ГАРДА
ТЕХНОЛОГИИ

АНАЛИТИКА DDOS-АТАК

ЗА IV КВАРТАЛ 2022 ГОДА

ВСТУПЛЕНИЕ

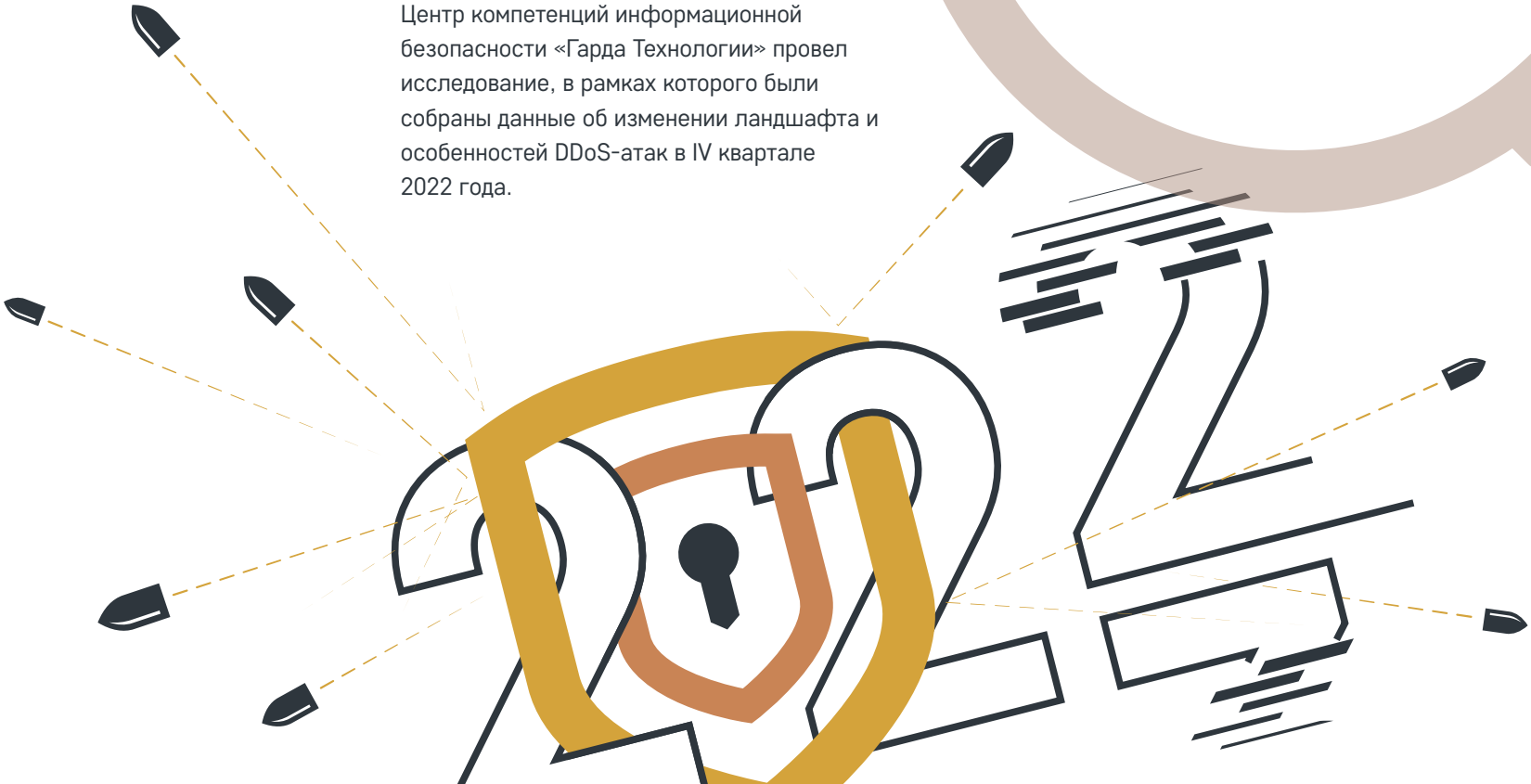
2022 год стал годом высокой активности киберперступников.

