ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ІШКІ ІСТЕР МИНИСТРЛІГІ
МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РЕСПУБЛИКИ КАЗАХСТАН

«КИБЕРҚЫЛМЫСТАРДЫ, ОНЫҢ ІШІНДЕ ИНТЕРНЕТ АЛАЯҚТАРДЫ АШУМЕН ТЕРГЕУДІ ЖҰМЫСТЫҢ ТИІМДІЛІГІН АРТТЫРУ»

атты Республикалық семинарының материалдар жинағы
2025 жыл 11 қаңтар

«ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ РАБОТЫ В РАСКРЫТИИ И РАССЛЕДОВАНИИ КИБЕРПРЕСТУПНОСТИ В Т.Ч. ИНТЕРНЕТ-МОШЕННИЧЕСТВО»

сборник материалов Республиканского семинара
11 января 2025 год

Астана, 2025 жыл

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ІШКІ ІСТЕР МИНИСТРЛІГІ
МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РЕСПУБЛИКИ КАЗАХСТАН

«КИБЕРҚЫЛМЫСТАРДЫ, ОНЫҢ ІШІНДЕ ИНТЕРНЕТ АЛАЯҚТАРДЫ АШУМЕН ТЕРГЕУДІ ЖҰМЫСТЫҢ ТИІМДІЛІГІН АРТТЫРУ»

атты Республикалық семинарының материалдар жинағы
2025 жыл 11 қаңтар

«ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ РАБОТЫ В РАСКРЫТИИ И РАССЛЕДОВАНИИ КИБЕРПРЕСТУПНОСТИ В Т.Ч. ИНТЕРНЕТ-МОШЕННИЧЕСТВО»

сборник материалов Республиканского семинара
11 января 2025 год

Астана, 2025 жыл

ӘОЖ 343
КБЖ 67.450

Киберқылмыстарды, оның ішінде интернет алаяқтарды ашумен тергеуді жұмыстың тиімділігін арттыру: Республикалық семнарының материалдар жинағы. *2025 жыл 11 қаңтар* // құр. ҚР ІІМ Тергеу департаменті; ҚР ІІМ Басқару академиясы. – Астана., 2025. – 49 б.

Жинаққа Қазақстан Республикасының Ішкі істер министрлігі 2025 жылғы 11 қаңтарда өткізген «Киберқылмыстарды, оның ішінде интернет алаяқтарды ашумен тергеуді жұмыстың тиімділігін арттыру» тақырыбындағы Республикалық семинарына қатысушылардың баяндамалары енгізілді.

Бұл материалдар жинағы көптеген оқырмандарға, ғылыми және педагогикалық қызметкерлерге, аспиранттарға, адъюнкттерге, сондай-ақ құқық қорғау және бақылау-қадағалау органдарының қызметкерлеріне арналған.

ӘОЖ 343
КБЖ 67.450

АДИЛОВ САНЖАР АСКЕНОВИЧ

Қазақстан Республикасы Ішкі істер министрінің орынбасары,
заң ғылымдарының кандидаты, полиция генерал-майоры

ҚҰРМЕТТІ ҚОНАҚТАР!

Бүгінгі семинар-кеңестің тақырыбы өзекті: «Интернет арқылы жасалатын алаяқтық қылмыстарын ашу және тергеу сапасын арттыру, сондай-ақ осы бағытта құқыққорғау және мүдделі мемлекеттік органдардың өзара іс-қимылын жетілдіру».

Тағы бір мақсатымыз – территориялық бөліністерімізге ұйымдастырушылық және практикалық көмек көрсету.

Барлығымыз білеміз, қазіргі таңда интернет-алаяқтық азаматтар мен еліміздің экономикасына елеулі қауіп төндіруде.

Соңғы 7 жылда мұндай қылмыстардың саны 10 есеге өсті (2017 ж. – **2046**, 2018 ж. – **4287**, 2019 ж. – **7733**, 2020 ж. – **14175**, 2021 ж. – **21275**, 2022 ж. – **20444**, 2023 ж. – **21621**).

2024 жылдың қорытындысы бойынша алаяқтық еліміздегі көптаралған қылмыс түріне айналып **(125,7 мың немесе 35%)**, олардың саны ұрлықтанда асып кетті.

Қазір еліміздегі әрбір екінші алаяқтық интернет арқылы жасалуда, олардан келген жалпы шығын былтыр**11 млрд** теңгеден асты.

Өкінішке орай қабылданған шараларға қарамастан, мұндай қылмыстардың ашылу деңгейі төмен күйде қалуда.

Оның әртүрлі объективті себептері де бар.

Бұл мәселелерді шешу үшін құқыққорғау және мемлекеттік органдардың бірлескен іс-қимылын нығайту, тергеу барысына ведомстволық бақылауды күшейту және қызметкерлеріміздің біліктілігін арттыру қажет.

В целях повышения эффективности противодействия интернет-мошенничествам МВД проводится комплекс организационных и практических

мероприятий, предусмотренных «Программой по противодействию киберпреступности, в том числе телефонным и интернет-мошенничествам на 2023-2025 годы».

Для оздоровления криминогенной ситуации в стране реализуется Дорожная Карта по противодействию кредитному мошенничеству.

Со своей стороны МВД **принимает необходимые меры** по профилактике и раскрытию указанных преступлений:

-С 22 июля 2024г. совместно с Национальным банком и банками второго уровня запущен **«Антифрод-центр»** по выявлению и пресечению мошеннических транзакций.

-1 ноября 2024г. в структуре МВД создан Департамент по противодействию киберпреступности.

-Для повышения эффективности работы следственных подразделений 29 ноября 2024г.в структуре всех территориальных Департаментов полиции созданы отделы по расследованию киберпреступлений с общей штатной численностью **233 единицы** *(в т.ч. 42 руководителя и 191 следователя)*.

-налажено взаимодействие с опытными сотрудниками IT-сферы *(к расследованию уголовных дел привлекаются специалисты Центра анализа и расследования кибератак, ТОО «Seven Hills», Холдинга «Каздрим Спешиал Систем» и др.)*.

-подписаны Меморандумы о взаимодействии и сотрудничестве с рядом государственных органов и субъектов частного сектора *(по противодействию кредитным мошенничествам с АРРФР и ГП; по фрод-звонкам с операторами связи («Кар-тел», «Кселл», «Теле-2», АО «Казахтелеком», «Транселеком»)*; для борьбы с мошенничествами на торговых площадках – с «Ассоциацией Цифровой Казахстан» *(Kaspi.kz, Kolesa.kz, Krysha.kz, Маркет.kz и др.)*; по киберинцидентам и экспертным исследованиям – с Центром анализа и расследования кибератак *(ОЮЛ «ЦАРКА»)*;

-выработаны законодательные поправки о введении административной и уголовной ответственности за «дропперство» *(реализация планируется в рамках проекта Закона «О профилактике правонарушений»)*, которые сейчас находятся на рассмотрении рабочей группы при Минюсте;

-достигнута договоренность о взаимодействии с интернет-платформами *(Телеграмм и Тик-Ток)* о предоставлении информации по санкционированным запросам;

-установлен технический заслон фрод-звонкам *(совместно с операторами связи заблокировано 64 млн. звонков с подменных номеров)*, изъято 23 SIM-бокса *(устройство агрегации незарегистрированных сим-карт – звонки через Интернет)* и более **6 тыс.** незарегистрированных SIM-карт *(гг. Астана, Алматы, Караганда, Атырау и Семей)*.

