# Центр мониторинга (SOC)

«Калуга Астрал»

@СТРАЛ БЕЗОПАСНОСТЬ

# Давайте познакомимся!

## Мин Дмитрий

Аналитик киберугроз

@СТРАЛ БЕЗОПАСНОСТЬ

# Розыгрыш

Участник задавший самый интересный вопрос **получит приз**

Яндекс станцию mini

Привет я **Алиса!**

## ИНТЕРЕСНЫЙ ВОПРОС

@СТРАЛ БЕЗОПАСНОСТЬ

# Калуга Астрал

**16 лет**

На рынке информационной безопасности

**100%**

Реализованных проектов

**32 000+**

Реализованных проектов

**80+**

Лицензий и сертификатов на осуществление деятельности

**70+**

Компаний-вендоров в нашем brand-листе

**Топ-30**

**CNews** и **Tadviser.** Крупнейшие компании России в сфере ИБ

**Топ-3**

**Magic People IT Channel Awards 2020.** В номинации «Антикризисная команда»

@СТРАЛ БЕЗОПАСНОСТЬ

# Направления «Астрал.Безопасность»

| | |
|---|---|
| 01 | Защита персональных данных |
| 02 | Защита конфиденциальной информации |
| 03 | Защита государственной тайны |
| 04 | Аудит информационной безопасности |
| 05 | Защита объектов КИИ |
| 06 | Поставка средств защиты информации |
| 07 | Проведение пентестов |
| 08 | Импортозамещение |
| 09 | Разработка информационных систем |
| 10 | Внедрение системы видеонаблюдения |
| 11 | Обучение в области информационной безопасности |
| 12 | Организация защищенного удаленного рабочего места |
| 13 | Подключение к корпоративному центру мониторинга ГосСОПКА |
| 14 | Аттестация государственных информационных систем (ГИС) |

@СТРАЛ БЕЗОПАСНОСТЬ

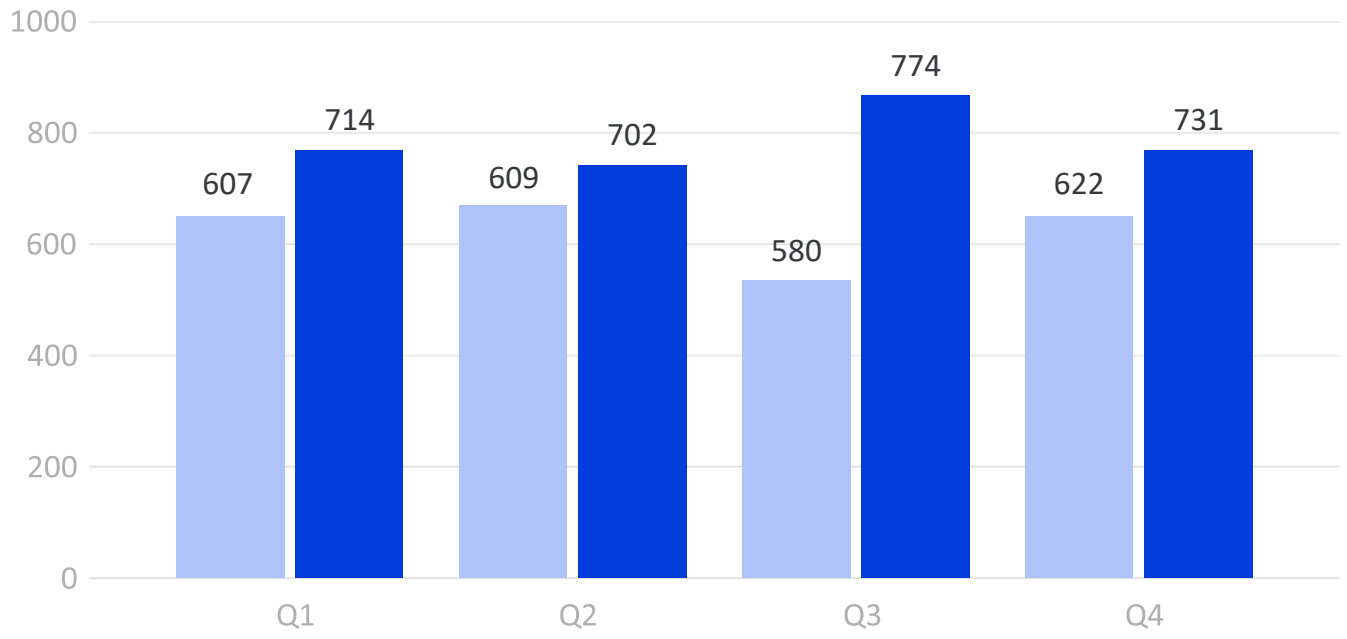
# О чём поговорим:

