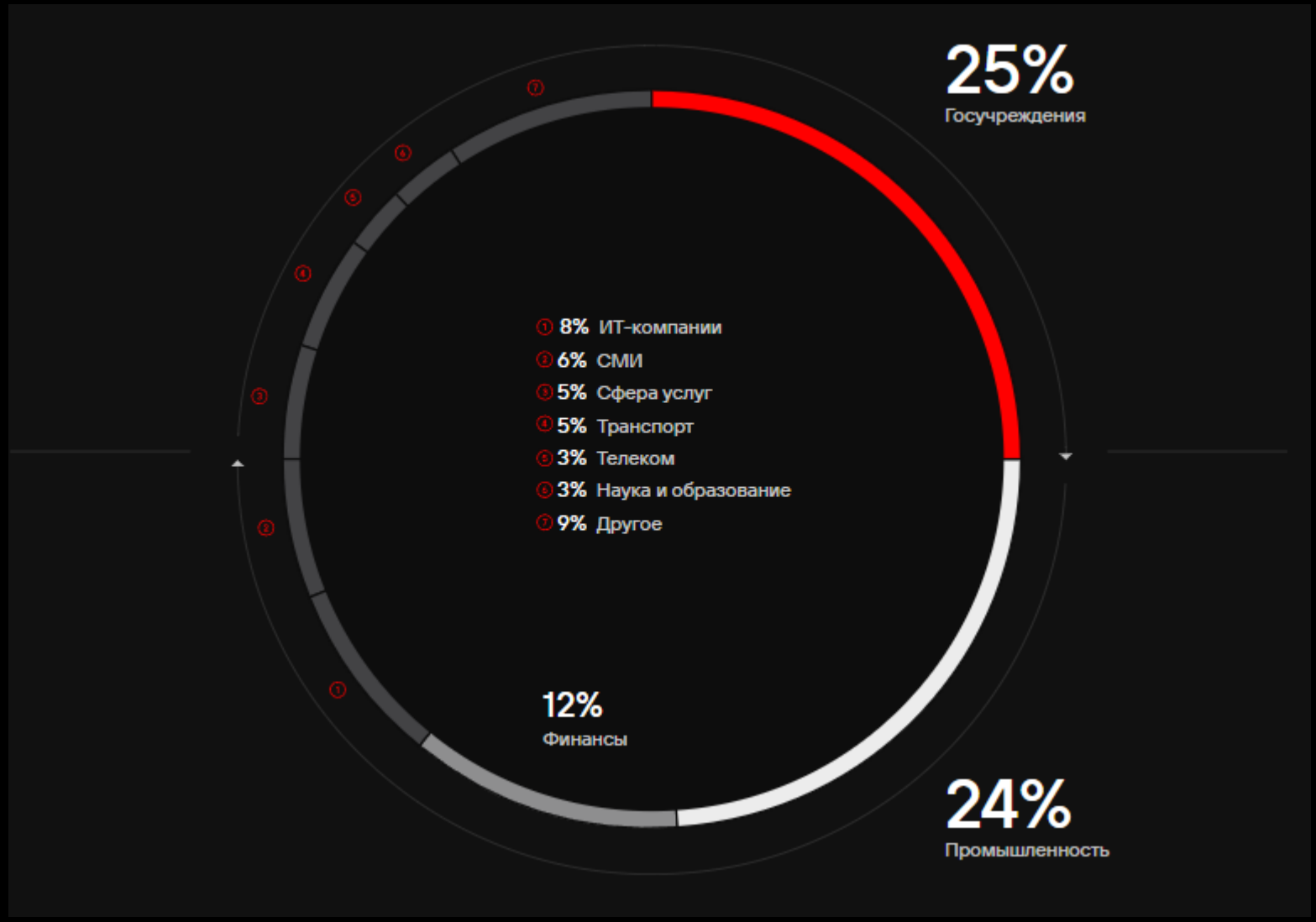
УЯЗВИМОСТЬ - ЭТО НЕДОСТАТОК ИЛИ СЛАБОСТЬ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ИЛИ АКТИВЕ, КОТОРЫЙ МОЖЕТ БЫТЬ ИСПОЛЬЗОВАН ДЛЯ РЕАЛИЗАЦИИ УГРОЗЫ.