Наряду с этим наращивается международное взаимодействие.

Так, в апреле 2024г. совместно с полицией Украины проведена спецоперация, в ходе которой ликвидировано **5** мошеннических колл-центров *(совершали преступления в отношении казахстанцев и граждан Чехии, задержано более 30 участников)*.

Аналогичная операция проведена в г.Алматы, где выявлены **4** центра, жертвами которых стали граждане других стран *(США, Китай, Малайзия, Иран)*.

Задержаны **47** иностранцев *(Китай, Малайзия, Узбекистан, Таджикистан)*.

В настоящее время продолжается совместная работа с украинскими, белорусскими и российскими коллегами по выявлению новых колл-центров.

Проводится работа по присоединению к Будапештской конвенции Совета Европы о компьютерных преступлениях *(в 2023 года Казахстан получил статус страны-наблюдателя в рамках данной Конвенции, ратификация запланирована на 2025 год)*.

Кроме этого, в 2024 году в рамках профилактической работы в ходе мониторинга интернет-пространства выявлено свыше **38 тыс.** зарубежных интернет-ресурсов, в т.ч. свыше **11 тыс.** с признаками мошенничеств и финансовых пирамид.

Информация о них размещена в информационной системе «Кибернадзор» *(МКИ)* для блокирования доступа казахстанских пользователей.

Наряду с этим, в рамках повышения правовой и финансовой грамотности населения в СМИ опубликовано свыше **11 тыс.** материалов, в общественных местах *(подъезды, остановки и т.д.)* размещено более **150 тыс.** буклетов с тематикой: «Осторожно, мошенники!», создано свыше **150** различных видеороликов *(с привлечением известных личностей)* с подробным описанием действий мошенников.

Также МВД инициирован ряд законодательных поправок, направленных на снижение рисков оформления мошеннических займов *(добровольный отказ от кредитов, обязательная биометрическая идентификация при оформлении онлайн-кредитов, приостановление претензионной работы банков по мошенническим кредитам)*.

В августе – сентябре прошлого года МВД по всей стране проведены кустовые семинар-совещания на тему противодействия интернет-мошенничествам, с приглашением судей, прокуроров, представителей банков второго уровня и других госорганов, а также всех следователей и оперуполномоченных территориальных ДП, задействованных в группах «Киберпол».

В ходе данных мероприятий обсуждены проблемные вопросы расследования интернет-мошенничеств и выработаны предложения по противодействию им, с учетом которых доработан пошаговый алгоритм неотложных следственно-оперативных мероприятий.

Кроме того, в октябре прошлого года с целью повышения уровня безопасности наших граждан и эффективного противодействия киберпреступности, МВД внесены ряд предложения в ГП, МЦРИАП и АРРФР, которые сейчас находятся на различных этапах реализации.

В настоящее время **МЦРИАП** рассматривает инициативу по ограничению количества SIM-карт на одно физическое лицо, исключению их регистрации на дистрибьюторов и дилеров, а также введению обязательной видео идентификации при покупке и активации SIM-карт.

Также обсуждаются меры по запрету и лицензированию устройств «SIM-box» и «SIM Gateway», усилению контроля за их ввозом и использованием, обязыванию операторов связи выявлять подозрительные действия с данными устройствами и активно сотрудничать с правоохранительными органами.

Совместно с банками прорабатывается вопрос внедрения системы единых номеров, исключающей использование стандартных сотовых номеров для обзвона клиентов.

Также **АРРФР** рассматривает вопросы усиления безопасности онлайн-кредитования, вводя двухфакторную аутентификацию, биометрическую идентификацию и требования к защите персональных данных.

Для повышения контроля за платежными картами вводится ограничение на их количество для одного клиента, а также рассматривается дальнейшее сокращение лимита.

Таким образом, предложения МВД находятся на стадии реализации в государственных органах, часть из них уже внедрена, а остальные включены в планы, для дальнейшей проработки.

В свою очередь, Правительство страны так же уделяет особое внимание вопросам борьбы с мошенничествами на финансовом рынке и киберпреступностью.

В ноябре 2024г. под руководством Администрации Президента состоялось совещание, где даны конкретные поручения:

-предложить новые инструменты профилактики кибермошенничеств.

-утвердить методические рекомендации для повышения эффективности раскрытия и расследования таких преступлений.

-Усилить работу киберподразделений МВД по выявлению новых схем мошенничеств и методов борьбы с ними.

Аталған шаралар интернет-алаяқтыққа қарсы іс-қимыл тиімділігін арттыруға, олардыңсанын азайтуға және азаматтардыңқұқықтарын қорғауға бағытталған.

Ішкі істер министрлігі еліміздің азаматтарының қауіпсіздігін қамтамасыз ету үшін барлық қажетті шараларды атқаруда.

Бүгінгі біздің семинарымызға сот және Бас прокуратура өкілдері, Қаржы нарығын реттеу және дамыту агенттігі, Қаржылық мониторинг агенттігі, Цифрлық даму министрлігі және IT компанияларының басшылары шақырылды.

Оларға уақыттарын бөліп келгені үшін алғысымызды айтамыз. Сіздердің бүгінгі айтатын ұсыныс-пікірлеріңіз біз үшін өте маңызды.

Бүгінгі семинарда келесіні талқылаймыз:

• Тергеу және жедел-іздестіру іс-шаралары алгоритмдері бойынша негізгі мәселелерді талқылау.

• Тергеу кезіндегі жиі жіберілетін қателіктерді талдау

• Интернет-алаяқтықтың алдыналу бойынша заңнамалық бастамаларды жетілдіру және жаңа тәсілдерді талқылау.

Біздің негізгі мақсатымыз – азаматтардың құқыққорғау органдарына сенімін арттыру, алаяқтықтан келтірілетін шығынды барынша азайту.

Біз тек бірлескен күш-жігердің, кәсібиліктің және жауапкершілігіміздің арқасында бұл мәселелерді шешуде нақты өзгерістерге қолжеткізе аламыз.

Сондықтан бүгінгі семинарға белсенді қатысуларыңызды сұраймын!

ҮМБЕТАЛИН ӘКІМЖАН ЕРКІНҰЛЫ
Заместитель начальника службы по надзору за досудебным расследованием и уголовным преследованием ГП

РОЛЬ ПРОКУРОРА ПРИ ОСУЩЕСТВЛЕНИИ ДОСУДЕБНОГО РАССЛЕДОВАНИЯ ПО ИНТЕРНЕТ - МОШЕННИЧЕСТВА

За последние 5 лет структура преступности кардинально изменилась.

Если раньше преобладали кражи, то сейчас - из года в год растут мошенничества.

Справочно: 2019г. - 31 318, 2020г. - 32 968, 2021г. - 40 402, 2022г. - 42 813, 2023г. - 43 895.

В прошлом году всего зарегистрировано 132 тысяч преступлений (132 778), из которых треть или 45 тысяч мошенничеств. Половина совершена через Интернет (22 870).

Ежедневно регистрируются свыше 60 фактов.

22 тысячи потерпевших потеряли более 11 млрд тенге. Возмещено всего 16% (1,5 млрд тенге).

Несмотря на тысячи разъяснительных мероприятий, люди все еще доверчивы.

Больше всего мошенничеств зарегистрировано **в Алматы** (9 469), **Астане** (8 098). Как и интернет-мошенничеств (Астана - 4 603, Алматы - 2 325).

Проблему не раз обсуждали с госорганами на площадке Генеральной прокуратуры.

