DNS Abuse в Беларуси

hoster.by

Антон Тростянко

начальник центра обеспечения
кибербезопасности 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

1000+

Клиентов пользуются услугами инфобеза

1-ое

Гибкое облако для бизнеса

140 000

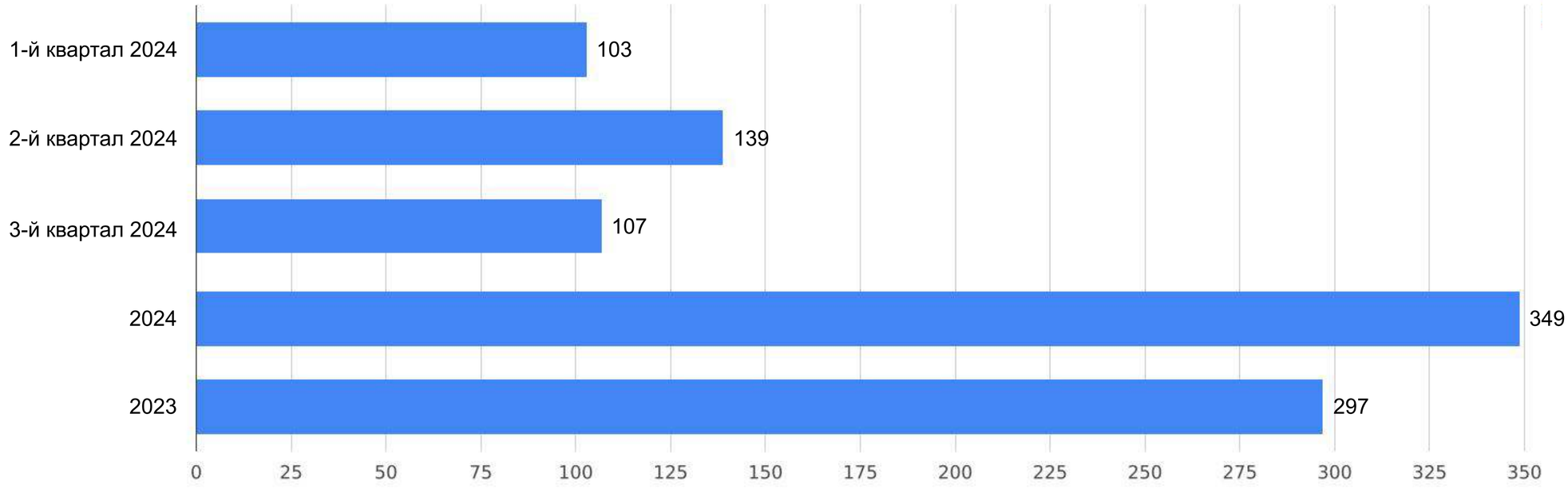
Довольных клиентов. hoster.by — синоним хостинга в Беларуси