DDoS-атаки стали едва ли не самым популярным их «оружием»: если с февраля эта тема постоянноприсутствовала в заголовках различных СМИ, то к четвертому кварталу общемировые тенденции несколько изменились.

Центр компетенций информационной безопасности «Гарда Технологии» провел исследование, в рамках которого были собраны данные об изменении ландшафта и особенностей DDoS-атак в IV квартале 2022 года.

Содержание

Методика исследования
Типы DDoS-атак
Распределение по дням недели
Страны и территории
География атак на ловушки
Заключение



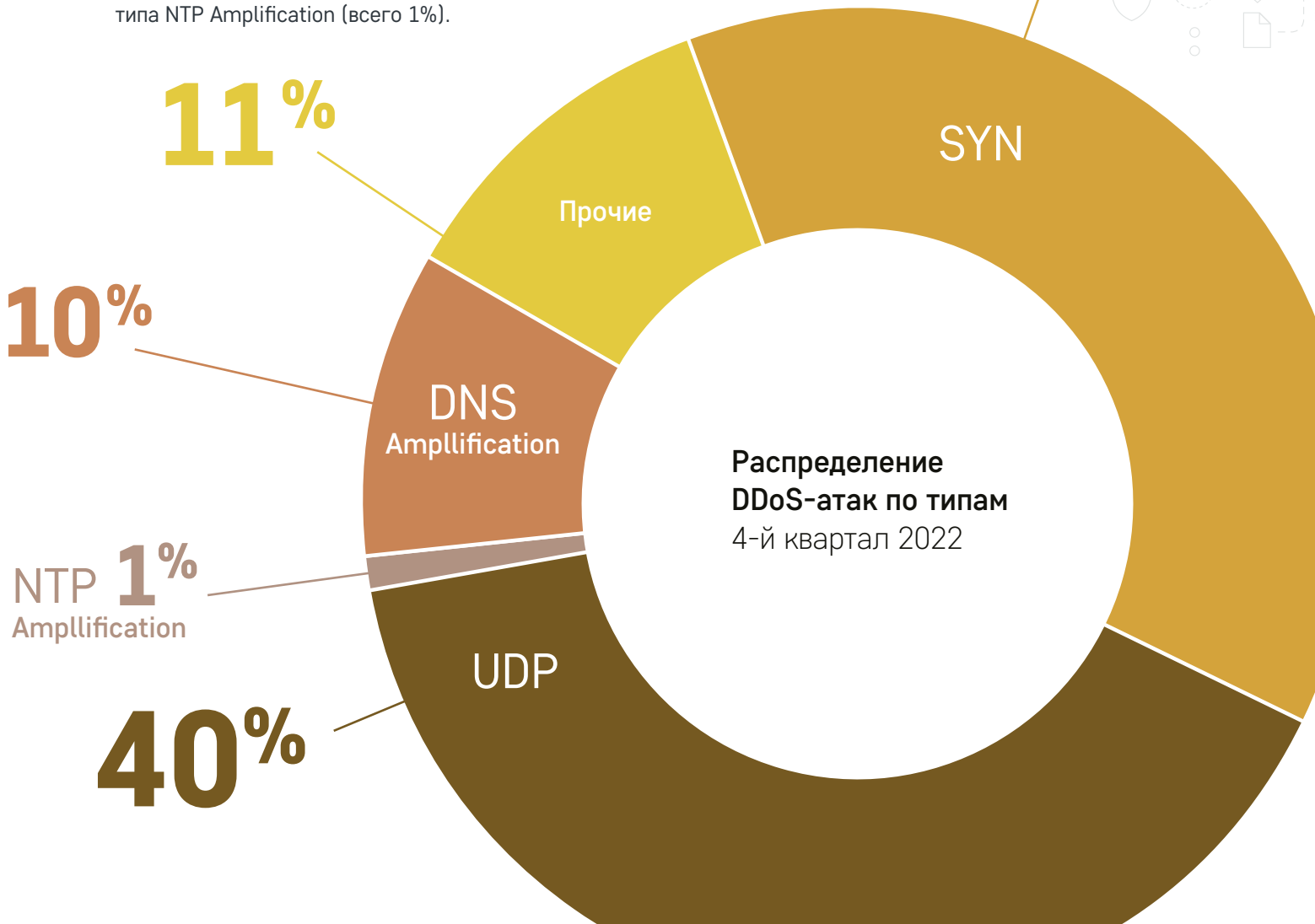
МЕТОДИКА ИССЛЕДОВАНИЯ

Цель исследования — определить основные типы атак, которым подвергались компании, и их распределение по странам и территориям.

