

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

В СТАРТАПАХ



ВКЛАДЫВАТЬ ДЕНЬГИ В БЕЗОПАННОСТЬ?



РАЗМЕР БИЗНЕСА

АКТУАЛЬНОСТЬ УГРОЗ

СУММА РИСКОВ

ЦЕЛИ СТАРТАПА. А ГДЕ БЕЗОПАСНОСТЬ?

- **ПОЛУЧЕНИЕ ПРИБЫЛИ**
- **РЕШИТЬ АКТУАЛЬНУЮ ПРОБЛЕМУ ПОЛЬЗОВАТЕЛЯ**
- **ВЫСОКАЯ УЗНАВАЕМОСТЬ**
- **КВАЛИФИЦИРОВАННАЯ КОМАНДА**
- **МАСШТАБИРУЕМОСТЬ**

- **БЕЗОПАСНОСТЬ?**



Зачем заморачиваться тем, что неизвестно еще, будет ли востребовано?

КОНЦЕПЦИЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОПЕРАЦИОННОЙ ДЕЯТЕЛЬНОСТИ НА РАННЕМ ЭТАПЕ

ПОЗЖЕ – ДОРОЖЕ! СЛОЖНЕЕ!

АКТУАЛИЗАЦИЯ УГРОЗ

- **Идентификация, локализация и классификация информационных активов.**

Какими данными располагает стартап? Где эта информация хранится? Насколько общедоступны или конфиденциальны ресурсы

- **Распознавание видов угроз и определение наиболее вероятных**
- **Разработка плана противодействия.**

Сопоставление результатов моделирования угроз и классификации информации для того, чтобы выяснить, на какие угрозы следует незамедлительно обратить внимание.

