САМАРСКИЙ УНИВЕРСИТЕТ[1]

КРЫМСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ[2]

ИНФРАСТРУКТУРА ДЛЯ ОБНАРУЖЕНИЯ ИСТОЧНИКОВ СЕТЕВЫХ ВТОРЖЕНИЙ С ЭЛЕМЕНТАМИ ТЕХНОЛОГИИ ПРОГРАММНО-КОНФИГУРИРУЕМЫХ СЕТЕЙ

Е.С. Сагатов[1], Д.А. Шкирдов[1], А.М. Сухов[1], А.С. Салимов[2]

Докладчик: Сагатов Евгений Собирович,
доцент кафедры суперкомпьютеров и общей информатики Самарского университета
sagatov@ya.ru

22 марта 2018

Конференция «РусКрипто'2018»

Основные сетевые угрозы для российских телекоммуникационных сетей

- Утечки информации при помощи технологий АНБ (SS7, 4G, IETF RFC, SSH и т.д.)
- Система доменных имён DNS
- Обслуживание внутрироссийского трафика на зарубежных маршрутах
- Использование бот сетей для поиска и эксплуатации уязвимостей

Требования к инфраструктуре для обнаружения сетевых вторжений

- Создание ловушек (приманка, honeynet) для наблюдения за трафиком
- Использование технологий программно-конфигурируемых сетей (software-defined networking, SDN)

У нас установлено 4 сервера-приманки:

- Крым
- Ростов-на-Дону
- Самара
- США

Данные снимаются больше года.

Основные сервисы на сервере-ловушке

№ пп	Сетевой протокол или служба	Программное обеспечение	Возможные типы атак	Путь к файлу с данными
1	VoIP SIP, интернет телефония	Asterisk	Подбор пароля, Входящий звонок для поиска существующего номера	/var/log/asterisk/messages
2	HTTP, веб сервис	Apache, Nginx	Попытка найти phpMyAdmin, админки WordPress и Joomla, Другие запросы	/var/log/nginx/*
3	POP3, IMAP, электронная почта	Dovecot, Exim	Подбор пароля	/var/log/mail.log
4	MySQL, СУБД	MySQL	Подбор пароля	/var/log/mysql/*
5	SMB, служба доступа к сетевым ресурсам	Samba	Подбор пароля	/var/log/samba/*
6	Web Proxy, сервер посредник с возможностью резервирования	Squid	Подбор пароля	/var/log/squid3/access.log
7	SSH, безопасное удаленное управление	OpenSSH-server	Подбор пароля	/var/log/auth.log
8	FTP, протокол передачи файлов	vsftpd	Подбор пароля	/var/log/vsftpd.log
9	DNS Сервис доменных имен	bind9	Уязвимости DNS	/var/log/named.log
10	Межсетевой экран	iptables	Сканирование портов	/var/log/iptables

Схема SDN сети

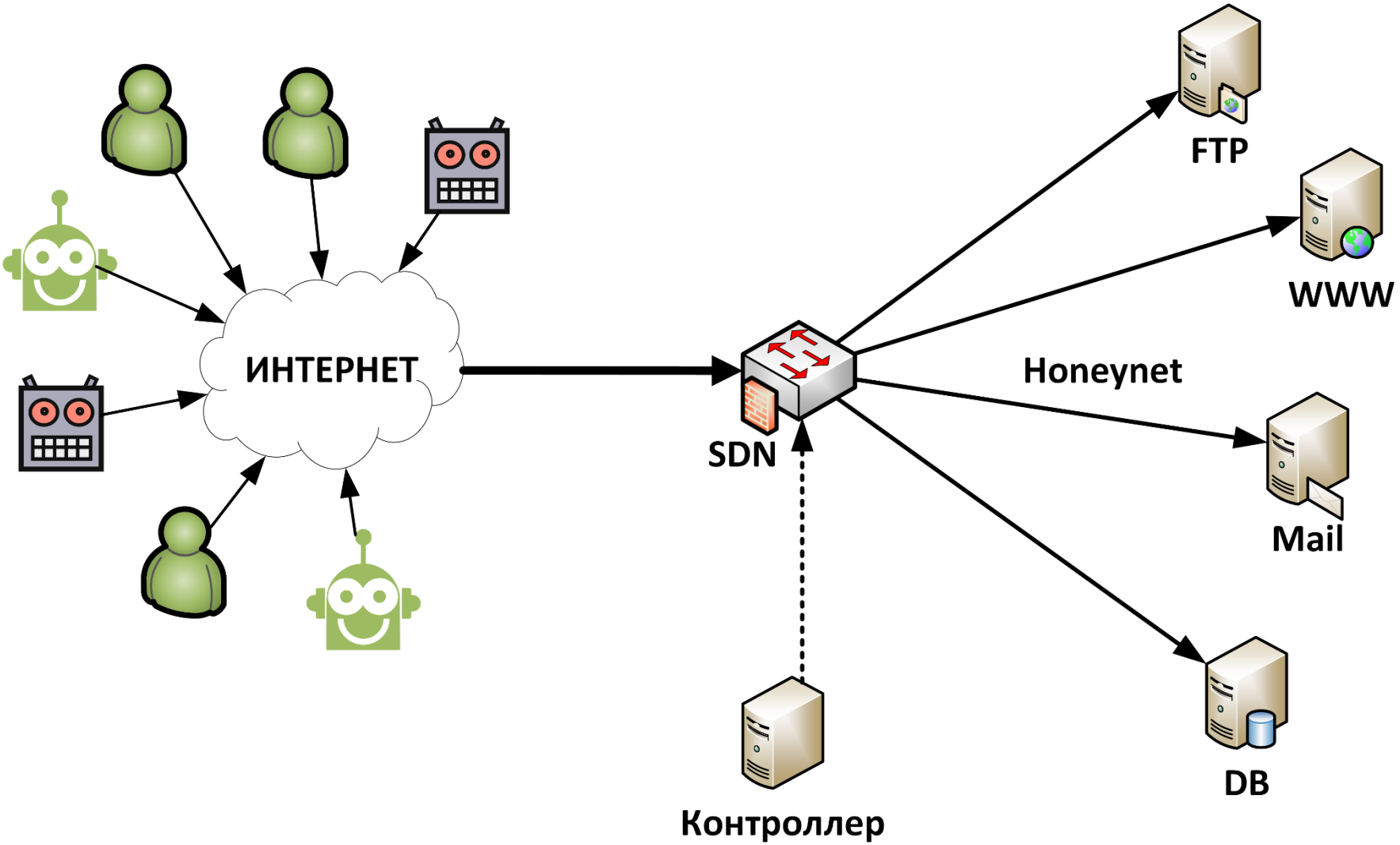
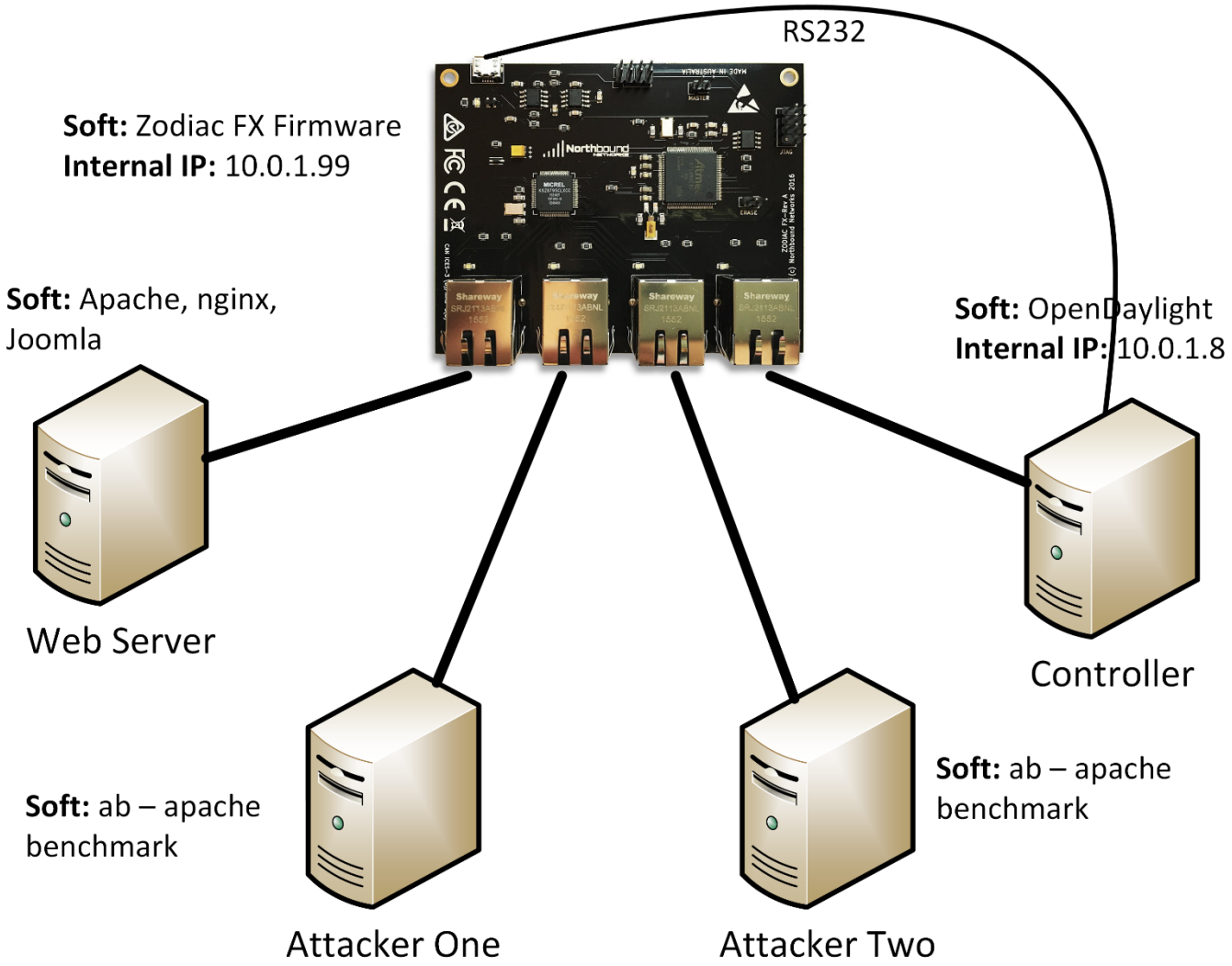


