Актуальные киберугрозы и риски безопасности для организаций

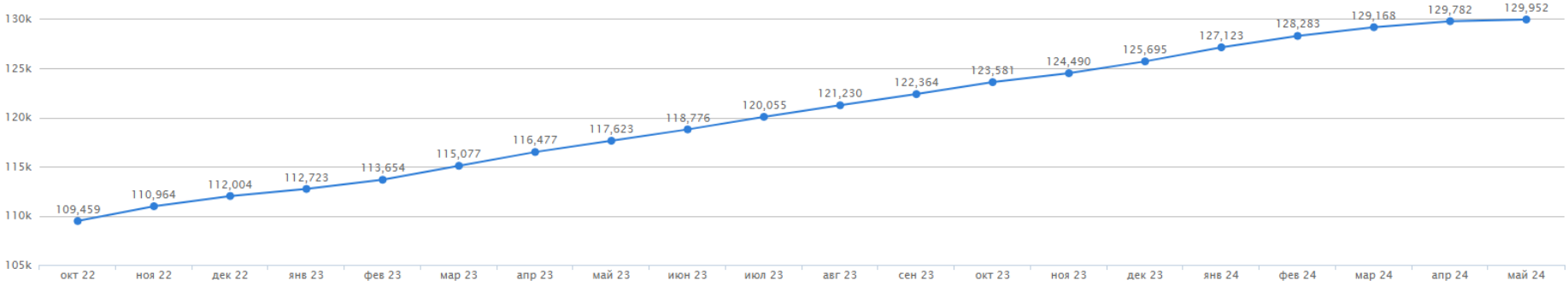
Начальник Отдела реагирования
на инциденты кибербезопасности
Эркин Халиков

Динамика узбекского киберпространства

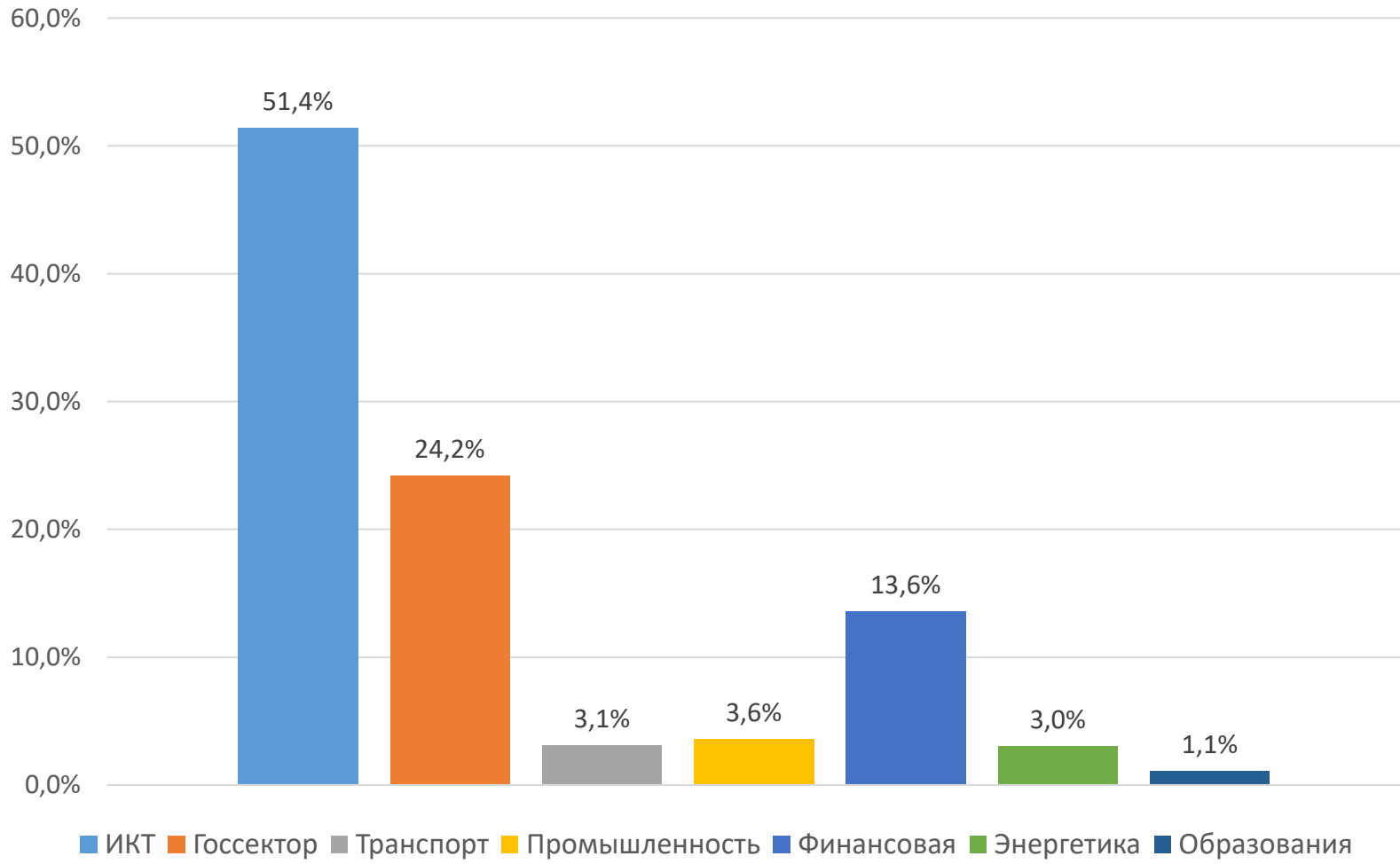
>800 гос. информационных систем и ресурсов