Провели Координационный совет (30.05.2024г.), приняли еще ряд дополнительных мер.

По нашей инициативе в отдельных регионах при содействии акиматов приобретены программы для территориальных подразделений «Киберпол».

Справочно: Шымкент, Алматы, Костанайская, Абай, Актюбинская, ВКО, СКО.

Это позволило в этом году разоблачить 60 кибергрупп, из них по инициативе прокуратуры - 42.

Недавно полицией Жетысу за соучастие задержана группа **Карагандинских** обнальщиков, основателей телеграмм канала **«Tokaev obnal»,** которые будучи в сговоре переводили похищенные средства на счета иностранных мошенников ***(общая сумма ущерба 100 млн тенге).***

Наряду с этим, за соучастие в мошенничестве по уголовным делам привлечено **118** дроперов.

При нашей координации потерпевшим разъясняется о порядке самостоятельного взыскания с дроперов причиненного им ущерба в порядке гражданского судопроизводства (статья 953 ГК).

На сегодня с дроперов уже взыскано около 1 млрд тенге.

Справочно: лучшие показатели в Павлодарской (150 млн тенге), Карагандинской (100 млн тенге) и ВКО (100 млн тенге).

Нацбанком запущен Антифрод-центр, который блокирует мошеннические транзакции. За прошлый год заблокировано **1,2 млрд** тенге.

Справочно: добровольно возвращено жертвам - 81 млн.

В ноябре прошлого года при координации прокуратуры г. Алматы заключен меморандум с АО «Казахтелеком», в результате за короткое время ликвидировали 6 устройств «SIM-бокс», имеются задержанные лица.

Это привело к временному снижению телефонных мошенничеств в целом

Если в среднем в т.г. ежедневно регистрировалось 25 телефонных мошенничеств (11 мес. т.г. - 8 363), то после изобличения устройств «SIM-бокс» наблюдается тенденция их снижения.

Так, по состоянию на 12 декабря т.г. начато 22 дела, в последующие дни - 15 (13.12.2024г.), 16 (14.12.2024г.), 10 (15.12.2024г.) и 6 (16.12.2024г.) соответственно.

В целом, борьба с мошенничеством не прерывается.

Несмотря на это ситуация существенно не улучшается.

Есть недостатки.

Банки и МФО продолжают упрощать процедуры выдачи кредитов, не обеспечивая защиту от мошеннических операций.

Также не соблюдают требования закона о приостановлении взысканий по мошенническим займам, что приводит к обоснованным жалобам пострадавших.

Операторы связи должным образом не обеспечивают безопасность своих клиентов. Мошеннические звонки не прекращаются.

К большому сожалению, ряд мошенничеств совершается при участии работников названных организаций.

В настоящее время проводятся досудебные расследования в отношении некоторых банков и операторов связи.

У нас низкая раскрываемость.

Из 52 тысяч дел о мошенничествах (52 039 с учетом дел прошлых лет) в суд направлено только 29% (14 879), из которых 78% это дела тяжкой категории (11 665).

По 28 тысячам (28242) сроки следствия прерваны.

В среднем по республике раскрывается всего 37% мошенничеств.

Справочно: небольшой - 45%, средней - 8%, тяжкие - 64%. Худшие показатели в ВКО (23%), Костанайской (24%) и области Абай (24%). Лучшие показатели в Мангистауской (72%), Туркестанской (65%) и Кызылординской (60%) областях.

В основном не раскрываются дела средней тяжести (раскрыто 8%), преимущественно это интернет-мошенничества ***(раскрываемость - 21%).***

К примеру, в Астане (4,6%), Абайской (4,7%) и Карагандинской областях (5,3%) раскрываемость мошенничеств средней тяжести - всего 5%.

1) От качества следствия зависит раскрываемость.

Все чаще кибермошенничества совершаются при непосредственном участии дропперов.

Вопрос об их ответственности прорабатывается.

Но есть положительные примеры по их привлечению в качестве соучастников мошенничества, однако, практика в регионах разная.

Как я уже говорил, к уголовной ответственности привлечено 118 дроперов, при этом 90% (91 дропер) из них привлечено в Шымкенте.

Другом случае, в Карагандинской области только по материалам уголовного дела недавно разоблачили целую сеть дроперов. В итоге дроповод объявлен в розыск.

2)Нужно обеспечить регистрацию каждого факта мошенничества. Это позволит исключить укрытие уголовных правонарушений.

С новыми поправками в Закон «О банках и банковской деятельности» финансовые организации на основании представления следователя (в порядке ст.200 УПК) либо постановления о признании лица потерпевшим обязаны бессрочно приостанавливать все процедуры взыскания по мошенническим кредитам на период расследования уголовного дела.

В случае укрытия мошенничеств у них не будет никаких оснований для реагирования, что приведет к обоснованным жалобам пострадавших и резонансным событиям.

Как например с коллективной жалобой 300 граждан. По их доводам уполномоченными органами проводится проверка в банках и МФО.

За 2 года мы выявили порядка 3 тысяч укрытых мошенничеств.

Справочно: больше всего в Алматы (739) и Астане (846).

В 2024 году путем соединения в связи с повторной регистрацией снято с учета 236 дел (в 2023г. - 1767).

Больше всего в Алматинской (116), ВКО (35) и г.Астана (30).

Необоснованно к ЕРДР без регистрации дела приобщено 1 438 заявлений Такие факты имеются во всех регионах без исключения.

В абсолютных лидерах Астана (499) и Алматы (367), Карагандинская (145), Павлодарская (82).

Установлено порядка 200 заявлений, необоснованно направленных в банк для рассмотрения по существу, без регистрации уголовных дел.

Первое. Незамедлительно регистрировать в ЕРДР каждое сообщение об интернет-мошенничестве и создавать Инциденты в системе Антифрод-центра НацБанка для блокирования мошеннических денежных переводов.

Исключить факты укрытия.

Второе. Своевременно признавать лиц потерпевшими и разъяснять их права на обращение в финансовую организацию о приостановлении мошеннического кредита.

При этом в течение трех дней после этого направлять соответствующее представление в порядке статьи 200 УПК в адрес финансовых организаций ***(на основании пункта 15 статьи 34 Закона «О банках и банковской деятельности»).***

В случае его неисполнения рассматривать вопрос о привлечении субъектов к административной ответственности в порядке статьи 664 КоАП.

Третье. Признавать потерпевшими финансовые организации в случае оформления банковского займа мошенническим способом без участия клиента ***(оформление займа путем удаленного доступа в результате обманного получения кода доступа, без прохождения полной биометрической идентификации и т.д.).***

Четвертое. Обеспечить своевременное и качественное исполнение отдельных поручений органов расследования, а также указаний надзирающего прокурора;

Пятое. Принять меры к установлению обстоятельств события, причин и условий, способствовавших совершению интернет-мошенничества.

В ходе досудебного расследования с привлечением специалистов исследовать соблюдение финансовыми организациями, операторами связи, маркетплейсами и другими организациями требований отраслевых законов ***(«О персональных данных и их защите», «О связи», «О банках и банковской деятельности» и др.),*** направленных на защиту персональных данных и предупреждение мошеннических действий.

Также устанавливать причину обслуживания операторами связи незарегистрированных абонентских номеров на предмет наличия состава уголовного правонарушения.

Для выявления источника утечки, выяснять У потерпевших, где и при каких обстоятельствах они предоставляли свои персональные данные.

По результатам решать вопрос о регистрации уголовных дел.