130+

Высококлассных специалистов

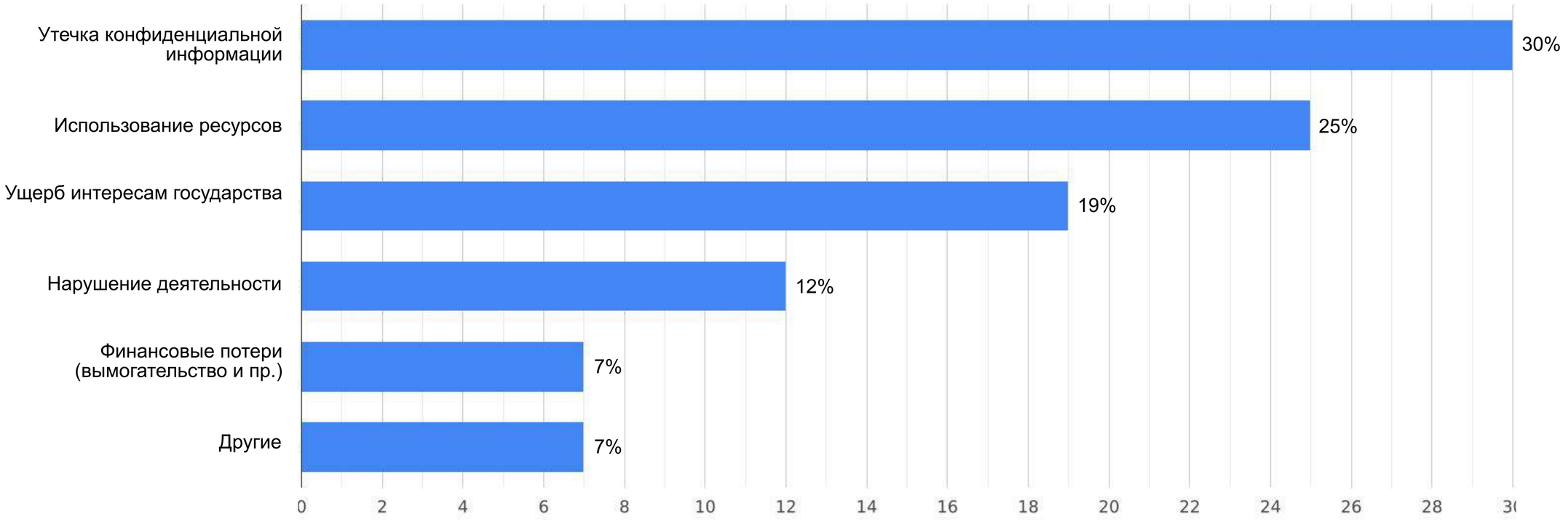
Зарегистрированные киберинциденты

Количество зарегистрированных киберинцидентов по статистике SOC hoster.by



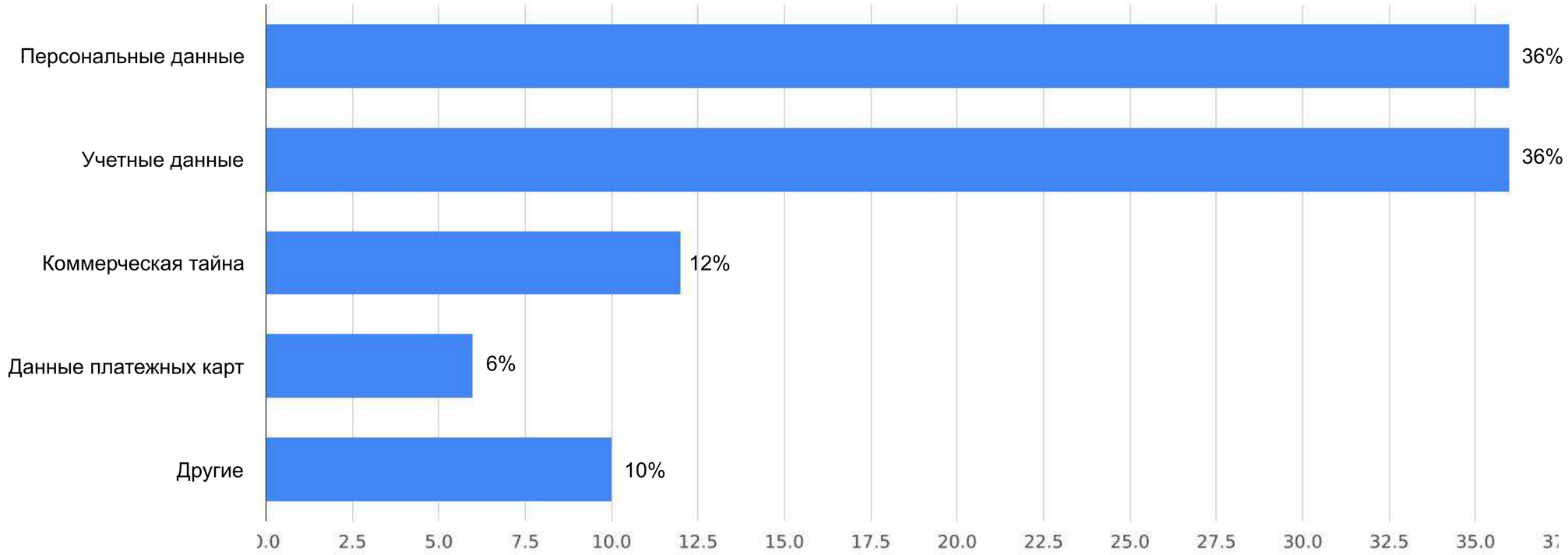
Последствия кибератак

Статистика SOC hoster.by