>570 видов электронных госуслуг

130 000 активных доменов



Киберугрозы по отраслям



Борьба с киберпреступностью

Предотвращение киберугроз и инцидентов кибербезопасности

Реагирование на кибератаки

Расследование киберинцидентов

Предотвращение угроз и инцидентов кибербезопасности

Система выявления и сбора данных об угрозах и уязвимостях кибербезопасности «Threat Intelligence»

Обрабатываемые данные:

Сбор информации о более 500 тыс. IP-адресов

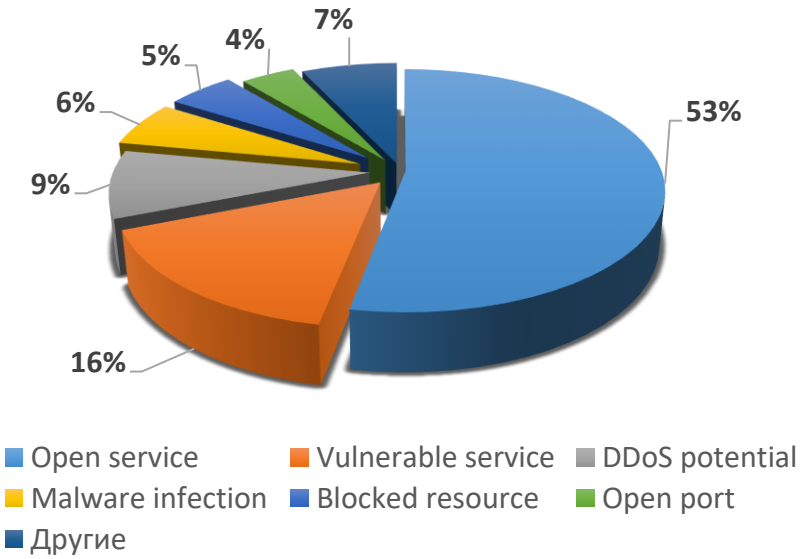
Более 130 тыс. доменов в зоне «UZ»

Более 2,5 млн. выявленных угроз и уязвимостей кибербезопасности

Предотвращение угроз и инцидентов кибербезопасности

Система выявления и сбора данных об угрозах и уязвимостях кибербезопасности «Threat Intelligence»

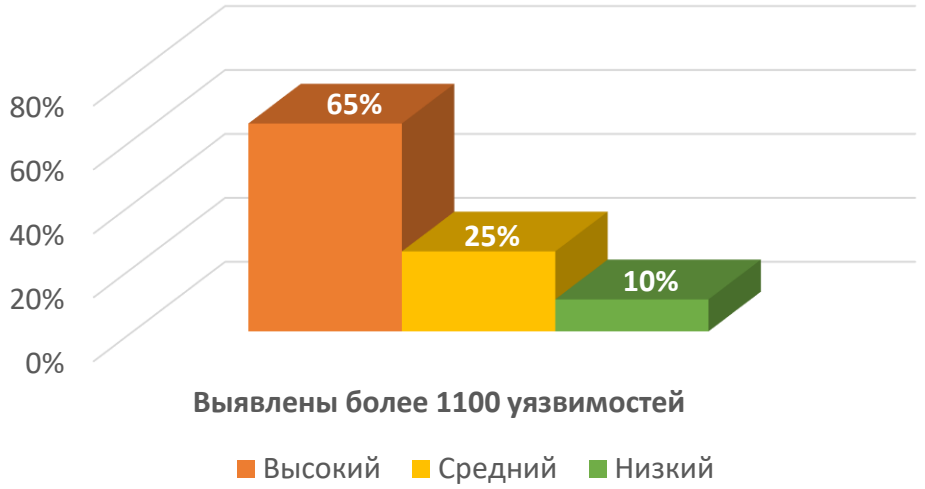
Выявлено более 2,5 млн. киберугроз в 2023 году