Справочно: по статьям 147 (Нарушение неприкосновенности частной жизни и законодательства о персональных данных и их защите), 211 (Неправомерное распространение электронных информационных ресурсов ограниченного доступа), 250 (Злоупотребление полномочиями) или 254 (Недобросовестное отношение к обязанностям) УК.

Шестое. Принятие комплекса оперативно-следственных мер по возмещению ущерба, выявлению похищенных средств и последующего возврата, в том числе путем наложения ареста на имущество и банковские счета.

При установлении легализации преступного дохода и имущества, приобретенного на средства, добытые преступным путем с вовлечением их в законный оборот ***(конверсии),*** рассматривать вопрос регистрации досудебного расследования по статье 218 УК.

Полагаю, эти меры значительно повысят эффективность борьбы с мошенничествами.

В целом мы подготовили проекты совместного Указания об усилении работы по противодействию интернет-мошенничествам, а также проект совместного приказа «Об утверждении критериев оценки».

Предлагаю МВД рассмотреть их и внести предложения.

КАНАТ ТОБАГАЛИҰЛЫ
Судья межрайонного суда по уголовным делам г. Астаны

ВОПРОСЫ, ВОЗНИКАЮЩИЕ ПРИ САНКЦИОНИРОВАНИИ ВЫЕМКИ СВЕДЕНИЙ ПО ИНТЕРНЕТ-МОШЕННИЧЕСТВАМ. ТИПИЧНЫЕ ОШИБКИ ДОПУСКАЕМЫЕ СЛЕДОВАТЕЛЯМИ. ПРЕДЛОЖЕНИЯ ПО ПОВЫШЕНИЮ КАЧЕСТВА МАТЕРИАЛОВ, ПРЕДОСТАВЛЯЕМЫХ СУДАМ НА САНКЦИОНИРОВАНИЕ, А ТАКЖЕ ПО АЛГОРИТМУ МВД. ПОЗИЦИЯ СУДА ПО ОТВЕТСТВЕННОСТИ ДРОППЕРОВ.

Киберпреступление согласно главы 7 также ст.148, 190 "Что такое компьютерные преступления и в чем оно состоит, ответить на данный вопрос весьма не просто так как границы подобной деятельности однозначно не определены, нет полной ясности относительно параметровым критериям по которым следует выделять, фиксировать компьютерные преступления попытки их совершить.

Однако законодательства многих стран сходится в том что, в компьютерных преступлениях и в самих общих формулировках есть любые противозаконные действия объектом по ситуации которые являеться - информация обрабатываемая в компьютерной системе, а орудием посягательств служит - компьютер.

Другими словами большинство случаев компьютерные преступления представляют собой давно известными традиционные виды преступления, но совершаемыми новыми орудием и в новой среде.

Киберпреступность - это незаконное противоправное действие которое осуществляется людьми использующие информационно-телекоммуникационные технологии компьютеров, компьютерные сети для преступных целей.

Киберпреступление могут совершаться как физическими лицами так и группами лиц, коммерческими организациями хотя данные субъекты могут применятся схожими тактическими методами, к примеру могут использовать вредоносных программных обеспечении, атаковать схожие цели, к примеру они имеют разные мотивы с намерениями к совершению киберпреступления.

В нашей деятельности в основном применяется по квалификации преступления глава 7 в основном ст.205, 206, 207, 211, 212, 213.

Однако хотелось бы остановится о дропперов. Дропперы - это те люди которые помогают пособничеству через 28ч. 5ч., но необходимо доказать субъективную сторону а именно умысел, а человек может передать незная об этом, поэтому мы и требуем при поступлении дела чтобы оно было уже доказанно. Однако доказать что дроппер действовал умышленно в совокупности а миенно с получателем иногда представляется сложным. В связи с этим, так как Конституция обязует защищать права граждан необходимо доказать умысел дропперов помогающему организатору преступления.

ХИСАМУТДИНОВА ЭЛЬМИРА РЕНАТОВНА
Национальный проектный менеджер
Военно-политического отдела офиса программ ОБСЕ в Астане

ПОДДЕРЖКА РЕСПУБЛИКИ КАЗАХСТАН В РАЗРАБОТКЕ СИСТЕМНОГО ПОДХОДА В ПРОТИВОДЕЙСТВИИ КИБЕРПРЕСТУПНОСТИ

Киберпреступность - сложное явление, требующее консолидированных усилий и комплексных подходов со стороны правоохранительных, государственных органов, бизнеса и общества в целом.

Безграничный характер киберпреступности означает, что правоохранительные органы сталкиваются с трудностями в эффективном противодействии этой форме преступлений из-за ограничений в проведении трансграничных расследований. Более того, правоохранительные органы в значительной степени зависят от ресурсов, которые до сих пор не обеспечены в должном объеме, а также от современных следственных навыков и компетенций.

В августе 2023 года совместно с Министерством внутренних дел Казахстана, Офис программ ОБСЕ в Астане запущен проект «Поддержка Республики Казахстан в разработке эффективной политики противодействия киберпреступности (Фаза I)».

Проект направлен на решение проблемы киберпреступлений, а также преступлений, совершаемых путем неправомерного использования информационно-коммуникационных технологий (ИКТ), включая кибермошенничество, сексуальную эксплуатацию женщин и детей в киберпространстве, гендерное насилие, отмывание денежных средств, незаконный оборот наркотиков, их торговля через Интернет, а также насильственный экстремизм, ведущий к терроризму.

Проект использует комплексный подход и затрагивает три основных направления:

а)законодательное (национальный стратегический документ и соответствующие внутренние правовые нормы);

б)внедрение комплексного и устойчивого подхода в систему образования правоохранительных органов путем разработки стратегии обучения для академий Министерства внутренних дел и Академии правоохранительных органов при Генеральной прокуратуре и подготовки их преподавателей;

в)повышение осведомленности населения для снижения воздействия киберпреступной деятельности на население.

Мероприятия проекта будут способствовать укреплению международного сотрудничества, опирающегося на прочную отечественную законодательную базу. Проект также будет способствовать скорейшему присоединению Казахстана к Будапештской конвенции и окажет поддержку стране в случае вступления в недавно разработанный Договор ООН о противодействии использованию информационно-коммуникационных технологий в преступных целях.

Это позволит укрепить межведомственное взаимодействие в Казахстане на основе общего понимания киберугроз и высокой важности создания соответствующих барьеров для их преодоления. Он также обеспечит прочную

основу для проведения структурных изменений в правоохранительной системе. Будет усовершенствована практика подготовки кадров путем внедрения новой стратегии обучения в учебных заведениях правоохранительной системы. Мероприятия в рамках проекта также позволят повысить устойчивость общества к киберпреступлениям.

В рамках проекта при Министерстве внутренних дел Республики Казахстан создана Межведомственная координационная группа по разработке Комплексного плана по противодействию киберпреступлениям и преступлениям с использованием информационно-коммуникационных технологий *(далее – МКГ).*

14-15 марта состоялось Первое заседание Межведомственной координационной группы по разработке Комплексного плана по противодействию киберпреступлениям и преступлениям с использованием информационно-коммуникационных технологий. На мероприятии участники ознакомились с целями и задачами проекта, совместным планом Офиса программ ОБСЕ в Астане и Министерством внутренних дел Казахстана, уставными документами проекта. Представители государственных и частных организаций, а также национальные и международные консультанты Офиса программ ОБСЕ в Астане обменялись своим экспертным мнением и обозначили повестку дня для Второго заседания.