Данные собирались с помощью территориально распределенных ловушек, расположенных в 10 крупнейших странах мира (США, страны Европы и др.), и обрабатывались собственной аналитической платформой «Гарда Технологии». Для получения более релевантных результатов, данные усреднялись по числу ловушек, расположенных в конкретном государстве, очищались от запросов поисковых роботов, сканеров сети интернет, и запросов прочих легальных сервисов, а дополнительное обогащение контекстом позволило точнее верифицировать результаты.

ТИПЫ DDOS-АТАК

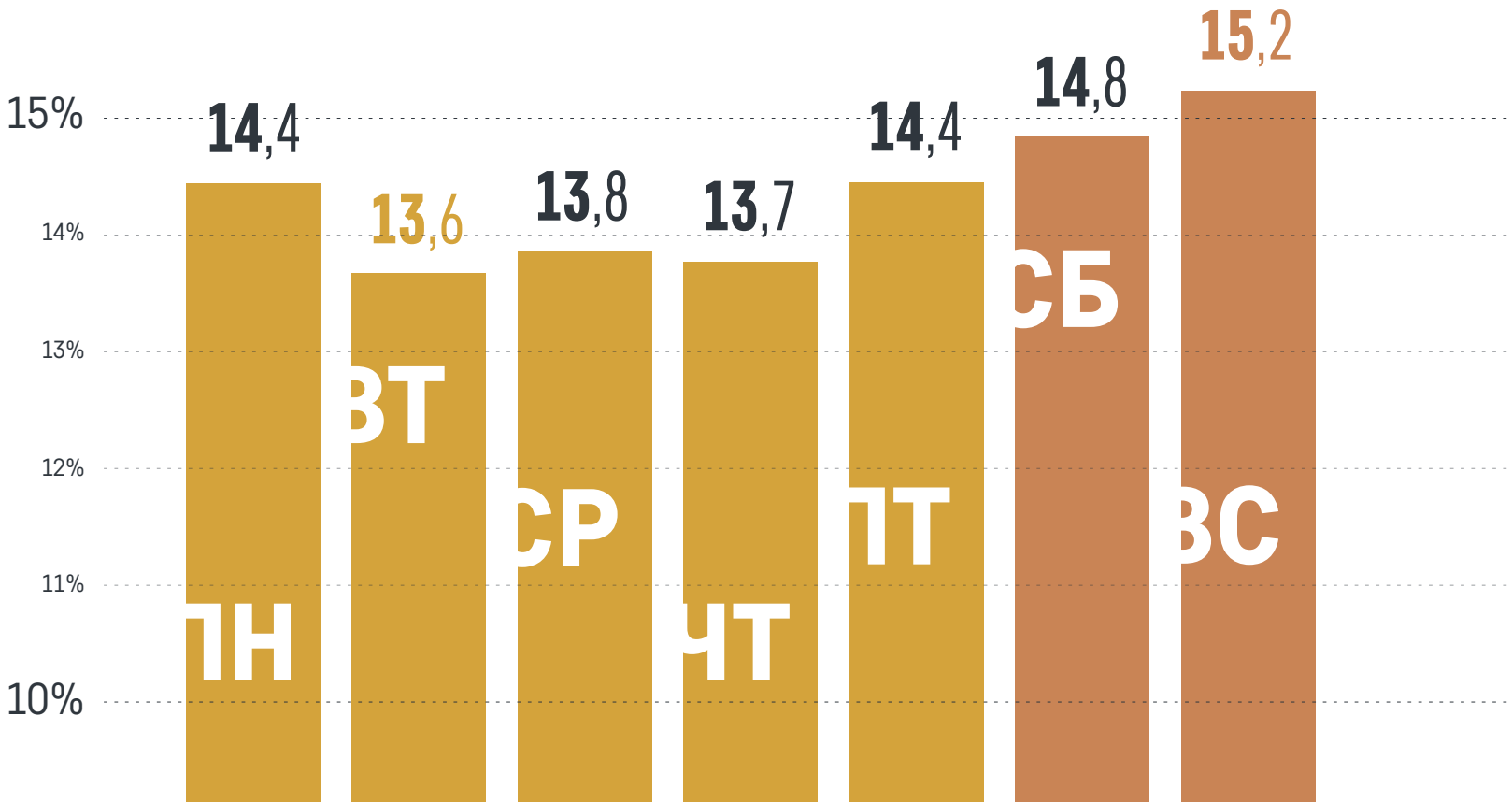
По результатам IV квартала по-прежнему остается высокой доля UDP-флуда (40%), SYN-флуд занимает второе место и практически догнал UDP (38%), при этом отмечается низкий уровень атак типа NTP Amplification (всего 1%).