Схема SDN сети



Сервис IP-телефонии

В настоящий момент обработаны данных с 19 марта по 20 сентября 2017 года.

Таблица 1 – Размеры собранных данных

Крым	Самара	Ростов на Дону	США
42,3 ГБ	44,3 ГБ	35,6 ГБ	12,5 ГБ

Основные виды атак на сервис IP-телефонии:

- Попытки дозвониться на внутренний номер с целью поиска номера для дальнейшего подбора пароля.
- Попытки подбора пароля к внутренним номерам.

Статистика по атакам на сервис IP-телефонии

Таблица 2 – Общее число запросов к сервису SIP-телефонии

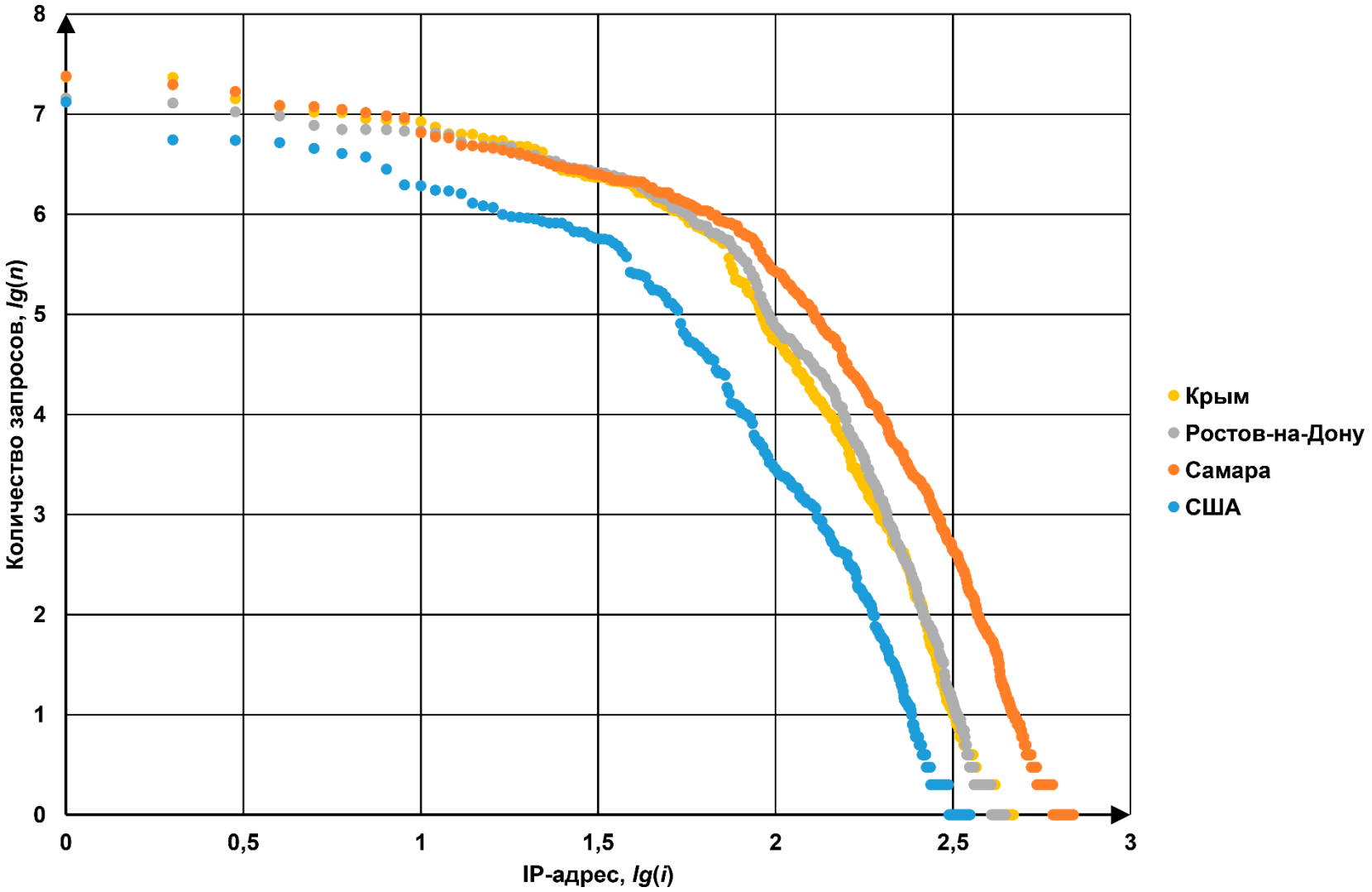
	Крым	Самара	Ростов-на-Дону	США
Попытки позвонить	49 028 881	23 647 564	18 058 059	12 567 250
Попытки подбора пароля	276 046 714	297 105 094	238 501 791	76 551 821
Всего	325 075 595	320 752 658	256 559 850	89 119 071

Таблица 3- Количество уникальных IP-адресов

	Крым	Самара	Ростов-на-Дону	США
Попытки позвонить	758	1098	807	735
Попытки подбора пароля	469	692	445	354

Статистический анализ

$$n_i = \frac{n_1}{i^{\propto}}$$



IP-адреса, с которых атаковали сервис IP-телефонии, на нескольких серверах-ловушках

Таблица 4 – Количество уникальных IP-адресов, совпавших между серверами-ловушками

	США	Крым	Ростов-на Дону	Самара
США	353	59%	23%	18%
Крым	304	468	45%	32%
Ростов-на-Дону	148	281	444	27%
Самара	160	279	304	691

Таблица 5 – Количество уникальных IP-адресов, участвовавших в атаках на три и четыре сервера

Крым, Самара, Ростов-на-Дону	237
Крым США, Ростов-на-Дону	113
Самара, США, Ростов-на-Дону	125
Крым, Самара, США	114
Крым, Самара, США, Ростов-на-Дону	105

Количество запросов с IP-адресов, с которых атаковали сервис IP-телефонии, на нескольких серверах-ловушках

Таблица 6 – Зависимость числа запросов от совпавших IP адресов от общего числа запросов серверов

	США	Крым	Ростов-на-Дону	Самара
США	76 551 821	52%	50%	53%
Крым	181 779 822	276 046 714	89%	76%
Ростов-на-Дону	158 100 459	456 197 846	238 501 791	77%
Самара	197 949 261	435 843 251	410 996 327	297 105 094

Таблица 7 – Зависимость числа запросов от совпавших IP адресов от общего числа запросов между тремя и четырьмя серверами

	Количество запросов	Соотношение от общего числа запросов
Крым, Самара, Ростов на Дону	609 677 640	75%
Крым США, Ростов на Дону	284 555 432	48%
Самара, США, Ростов на Дону	292 186 597	48%
Крым, Самара, США	316 329 671	49%
Крым, Самара, США, Ростов на Дону	416 219 601	47%