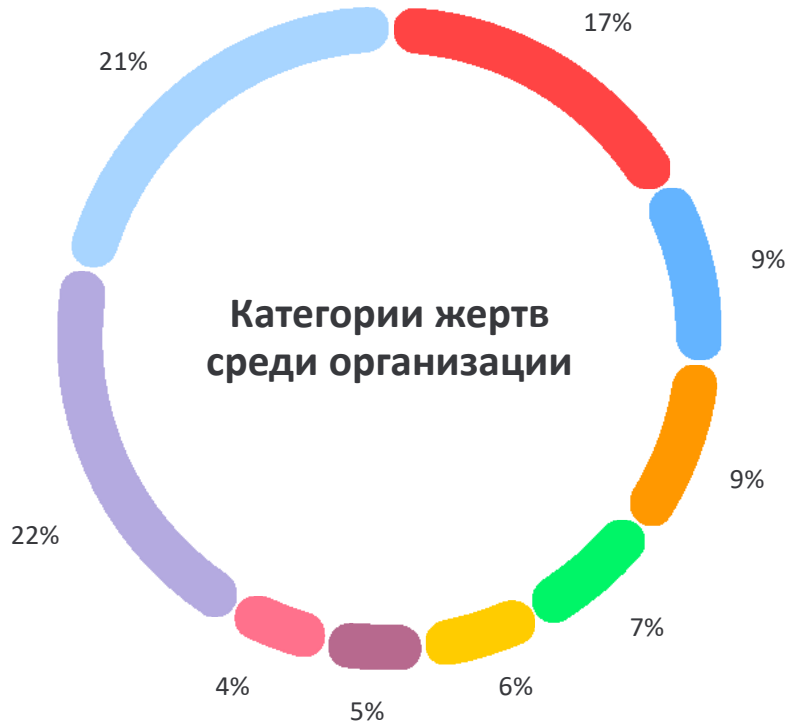
1. Темпы и тенденции роста киберугроз, актуальные уязвимости в самом распространенном программном обеспечении
2. Изменения законодательства за последний год в части деятельности SOC
3. Как изменения влияют на деятельность организаций
4. Центр мониторинга (SOC), как актуальная защита от современных угроз

@СТРАЛ БЕЗОПАСНОСТЬ

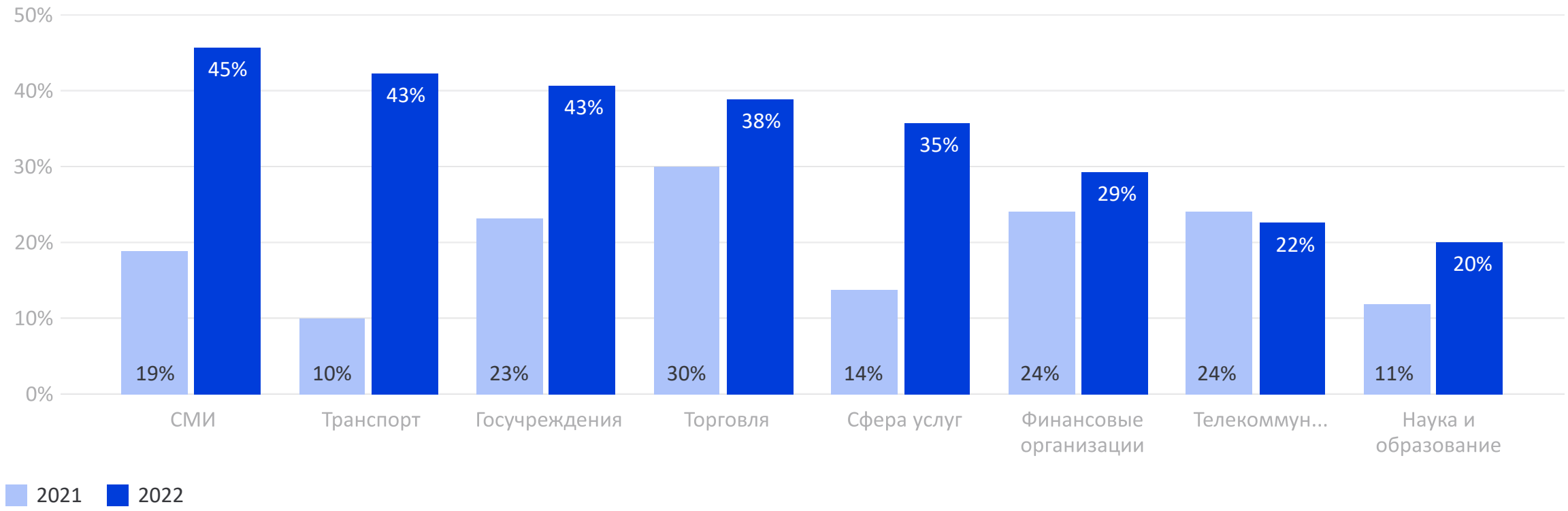
# Тенденции кибер-атак на компании РФ за 2022

