Антон Тростянко

начальник центра обеспечения
кибербезопасности hoster.by

Киберугрозы в Беларуси:

Статистика. Угрозы. Опыт реагирования на значимые киберинциденты

hoster.by

О компании hoster.by

Решаем любые задачи, в которых есть приставка “онлайн”

1-й

Коммерческий аттестованный SOC (Security Operation Center)

1-й

Облачный маркетплейс приложений для бизнеса

1-й

Облачный маркетплейс приложений для бизнеса

1-ое

Гибкое облако для бизнеса

140 000

Довольных клиентов. hoster.by — синоним хостинга в Беларуси

130+

Высококлассных специалистов

Мировая статистика утечки данных

Количество утечек в мире за 2023 год выросло более чем на 60%, а количество скомпрометированных персональных данных — более чем в два раза.

hoster.by

Киберинцидиенты. Уровни

К киберинцидентам высокого уровня относятся:

- внедрение и функционирование вредоносных программ;
- несанкционированный доступ;
- использование объектов информационной инфраструктуры для осуществления кибератак и (или) распространения вредоносных программ;
- прослушивание, захват, перенаправление сетевого трафика;
- рассылка незапрашиваемой информации (спама);
- эксплуатация уязвимостей;
- прекращение функционирования, вызванное кибератакой типа «отказ в обслуживании»

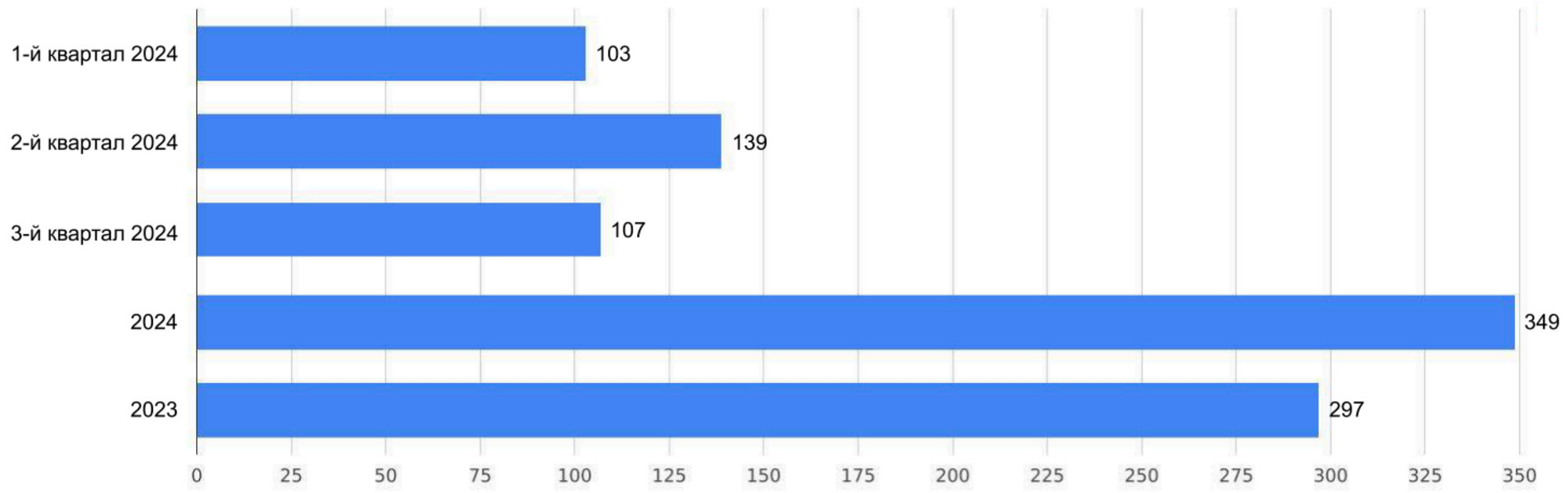
К киберинцидентам низкого уровня относятся:

- попытка внедрения вредоносных программ;
- проведение кибератаки типа «отказ в обслуживании», не вызвавшей негативных последствий;
- попытка эксплуатации уязвимостей;
- сканирование в целях поиска уязвимостей;
- попытка несанкционированного доступа;
- прекращение функционирования объектов информационной инфраструктуры, не связанное с киберинцидентом высокого уровня;
- попытка распространения вредоносных программ;
- попытка проведения кибератаки на веб-приложения и иные сетевые протоколы и службы;
- использование вычислительных мощностей объектов информационной инфраструктуры для проведения кибератак.