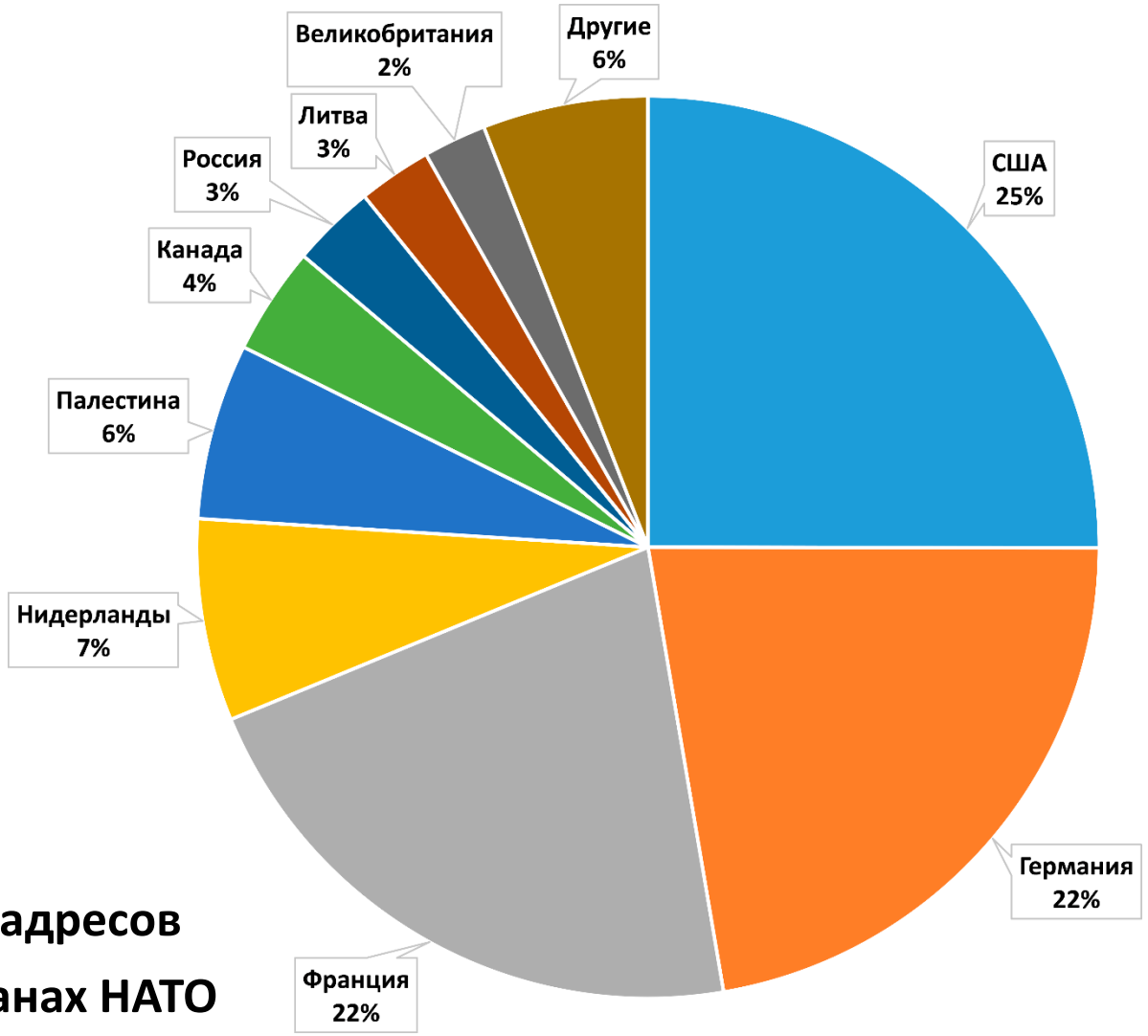
Порядок составления чёрных списков

В чёрный список для IP-телефонии попадают IP-адреса, соответствующие двум критериям:

1) IP-адрес был записан в файлы журналов на двух или более серверах-ловушках;
2) С IP-адреса поступило не менее трёх запросов.

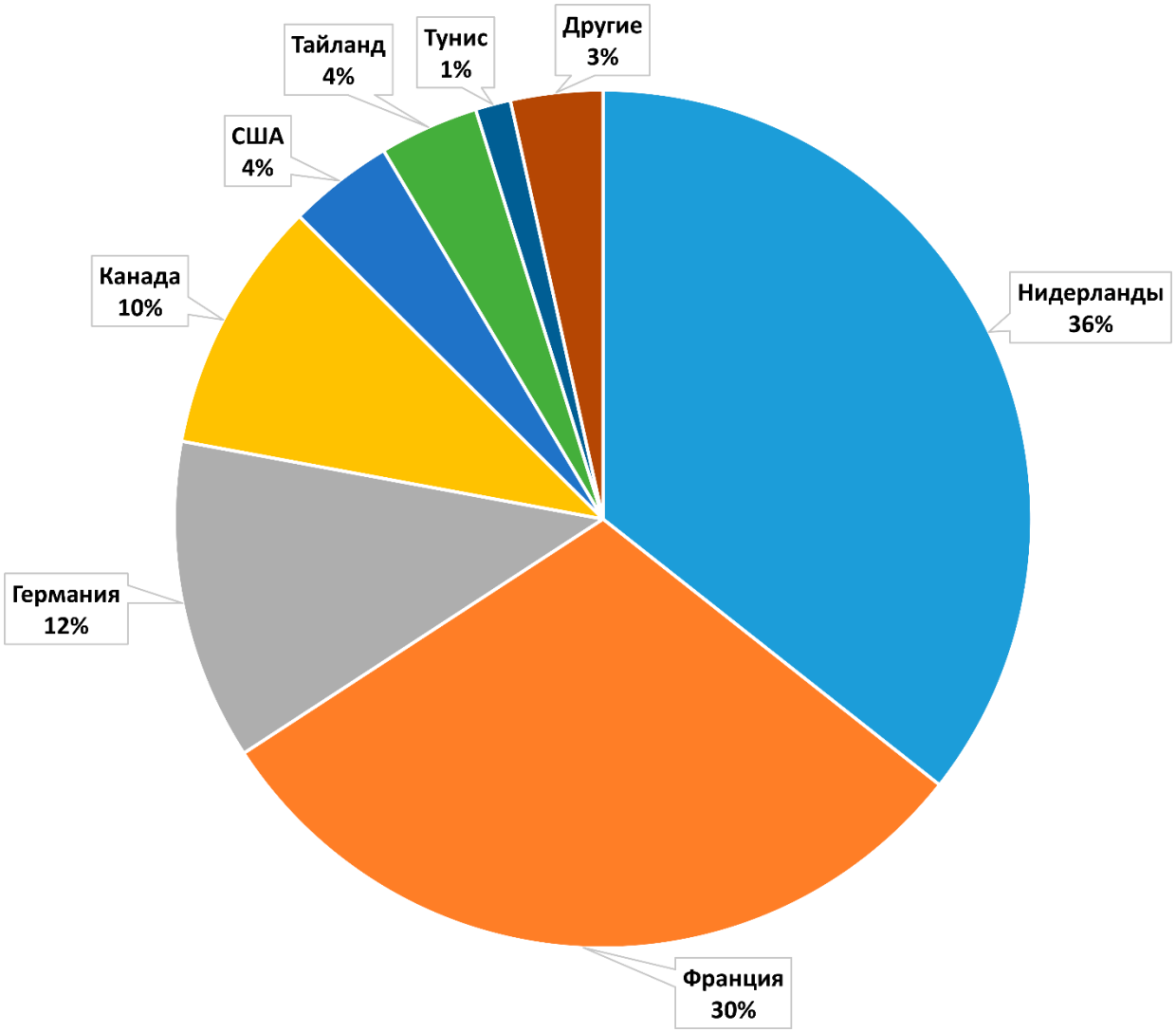
- В настоящий момент в базу вошло 1063 IP-адреса.

Распределение IP-адресов по странам для IP-телефонии



*** 84,7% атакующих адресов расположены в странах НАТО**

Распределение количества запросов по странам для IP-телефонии



Веб-сервис

В настоящий момент обработаны данных с 19 марта по 20 сентября 2017 года.