РАСПРЕДЕЛЕНИЕ ПО ДНЯМ НЕДЕЛИ

Наибольшую активность преступники проявляют в выходные дни. В целом, однако, общий фон атак довольно равномерен — вне зависимости от дня недели.

Распределение DDoS-атак по дням недели / за 4-й квартал 2022

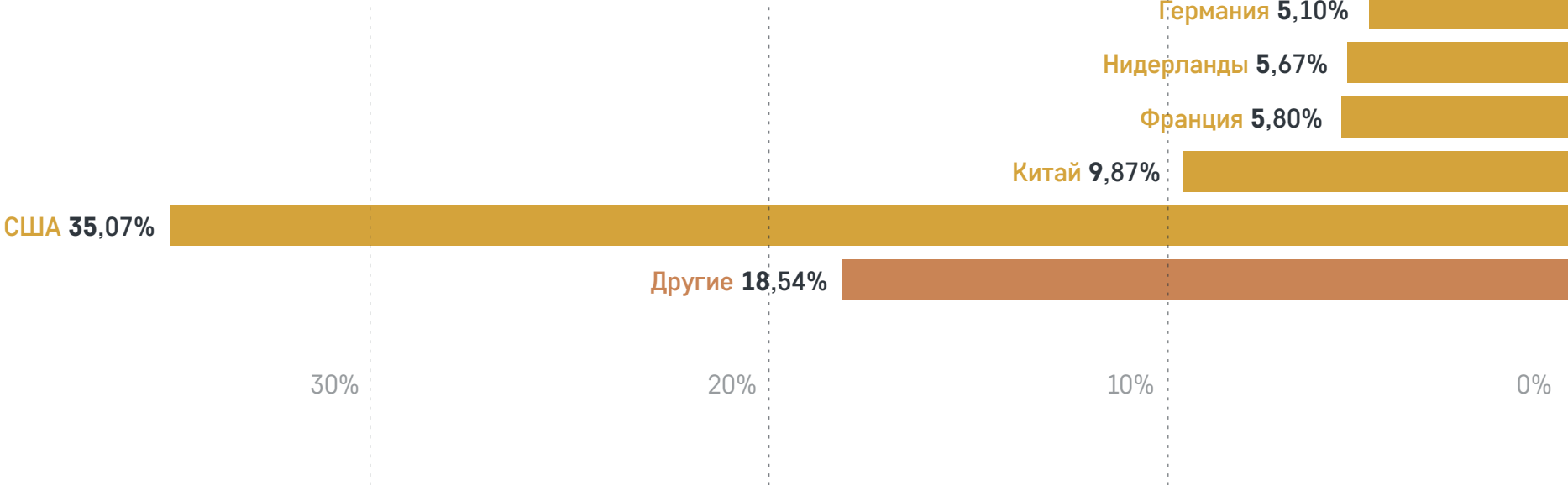


СТРАНЫ И ТЕРРИТОРИИ

Вопреки мнению о том, что геополитические события сделали Россию самой популярной мишенью для хакеров, в общемировом раскладе страной, в которой зафиксировано максимальное количество DDoS-атак, стали США (35%), за ними с большим отставанием следует Китай (почти 10%). При этом Китай