Кому: Министерству внутренних дел Республики Казахстан

ФИО и должность автора: Дуйсеков Тимур Мухитович, руководитель Управления мобилизационной работы Департамента информационной безопасности, по защите государственных секретов и мобилизационной работы Министерства науки и высшего образования Республики Казахстан

Дата: 11.02.2025 г.

Аналитическая записка
Тема: Борьба с мошенничеством в РК

Ключевые слова: интернет-мошенничество, профилактика киберпреступности.

Введение

Проект заключается в создании системы для государственного органа Министерства внутренних дел республики Казахстан. Информационная система создается для работы с киберпреступностью (мошенничество), заключается она в следующих действиях:

1. Заключение договора с операторами связи.
2. Предоставление данных в виде предоставления персональных данных на физических и юридических лиц, зарегистрировавших на свое имя телефонные номера.
3. Участковые инспектора при оформлении смерти человека, заносят информацию в систему для отключения в последующем номеров умершего, чтоб в последующем данные номера не использовались для преступных действий.
4. Так как сотовые номера зачастую используются для регистрации Логинов в пространстве сети Интернет, считаем целесообразным регистрировать сотовые номера на лицо и вести учет на базе вышеупомянутой системы, так как все действии регистрации в социальных сетях проходят аутентификацию, зачастую двухфакторную аутентификацию.

В этой связи, когда лицо объявляет себя банкротом либо участковый инспектор регистрирует смерть, номера должны будут уничтожены операторами связи без возможности восстановления. Данная система предназначена в целях избежание мошеннических действий используя незарегистрированные номера либо номера несуществующих фирм и умерших людей.

В настоящее время Министерство внутренних дел Республики Казахстан выпускает постоянные ролики и ведут семинары в различных местах, ведут уголовные дела, которые так и останутся незаконченными. Вышеуказанная система может интегрироваться с системой егов (**по ситуации**) в последующем, после прохождения опытной эксплуатации и положительным решением комиссии на предмет прохождения

соответствия информационной безопасности от компетентных органов с соблюдением всем норм законодательства Республики Казахстан по желанию МВД РК.

Создание информационной системы можно заказать у местных третьих лиц, можно заняться созданием самостоятельно, в целях соблюдения секретности с целью нераспространенная персональных данных.

Даже банковский сектор используют частные номера, тогда как именно для банковского сектора может быть использован специальный общий номер с четырехзначным номером. Использование в банковской системе говорит, о том, что даже в банковском секторе не следуют гигиене в информационной безопасности, оттуда и уходят наши персональные данные в пространство интернет, а возможно кто-то и сливает данную информацию специально

Текущее состояние проблемы

В настоящее время Министерство внутренних дел Республики Казахстан (МВД РК) ведет активную борьбу с киберпреступностью, связанной с мошенничеством. Однако ряд системных проблем затрудняет эффективное противодействие:

1. Использование номеров умерших лиц и банкротов

2. Отсутствует автоматизированный механизм передачи данных операторам связи о смерти владельцев номеров и банкротстве юридических лиц.

3. Это позволяет мошенникам использовать такие номера для преступных действий, включая социальную инженерию, финансовое мошенничество и подделку личных данных.

4. Проблема анонимности и фиктивных регистраций

5. Операторы связи не всегда могут оперативно верифицировать владельцев SIM-карт, что создает лазейки для мошенников.

6. Многие номера оформлены на подставные или фиктивные лица, что затрудняет идентификацию преступников.

7. Отсутствие интеграции между МВД, операторами связи и госорганами

8. МВД не имеет прямого автоматизированного доступа к данным об абонентах. Вся информация запрашивается вручную, что замедляет расследования.

9. Операторы связи не обязаны в реальном времени получать данные о смерти владельцев номеров или банкротстве юрлиц, что приводит к задержкам в деактивации таких номеров.

10. Отсутствие обязательной централизованной аутентификации номеров

11. Двухфакторная аутентификация через SMS широко используется, но нет механизма контроля, действительно ли номер принадлежит человеку, который его использует.

12. Это позволяет мошенникам регистрировать подставные аккаунты в социальных сетях и мессенджерах, используя “серые” номера.

13. Роль операторов связи в деактивации номеров

14. В настоящее время именно операторы связи несут ответственность за отключение номеров, но у них нет автоматизированного процесса для этого.

15. Уведомления о смерти или банкротстве не поступают им напрямую, а приходят только при официальных запросах от госорганов.

16. Это приводит к задержкам, в течение которых номера остаются активными и могут быть использованы в мошеннических схемах.

Необходимые доработки в системе

- Создание автоматизированной информационной системы
- Интеграция с МВД, eGov и базами операторов связи для передачи информации в режиме реального времени (**по ситуации**).
- Обязательная регистрация всех мобильных номеров в этой системе для прозрачности учета.
- Разработка регламента взаимодействия с операторами связи
- Введение юридически обязывающих норм, требующих от операторов автоматической деактивации номеров при получении подтвержденных данных от МВД.
- Операторы связи должны получать уведомления о смерти владельца или банкротстве юрлица сразу после регистрации этого факта в системе.
- Централизованная проверка мобильных номеров
- Создание базы данных всех зарегистрированных номеров с указанием их статуса (активен, заблокирован, деактивирован).
- Обязательная проверка номеров при регистрации в онлайн-сервисах, банках и государственных системах.
- Разработка механизма уничтожения номеров
- Внедрение юридических норм, запрещающих повторную активацию номеров, принадлежащих умершим лицам и банкротам.
- Введение штрафов для операторов за нарушение этого требования.