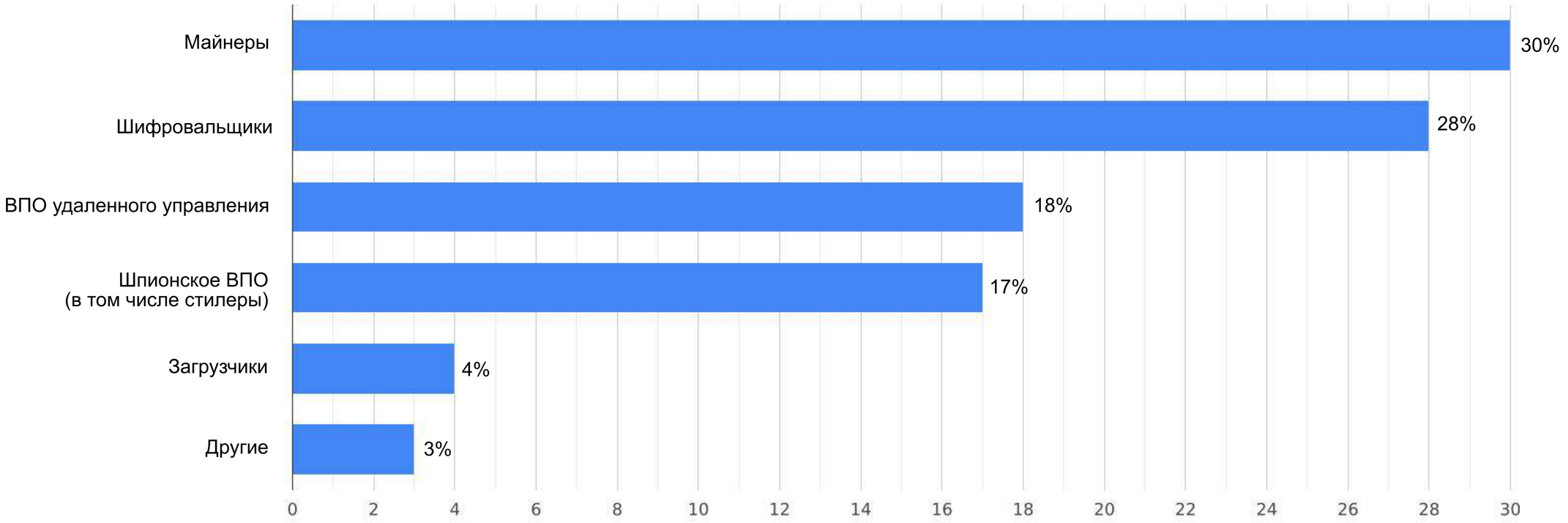
Типы данных

Статистика SOC hoster.by



Типы ВПО

Статистика SOC hoster.by



Самые распространенные формы DNS Abuse по статистике hoster.by

- Вредоносное ПО
- Ботнет
- Фишинг
- Спам
- Фарминг
- DoS и DDos-атаки
- Эксплуатация уязвимостей