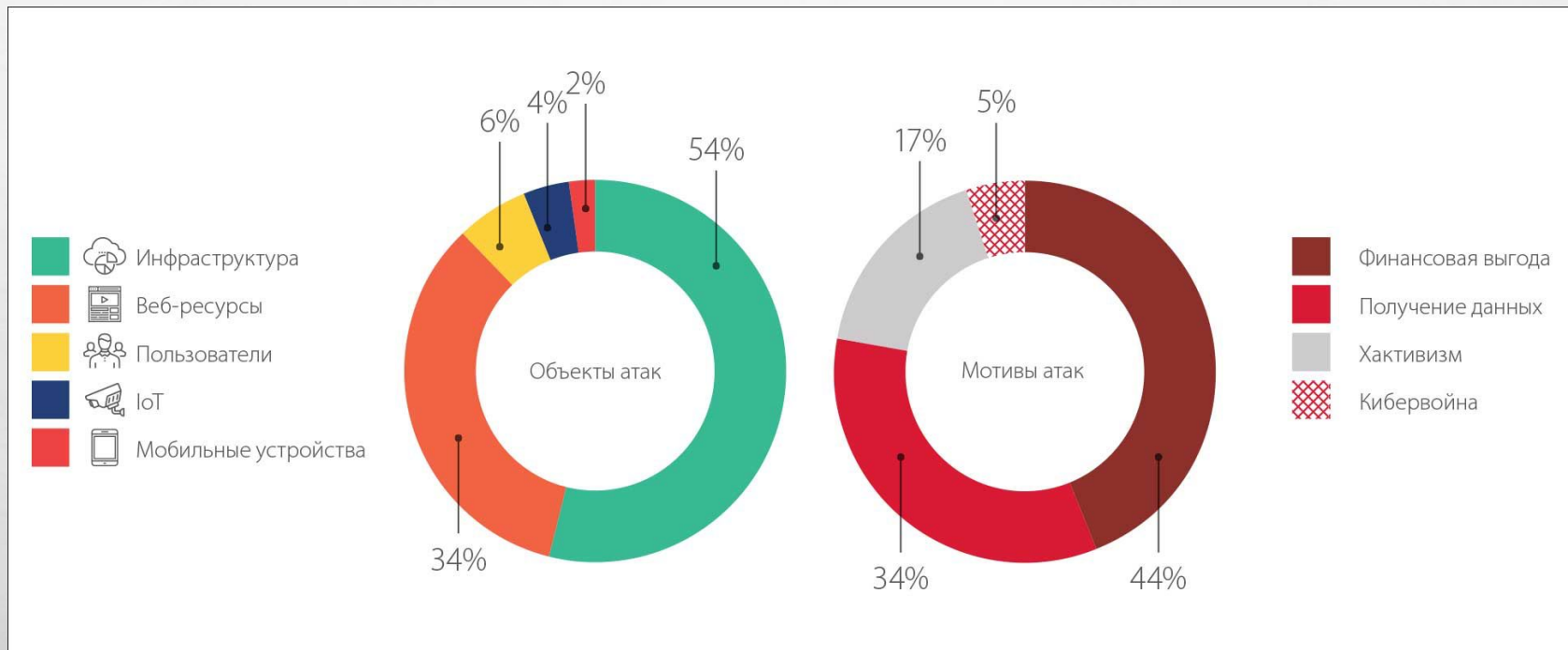


ЧЕМ РИСКУЕМ?

- **Коммерческая информация**
- **Клиентские базы**
- **Учетный записи пользователей**
- **Аккаунты сторонних сервисов**