Таблица 8 – Размеры собранных данных

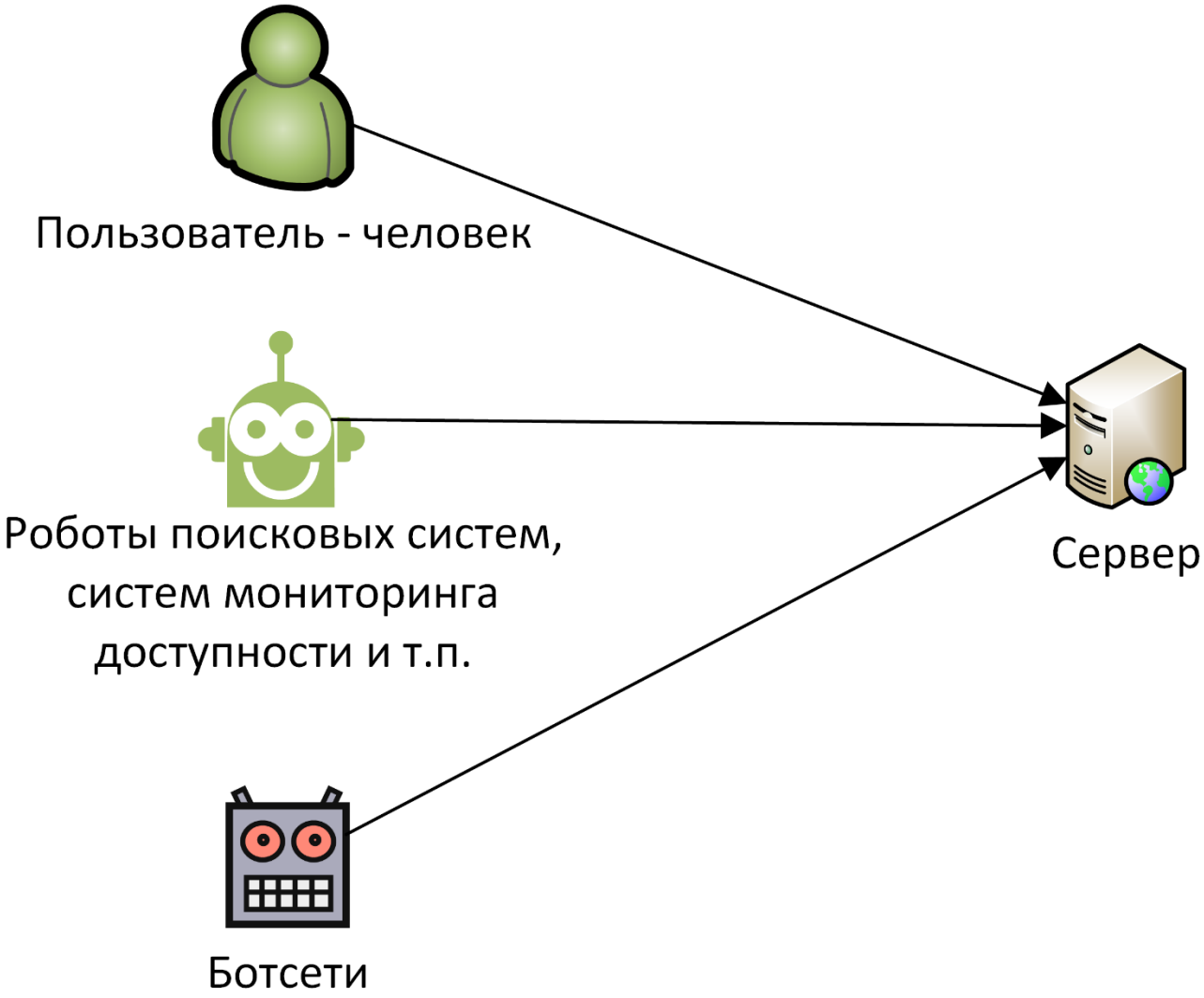
Крым	Самара	Ростов на Дону	США
34,6 МБ	42,0 МБ	154 МБ	34,7 МБ

Основные виды запросов к веб-сервису:

- Попытки доступа к редактору баз данных phpMyAdmin.
- Попытка доступа к административному интерфейсу Joomla.
- Попытки доступа к административному интерфейсу WordPress.
- Оставшиеся запросы (Не отнесенные другим типам) (Требуется доп. анализ запросов)

Необходимо исключить легальные боты Yandex, Google и т.д.

Кто делает запросы к веб-сервисам



Статистика по атакам на веб-сервис

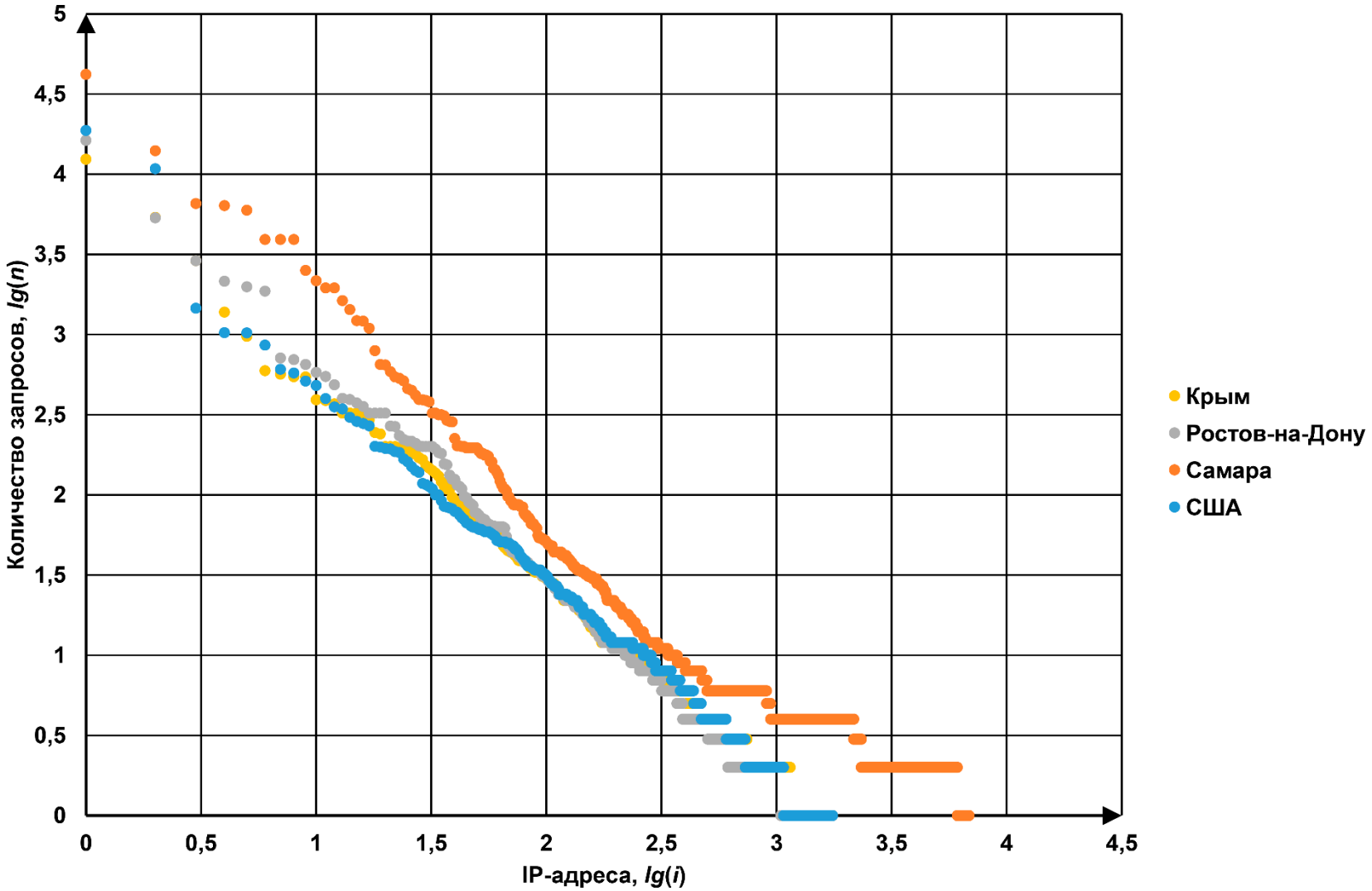
Таблица 9 – Общее число запросов к веб-сервису

	Типы запросов	Крым	Самара	Ростов-на-Дону	США
1	Поиск phpMyAdmin	7 619	11 351	10 333	6 999
2	Админка Joomla	883	2 171	203	144
3	Админка WordPress	11	91 467	3 915	638
4	Боты поисковиков	286	747	715	643
5	Остальное	17 584	16 189	16 041	19 078
	Всего	26 383	121 921	31 207	27 502

Таблица 10- Количество уникальных IP-адресов

		Крым	Самара	Ростов-на-Дону	США
1	Поиск phpMyAdmin	151	206	148	160
2	Админка Joomla	176	38	33	23
3	Админка WordPress	5	4 756	9	16
4	Боты поисковиков	77	143	95	102
5	Остальное	1 355	1 882	1 318	1 270
	Всего	1 644	6 861	1 490	1 461

Статистический анализ для веб-сервиса



IP-адреса, с которых атаковали веб-сервис, на нескольких серверах-ловушках

Таблица 11 – Количество уникальных IP-адресов, совпавших между серверами-ловушками

	США	Крым	Ростов-на-Дону	Самара
США	1 461	15%	15%	6%
Крым	411	1 644	19%	7%
Ростов-на-Дону	391	511	1 490	6%
Самара	454	537	506	6 861

Таблица 12 – Количество уникальных IP-адресов между тремя и четырьмя серверами

Крым, Самара, Ростов-на-Дону	397
Крым США, Ростов-на-Дону	323
Самара, США, Ростов-на-Дону	313
Крым, Самара, США	328
Крым, Самара, США, Ростов-на-Дону	285

Количество запросов с IP-адресов, с которых атаковали веб-сервис, на нескольких серверах-ловушках

