***Информация к тематическому заседанию***

 ***«Актуальные вопросы борьбы***

***с киберпреступностью»***

 В условиях развития цифровых услуг отмечается рост киберпреступлений, основную долю которых составляют интернет-мошенничества. С учетом темпов их внедрения, в том числе в банковской сфере и онлайн-торговле, количество совершаемых интернет-мошенничеств ежегодно увеличивается. Сегодня указанным видом преступлений поражены практически все страны, в том числе развитые в области информационных технологий.

 За последние 7 лет их количество в Казахстане выросло более чем в 10 раз *(2017г. – 2046, 2018г. – 4287, 2019г. – 7733, 2020г. – 14175, 2021г. – 21275, 2022г. – 20444, 2023г.- 21637)*.

При этом, в 2023г. их доля в числе всех мошенничеств составила 50% *(21637 из 43895 преступлений)* и 18,7% от всех общеуголовных преступлений, а причиненный гражданам ущерб составил 21 млрд. тенге.

*Справочно: в январе т.г. зарегистрировано 1871 интернет-мошенничество, что на 16,8% выше прошлогоднего показателя, составившего 1602 преступления. Их доля за январь т.г. составляет 15% от всех преступлений и 45% от мошенничеств.*

МВД РК в рамках компетенции принимает организационные меры по противодействию данному виду преступлений.

 Реализуются соответствующие ведомственные и межведомственные нормативные акты:

- Программа МВД «По противодействию киберпреступности, в том числе телефонным и интернет-мошенничествам на 2023-2025 годы»;

- Дорожная Карта на 2023-2024 годы по реализации механизмов противодействия кредитному мошенничеству, утвержденная заместителем Премьер-Министра РК – Министром финансов РК Жамаубаевым Е.К.;

- «Комплекс совместных мероприятий по противодействию мошенничествам и финансовым пирамидам на 2023-2024 годы», утвержденный совместными приказами гос.органов и финансовым сектором *(ГП, АФМ, МВД, АРРФР, НБ и т.д.).*

С учетом анализа выделены следующие распространенные способы совершения интернет-мошенничеств:

- размещение онлайн объявлений о продаже товаров и предоставления услуг;

- хищение денег со счетов граждан, путем их обзвона под видом сотрудников банков и правоохранительных органов;

- предложение выгодных вложений денег в различные инвестиционные проекты;

В то же время, практически всеинтернет-мошенничества, **связанные с оформлением** на доверчивых граждан **онлайн-кредитов и займов**, а такжехищением их банковских накоплений, **совершаются преступниками из-за рубежа,** так называемыми «зарубежными интернет-мошенниками».

 **Сложность расследования** и пресечения трансграничной преступной деятельности **заключается** не только в их местонахождении за пределами Республики Казахстан, но и использовании ими современных «хакерских» программ *(более подробно описано ниже в разделе: причины и условия, совершения интернет-мошенничеств).*

 При этом, для обеспечения анонимности, такие преступления совершаются в отношении граждан зарубежных стран. К примеру, в конце 2023 года в г.Астана выявлены 4 мошеннических Call-центра.

 Установлено, что их работники звонили только на номера операторов связи ближнего *(постсоветского пространства)* и дальнего зарубежья *(европейские государства)*.

 В ходе обысковых мероприятий изъято 170 ноутбуков с гарнитурой (наушники и микрофоны), сетевое оборудование, доступ к которым защищен специальными программами.

 *Справочно: На изъятых ноутбуках обнаружены установленные приложения для удаленного доступа к другим устройствам (AnyDesk, TeamViewer), таблицы в формате excel с ссылками на фишинговые сайты, приложения для изменения IP-адресов (VPN). В рамках расследований назначены экспертизы, направлены международные запросы.*

 Аналогично, в отношении казахстанцев такие преступления совершаются из-за рубежа.

 Похищенные деньги снимаются со счетов и перенаправляются за границу ещё до того, как граждане осознают, что стали «жертвами» мошенников. В среднем срок их обращения в органы внутренних дел с момента совершения преступлений, составляет от 3 дней до нескольких месяцев.