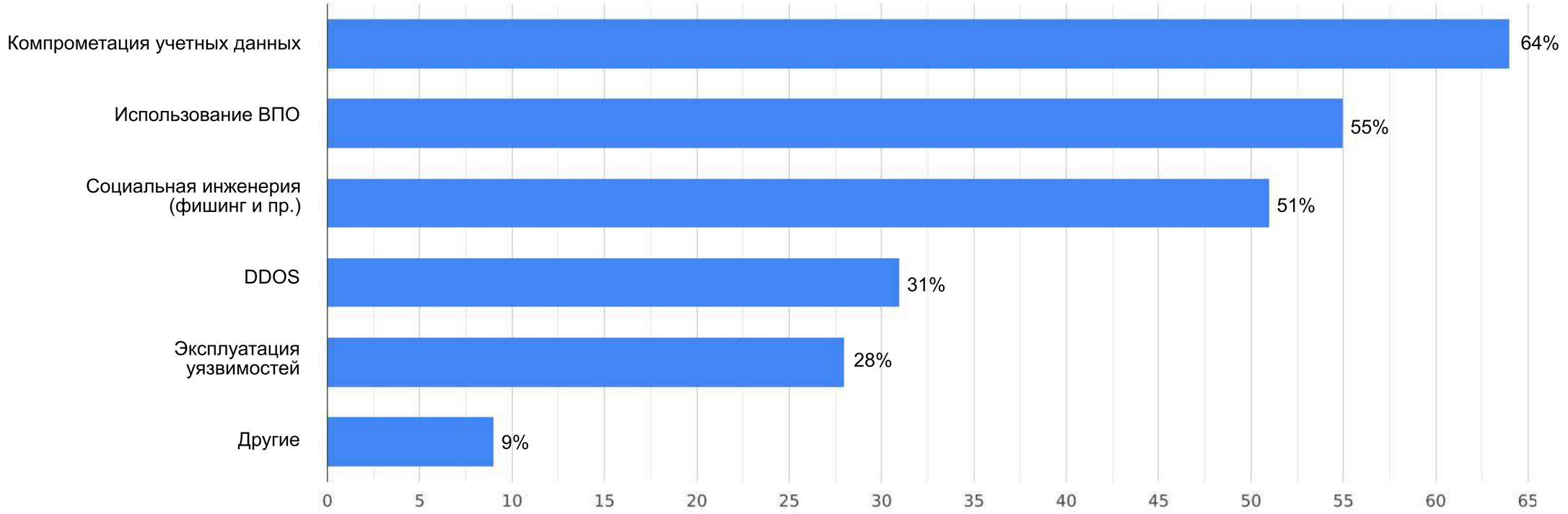
DNS Abuse

Векторы атак в Беларуси, статистика hoster.by

- Получение несанкционированного доступа;
- «Подмена» ресурса;
- Эксплуатация уязвимостей ПО, кода и протоколов;
- Распространение ВПО;
- Социальная инженерия;
- Отказ в обслуживании.

DNS Abuse. Методы атак

Статистика SOC hoster.by



DNS Abuse

Статистика индикаторов компрометации
по данным hoster.by

hoster.by

Сетевые

- Доменные имена
- URL
- Почтовые адреса
- Совокупность IP-адресов и портов
- Аномальный сетевой траффик

Хостовые

- Хэш
- Запущенные процессы
- Изменения веток реестра и файлов
- Идентификаторы уязвимости