РИСК - ЭТО ВЕРОЯТНОСТЬ ТОГО, ЧТО УГРОЗА БУДЕТ РЕАЛИЗОВАНА И К КАКИМ ПОСЛЕДСТВИЯМ ЭТО ПРИВЕДЁТ.

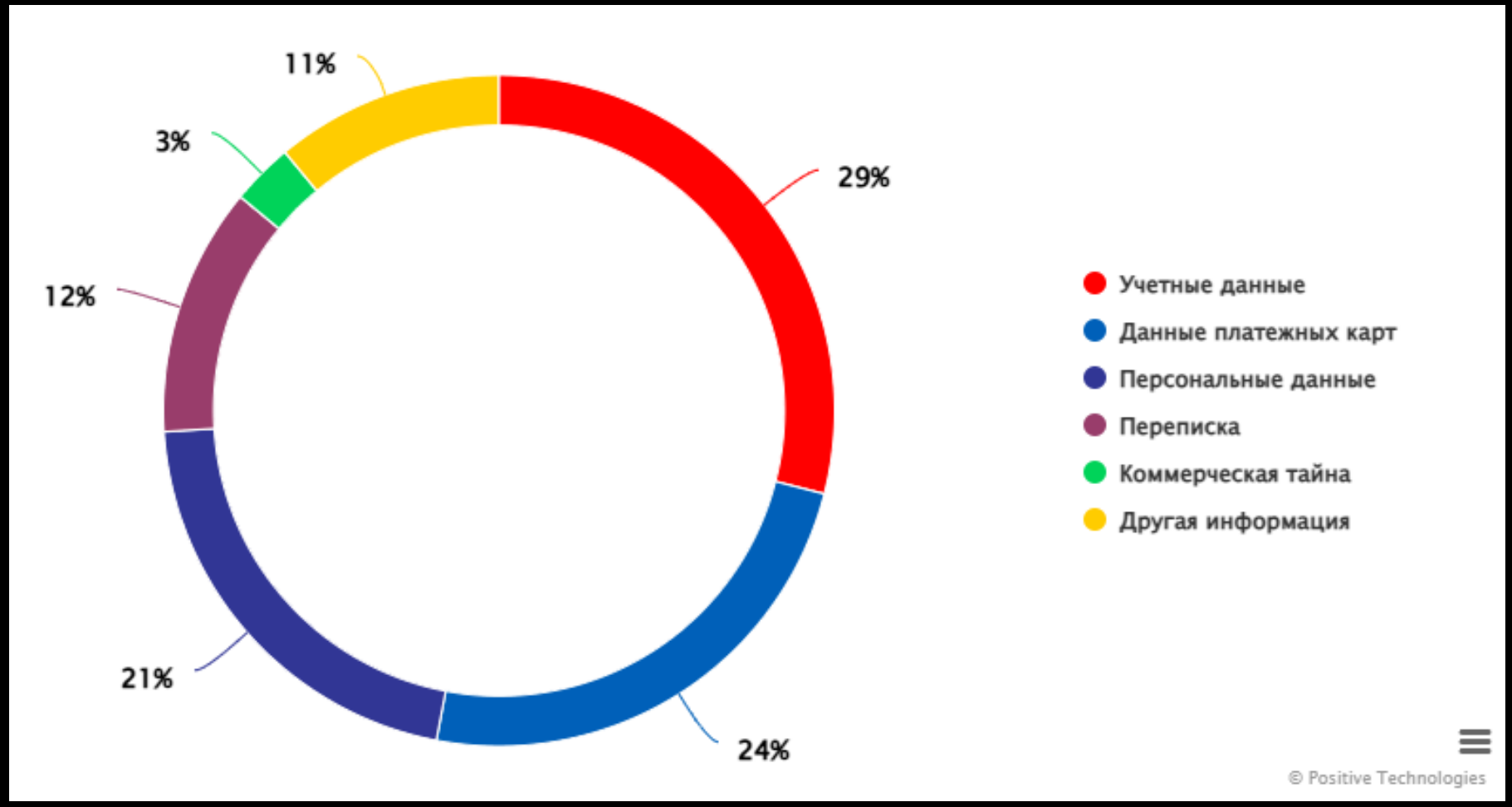
КОЛИЧЕСТВО ИНЦИДЕНТОВ В 2023 И 2024 ГОДАХ (ОТЧЁТ POSITIVE TECHNOLOGIES)