атакуют вдвое активнее, чем Францию или Германию, хотя совсем недавно они были на одном уровне. Россия занимает 13 место (1%).

Распределение DDoS-атак по странам и территориям

4-й квартал 2022

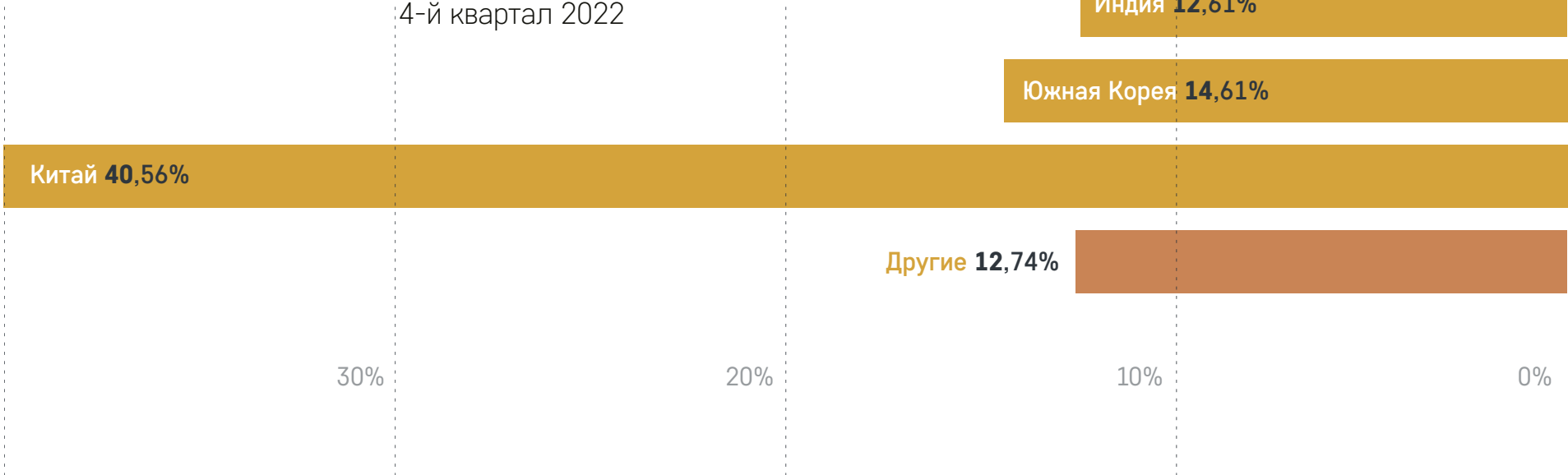


ГЕОГРАФИЯ АТАК НА ЛОВУШКИ

Ловушки «Гарда Технологии» имеют широкое территориальное распределение, что позволяет выявить наиболее активных злоумышленников по географическому принципу, исходя из числа устройств, при использовании которых организуются DDoS-атаки. Так, чаще всего ловушки атаковали из Китая (почти 40%), Южной Кореи (15%) и Индии (13%).