hoster.by

Зарегистрированные киберинциденты

Количество зарегистрированных киберинцидентов по статистике SOC hoster.by



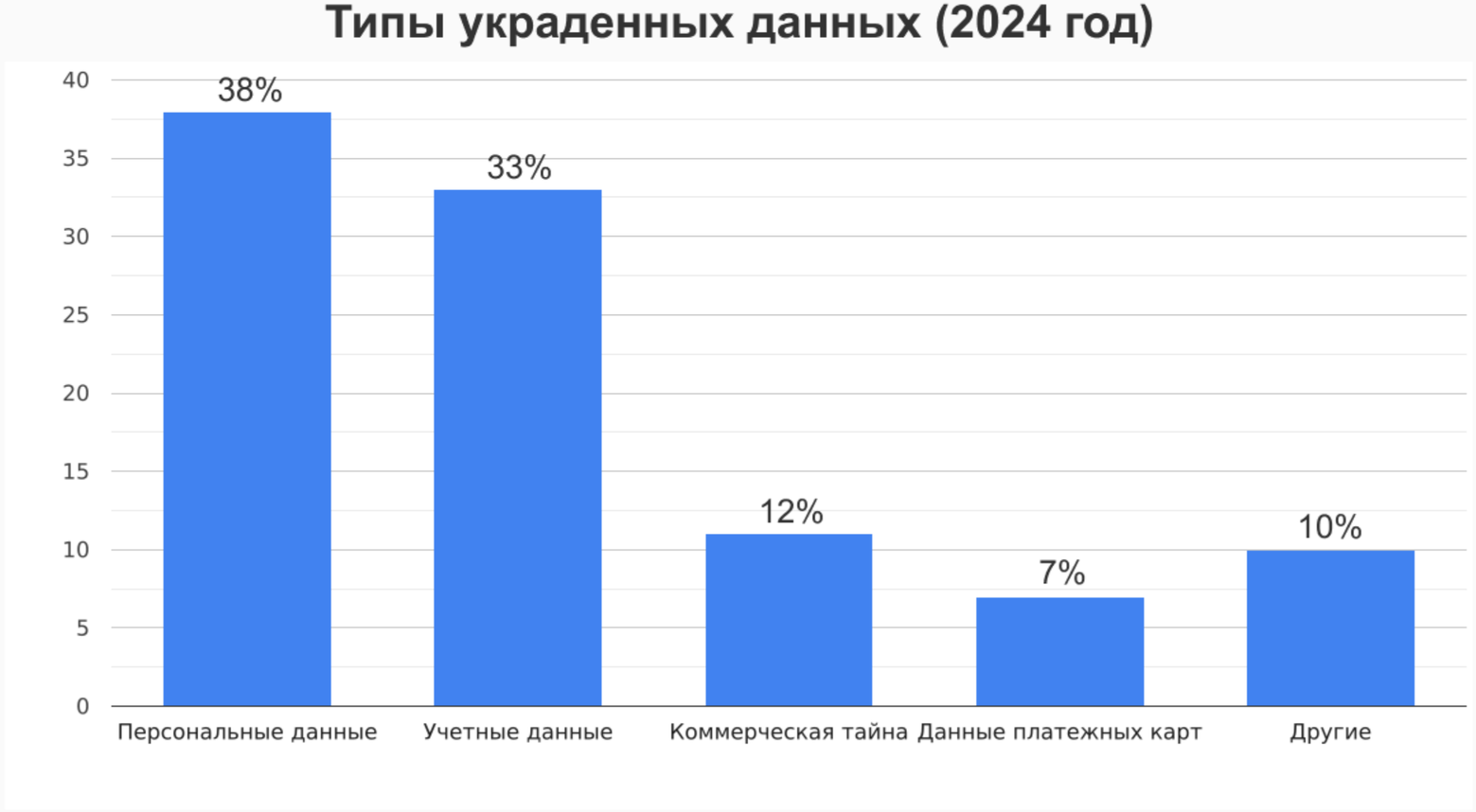
Статистика SOC hoster.by

Информационная безопасность.
С каким вызовами сталкивается бизнес.

Утечка конфиденциальной информации может приводить к прямому финансовому ущербу, ухудшению репутации компании, потере клиентов.