16-17 мая 2024 года состоялось Второе заседание Межведомственной координационной группы по разработке Комплексного плана по противодействию киберпреступлениям и преступлениям с использованием информационно-коммуникационных технологий. В рамках мероприятия были изучены результаты проведенного Анализа текущей ситуации в сфере противодействия киберпреступности и преступлениям с использованием информационно-коммуникационных технологий, а также анализа международного опыта.

Свои заключения предоставили эксперты в сфере нормативно-правового регулирования, технического и технологического развития, прав человека и современных методов борьбы с киберпреступностью.

В рамках Анализа были определены следующие системные проблемы в противодействии киберпреступности:

1. Отсутствие в системе государственного планирования систематического подхода к прогнозированию влияния глобальных киберугрозна Казахстан, включая систему оценки рисков и план по реагированию на эти риски.

2. Отсутствие стандартов по технической совместимости инабору инструментов для сбора и хранения цифровых доказательств в контексте международного сотрудничества в борьбе с киберпреступностью.

3. Отсутствие системы и методов оценки объема криптовалютного рынка.

4. Отсутствие в системах КПСиСУ отдельного учета преступлений, совершенных посредством ИКТ и отсутствие отдельных аналитических исследований таких данных.

5. Отсутствие систематического учета хищений средств клиентов финансовых организацийс централизованным сбором информации.

6. Отсутствие дезагрегации преступлений по гендерному, или половому признаку.

7. Отсутствие систематического криминологического анализа киберпреступности, включая по гендерному признаку.

8. Проблемы квалификации новых видов преступных действий, нарушающих права человека в виртуальном пространстве, некоторые из которых не предусмотрены законодательством либо сложны в установлении статьи.

9. Отсутствие единообразного понимания и определения понятия «кибербуллинг»в юридическом контексте также как и сложность доказательства факта кибербуллинга.

10. Отсутствие анализа по совокупному прямому финансовому и косвенному ущербу населению/бизнесу от кибер преступлений.

11. Отсутствие статистикипо использованию криптовалюты при отмывании денег и в коррупционных преступлениях.

12. Недостаточное количество профессорско-преподавательского состава в вузах правоохранительной системы по специализации в сфере борьбы с киберпреступностью.

13. Текущий и прогнозируемый кадровый голод специалистов в сфере как ИТ и кибербезопасности, так и в противодействии кибер преступности.

14. Отсутствие методик и НПА для сбора и анализа электронных (цифровых) доказательств.

15. В Уголовном Кодексе (ст. 3 «Разъяснение некоторых понятий, содержащихся в настоящем Кодексе») не дано разъяснение ни одному термину, используемому в контексте преступлений в сфере информационных технологий.

16. Проблема с квалификацией интернет-мошенничества, под которые подпадают как компьютерные преступления,так и телефонные.

17. Низкий процент раскрываемости преступлений в сфере информатизации и связи (Глава 7), ввиду отсутствия практики расследования, в т.ч. судебной.

18. Отсутствие инструментов международного взаимодействия с правоохранительными органами и частным сектором зарубежных стран по оперативному получению электронных доказательств в рамках уголовных дел, связанных с использованием ИКТ.

19. Отсутствие точного определения «интернет-мошенничества» и «вредоносные компьютерные программы».

20. Отсутствие квалифицирующего признака «…с использованием сетей телекоммуникаций» в статьях против половой неприкосновенности несовершеннолетних - 124 «Развращение малолетних», 312 «Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних либо их привлечение для участия в зрелищных мероприятиях порнографического характера», 144 «Вовлечение несовершеннолетних в изготовление продукции эротического содержания» создает правовую коллизию и возможность избежания соответствующего наказания преступников.

21. Отсутствие в законодательстве, включая и уголовное, определений киберпреступленийи преступлений, совершенных с использованием ИКТ.

22. Отсутствие четких алгоритмов (стандартных операционных процедур) по применению того или иного метода противодействия киберпреступности, включая алгоритмыпо международному взаимодействию.

23. Недостаток финансирования НИОКР в сфере создания программных продуктов и других исследований в области противодействия киберпреступности.

24. Отсутствие методик и систематического проведения технического и технологического аудита ИТ систем в правоохранительной сфере.

25. Отсутствие информации о количестве разработанных отечественных технологий защиты информации и о доле их применения в реальных проектах и системах.

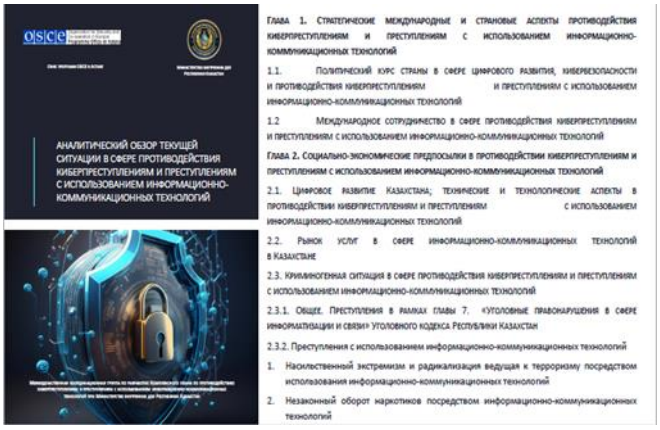
26. Искусственный интеллект не применяется в расследованиях киберпреступлений из-за отсутствия четкого понимания способов его применения.

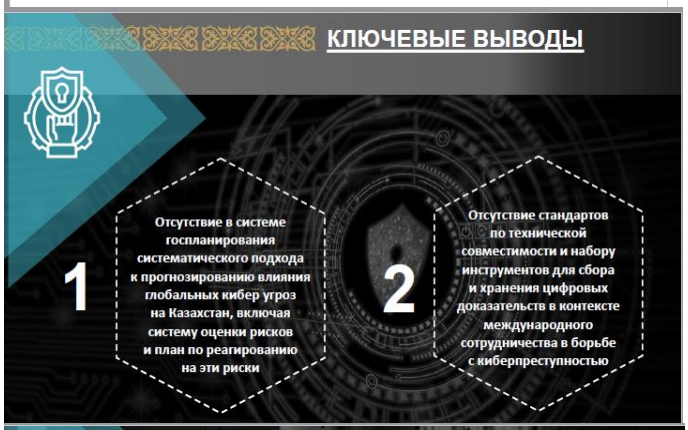
27. Отсутствие анализа существующих потребностей по использованию программного обеспечения в раскрытии киберпреступлений, их эффективности и целесообразности применения.

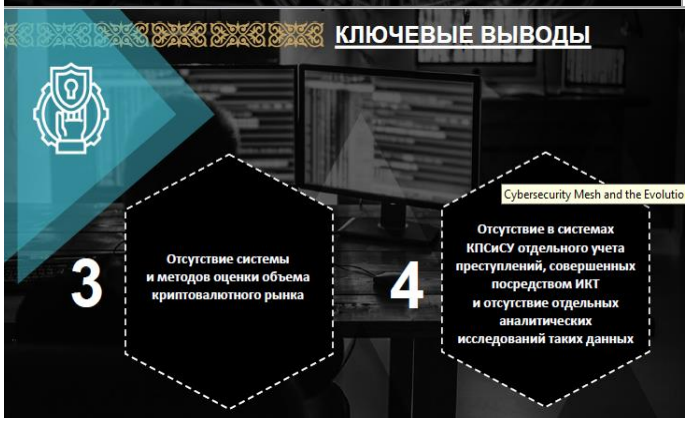
В рамках Третьего заседания МКГ обсуждался проект Комплексного плана по противодействию киберпреступлениям и преступлениям с использованием информационно-коммуникационных технологий на пять лет, корректировка мероприятий плана, определение сроков и основных индикаторов.