ОБЪЕКТЫ И МОТИВЫ



УТЕЧКИ ИНФОРМАЦИИ

32%



Информация о
клиентах и сделках

26%



Техническая
информация

21%



Персональные
данные

14%



Информация о
партнерах

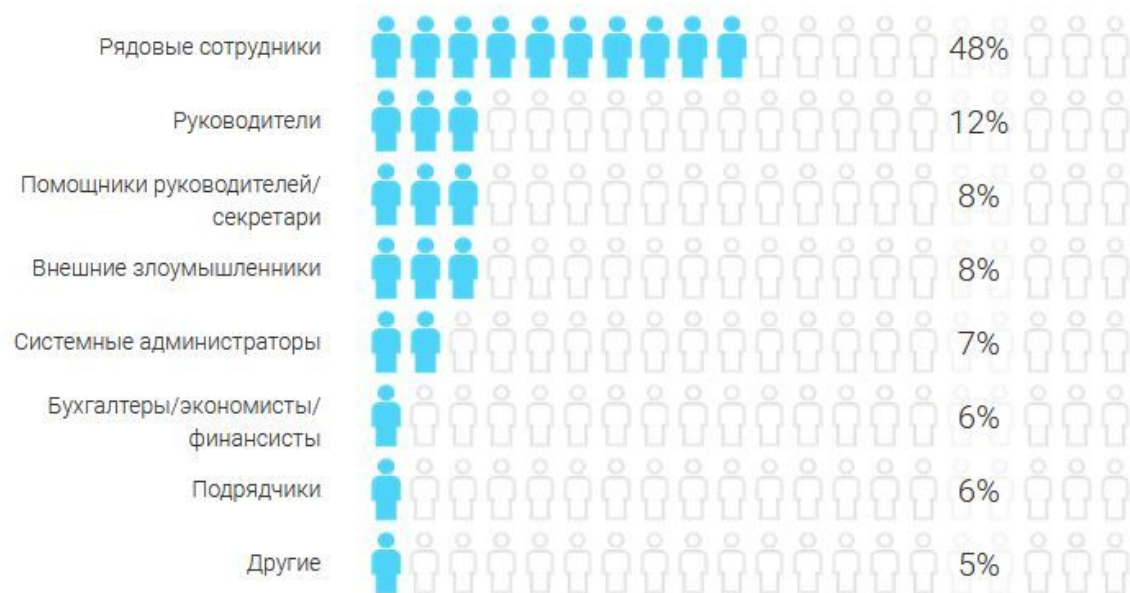
7%



Внутренняя
бухгалтерия

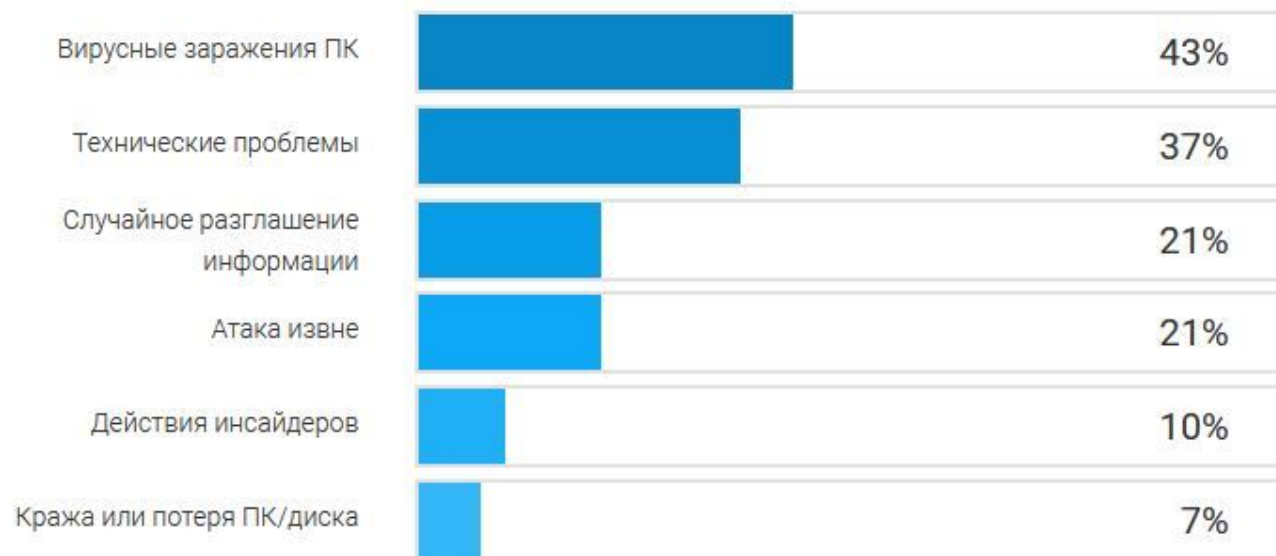
УТЕЧКИ ИНФОРМАЦИИ

ВИНОВНИКИ ИБ-ИНЦИДЕНТОВ:



УТЕЧКИ ИНФОРМАЦИИ

ПРИЧИНЫ ИБ-ИНЦИДЕНТОВ:



* Респонденты могли выбрать несколько вариантов ответов.

УГРОЗЫ И ЗАЩИТА

Внутренние утечки информации

Разграничение прав пользователей

Шифрование

SIEM системы

DLP системы

IDS/IPS

УГРОЗЫ И ЗАЩИТА

ФИШИНГ

любая атака в результате которой пользователи делятся своими паролями. Классика фишинга
– отправка пользователям электронных писем, требующих паролей для доступа в онлайн-банк, аккаунт в Facebook или на любой другой сайт

**МУЛЬТИФАКТОРНАЯ АВТОРИЗАЦИЯ.
Подготовка сотрудников**

УГРОЗЫ И ЗАЩИТА

Вредоносное ПО

Троянцы, malware

Установленная антивирусная защита

Использование фаервола

Использование актуальных версий браузера

Использование «песочницы»

УГРОЗЫ И ЗАЩИТА

Крипто-вымогатели

Автономное резервное копирование

УГРОЗЫ И ЗАЩИТА

0 day уязвимости

неустраненные уязвимости, а также вредоносные программы, против которых еще не разработаны защитные механизмы

Постоянные обновления software/firmware

УГРОЗЫ И ЗАЩИТА

Кражи / потеря устройств

Пароль/PIN код

Шифрование

Актуальные операционные системы

УГРОЗЫ И ЗАЩИТА

Атака на web порталы

Распределение сервисов

Делегирование сторонним провайдерам

Использование облачных решений

СПАСИБО ЗА ВНИМАНИЕ

Борощук Дмитрий

Независимый эксперт в области ситуационной безопасности

beholder@me.com

t.me/beholderishere