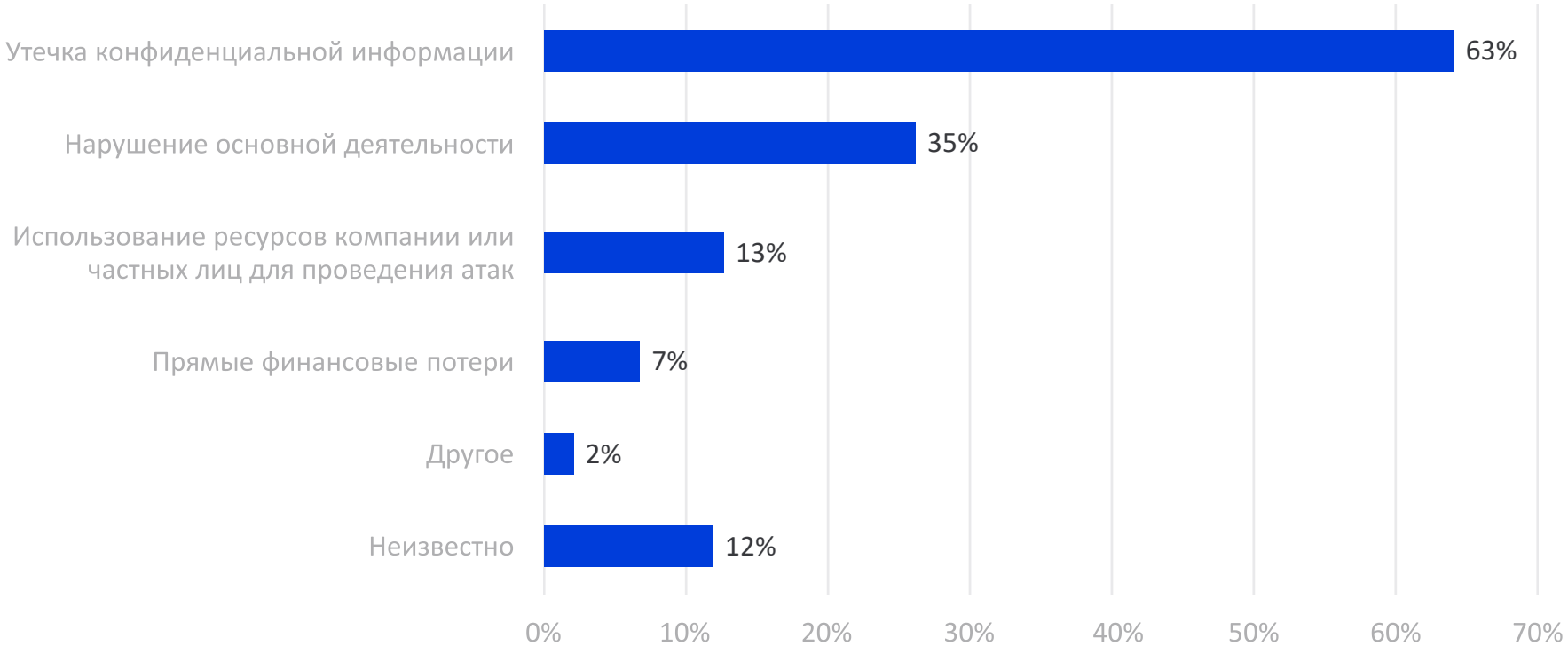
® Positive Technologies




@СТРАЛ БЕЗОПАСНОСТЬ

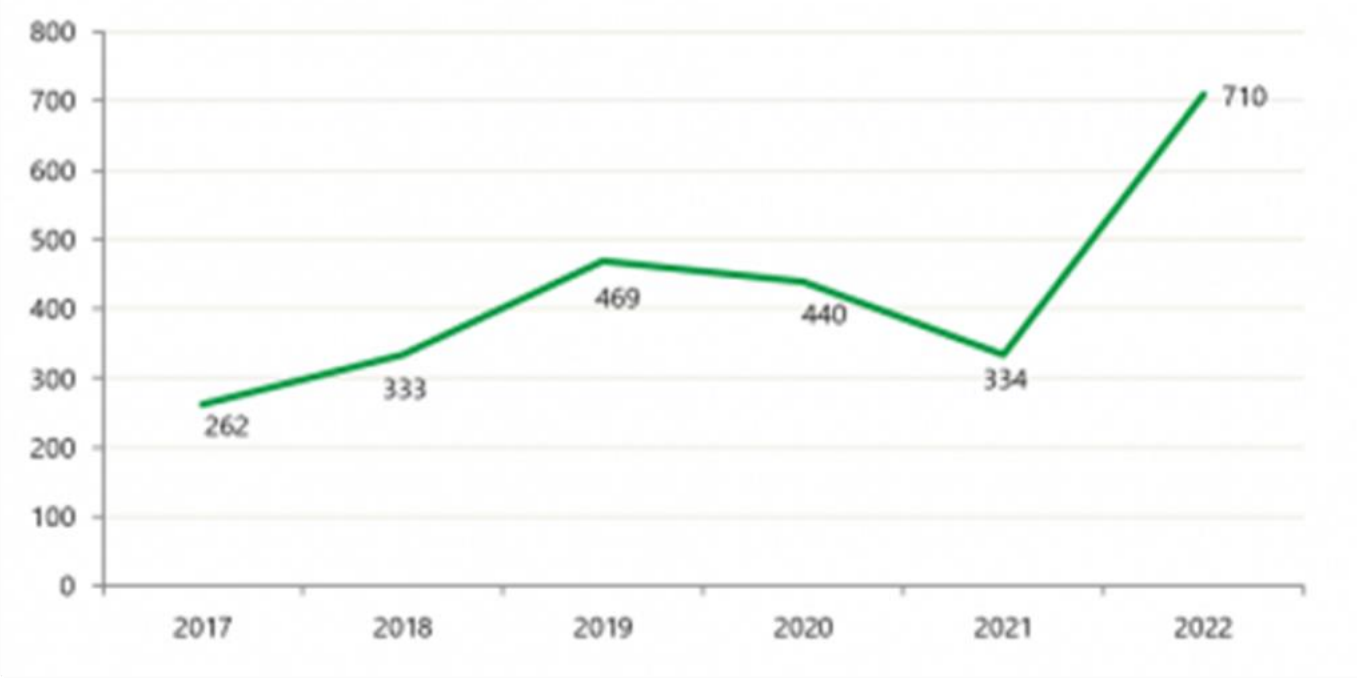

50%
40%
30%
20%
10%
0%
45%
43%
43%
38%
35%
29%
22%
20%
19%
10%
23%
30%
14%
24%
24%
11%
СМИ
Транспорт
Госучреждения
Торговля
Сфера услуг
Финансовые организации
Телекоммун...
Наука и образование
2021
2022

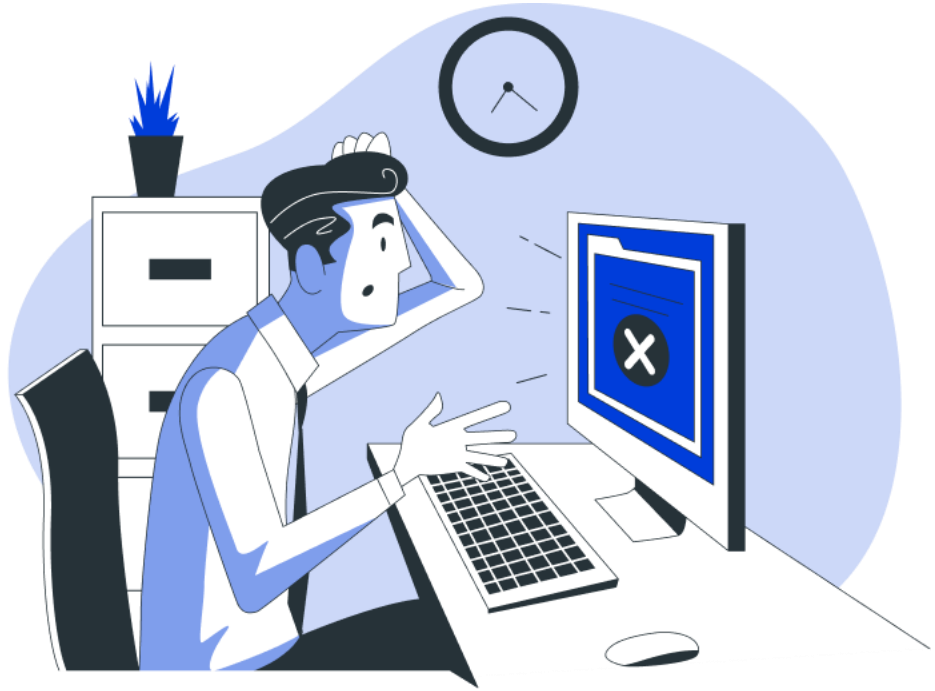



Последсвия атак на IT-компании (доля успешных атак)