Проект способствует достижению Целей устойчивого развития ООН № 16: «Мир, справедливость и сильные институты» и № 17: «Партнерство во имя достижения целей».

ПРОВЕДЕННАЯ РАБОТА В ЦИФРАХ








КЛЮЧЕВЫЕ ВЫВОДЫ
7
Проблемы квалификации новых видов преступных действий, нарушающих права человека в виртуальном пространстве, некоторые из которых не предусмотрены законодательством либо сложны в установлении статьи
8
Отсутствие единообразного понимания и определения понятия «кибербуллинг» в юридическом контексте также как и сложность доказательства факта кибербуллинга


КЛЮЧЕВЫЕ ВЫВОДЫ
9
Отсутствие систематического криминологического анализа киберпреступности
10
Отсутсвие анализа по совокупному прямому финансовому и косвенному ущербу населению/бизнесу от кибер преступлений


КЛЮЧЕВЫЕ ВЫВОДЫ
11
Отсутствие статистики по использованию криптовалюты при отмывании денег и в коррупционных преступлениях
12
Недостаточное количество профессорско-преподавательского состава в вузах правоохранительной системы по специализации в сфере борьбы с киберпреступностью
(2 в АПО на 5000 прокуроров и около 30 в вузах МВД на 76 тысяч полицейских)

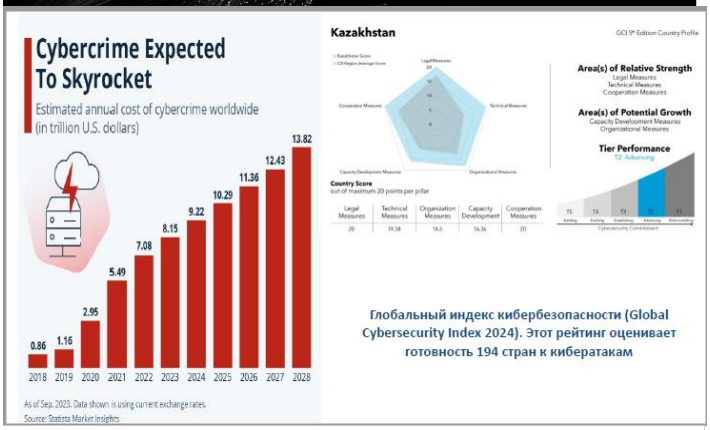

КЛЮЧЕВЫЕ ВЫВОДЫ
13
Текущий и прогнозируемый кадровый голод специалистов в сфере как ИТ и кибербезопасности, так и в противодействии кибер преступности
14
Отсутствие методик и НПА для сбора и анализа электронных (цифровых) доказательств


КЛЮЧЕВЫЕ ВЫВОДЫ
17
Низкий процент раскрываемости преступлений в сфере информатизации и связи (Глава 7), ввиду отсутствия практики расследования, в т.ч. судебной
18
Отсутствие инструментов международного взаимодействия с правоохранительными органами и частным сектором зарубежных стран по оперативному получению электронных доказательств в рамках уголовных дел, связанных с использованием ИКТ


КЛЮЧЕВЫЕ ВЫВОДЫ
19
Отсутствие точного определения «интернет-мошенничества» и «вредоносные компьютерные программы»
20
Отсутствие квалифицирующего признака «...с использованием сетей телекоммуникаций» в статьях против половой неприкосновенности несовершеннолетних - 124 «Развращение малолетних», 312 «Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних либо их привлечение для участия в зрелищных мероприятиях порнографического характера», 144 «Вовлечение несовершеннолетних в изготовление продукции эротического содержания» создает правовую коллизию и возможность избежания соответствующего наказания преступников.


КЛЮЧЕВЫЕ ВЫВОДЫ
2
Низкий процент раскрываемости преступлений в сфере информатизации и связи (Глава 7), ввиду отсутствия практики расследования, в т.ч. судебной
22
Отсутствие инструментов международного взаимодействия с правоохранительными органами и частным сектором зарубежных стран по оперативному получению электронных доказательств в рамках уголовных дел, связанных с использованием ИКТ


КЛЮЧЕВЫЕ ВЫВОДЫ
23
Отсутствие в законодательстве, включая и уголовное, определений киберпреступлений и преступлений, совершенных с использованием ИКТ
24
Не систематизирован подход к профилактике киберпреступности.
Недостаточное вовлечение всего общества в данный процесс



РАСПРОСТРАНЕННЫЕ ПРЕСТУПНЫЕ ТРЕНДЫ В КИБЕР ПРОСТРАНСТВЕ

1. ***Всплеск фишинга, связанный с пандемией:*** Пандемия COVID-19 вызвала значительное увеличение числа фишинговых атак, причем киберпреступники используют страх и дезинформацию населения.
2. ***Ransomware:*** атаки по-прежнему широко распространены, причем значительная часть жертв предпочитает заплатить выкуп, несмотря на риск не восстановить свои данные.
3. ***Рост числа случаев компрометации деловой электронной почты (BEC):*** Заметно увеличилось количество атак BEC, когда киберпреступники перехватывают деловые транзакции для кражи средств.
4. ***Эволюция вредоносного ПО для мобильных устройств:*** Атаки мобильного вредоносного ПО становятся все более изощренными.
5. ***Рост киберактивизма:*** хактивисты используют кибератаки для продвижения социальных и политических целей.
6. ***Уязвимости ИИ и IoT:*** Технологии искусственного интеллекта и IoT все чаще используются киберпреступниками. По прогнозам, к 2040 году киберпреступность, основанная на искусственном интеллекте, превзойдет атаки, основанные на человеческом факторе.
7. ***Атаки на цепочки поставок:*** Эти атаки, хотя и менее распространены, могут нанести огромный ущерб, используя уязвимости в системах третьих лиц.
8. ***Постоянные утечки данных:*** Угроза утечки данных продолжает расти, причем количество инцидентов, о которых сообщается ежегодно увеличивается.
9. ***Угроза криптоджекинга:*** Кибер преступники используют вредоносное ПО для добычи криптовалюты, становится все более серьезной угрозой, предлагая злоумышленникам малорискованную статью дохода.
10. ***Сложные DDoS-атаки:*** Распределенные атаки типа DDoS становятся все более сложными и частыми, особенно в период пандемии они затронут такие важные отрасли, как электронная коммерция и здравоохранение.
11. ***Риски устаревшего программного обеспечения с открытым исходным кодом***
12. ***Устойчивость социальной инженерии:*** остается распространенным методом кибератак, особенно с помощью фишинга и приманки.
13. ***RDP-атаки на подъеме:*** атаки по протоколу удаленного рабочего стола становятся все более распространенными и нацелены на малые и средние предприятия для внедрения программ-вымогателей.

