

Кому: Правительству Республики Казахстан

ФИО и должность автора: Мейржан Арайлым Мейржанкызы
руководитель управления по взаимодействию со СМИ и обращениями физических и юридических лиц Министерства промышленности и строительства РК.

Дата: 19.10.2024 г.

Аналитическая записка

Тема: Профилактика интернет-мошенничества в Республике Казахстан с учетом положений Конвенции по борьбе с киберпреступностью

Ключевые слова: интернет-мошенничество, профилактика киберпреступности, цифровая грамотность, социальные сети

Введение

Цель данной аналитической записки – проанализировать текущую ситуацию с интернет-мошенничеством в социальных сетях в Республике Казахстан и предложить эффективные инструменты для его профилактики с учетом положений Конвенции по борьбе с киберпреступностью.

С развитием технологии и активным использованием гражданами интернет-коммуникаций в виде социальных сетей и мессенджеров в стране наблюдается рост числа киберпреступности.

Рост числа киберпреступлений, в частности мошенничества в социальных сетях, представляет серьезную угрозу для граждан и экономики страны. Для эффективного противодействия этой угрозе необходимы комплексные меры, включающие в себя как технологические решения, так и образовательные программы, а также гармонизацию национального законодательства с международными стандартами. В данной записке рассматриваются основные положения Конвенции по борьбе с киберпреступностью, ратифицированной Республикой Казахстан, и предлагаются рекомендации по их имплементации в национальную правовую систему.

Основная часть

Интернет-мошенничество в Казахстане принимает различные формы, включая фишинг, мошенничество с кредитными картами, продажу поддельных товаров и инвестиционные схемы. По данным правоохранительных органов, количество зарегистрированных случаев мошенничества в сети возросло на 30% за последние два года.

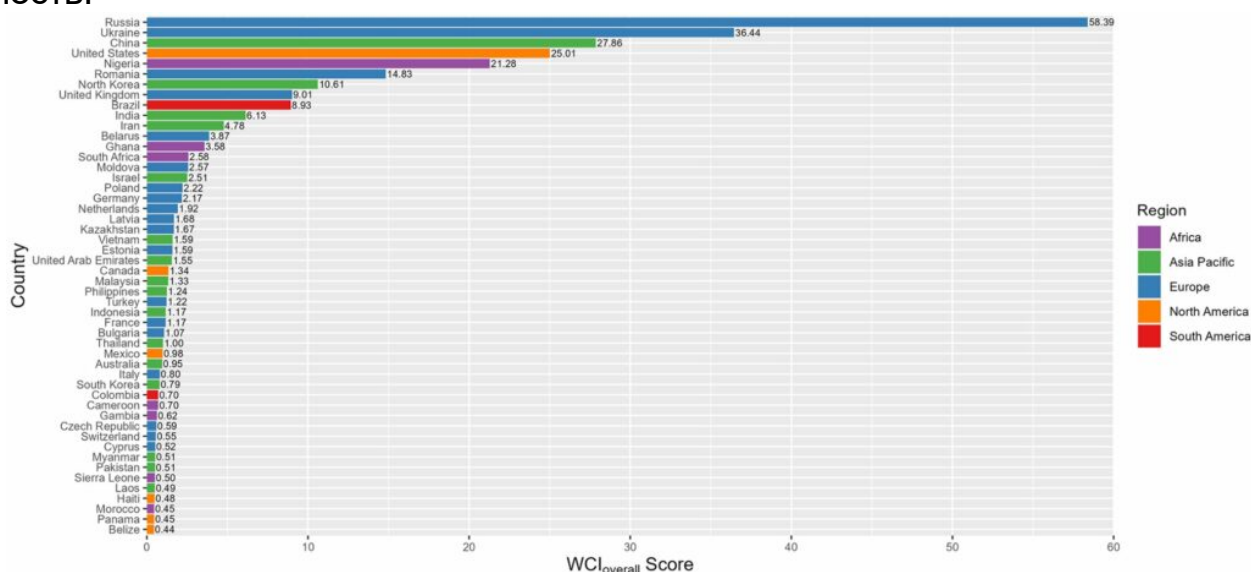
Наиболее часто жертвами киберпреступлений в Казахстане в 2023 и 2024 годах становились СМИ (19%), госучреждения (12%), финансовые организации (12%) и телекоммуникации (7%). Высокая

доля атак на СМИ обусловлена тем, что на казахстанские СМИ с ноября 2023 года обрушилась волна DDoS-атак. Кибератаки были направлены как минимум на девять независимых СМИ и на аккаунты нескольких журналистов в мессенджерах и социальных сетях.