# Утечки информации

Колличество утечек данных: Россия, **2017-2022**

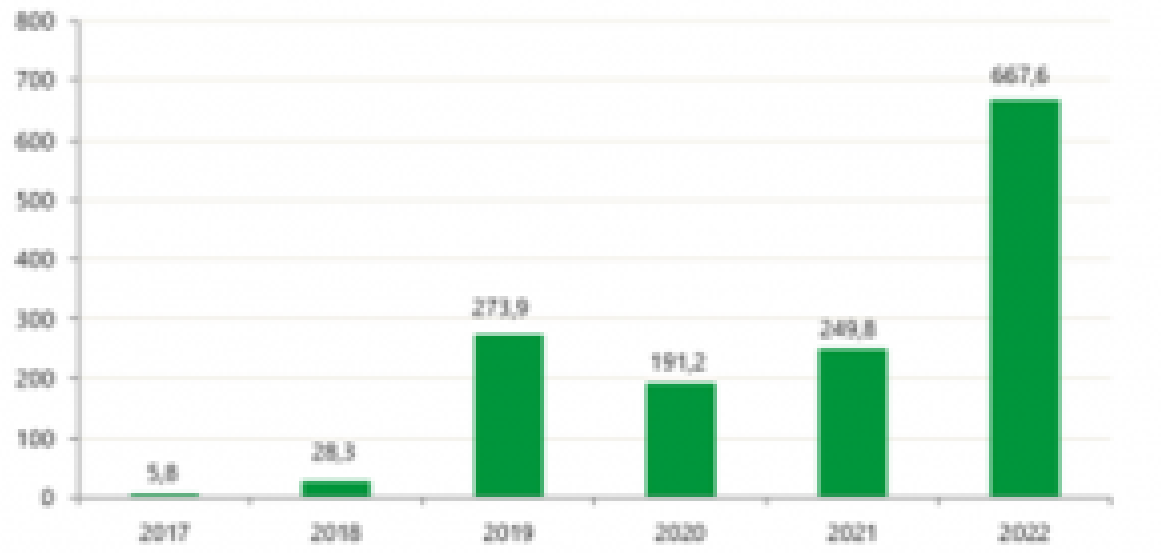


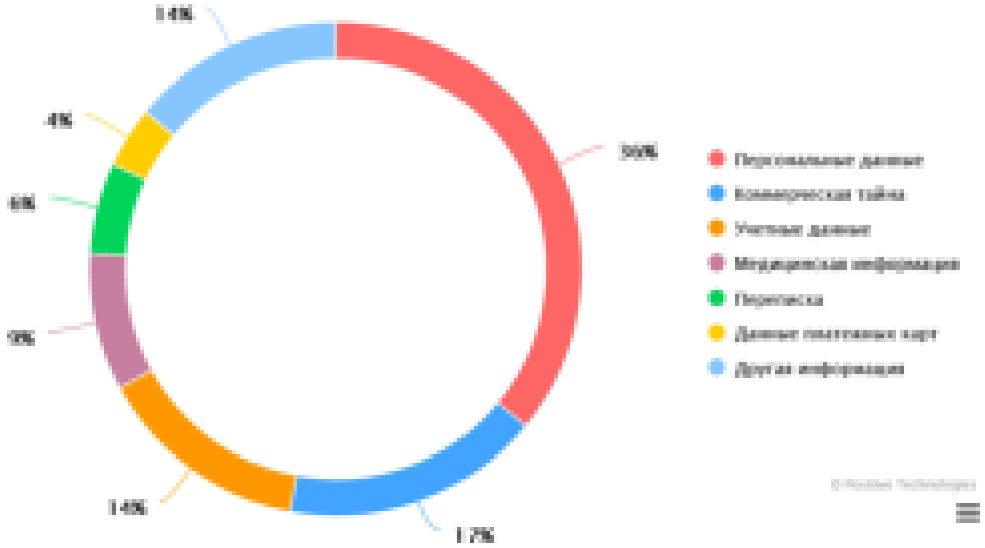
@СТРАЛ БЕЗОПАСНОСТЬ

# Утечки информации

Количество утекших записей Пдн и платежной информации, млн: Россия, **2017-2022**