THE WORLD BANK

ТИПОЛОГИЯ ОНЛАЙН ВРЕДА (DIGITAL HARMS)

СЕМБАЕВ ДУМАН БЕКБОЛАТОВИЧ
Генеральный директор ТОО "Каздрим Спешлсистемс"

НОВЫЕ МЕТОДЫ УСТАНОВЛЕНИЯ АНОНИМНЫХ ПОЛЬЗОВАТЕЛЕЙ МЕССЕНДЖЕРОВ И СОЦИАЛЬНОЙ СЕТЕЙ

На протяжение 10 лет разрабатыеваем различные IT решения для правоохранительных органов нашей Республики, в последние пять лет вышли за пределы нашей Республики. Также работаем в странах Африки и ближнего Востока, Кавказа, Центральной Азии и Юго-восточной Азии.

Сотрудники IT технологии - это люди которые работают над созданием полезного для общества решения. Ну а в последние годы в рамках взаимодействия с полицией активно поступали запросы по работе в информационном поле (что делать? как быть?) так, как вся преступность уходит в информационное поле а именно буллинг, склонение к суициду, мошенничество и прочее.

Далее, данная информация состоит по двум напарвлениям а начнем с профилактики. Профилактику мы назовем как деструктивных аккаунтов и элементов что то же самое торговля наркотиков, наркошопов по текущему мониторингу.

Нами осуществляемый текущий мониторинг показывает что как отдельную картину о существовании около трехсот наркошопов, наркочатов по вовлечению людей в финпирамиды, по склонению к суициду, по распространению материалов порнографического, в том числе по пидофелии и религиозного экстремизма, криминала, сепаратизма а значит все это потребляют наши граждане которые в последующем могут стать потенциальными жертвами.

Цель самого мониторинга - это оценка влиянии деструктивных идей на наше населения, накопление этих публикации для чего, чтоб в последующем имелась доказательная база а также учет и категоризация самих деструктивных аккаунтов.

Если затронуть речь о профилактике то на сегодняшний день государство предпринимает меры по работе профилактики где привлечены генпрокуратура, МВД в целом весь правоохранительный блог, различные министерства, образования и науки. Но основная проблема в том что большая часть контента она все таки продвегается цифровом поле тоесть в онлайне, тоесть а государство пытается работать в оффлайне а в итоге между ними та самая большая стена в котором из оффлайна на онлайн пройти не удавалось.

В итоге все это приводит к тому что мы начинаем работать с последствиями так как это та самая воронка занимающиеся продажами как завлекающий канал потребителей а далее кто куда уходит сигментирование, привлечение и конверсия либо с достижением поставленной цели.

Зачастую правоохранительные органы начинают работать с той самой аудиторией которые в самом низу этой воронки, здесь люди как правило если это суицид то он уже либо мертвый или же проиграл все деньги на ставках, или же отдал все деньги финпирамиде, мошенникам тоесть таких людей необходимо не то что профилактировать а стоит лечить.

Все деструктивные группы должны быть под постоянным контролем

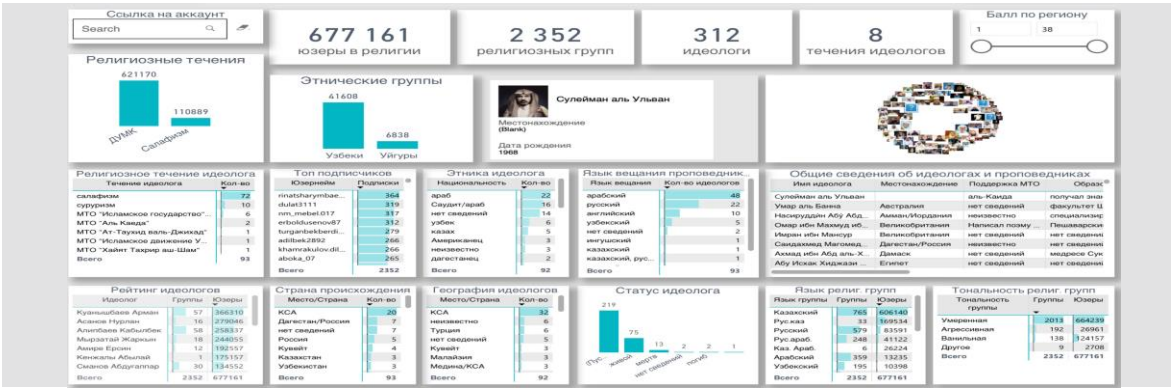
Группы и каналы

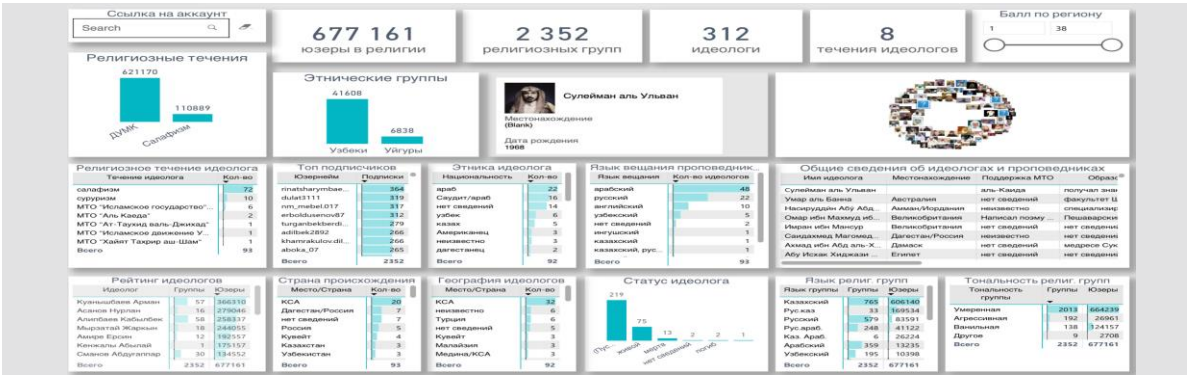
#Нарко	321
#Финпирамида	543
#Суицид	1759
#Педофилия	118
#Религиозный радикализм	1721
#Криминал	49
#Сепаратизм	1400

→ **Мониторинг**

Цели мониторинга

1. **Оценка влияния деструктива в регионе**
   Масштабы, методы, аномалии
2. **Хранение всех публикаций и участников для доказательной базы**
3. **Учет и категоризации деструктивных аккаунтов**
   Подстрекатели, слушатели, случайные





Профилактика ведется не в той плоскости

Оффлайн

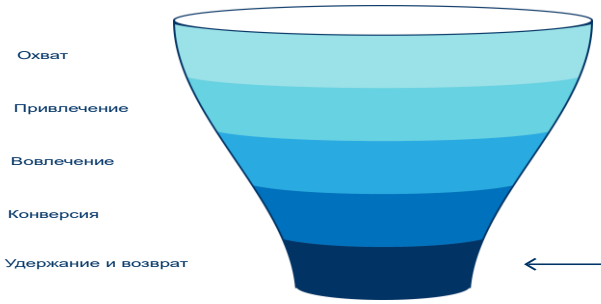
Госорганы пытаются работать с населением офлайн

Онлайн

Граждане потребляют деструктивный контент онлайн

Профилактика деструктивных аккаунтов

Работа с последствиями



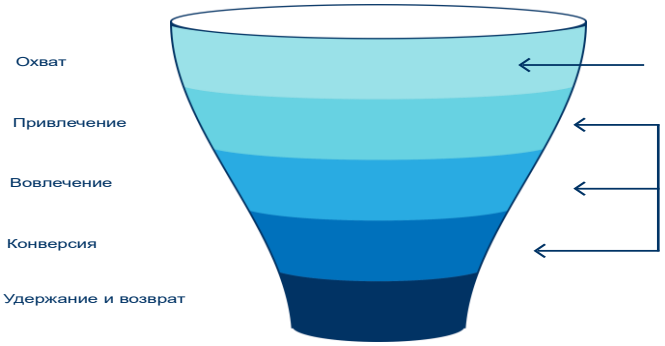
Сейчас, зачастую, работа ведется с последствием проблемы

Но!