Лидирующие позиции по числу участников botnet-сетей сейчас занимает Китай, замыкают тройку лидеров Южная Корея и Индия, значительные доли демонстрируют Тайвань, США, Россия, Бразилия и Индонезия. График демонстрирует корреляцию botnet-сетей и общего числа «умных» устройств в стране.

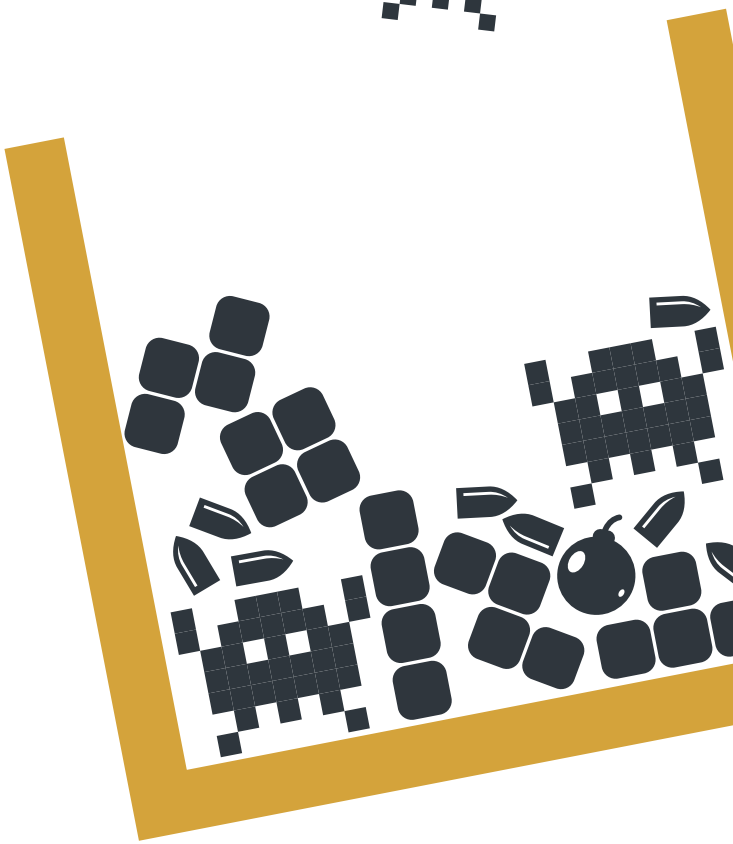
ТОР 10 стран и территорий по числу устройств, с которых осуществлялись атаки на ловушки «Гарда Технологии»
4-й квартал 2022



ЗАКЛЮЧЕНИЕ

В IV квартале 2022 ситуация с DDoS-атаками продолжает оставаться непростой. С одной стороны, наблюдается некоторая нормализация DDoS-активности по сравнению с предыдущими периодами, особенно для России. С другой стороны — DDoS не утратил своей актуальности в киберпреступной среде, и продолжает активно использоваться для атак на информационные ресурсы Учитывая это, важно сохранять повышенную готовность к отражению атак.

Наиболее эффективным подходом остается организация эшелонированной защиты: от объемных атак на уровне оператора связи и использованием локальных комплексов antiDDoS для тонкой очистки и повышения скорости реакции на возникающие угрозы.



ГАРДА
ТЕХНОЛОГИИ

АНАЛИТИКА DDOS-АТАК ЗА IV КВАРТАЛ 2022 ГОДА

Аналитический центр
«Гарда Технологии»
2023 г.

+7 (831) 422-12-21
Нижний Новгород, проспект Гагарина, д. 50, корп. 9
pr@gardatech.ru