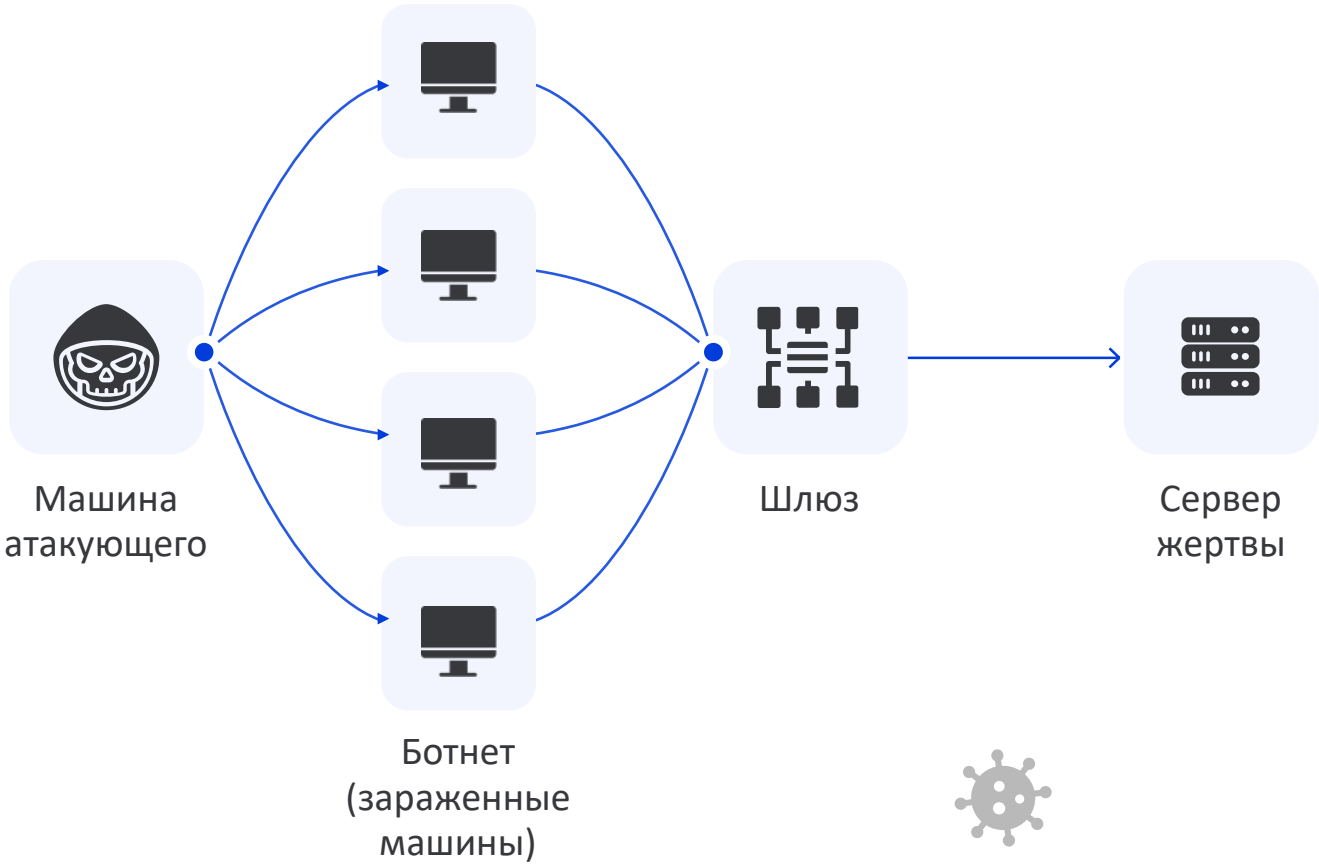



Типы украденных данных (в успешних атаках на организации)