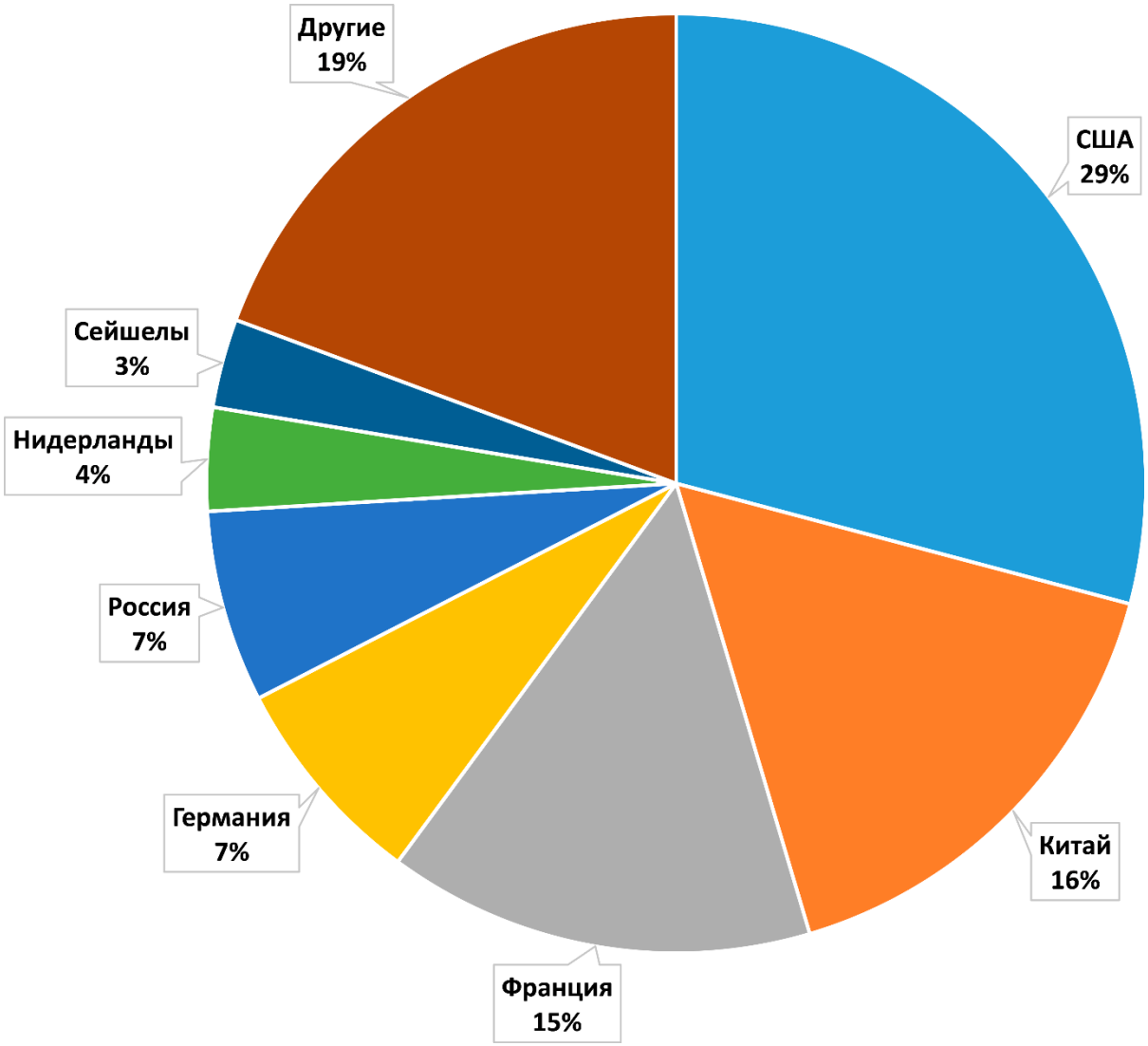
Таблица 13 – Зависимость числа запросов совпавших IP адресов от общего числа запросов серверов

	США	Крым	Ростов-на-Дону	Самара
США	50 463	35%	33%	32%
Крым	31 862	40704	18%	24%
Ростов-на-Дону	32 845	3446	49495	25%
Самара	60 778	44391	47715	141329

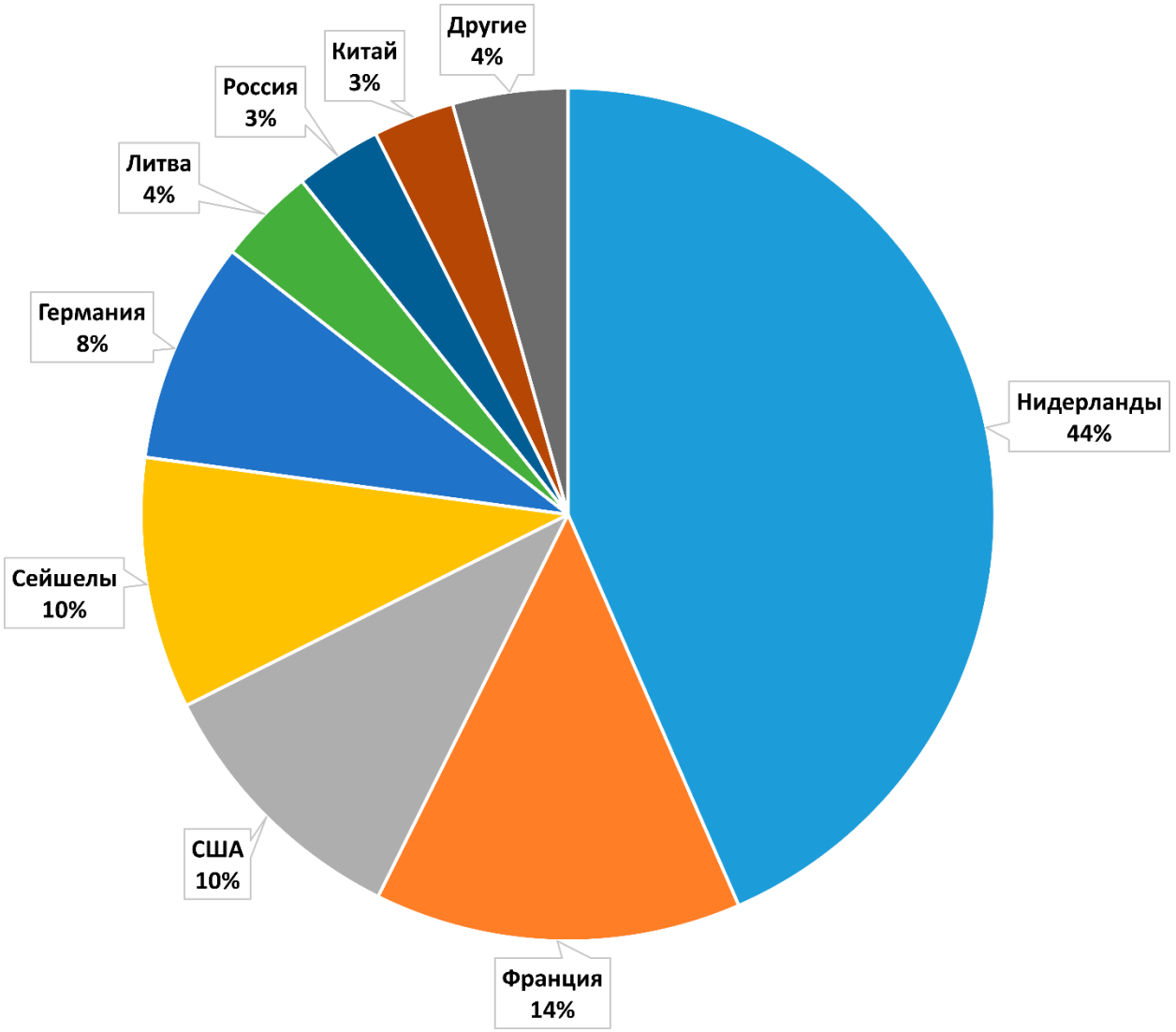
Таблица 14 – Зависимость числа запросов совпавших IP адресов от общего числа запросов между тремя и четырьмя серверами

	Количество запросов	Соотношение от общего числа запросов
Крым, Самара, Ростов-на-Дону	42626	18%
Крым, США, Ростов-на-Дону	42899	30%
Самара, США, Ростов-на-Дону	46765	19%
Крым, Самара, США	45461	20%
Крым, Самара, США, Ростов-на-Дону	56131	20%

Распределение IP-адресов по странам для веб-сервиса



Распределение количества запросов по странам для веб-сервиса



Порядок составления чёрных списков для веб-сервиса

В чёрный список для веб-сервисов попадают IP-адреса, соответствующие двум критериям:

1) IP-адрес был записан в файлы журналов на двух или более серверах-ловушках;
2) С IP-адреса поступило не менее трёх запросов.

- В настоящий момент в базу вошло 817 IP-адресов.

Сервис DNS

В настоящий момент обработаны данных с 19 марта по 20 сентября 2017 года.