В своих преступных целях «зарубежные мошенники» используют так называемых «дропов» *(«низшее» звено преступной цепи, человек, который соглашается, чтобы его банковская карта стала «транзитной» для украденных денег)*, из числа граждан Казахстана, которых они находят через телеграмм-каналы. Они предлагают им работу в качестве «курьера», и при согласии, требуют предоставить о себе всю персональную информацию, включая документы, удостоверяющие личность и номера банковских карт. После поступления денежных средств на счета «дропов», последние оставляют себе до 10 %, остальные снимают и/или переводят на указанные мошенниками банковские и иные электронные счета. Так из страны **выводится** порядка **90 %** из всех похищенных денег, следы которых в дальнейшем «теряются» из-за различных теневых схем криптовалютной системы *(«Блокчейн»)*.

* **Для борьбы с «интернет-мошенничествами»** МВД продолжает **принимать меры, с внедрением новых методов и подходов**, так:
* В результате разработанного совместно с МЦРИАП и операторами сотовой связи **механизма блокирования** «зарубежных» звонков с подменных номеров **пресечено** **44 млн. попыток** «зарубежных мошенников» дозвонится до казахстанских граждан для реализации своих преступных целей.

В результате принимаемых мер, по итогам 2023 года **на 31 % снижено** количество интернет-мошенничеств, совершаемых двумя наиболее распространенным способами (с 6471 в 2022 году до 4460 в 2023 году), это когда преступники:

- «представляются сотрудниками банков и правоохранительных органов», и после завладевают их деньгами, под предлогом вывода на безопасный счёт;

- получают удаленный доступ к мобильному устройству и оформляют онлайн-займы.

**На 18 % уменьшилось** и количество зарегистрированных интернет-мошенничеств, относящихся к тяжкой и особо тяжкой категории *(с 2717 до 2230*).

 Продолжается внедрение новых методов борьбы с телефонными мошенничествами. В ноябре 2023 года по инициативе МВД во взаимодействии с АО «Казахтелеком» апробирован механизм распознавания и блокирования звонков с мошенническими признаками, поступающих из-за рубежа на городские линии связи Казахстана. Системой заблокировано более 300 тыс. подобных звонков *(в сутки в среднем 8,5 тыс.)*.

 На стадии проработки находятся и другие меры по повышению эффективности противодействия мошенничествам.

* С июля 2023 года, после апробированного в столице пилотного проекта, во всех регионах **созданы подразделения «CyberPol».**

 Это специализированные группы, в составе оперативников, следователей и криминалистов. Проводится повышение квалификации на базе открытого «Кибер Центра по подготовке специалистов» Алматинской Академии МВД.

 Дополнительно, для повышения их профессионального уровня и регулярного консультирования привлекаются опытные сотрудники
IT-сферы *(Центр анализа и расследования кибератак, Холдинг «Каздрим Спешиал Систем» и др.)*.

 Сотрудники указанных подразделений напрямую взаимодействуют с банками и операторами сотовой связи, что позволяет, в случае своевременного обращения потерпевших в полицию, снизить риски потери денег, на стадии их вывода за пределы страны.

 В результате предпринятых мер гражданам возмещено **850** **млн.** тенге. Всего за 2023 год раскрыто более 3,7 тыс. таких преступлений *(за январь т.г. - 222)*. Принятыми мерами задержано и привлечено к уголовной ответственности 1891 лицо, из них 460 лиц изобличены в совершении мошенничеств в отношении 2-х и более лиц. Ими совершено 2,3 тыс. мошенничеств.

 Установлено более **1 тыс.** «дропов», которые за денежное вознаграждение обналичивали и переводили похищенные средства организаторам. Каждому из них даётся процессуальная оценка *(о проблемах привлечения их к уголовной ответственности подробно отражено ниже в разделе: причины и условия, совершения интернет-мошенничеств).*

* **На постоянной основе осуществляется мониторинг интернет-пространства** для выявления противоправного контента. В результате, в 2023 году выявлено 23 228 подозрительных зарубежных интернет-ресурсов, сведения о которых переданы в уполномоченные органы.