Тенденция снижения киберугроз

Оценка кибербезопасности информационных систем и ресурсов

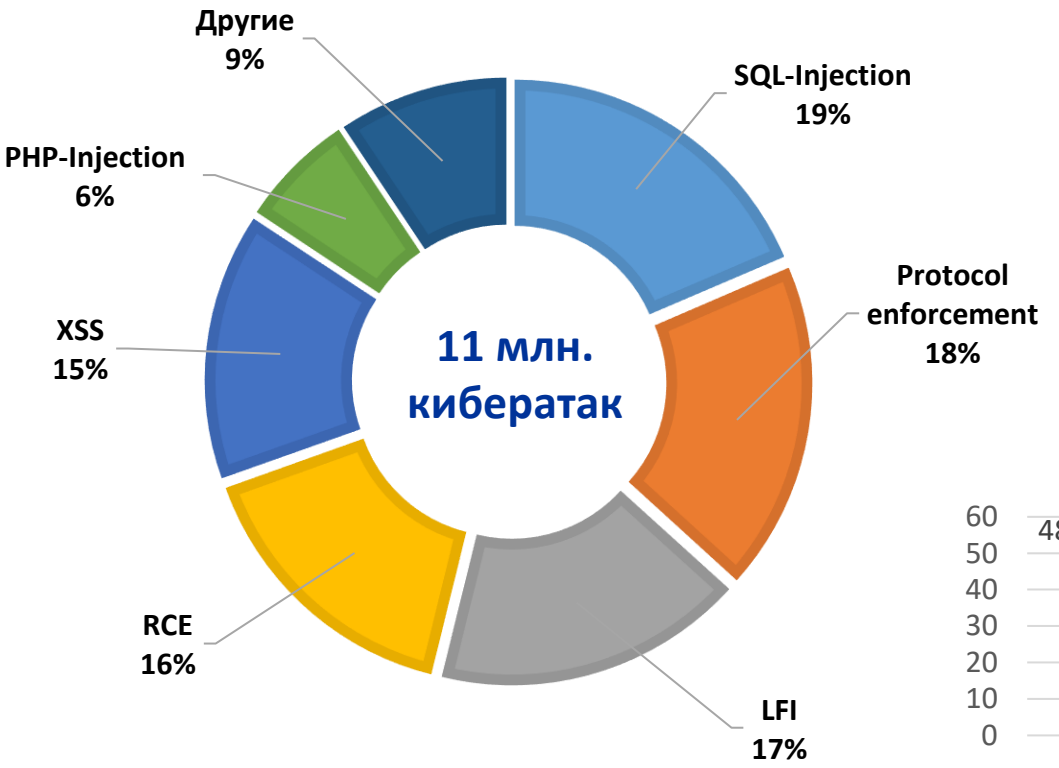
Проведены изучения более 600 информационных систем и ресурсов