Таблица 15 – Размеры собранных данных

Крым	Самара	Ростов на Дону	США
11,6 МБ	3,62 МБ	11 МБ	1,12 МБ

Основные виды запросов в журналах DNS службы:

1. Denied – запрещённые внутренними политиками bind;
2. Resolving error – ошибка при разрешении имени.

Статистика по атакам на DNS сервис

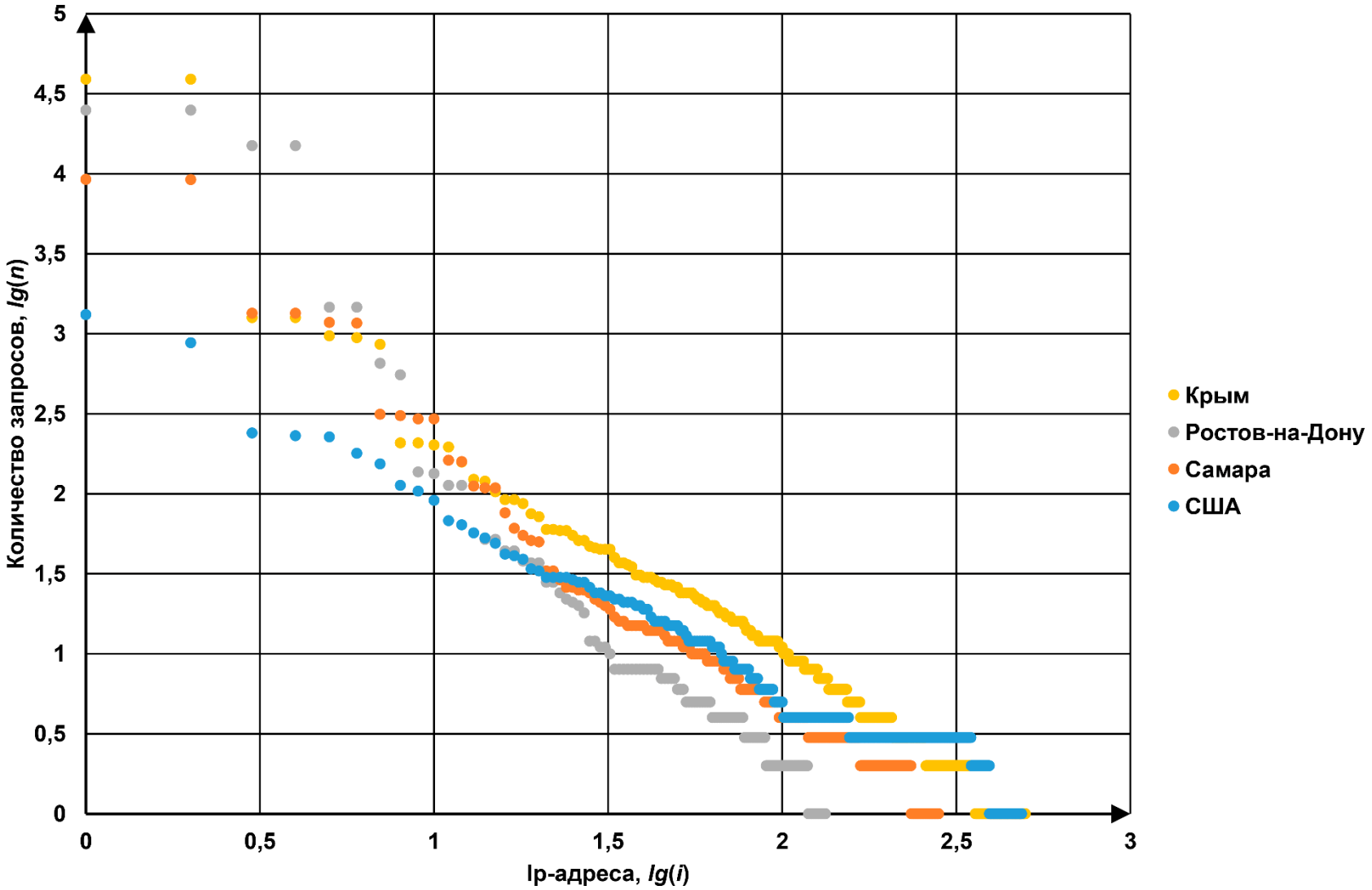
Таблица 16 – Общее число запросов к DNS сервису

	Типы запросов	Крым	Самара	Ростов-на-Дону	США
1	Denied	2 985	1 436	0	6 084
2	Resolving errors	85 306	25 499	85 591	0
	Всего	88 291	26 935	85 591	6 084

Таблица 17- Количество уникальных IP-адресов

	Типы запросов	Крым	Самара	Ростов-на-Дону	США
1	Denied	308	201	0	487
2	Resolving	191	81	133	0
	Всего	499	281	133	487

Статистический анализ для сервиса DNS



IP-адреса, с которых атаковали DNS сервис, на нескольких серверах-ловушках

Таблица 18 – Количество уникальных IP-адресов, совпавших между серверами-ловушками

	США	Крым	Ростов-на-Дону	Самара
США	487	36%	0%	31%
Крым	209	308	27%	0%
Ростов-на-Дону	0	93	133	36%
Самара	135	0	57	81

Таблица 19 – Количество уникальных IP-адресов между тремя и четырьмя серверами

Крым, Самара, Ростов на Дону	53
Крым США, Ростов на Дону	0
Самара, США, Ростов на Дону	0
Крым, Самара, США	118
Крым, Самара, США, Ростов на Дону	0

Количество запросов с IP-адресов, с которых атаковали DNS сервис, на нескольких серверах-ловушках

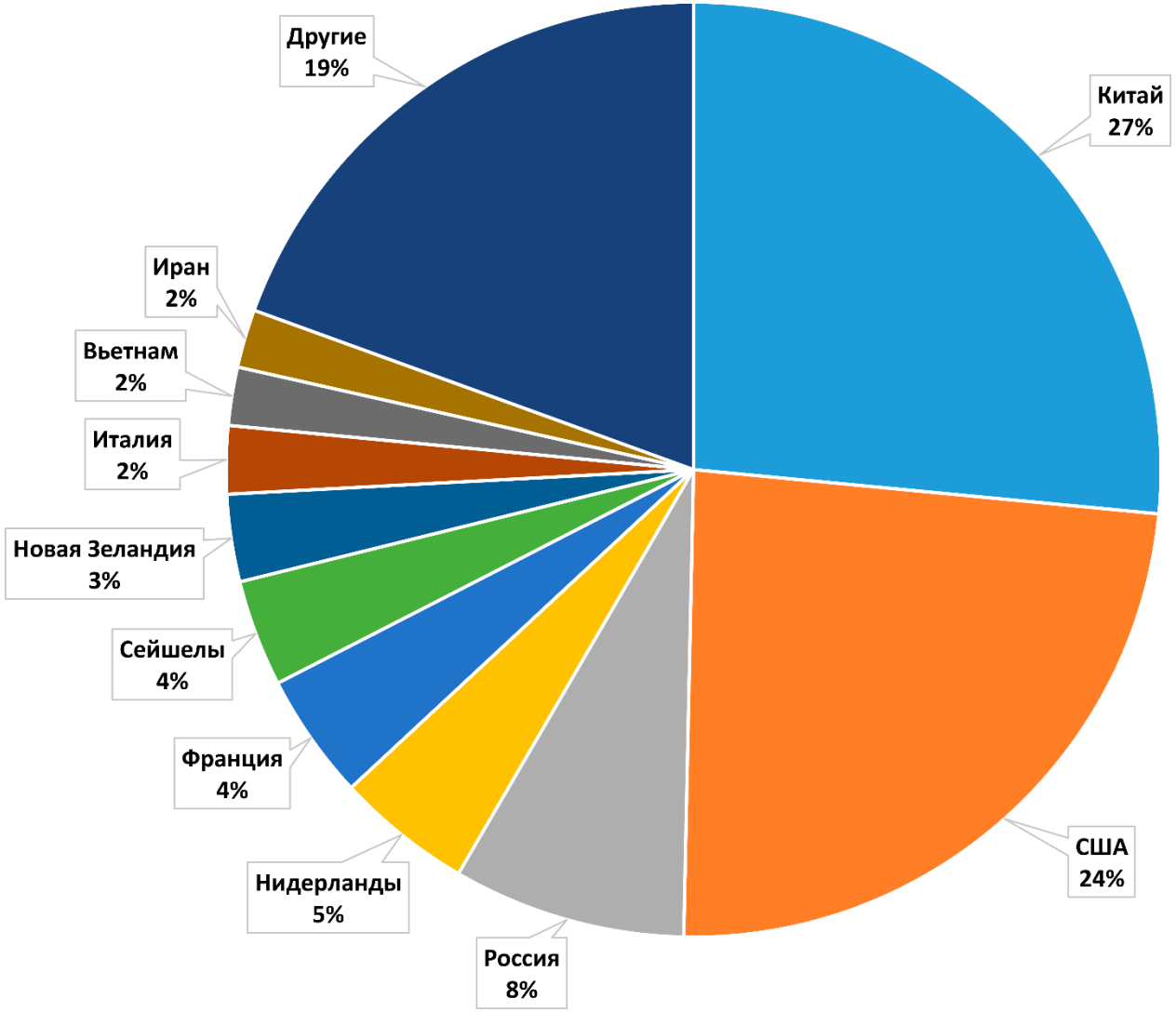
Таблица 20 – Зависимость числа запросов совпавших IP адресов от общего числа запросов серверов