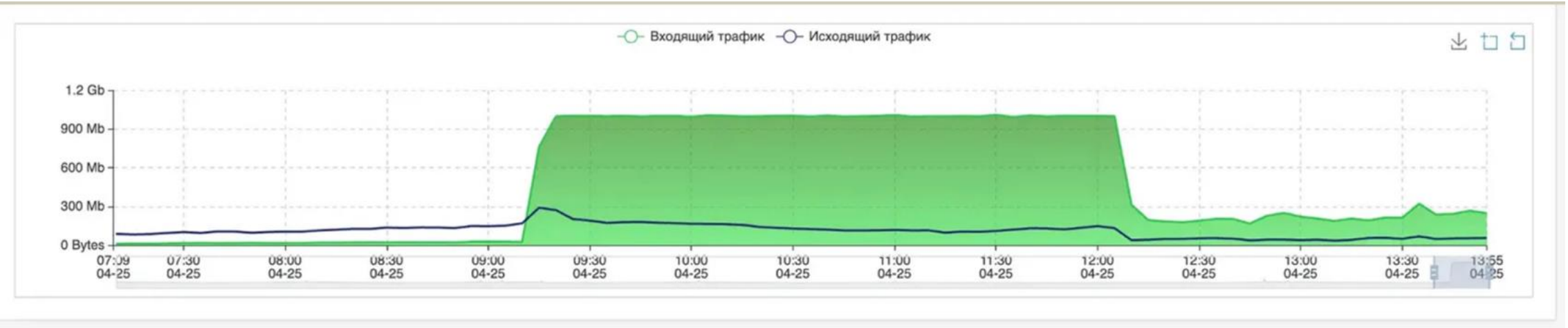

@СТРАЛ БЕЗОПАСНОСТЬ

# Что такое DDoS:



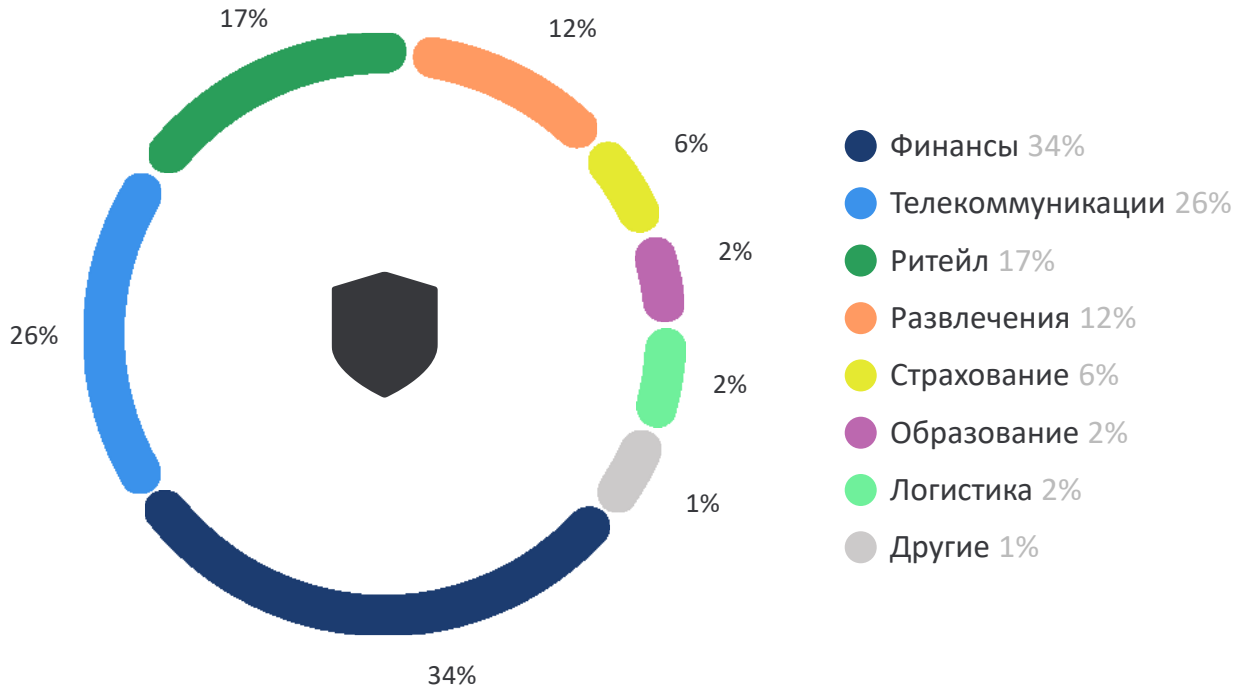

@СТРАЛ БЕЗОПАСНОСТЬ

# DDoS (пример)



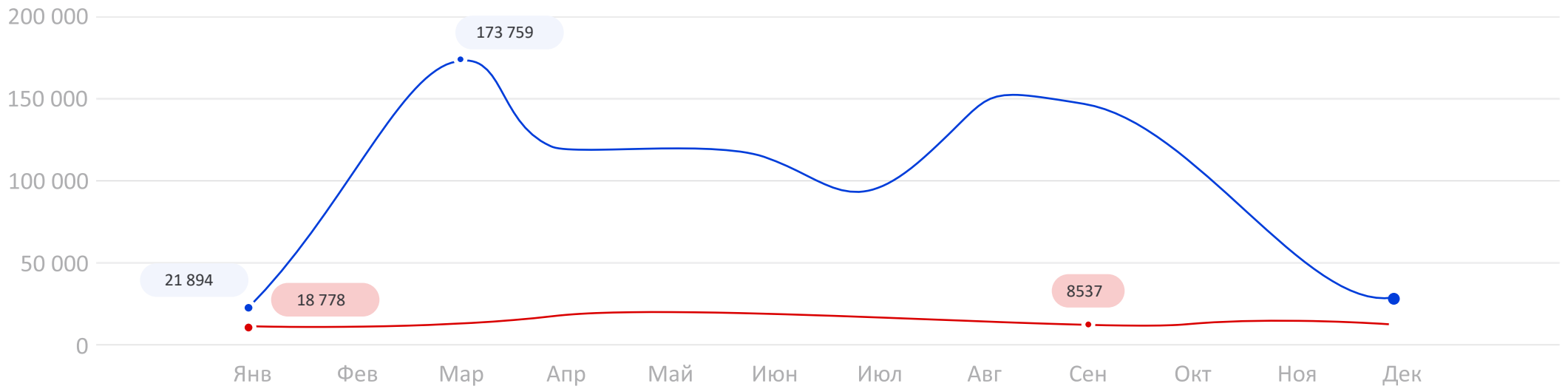

@СТРАЛ БЕЗОПАСНОСТЬ

# DDoS (статистика)




@СТРАЛ БЕЗОПАСНОСТЬ

# DDoS (статистика)




**2021** **2022**

**До 20 минут**
698 4333

**20-60 минут**
281 399

**1-6 часов**
178 058

**6-12 часов**
26 558

**12-24 часа**
68 234

**Больше 24 часов**
2 889

@СТРАЛ БЕЗОПАСНОСТЬ

# Атаки шифровальщиков

**Зашифрованные:**

число кибератак в 2022 году в России выросло в три раза, большинство из них были связаны с вымогательством*

**68%** Исследованных Group-IB кибератак в 2022 году в России завершались шифрованием данных и вымогательством выкупа.

Топ-3 самых активных групп программ-вымогателей в России в прошлом году:

1. **Phobos**
2. **CryLock**
3. **Sojusz**

**14 дней** — Среднее время простоя атакованной организации

**Известные атаки вымогателей LokiLocker и BlackBit**

| | BlackBit | LokiLocker |
|---|---|---|
| **Россия** | 11 | 10 |
| **Белоруссия** | 3 | 3 |
| **Всего в мире** | 33 | 29 |

**Group-IB**

Самые популярные техники, используемой злоумышленниками для получения первоначального доступа к корпоративной сети:

**61%** Эксплуатация публично доступных приложений

**22%** Фишинг

**17%** Компрометация служб удаленного доступа

Сумма выкупа за расшифровку:

От 10 000 $

До 100 000 $