Карточка инцидента

Пример карточки по инциденту, зафиксированному SOC hoster.by

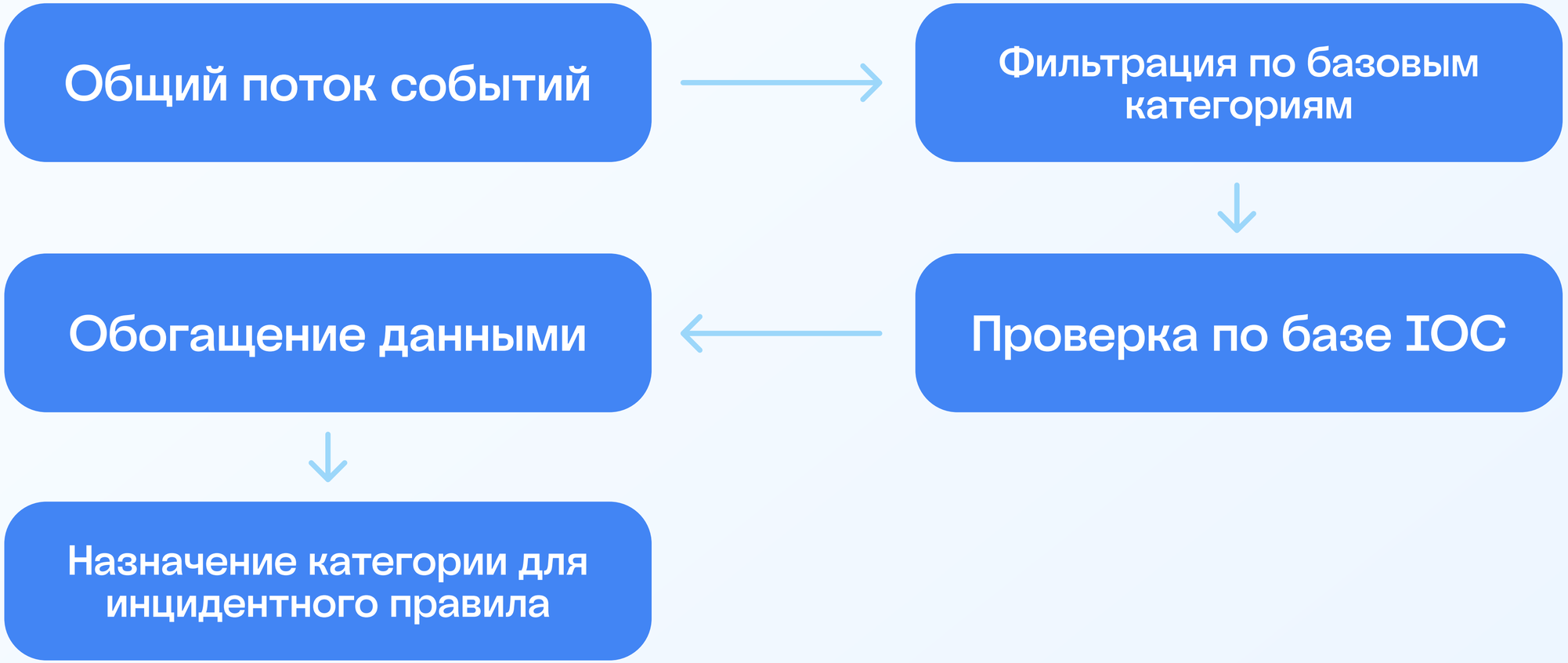
hoster.by

1	**Клиент**			
2	**Индикатор компрометации**		**Результат проверки**	**Заблокировано средствами SOC**
3	**IP-adress**	31.119.199[.]222 87.120.97[.]142 195.91.122[.]213 87.131.62[.]15 46.48.118[.]10	Выявлены сработки (результаты во вложении)	Да
4	**FQDN**	zavodpiva[.]top pochta-medica[.]com business[.]xyz teaspot[.]by	Срабатываний не выявлено	Да
5	**E-mail**	gdc-1971@yandex[.]ru roman.potapov@rambler[.]ru 2098765@gmail[.]com olya-92@mail[.]ru	Данные индикаторы проверить не удалось (не заведены источнкики в SOC)	Нет
6	**Process**	wscript.exe telegram.exe mailby.exe	Срабатываний не выявлено	Нет
7	**File Hash**	"CycK.exe" MD5 dd2739067bfd088a6a1e5f7502105643 SHA1 819dd6a079abab8d34f85d9a1d06a0d556745fb7 SHA256 0b5b79893faa97f10737f52617ff8cdf0de0c0e064ae8303cd12eddf23ee2141	Срабатываний не выявлено	Нет
8	**Прочее**	12.216.18[.]97	Данные индикатор заражения уже находится на онлайн мониторинге	Да