Эти меры позволят повысить уровень информационной безопасности и снизить случаи мошенничества, связанные с использованием номеров умерших людей и ликвидированных компаний.

Выводы

Создание автоматизированной информационной системы для учета, контроля и деактивации мобильных номеров в Республике Казахстан

принесет значительные преимущества не только для МВД, но и для операторов связи, финансового сектора и общества в целом.

1. Повышение эффективности борьбы с киберпреступностью

- Автоматическая передача данных о номерах умерших граждан и банкротов в систему исключит возможность их использования в мошеннических схемах.
- Сократится количество преступлений, связанных с использованием подставных или анонимных номеров.
- МВД получит доступ к актуальной информации по номерам, что ускорит расследование преступлений.

2. Усиление контроля за регистрацией мобильных номеров

- Все номера будут жестко привязаны к личности владельца, что снизит вероятность использования фальшивых документов для регистрации SIM-карт.
- Исключается массовая продажа номеров без проверки личности, что затруднит мошенникам создание “серых” номеров для преступной деятельности.

3. Интеграция с государственными системами (eGov, МВД, ЦОН)

- Автоматическая синхронизация с базами данных госорганов обеспечит своевременное обновление информации об абонентах.
- Система будет взаимодействовать с ЦОНами, что упростит процесс подтверждения личности при регистрации или деактивации номера.
- Операторы связи получат оперативные данные о смерти владельцев номеров и ликвидации юридических лиц без необходимости долгих запросов.

4. Повышение уровня информационной безопасности

- Исключение “заброшенных” номеров, которые могут быть использованы для мошенничества.
- Ограничение использования номеров банкротов в финансовых операциях, что снизит риски кредитных мошенничеств.
- Уменьшение вероятности утечек персональных данных через незащищенные номера.

5. Упрощение работы операторов связи

- Операторам не придется вручную обрабатывать запросы от госорганов на блокировку номеров – процесс станет автоматизированным.
- Улучшится учет абонентов, что упростит контроль за подлинностью данных клиентов.
- Исключится юридическая ответственность операторов за использование мошенниками номеров умерших людей или ликвидированных организаций.

6. Повышение доверия к мобильной связи и цифровым сервисам

- Граждане получат уверенность, что их номера защищены и не могут быть использованы после смерти или банкротства без их ведома.

- Онлайн-сервисы смогут проверять подлинность номеров, снижая риски мошенничества при регистрации аккаунтов.
- Банковский сектор получит инструмент для точной идентификации клиентов по телефонным номерам.

7. Введение законодательных норм для контроля над операторами связи

- Законодательно будет закреплена обязанность операторов связи отключать номера умерших и банкротов без возможности их повторной активации.
- Будут введены штрафные санкции за несоблюдение требований, что повысит ответственность операторов.
- Внедрение такой системы позволит Казахстану соответствовать международным стандартам защиты персональных данных и цифровой безопасности.

Вывод

Внедрение единой автоматизированной системы учета и деактивации мобильных номеров позволит значительно сократить уровень мошенничества, повысить кибербезопасность и создать прозрачный механизм взаимодействия между МВД, операторами связи и госорганами. Это приведет к укреплению доверия граждан к цифровым сервисам, а также упростит контроль за регистрацией и использованием мобильных номеров в стране.

Рекомендации

1. Создание автоматизированной системы учета номеров
2. Интеграция МВД, eGov, ЦОН и операторов связи для оперативного обмена данными.
3. Автоматическая деактивация номеров умерших лиц и банкротов.
4. Ужесточение контроля за регистрацией SIM-карт
5. Обязательная верификация личности при покупке номера.
6. Запрет на массовую продажу SIM-карт без проверки данных.
7. Разработка законодательных норм
8. Введение обязанности операторов связи отключать номера на основании данных МВД.
9. Установление штрафов за повторную активацию номеров умерших и банкротов.
10. Централизованная проверка номеров в онлайн-сервисах
11. Внедрение системы проверки подлинности номеров при регистрации в банках и цифровых сервисах.
12. Использование подтвержденных номеров для двухфакторной аутентификации.
13. Усиление кибербезопасности и защиты персональных данных
14. Исключение “серых” номеров из оборота.
15. Мониторинг утечек данных и предупреждение мошеннических схем.

Эти меры помогут повысить безопасность мобильной связи, снизить уровень мошенничества и усилить защиту персональных данных граждан.

Литература

1. Конвенция о киберпреступности (Будапештская конвенция, 2001 г.) – международный правовой акт, регулирующий сотрудничество стран в борьбе с киберпреступностью, включая незаконный доступ к данным и мошенничество с использованием информационных технологий.
2. Закон Республики Казахстан «О связи» – регулирует вопросы регистрации абонентов, работы операторов связи и защиты персональных данных.
3. Закон Республики Казахстан «Об информатизации» – устанавливает правила обработки и защиты информации в государственных и частных информационных системах.
4. Общий регламент по защите данных (GDPR, ЕС) – нормативный акт Европейского Союза, регулирующий обработку и защиту персональных данных, включая правила идентификации абонентов мобильной связи.
5. Международная практика регулирования мобильной связи (США, Великобритания, Китай, Индия) – опыт внедрения систем обязательной идентификации номеров, автоматической деактивации номеров умерших и контроля за SIM-картами.