Статистика SOC hoster.by

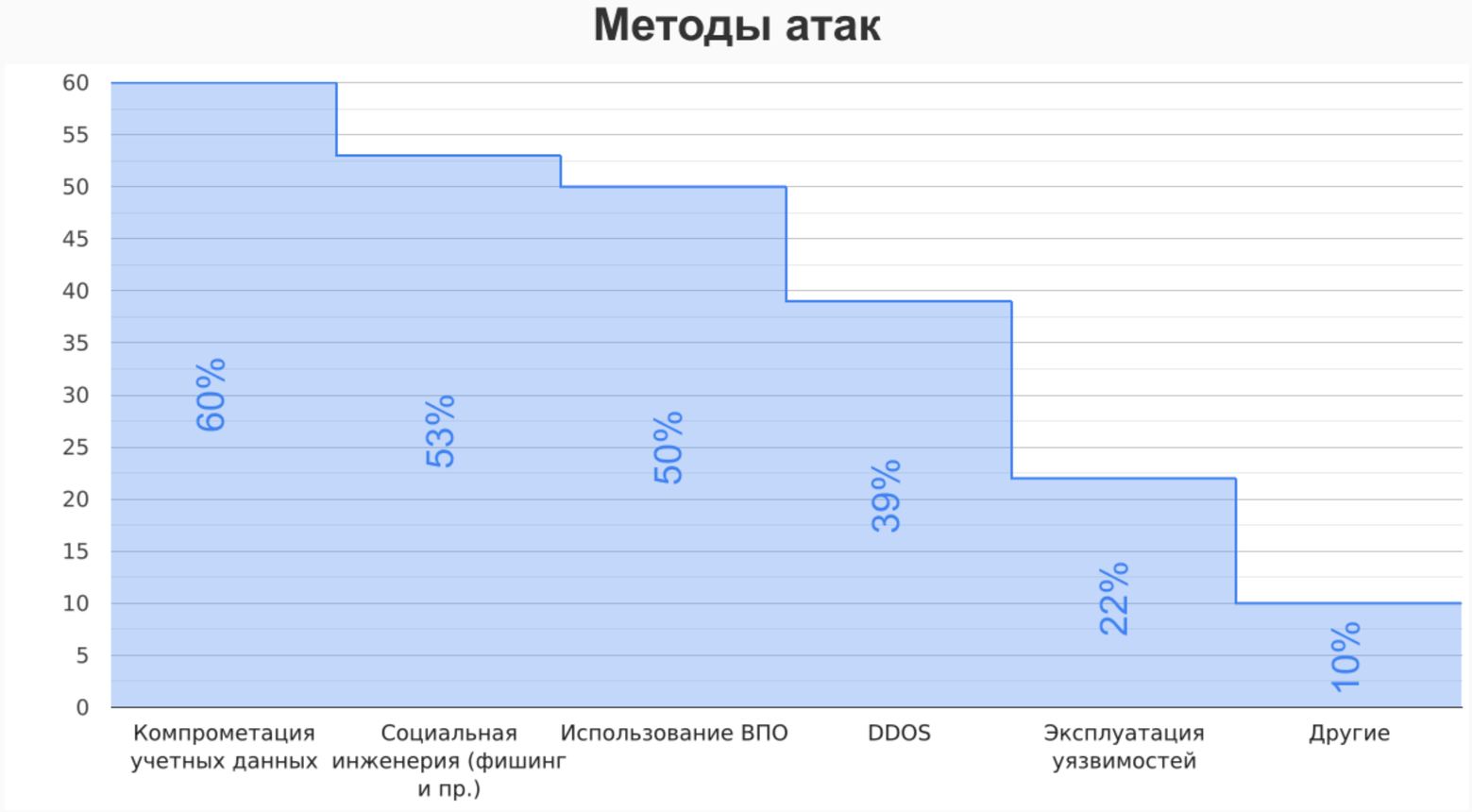
Информационная безопасность.
С каким вызовами сталкивается бизнес.



Персональные данные пользователей интересуют киберпреступников все больше

Статистика SOC hoster.by

Информационная безопасность.
С каким вызовами сталкивается бизнес.



На протяжении последних лет заметен рост числа кибератак, связанных с компрометацией учетных данных

Причины роста кибератак

- Развитие e-commerce
- Приход в РБ крупных компаний из других стран
- Спрос на покупку персональных данных и их доступность
- Доступность информации по хакингу
- Отсутствие мер защиты информации

hoster.by

Кейс 1. Исходные данные

Крупная компания с филилиалами по стране

Масштабы:
150 АРМ+
вирт. инфраструктура

Нет аттетстата СЗИ

ЛНПА:
отсутсвуют политики, регламенты и тд

Наличие СрЗИ

AV

Персонал:
Вопросами ИБ занимается 3 человека

hoster.by

Кейс 1. Проблемы для SOC

- Отсутвие логирования
- Не обновленное ПО
- Отсутсвие сегментирования сети
- Отсутствие разграничения доступа
- Не лицензионное ПО
- Отсутствие контроля за соблюдением парольной политики
- Слабые компетенции персонала
- Отсутствие ЗИП для сбора данных

hoster.by

Кейс 2. Исходные данные

Крупное промышленное предприятие

Масштабы: Технологический сегмент + ~200 АРМ

Аттетсованная СЗИ

ЛНПА: разработаны полтики, инструкции и тд

Наличие СрЗИ

NGFW, SIEM, AV

Персонал: Вопросами ИБ занимается 1 человек

hoster.by

Кейс 2. Проблемы для SOC

- Не настроенная SIEM
- Не настроенный NGFW
- Отсутсвие сегментирования сети
- Отсутсвие администраторов СрЗИ
- Слабые компетенции персонала
- Сбор только дефолтных логов
- Рельное отсутвие разграничения доступа
- Не обновленное ПО
- Отсутствие контроля за соблюдением парольной политики
- Отсутствие ЗИП для сбора данных

hoster.by

Антон Тростянко

начальник центра обеспечения
кибербезопасности hoster.by

hoster.by

Связаться со мной:

+375-29-175-25-15
Tlg: trostyanko_av
anton.trostyanko@hoster.by

Сообщить о киберинциденте:

security@hoster.by