DNS Abuse

Выявление индикаторов компрометации
в hoster.by

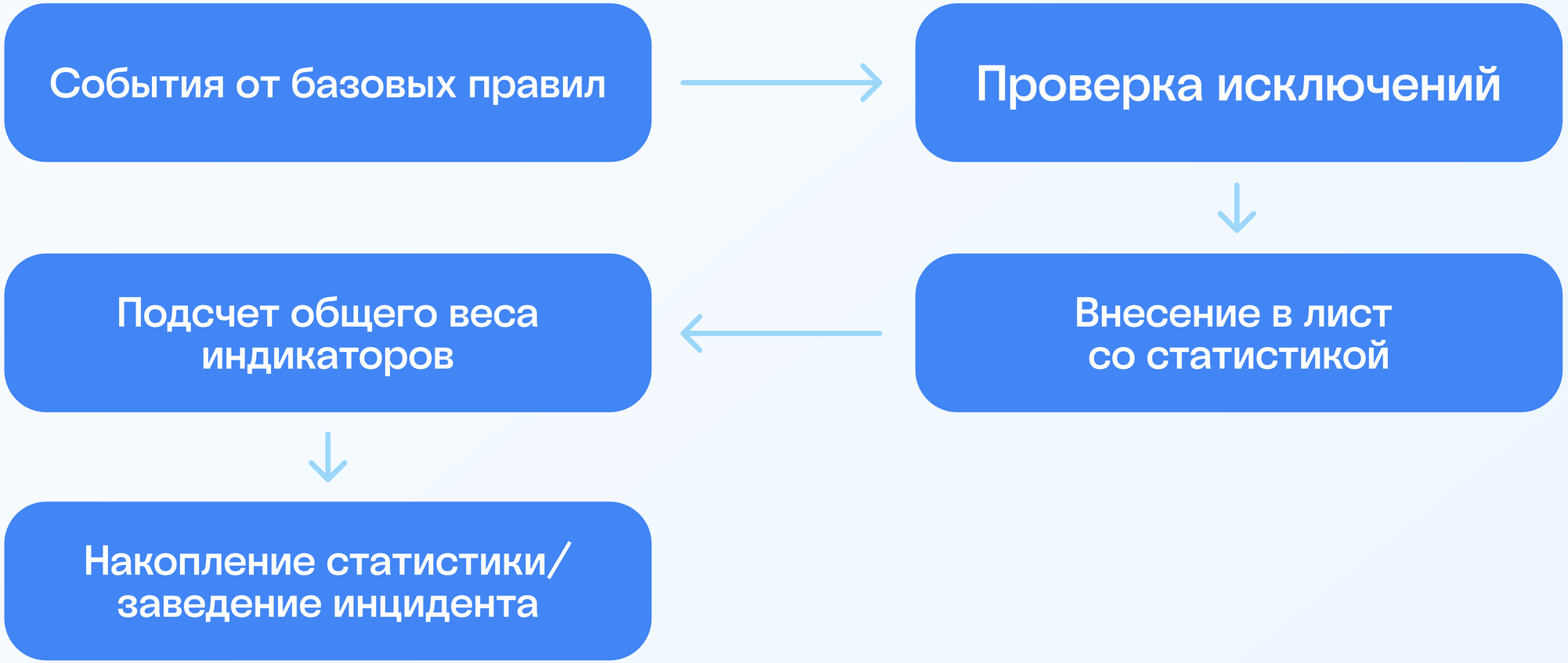
hoster.by



DNS Abuse

Выявление индикаторов компрометации
в hoster.by

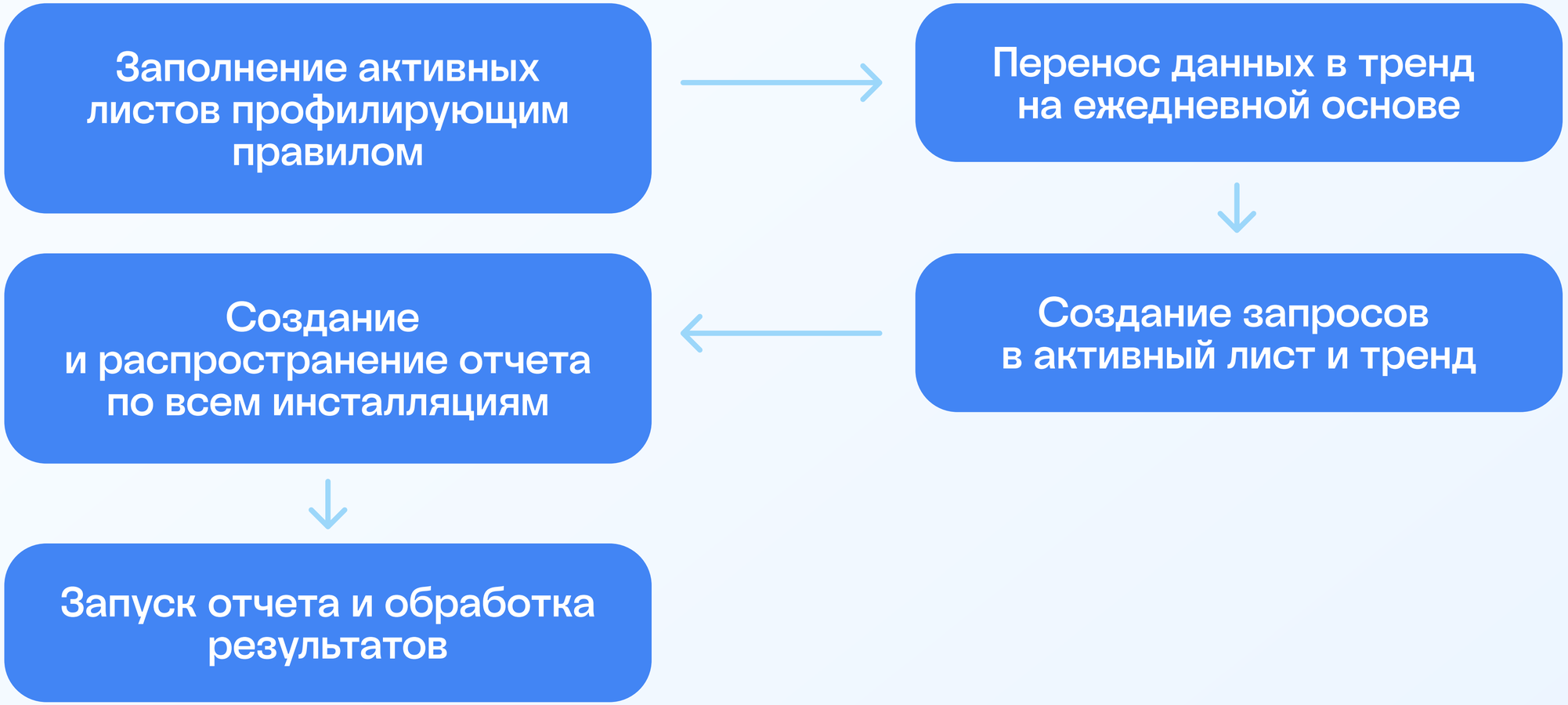
hoster.by



DNS Abuse

Выявление и ретроспективный анализ
индикаторов компрометации в hoster.by

hoster.by



Регистрация и проверка доменных имен

Регистрация доменных имен в национальной доменной зоне осуществляется на основании Приказа Оперативно-аналитического центра при Президенте Республики Беларусь от 18 июня 2010г. №47.

Приказ определяет

- Порядок регистрации доменного имени
- Понятие нарушения порядка регистрации
- Порядок информирования о выявленном нарушении и его устранении
- Порядок и сроки уточнения сведений о владельце доменного имени
- Понятие приостановки администрирования доменного имени и порядок её осуществления

Спасибо за внимание!

hoster.by

Антон Тростянко | начальник SOC hoster.by

security@hoster.by

+375 29 175 25 15

тел. +375 17 239 57 02
A1 +375 29 604 57 02
МТС +375 33 604 57 02
Life:) +375 25 604 57 02