# Почему это важно?

**Указ Президента РФ № 250**

Все субъекты критической информационной инфраструктуры Российской Федерации (КИИ) должны обеспечить мероприятия по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты собственными силами или с привлечением организации, имеющей лицензию на осуществление деятельности по технической защите конфиденциальной информации

**Федеральный закон №187-ФЗ**

Субъекты КИИ обязаны незамедлительно информировать о компьютерных инцидентах центр ГосСОПКА

**Федеральный закон №152-ФЗ**

Операторы персональных данных обязаны обеспечивать взаимодействие с центром ГосСОПКА, включая информирование его о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных.

# Кому это необходимо?

### Субъектам КИИ

Государственным структурам/органам, полугосударственным и частным организациям, являющимся субъектами критической информационной инфраструктуры.

### Операторам ПДн

Всем организациям и структурам, работающим с персональными данными.

### Частным организациям

для которых потеря контроля над своими информационными ресурсами или утечка данных может стать критичной для деятельности организации и привести к финансовым или репутационным потерям.

@СТРАЛ БЕЗОПАСНОСТЬ

# Что такое SOC и для чего он нужен?

**SOC (Security Operations Center)** — это непрерывный мониторинг событий информационной безопасности, происходящих в ИТ-инфраструктуре и своевременное реагирование на возникающие инциденты.