 Параллельно МВД заблокировано 4 тыс. различных сайтов и ссылок, в том числе с признаками мошенничеств и финансовых пирамид.

 *Справочно: в т.г. выявлено 2517 зарубежных интернет-ресурсов с противоправным содержанием, в том числе 1,5 тыс с признаками финансовой пирамиды и других мошеннических организаций.*

 Вместе с тем, администраторы крупных интернет-сайтов и хостингов, на которых размещается противоправная информация, активно рассматривают жалобы пользователей с указанием причин для блокирования (мошенничество и т.д.).

 В этой связи, для построения эффективной защиты информационного пространства, в популярных мессенджерах *(«WhatsApp», «Telegram», «Instagram» и др.)* созданы специальные группы «Cyberbot», в которые включены сотрудники центрального аппарата, Департаментов полиции, Академий МВД и волонтеры.

 Принцип работы групп состоит в выявлении фишинговых ссылок *(мошеннические рекламы и др.)* в социальных сетях, мессенджерах и т.д. Все участники массово направляют жалобу в администрацию интернет ресурса на блокировку. Наличие большого количества жалоб увеличивает вероятность блокирование ссылок.

 Только за месяц такой работы администраторами удалено свыше 300 мошеннических ресурсов.

 Для выявления мошеннических объявлений также достигнута договоренность о взаимодействии с крупными международными и отечественными компаниями *(Тик-Ток, Яндекс, Индрайвер, Крыша, Колеса, Каспий и Маркет КЗ, а также ряд др.)*, что позволит осуществлять поиск их на указанных ресурсах.

* Принимаются меры **по укреплению международного сотрудничества,** в том числе взаимодействия с правоохранительными органами стран СНГ.

 После получения приглашения к присоединению к Конвенции Совета Европы о компьютерных преступлениях Казахстан получил статус страны-наблюдателя. Это позволяет участвовать во всех международных мероприятиях, проводимых в рамках Конвенции.

 После ее ратификации Казахстан станет полноправным ее членом и расширит свои возможности в части международного взаимодействия с 69-ми странами.

Казахстанская делегация (МВД, КНБ, МЦРИАП) принимает активное участие в разработке Всеобъемлющей международной конвенции ООН по противодействию использованию ИКТ в преступных целях. Представителями МВД трижды принято участие в заседаниях Специального комитета ООН по разработке Конвенции *(последний раз в период 29.01-09.02.2024г.)*.

С декабря 2023 года совместно с Офисом программ ОБСЕ в г.Астана, прорабатывается проект «Поддержка Казахстана в разработке эффективной политики противодействия киберпреступности и преступлениям с использованием информационно-коммуникационных технологий» *(на 2024-2027г.г.)*, предусматривающий мероприятия по совершенствованию национального законодательства, расширения международного сотрудничества, а также широкомасштабного обучения сотрудников правоохранительных органов. В настоящее время созданной Межведомственной координационной группой *(15 госорганов)* разрабатывается проект Комплексного плана по противодействию киберпреступлениям и преступлениям совершаемым с использованием информационно-коммуникационных технологий.

* На системной основе **проводится разъяснительная работа** среди населения. Анализируются данные и о самих потерпевших, которые в последующем используются для точечной адресной профилактической работы.

Населению регулярно доводится информация о способах совершения интернет-мошенничеств и мерах предосторожности. В прошлом году ОВД опубликовано более 20 тыс. профилактических материалов, в том числе в СМИ - 8 тыс. и социальных сетях – 12 тыс. публикаций *(в январе т.г. – 2 тыс.)*.

В общественных местах *(подъезды, остановки и т.д.)* размещено более 250 тыс. буклетов с тематикой: «Осторожно, мошенники!».

Создано свыше 100 различных видеороликов, с подробным описанием действий мошенников. Для расширения охвата аудитории и масштабирования информационно - профилактической работы, к участию в подобных инициативных проектах МВД привлечены известные блогеры, актеры, спортсмены и иные категории известных личностей.

На официальном сайте МВД функционирует страница «Борьба с киберпреступностью», где размещается вся необходимая информация. Этим же контентом регулярно пополняются ведомственные каналы в популярных социальных сетях и мессенджерах.