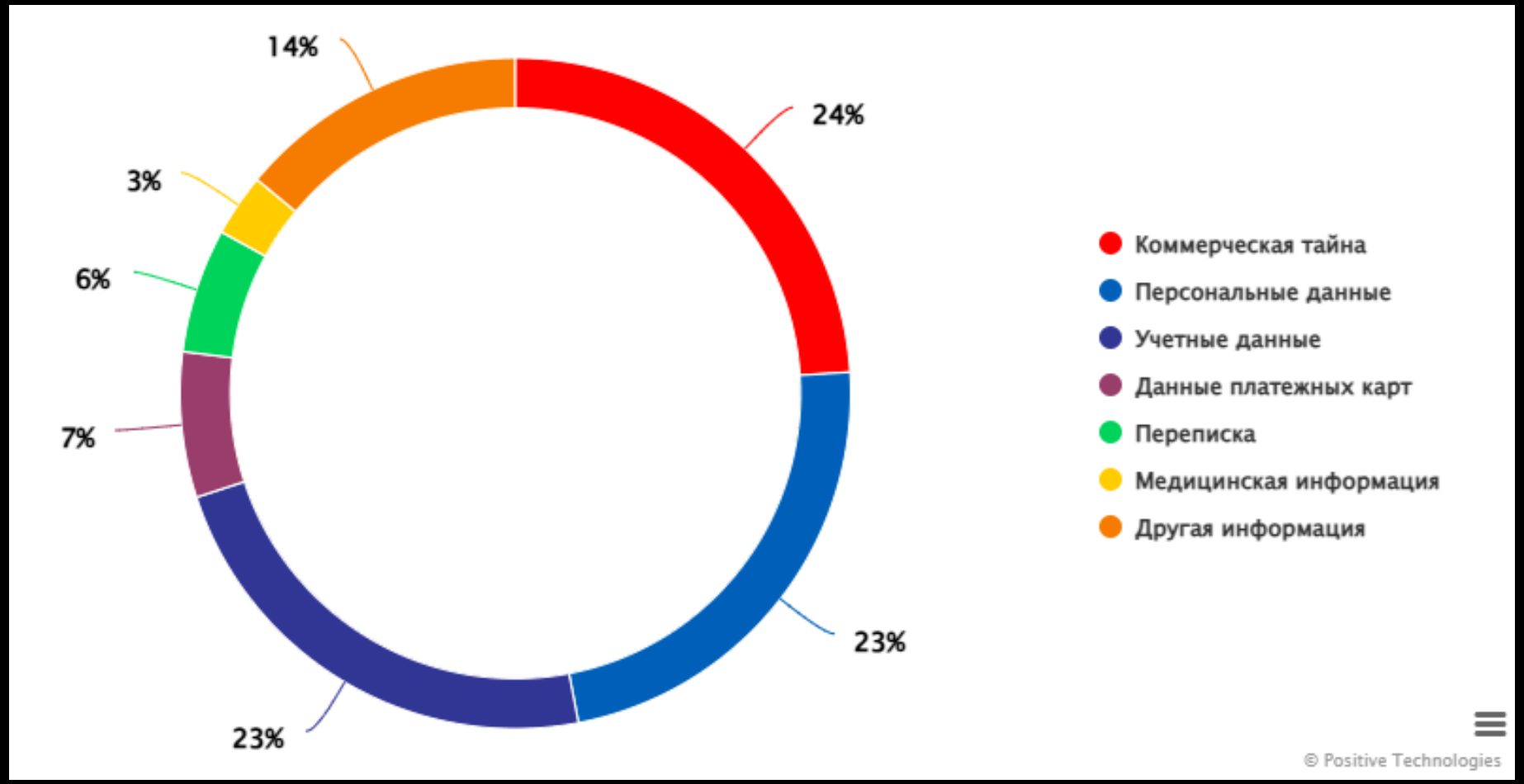
РАСПРЕДЕЛЕНИЕ ЖЕРТВ КИБЕРАТАК ПО ОТРАСЛЯМ (ОТЧЁТ POSITIVE TECHNOLOGIES)