	США	Крым	Ростов-на-Дону	Самара
США	6 063	7%	0%	14%
Крым	6 434	88 291	68%	80%
Ростов-на-Дону	0	117 624	85 591	98%
Самара	4 683	92 383	110 009	26 935

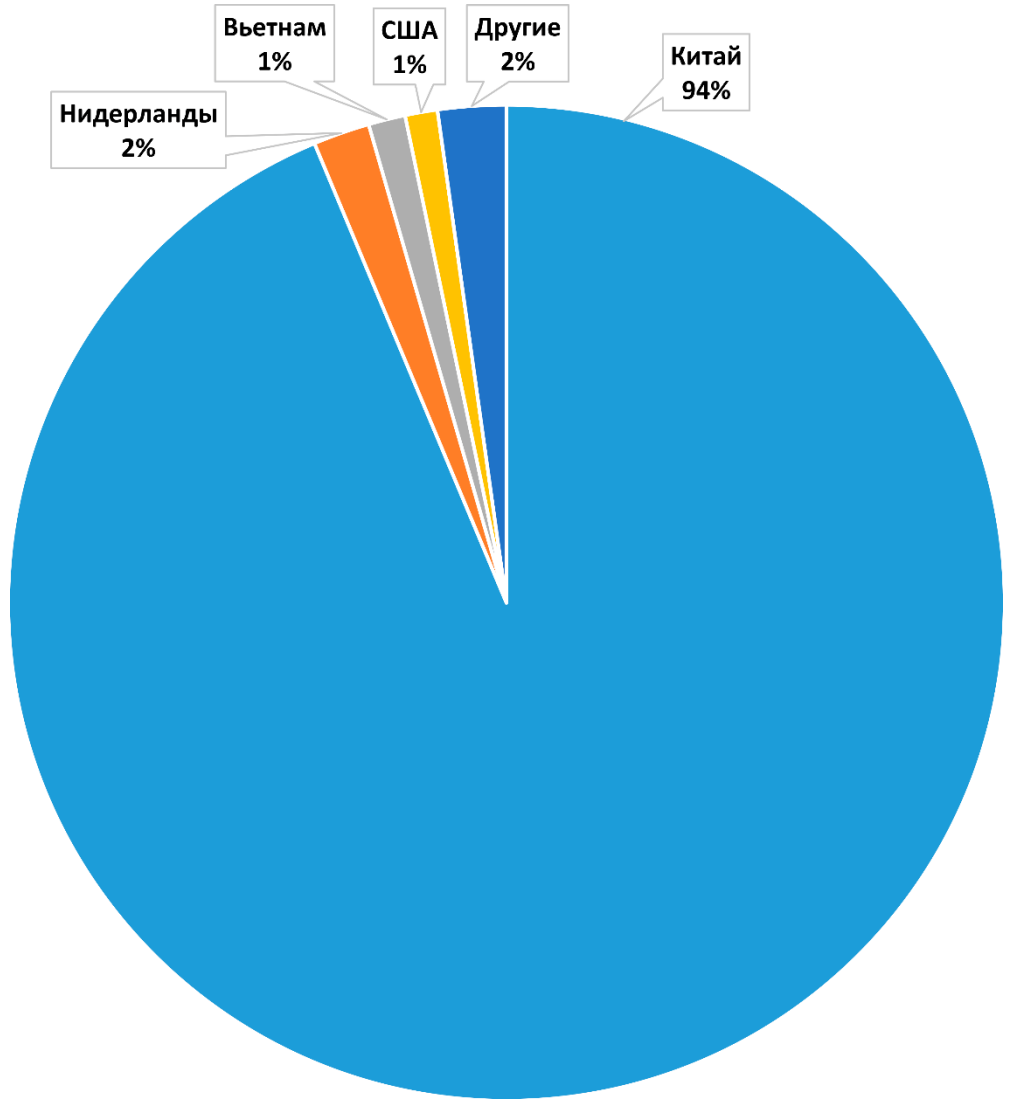
Таблица 21 – Зависимость числа запросов совпавших IP адресов от общего числа запросов между тремя и четырьмя серверами

	Количество запросов	Соотношение от общего числа запросов
Крым, Самара, Ростов на Дону	122 996	61%
Крым США, Ростов на Дону	0	0%
Самара, США, Ростов на Дону	0	0%
Крым, Самара, США	7 184	6%
Крым, Самара, США, Ростов на Дону	0	0%

Распределение IP-адресов по странам для сервиса DNS



Распределение количества запросов по странам для сервиса DNS



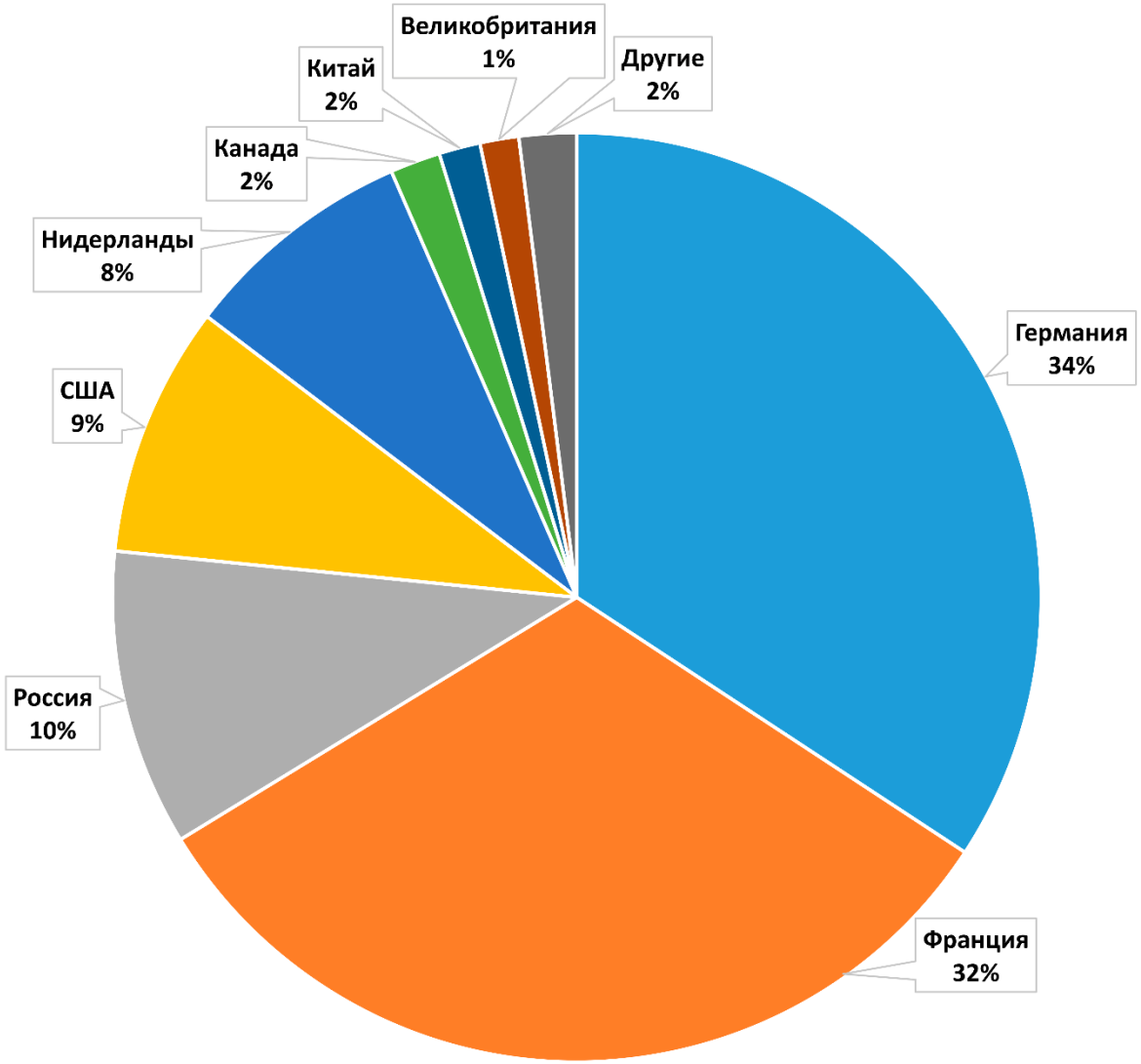
Порядок составления чёрных списков для DNS сервиса

В чёрный список для DNS сервиса попадают IP-адреса, соответствующие двум критериям:

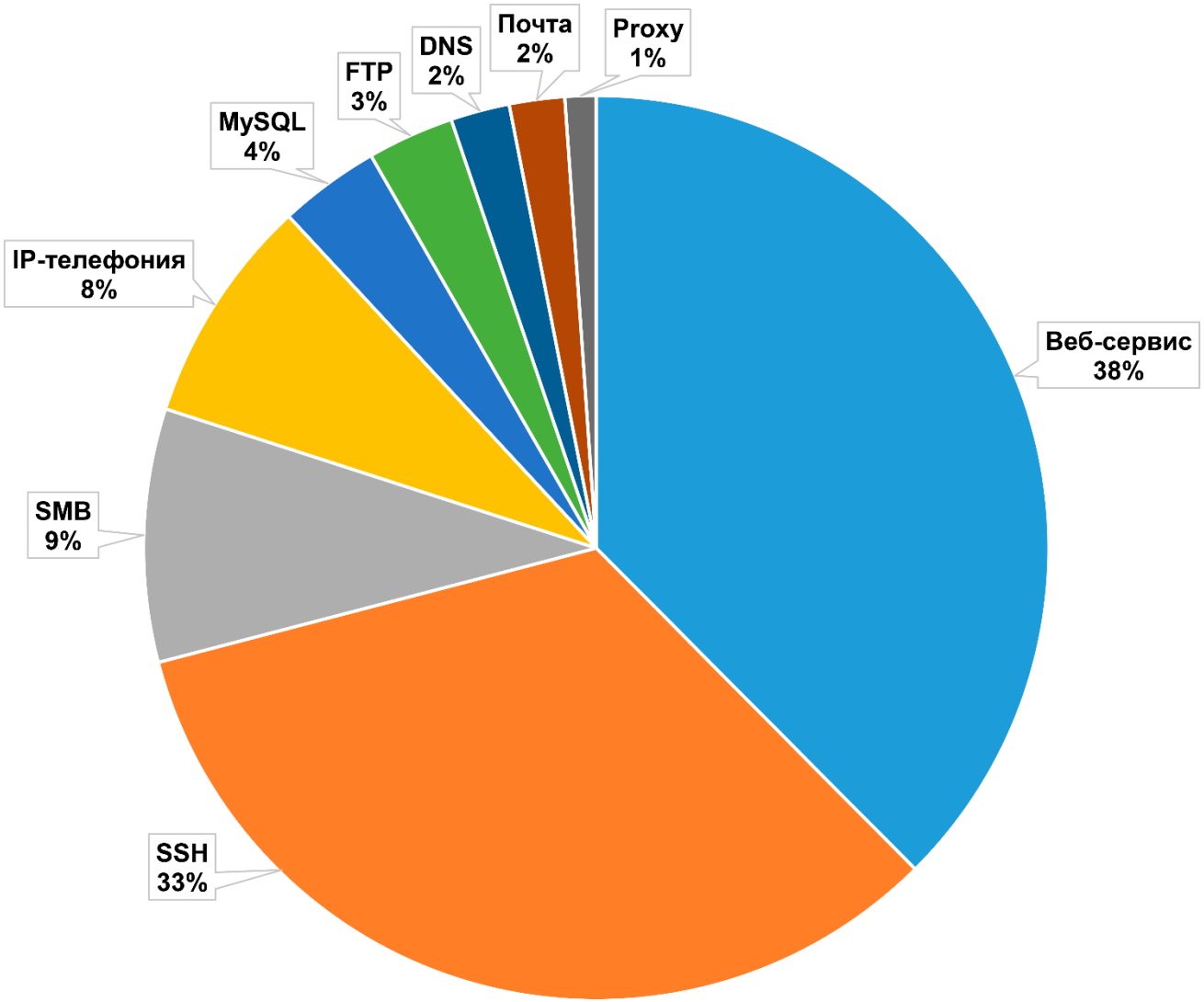
1) IP-адрес был записан в файлы журналов на двух или более серверах-ловушках;
2) С IP-адреса поступило не менее трёх запросов.

- В настоящий момент в базу вошло 352 IP-адреса.

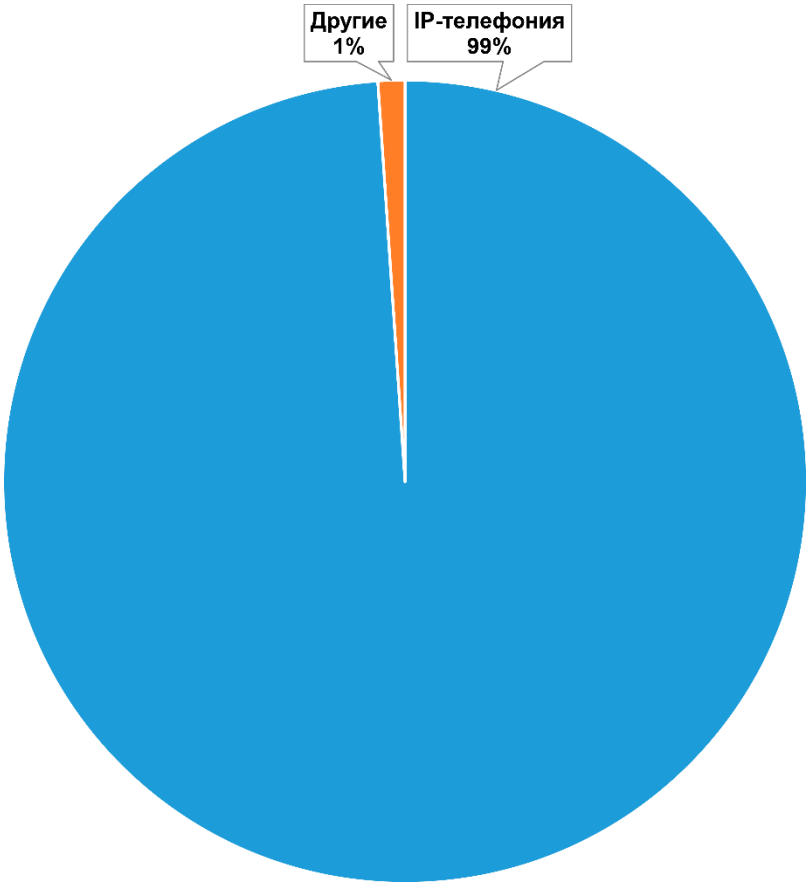
Распределение количества запросов по странам для сканирования портов



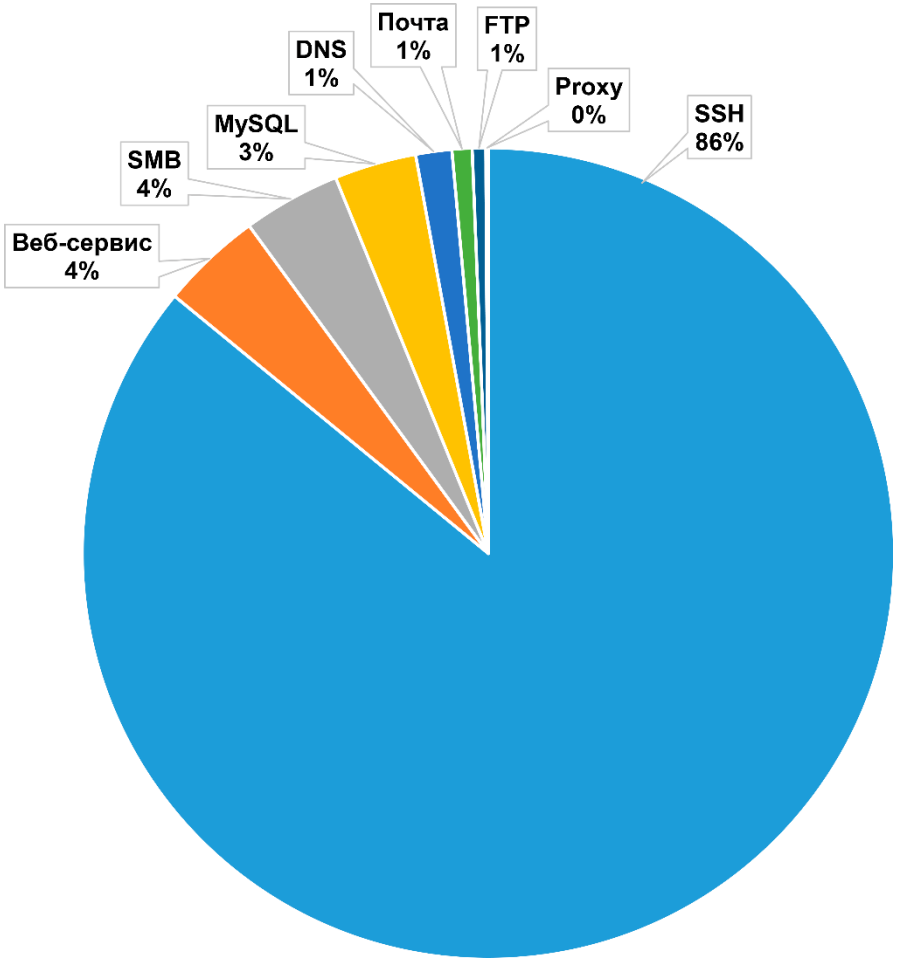
Количество уникальных адресов для каждого сервиса



Количество записанных запросов для каждого сервиса



Другие сервисы без IP-телефонии



Спасибо за внимание!

Контакты: Сагатов Евгений Собирович

sagatov@ya.ru

Работа выполняется в рамках государственного задания Министерства образования и науки РФ (проект 2.974.2017/4.6) и при поддержке гранта РФФИ № 16-07-00218а.