В регионах также организована работа по повышению информационной и правовой грамотности населения.

*Справочно:*

*- при поддержке отечественных предпринимателей и бизнесменов, на различной торговой продукции, в том числе продуктах питания, имеющих специальную упаковку, размещаются буклеты ОВД предупредительного характера.*

*- на баннерах центральных улиц городов демонстрируются предупреждающие выступления сотрудников полиции;*

*- в «перерывах» крупных спортивных соревнований и иных массовых мероприятий транслируются профилактические видеозаставки на тему интернет-мошенничеств;*

*- полицейскими даются разъяснения прихожанам в религиозных учреждениях.*

Буквально недавно столичным Департаментом полиции в целях профилактики интернет-мошенничеств организована СМС – рассылка с текстами предупредительного характера.

Несмотря на это, некоторые граждане не прислушиваются к рекомендациям и попадаются на «уловки» мошенников. Практика показывает, что большинство потерпевших фактически были осведомлены и знали о подобных мошеннических способах, на которых указывала полиция.

В этой связи работа по повышению финансовой грамотности населения будет продолжена и расширена.

Учитывая необходимость масштабирования данного направления в утвержденной в декабре прошлого года «Концепции обеспечения общественной безопасности в партнерстве с обществом на 2024-2028 годы», вопросам противодействия киберпреступности уделён отдельный блок.

* **На постоянной основе проводится анализ указанных видов преступлений**, выявляются **причины создающие условия для их совершения:**

 1. Наибольшее количество интернет-мошенничеств совершается в сфере онлайн-торговли путем размещения заведомо ложных объявлений.

 *Справочно: таким способом в январе т.г. совершено 741 из 1871 интернет-мошенничеств (2023г.- 8191 из 21637).*

 При этом мошенники размещают объявления с зарубежных технических площадок либо используют иностранные сервисы для сокрытия своего местоположения *(IP-адреса)*. Для авторизации на сайтах используются номера казахстанских и иностранных сотовых компаний,оформленных на «подставных лиц».

 В целях защиты граждан от мошеннических объявлений уполномоченным госорганам совместно с торговыми онлайн-площадками *(«Колеса», «Крыша», «Маркет», «ОЛХ», «Каспи», «Озон» и др.*) предлагается:

* исключить авторизацию владельца объявления по номеру иностранного оператора связи, а также информирование казахстанских пользователей при размещении объявлений с зарубежных технических площадок *(с учетом участившихся случаев совершения преступлений с иностранных IP-адресов)*;
* организовать предупреждение пользователей при размещении ими объявлений в части запрета перехода по ссылкам, направляемым потенциальными покупателями *(фишинговые ссылки, направленные на получение персональных данных, номеров карт и т.д.)*;
* проработать технические решения по выявлению IP-адресов, с которых размещены одинаковые объявления с указанием разных регионов. К примеру, подача с одного IP-адреса объявлений о продаже одной и той же автомашины либо сдачи в аренду квартиры в разных городах.

 2. При совершении мошенничеств с использованием маркетплейсов банковских мобильных приложений преступным элементом активно используются личные кабинеты индивидуальных предпринимателей. К примеру, в т.г. почти 300 мошенничеств совершено с использованием личных кабинетов ИП.

 Как правило, их владельцы сдают в аренду посторонним лицам свои недействующие личные кабинеты и управление банковским счетом.

 В этой связи необходимо проработать с банками второго уровня вопрос минимизации рисков использования банковских счетов юридических лиц и индивидуальных предпринимателей путем:

 - применения дополнительных мер, таких как биометрическая идентификация при совершении операций (перевод, снятие денег);

 - введения ответственности предпринимателей за передачу третьим лицам своих личных кабинетов в банковских приложениях.

 3. Остается актуальным вопрос привлечения к ответственности лиц, оказывающих содействие в выводе похищенных денег или так называемых »дропов». Как правило, они за вознаграждение передают свои банковские карты посторонним лицам либо сами получают на свои карты деньги и переводят их на счета, указанные мошенниками. Впоследствии через них выводятся крупные суммы денег на зарубежные счета или криптовалюту.