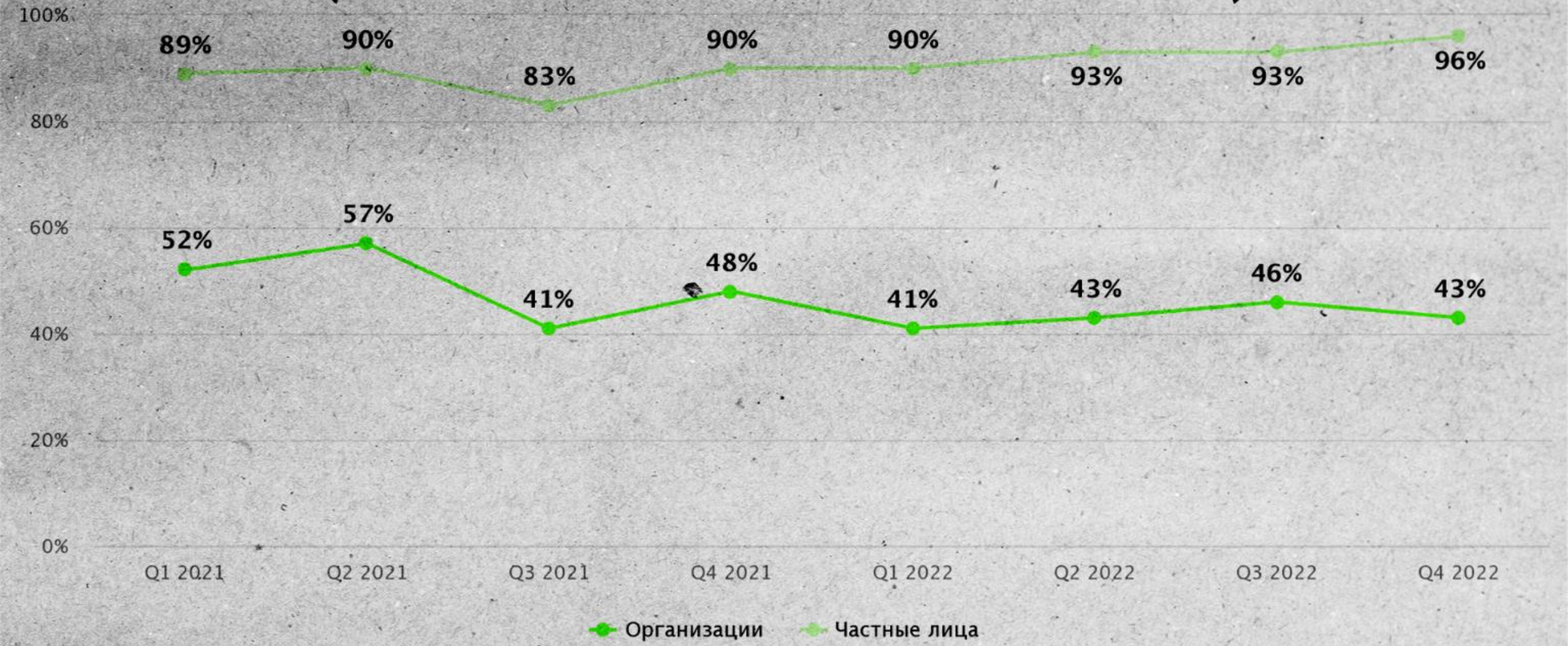
ТИПЫ УКРАДЕННЫХ ДАННЫХ (ЧАСТНЫЕ ЛИЦА) (ОТЧЁТ POSITIVE TECHNOLOGIES)



ТИПЫ УКРАДЕННЫХ ДАННЫХ (ОРГАНИЗАЦИИ) (ОТЧЁТ POSITIVE TECHNOLOGIES)



ИСПОЛЬЗОВАНИЕ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ (ОТЧЁТ POSITIVE TECHNOLOGIES)



[Методы социальной инженерии]

Домашнее задание

1. Ко второму занятию просьба загрузить и установить VirtualBox: Скачать Virtual Box
2. Скачать iso-образ Kali Linux:
   Kali Linux
1. Просьба помимо этих файлов, так же загрузить iso-образ Windows Server
   Windows Server
1. Скачать Ubuntu Desktop
2. Скачать Ubuntu Server
3. Пройти все комнаты tryhackme, которые я закинул в чат в TG