Две трети всех атак на Казахстан (65%) было связано с использованием вредоносного ПО, а в каждой второй (53%) применялись методы социальной инженерии. Более трети атак (35%) заканчивалось утечкой конфиденциальной информации. Наибольшим спросом пользовались персональные и учетные данные¹.



Казахстан занял 21 строчку первого в истории мирового рейтинга киберпреступности, созданного специалистами из Великобритании, Франции и Австралии. Рейтинг ранжирует страны по уровню киберугроз, обозначая государства, откуда может исходить опасность.²



¹ <https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-v-stranah-sng-2023-2024/>

² <https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0297312>

Законодательные меры и национальная политика

Казахстан активно работает над улучшением законодательства в области кибербезопасности. В 2018 году была принята Концепция кибербезопасности, которая определяет стратегию по защите информации и предотвращению киберпреступлений. Основные законодательные акты, регулирующие эту сферу, включают:

- Уголовный кодекс Республики Казахстан (статьи, касающиеся киберпреступлений).
- Законодательство о персональных данных и защите информации.

Тем не менее, существует необходимость в дальнейшей гармонизации с международными стандартами, в том числе положениями Конвенции по борьбе с киберпреступностью.

В свете положений Конвенции по борьбе с киберпреступностью (ETS № 185), ратифицированной Республикой Казахстан, особое внимание следует уделить следующим аспектам:

- **Уголовная ответственность за киберпреступления.** Статья 2 Конвенции обязывает государства-участники криминализировать деяния, связанные с незаконным доступом, перехватом, вмешательством в данные, подделкой компьютерных данных, мошенничеством, связанным с использованием компьютеров, преступлениями, связанными с детской порнографией, и нарушениями авторских прав. В национальном законодательстве необходимо предусмотреть четкие и соразмерные санкции за эти преступления.
- **Процессуальные полномочия.** Конвенция предоставляет правоохранительным органам широкие полномочия для расследования киберпреступлений, включая возможность получения данных от провайдеров интернет-услуг, проведения обысков и выемок электронных данных, а также международного сотрудничества в расследовании киберпреступлений. Необходимо обеспечить эффективную реализацию этих полномочий в национальной правовой системе.
- **Защита данных.** Конвенция подчеркивает важность защиты персональных данных и предусматривает меры по их защите при расследовании киберпреступлений. Необходимо обеспечить соответствие национального законодательства в области защиты данных положениям Конвенции.

Выводы

Профилактика интернет-мошенничества в Казахстане требует комплексного подхода, включающего законодательные изменения, образовательные инициативы и активное сотрудничество между государственными органами и частным сектором. Применение международных стандартов, таких как Конвенция по борьбе с

киберпреступностью, может значительно повысить эффективность борьбы с этой проблемой и защитить граждан от мошеннических действий в интернете.

Рекомендации

- **Гармонизация национального законодательства.** Провести анализ национального законодательства на предмет его соответствия положениям Конвенции по борьбе с киберпреступностью и внести необходимые изменения для обеспечения полной имплементации Конвенции.
- **Повышение квалификации правоохранительных органов и граждан.** Организовать специализированные тренинги для сотрудников правоохранительных органов по расследованию киберпреступлений с учетом положений Конвенции и передового международного опыта. Проводить разъяснительные работы среди граждан.
- **Международное сотрудничество.** Активизировать международное сотрудничество в области борьбы с киберпреступностью, в том числе обмен информацией и опытом с другими государствами-участниками Конвенции.

Список использованных источников

1. <https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-v-stranah-sng-2023-2024>
2. <https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0297312>
3. Конвенция о киберпреступности (ETS № 185) // [https://rm.coe.int/1680081580]