 В рамках досудебных расследований устанавливаются лица, которые занимаются организацией обналичивания, т.е. поиском «дропов», сбором банковских карточек, абонентских номеров. Такие лица привлекаются к ответственности по ст.190 УК (мошенничество). Вместе с тем, из установленных свыше 1 тыс. лиц, только 114 привлечены к ответственности, остальные 90% имеют статус свидетелей.

 При этом, все эти лица получают лишь определенные проценты от похищенных денег, а основная их часть выводятся на счета организаторов таких схем.

 Полагается, что установление ответственности за передачу посторонним лицам банковских карт и абонентских номеров будет являться превентивной мерой и значительно сократит количество казахстанцев, вовлеченных в нелегальные схемы обналичивания похищенных денег.

 *Справочно: Ранее данная мера прорабатывалась в рамках законопроекта «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам минимизации рисков при кредитовании и защиты прав заемщиков». Однако, впоследствии не поддержана Правительством.*

 4. Принятыми мерами операторы сотовой связи блокируют зарубежные звонки с использованием подменных номеров. Однако, мошенники в обход данной системы начали использовать звонки путем использования SIP-телефонии, а также SIМ-боксы для преобразования телефонного трафика в Интернет. Таким способом совершено 288 преступлений.

 В этой связи необходимо законодательно закрепить ответственность за создание неправомерного трафика путем изменения установленного порядка его маршрутизации, в том числе неправомерное изменение вызывающего номера.

 Кроме того, до настоящего времени деятельность, связанная с предоставлением услуг связи посредством интернет-телефонии законодательно не урегулирована. При этом, лица, занимающиеся такой деятельностью не подпадают под действие законодательства в области связи. Это дает им возможность бесконтрольного предоставления своих услуг без соблюдения правил оказания услуг связи *(утверждены приказом и.о. Министра по инвестициям и развитию Республики Казахстан от 24 февраля 2015 года № 171.)*, не сохраняя данные о предоставленных интернет-соединениях *(лог-файлы, электронный журнал)*.

 5. В нарушение Правил регистрации абонентских устройств сотовой связи *(утверждены приказом Министра информации и коммуникаций №226 от 23.05.2018г.)* продолжают иметь место факты регистрации абонентских номеров сотовых операторов на дистрибьюторов и дилеров *(ТОО «Сотакс», ИП «Райских Ю.В.», ИП «Яиков Д.С.» или ИП «Communication Assistent» или и др.)*, что затрудняет установление реального пользователя абонентского номера.

 В этой связи уполномоченному органу (МЦРИАП) необходимо принять комплекс мер, направленных на соблюдение требований действующего приказа с аннулированием регистрации абонентских номеров на дистрибьюторов и дилеров. В случаях необходимости внести изменения и дополнения в Кодекс Республики Казахстан об административных правонарушениях в отношении операторов связи *(АО «Кселл», ТОО «Кар-Тел», ТОО «Мобайл Телеком-Сервис»)* за регистрацию абонентских номеров на дистрибьюторов и дилеров.

 6. Необходимо отметить, что предпосылками для совершения преступлений является утечка личных данных граждан в руки мошенников. Граждане регистрируясь на тех или иных платформах *(онлайн магазины, услуги такси и т.д.)* оставляют там свои личные данные, номера телефонов, место проживания, номера банковских карт и иную информацию. Не во всех организациях информационная безопасность находится на должном уровне, что позволяет мошенникам с использованием специальных хакерских программ взламывать их базы и завладеть их персональными данными граждан.

 В этой связи полагается необходимым уполномоченному органу усилить контроль за порядком их сбора, обработки и хранения.

 7. Важным аспектом в противодействии интернет-мошенничествам является проведение широкой разъяснительной работы с населением по повышению правовой и финансовой грамотности, информирование о видах интернет-мошенничеств, способах их совершения и соответствующих мерах предосторожности.

 Для этого уполномоченным государственным органам необходимо проработать вопрос запуска в новостных сайтах, социальных сетях и мессенджерах таргетированной рекламы (всплывающее окно) предупредительного характера.

**Министерство внутренних дел Республики Казахстан.**