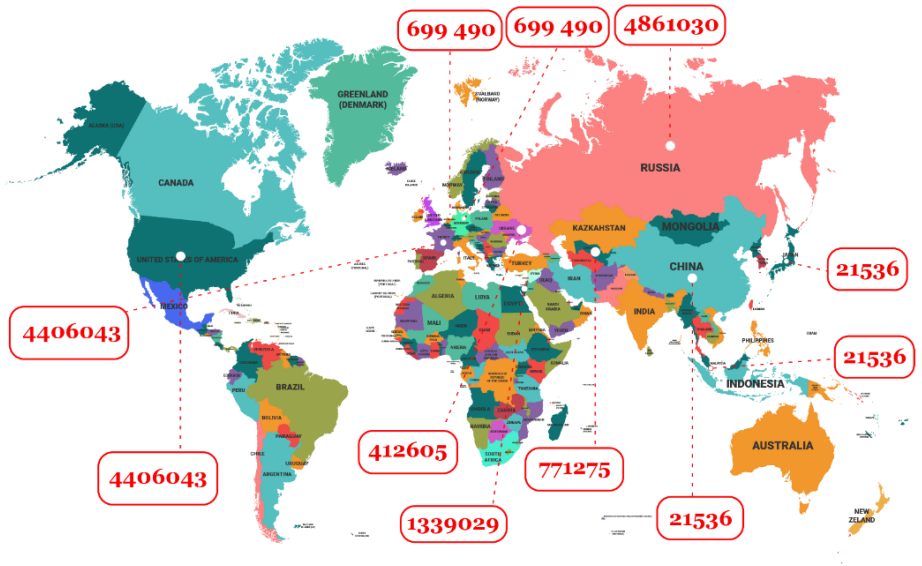


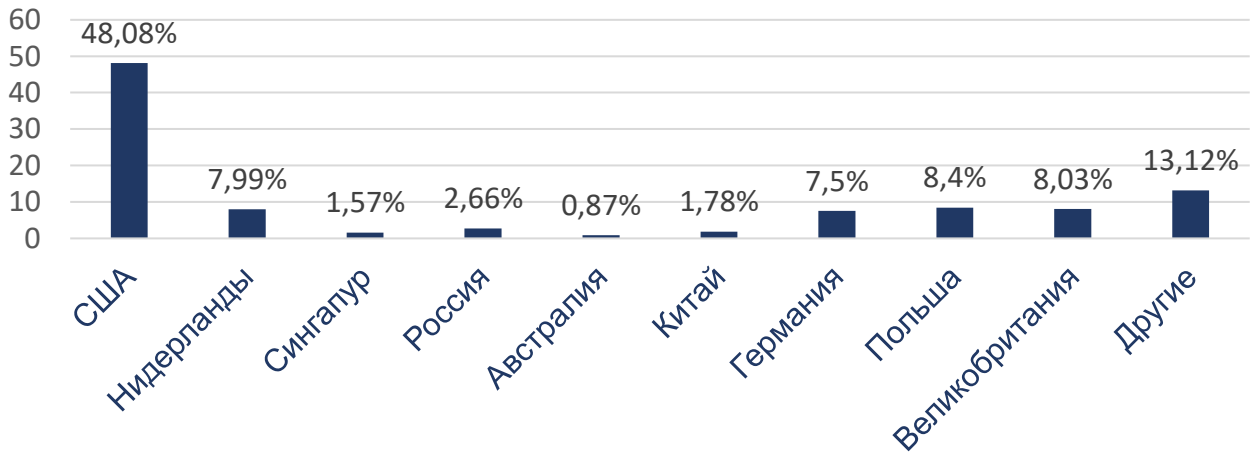
Реагирование на кибератаки

Система выявления и отражения кибератак в реальном времени

ВИДЫ КИБЕРАТАК







Мониторинг событий безопасности

Система мониторинга веб-сайтов в доменной зоне «UZ»

Круглосуточный мониторинг более 130 000 веб-сайтов

Расследование киберинцидентов

В 2023 году проведено более 60 расследований инцидентов по следующим направлениям:

Инциденты на веб-сайтах госорганов;

Инциденты, связанные с вирусами-шифровальщиками;

Инциденты, связанные с компрометацией электронной почты организации;

Инциденты, связанные с компрометацией сети организации.

Примеры рисков ИБ для организации

- Утечка или уничтожение конфиденциальной информации

- Недоступность важных данных или сервисов

- Несанкционированное проникновение в сеть

- Заражение конечных устройств ВПО

Ущерб от реализации рисков ИБ

Репутационный ущерб

Незначительный или крупный материальный ущерб

ВЫВОД

Материально-техническое обеспечение службы ИБ

Принятие эффективных мер по обеспечению кибербезопасности

Поиск и устранение киберугроз и уязвимостей

Регулярное повышение квалификации специалистов ИБ

Создание отраслевых CERT/CSIRT служб

БЛАГОДАРЮ ЗА ВНИМАНИЕ!

г. Ташкент, Мирабадский район, ул. Т. Шевченко, 20А
+998-71-203-55-11
Email: info@csec.uz
https://csec.uz