**SOC — центр мониторинга**

Непрерывный контроль за безопасностью организации

Централизованное хранение сведений о вторжениях и киберугрозах

Реагирование на инциденты ИБ

Снижение затрат на кибербезопасность

Оперативное решение возникающих вопросов безопасности

Сокращение рисков для организации

@СТРАЛ БЕЗОПАСНОСТЬ

# Услуги центра мониторинга

## Мониторинг событий ИБ

- Подключение и настройка источников событий ИБ
- Настройка правил корреляции
- Обеспечение неприрывности мониторинга
- Регистрация и классификация подозрений на инцидент

## Анализ инцидента ИБ

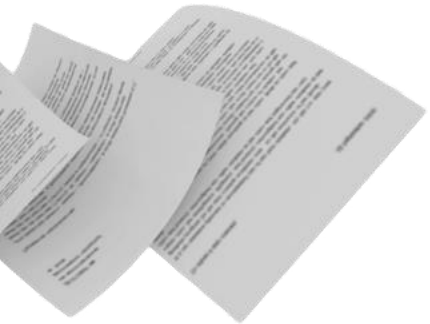
- Базовый анализ
- Формирование оперативной отчетности
- Оповещение о выявлении инцидента
- Углубленный анализ

## Реагирование на инцидент

- Выработка мер реагирования
- Реагирование в зоне ответственности
- Координация при реагировании

## Аналитика

- Пост-инцидент анализ
- Расследование инцидентов
- Отчетность по инцидентам

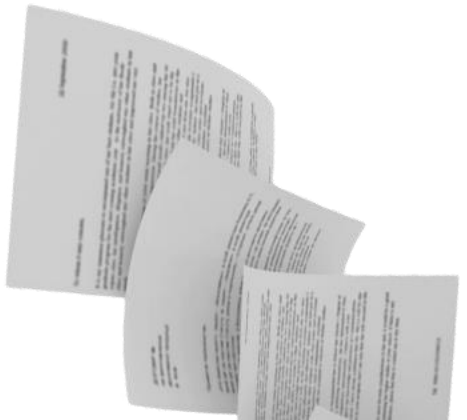


## Контроль уязвимостей

- Сканирование на уязвимости
- Выработка мер по устранению уязвимостей
- Контроль устранения уязвимостей

## Анализ защищенности

- Тестирование на проникновение
- Внешний аудит ИБ



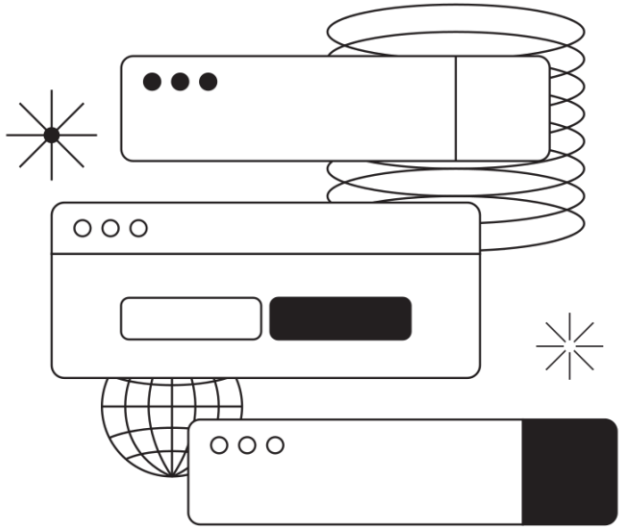
@СТРАЛ БЕЗОПАСНОСТЬ

# Виды центров мониторинга

Внутренний (ведомственный) SOC

Внешний (корпоративный) SOC

Гибридная модель



## Режимы работы

1

**24** часа в сутки

**7** дней в неделю

**365** дней в году

2

**8** часов в сутки

**5** дней в неделю

**247** дней в году

# Схемы подключения вариант 1

SIEM установлена в «Калуга Астрал»


+ Выгодно по затратам

- Нагружается канал связи

# Схемы подключения вариант 2

SIEM установлена у Заказчика


\+ Не нагружается канал связи

\- Повышенные затраты и требуется постоянный доступ к системе

# Подключение к ЦМ Калуга Астрал

## Порядок подключения

**01** Определить перечень ИТ-ресурсов для постановки на мониторинг и выбрать удобный вариант взаимодействия

**02** Заключить договор с «Калуга Астрал»

**03** Подключить ИТ-ресурсы к центру мониторинга

**04** Уведомить НКЦКИ о включении своих информационных ресурсов в зону ответственности корпоративного центра мониторинга информационной безопасности «Калуга Астрал»

## Преимущества

+ Нехватка, отсутствие или загруженность собственного персонала для сбора и анализа данных

+ Все требуемые лицензии, соглашение с НКЦКИ и штат сотрудников имеются в наличии у «Калуга Астрал»

+ Быстрый старт

+ Выполнение организационных и технических требований

+ Понятные и прогнозируемые затраты

# Будьте в курсе последних новостей

is.astral.ru

vk.com/is.astral

t.me/is_astral

@СТРАЛ БЕЗОПАСНОСТЬ