Здесь люди уже мертвы/проиграли все деньги на ставках/попали в фин.пирамиду и т.д.

Профилактика деструктивных аккаунтов

Работа с последствиями

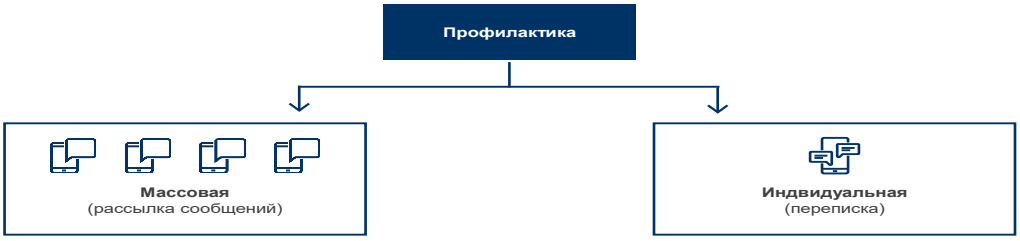


Борьба с деструктивом должна начаться здесь

И продолжаться на всех этапах

Профилактика деструктивных аккаунтов

Профилактика деструктивных аккаунтов

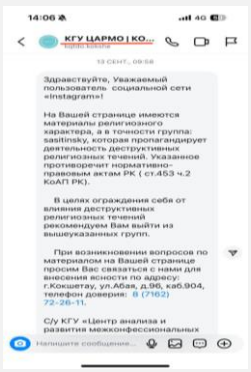


Профилактика деструктивных аккаунтов

Пример **массовой рассылки**

Рассылка участникам финпирамид

Рассылка участникам религиозно-радикальных групп



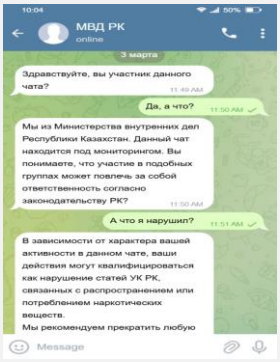
Профилактика деструктивных аккаунтов

Профилактика деструктивных аккаунтов

Пример **индивидуальной переписки**

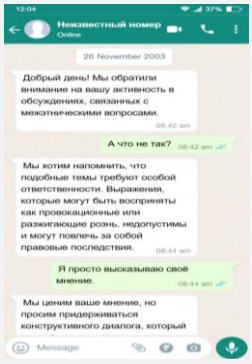
Участник нарко-чата

Telegram



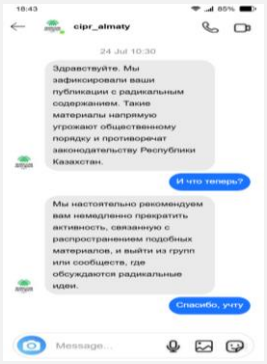
Участник чата по межэтнике

WhatsApp



Участник радикального чата

Instagram



Профилактика деструктивных аккаунтов

Финансовые пирамиды

С 2022 года было выявлено 534 068 аккаунтов подписанных на источники фин пирамид

200 389 аккаунтов отписались от истоников фин пирамид

85 источников фин пирамид было закрыто/удалено в ходе индивидуальной работы которые охватывали 211 226 аккаунтов

На 2024 года 122 453 аккаунта подписано на источники фин пирамид

За 3 года было снижено на 77%

Деанон
соцсетей

Установление личности анонимных акаунтов социальных сетей и мессенджеров

Анонимные пользователи в соцсетях

- Анонимность позволяет открыто заниматься противоправной деятельностью
- Анонимность способствует повышению преступности и деструктивности в сети
- Уровень анонимности бывает разный, в зависимости от подготовки владельца аккаунта

Деанон соцсетей

Бесконтактные способы

10% Поиск в утечках
Поиск номера телефона аккаунта по накопленным базам из darknet

12% Social Engeneering
Применение уязвимостей социальной сети по установлению привязанного к аккаунту номера

13% Face Recognition
Определение и идентификация лиц на публикациях в социальных сетях

8% Voice Recognition
Идентификация аудио или видео сообщения по голосу путем сличения с образцами голосов всех абонентов

20% Matching
Сопоставление действий в социальной сети с активностями в интернете

В среднем **90%** идентификации

Контактные способы

16% Phishing
отправка ссылки или документа для перехвата IP-адреса

21% Ping VPN
Глубокий анализ сигнатур в VPN

7 этапная технология по установлению личности анонимного аккаунта

Способ №1

Поиск в утечках

Поиск идентификатор аккаунта по накопленным базам из darknet

Анонимный аккаунт → @userid, @username проверяем по утечкам

← Номер телефона

Собранный утечки по социальным сетям и мессенджерам с привязкой к номеру телефона

Telegram	77 604 565	16.11.2019
Facebook	40 217 729	12.12.2019
OK	101 042	15.10.2020
VK	12 643 414	13.08.2020
Instagram	734 384	08.04.2021
Linkedin	16 003 438	15.09.2020

Способ №2

Social Engeneering

Использование уязвимость социальной сети и особенности выдачи привязанных к аккаунту номеров телефонов

Например, при условии сохранения абонентского номера в телефонную книгу Telegram, Instagram, Facebook деляться связанным с ним аккаунтом.

При этом, для 1 пользователя (бота) в день возможно собирать 10 аккаунтов с номерами.

Абонентская база KZ

Добавление номеров телефонов в телефонную книгу

Имитация восстановлени е пароля по номеру

Сличаем аккаунт анонима

Способ №3

Face Recognition

Определение и идентификация лиц на публикациях в социальных сетях

1

Собираем фотографии анонимов в:

- **аватарках** Telegram, Whatsap, Instagram, FaceBook, Tiktok
- **публикациях** Instagram, FaceBook, Tiktok

2

Сверяем с накопленной базой, где **более 1,2 млрд лиц** из соцсетей:

Instagram	**31 560 864**	WhatsApp	**426 891**
Telegram	**76 859**	Linkedin	**1 123 193**
FaceBook	**11 484 907**	OK	**277 480 366**
VK	**436 596 336**	Twiter	**15 019 472**
TikTok	**176 480 736**		

Способ №3

Face Recognition

Определение и идентификация лиц на публикациях в социальных сетях

Деанон соцсетей

1

Собираем фотографии анонимов в:

- **аватарках** Telegram, Whatsap, Instagram, FaceBook, Tiktok
- **публикациях** Instagram, FaceBook, Tiktok

2

Сверяем с накопленной базой, где **более 1,2 млрд лиц** из соцсетей:

Instagram	**31 560 864**	WhatsApp	**426 891**
Telegram	**76 859**	Linkedin	**1 123 193**
FaceBook	**11 484 907**	OK	**277 480 366**
VK	**436 596 336**	Twiter	**15 019 472**
TikTok	**176 480 736**		

NIST National Institute of Standards and Technology U.S. Department of Commerce

Наш FRS - сертифицированна NIST (National Institute of Standards and Technology USA)

Точность распознавания: **98,7%**
Время поиска: **2 секунды** по базе данных с более 1 млрд лиц

Способ №3

Face Recognition

Определение и идентификация лиц на публикациях в социальных сетях

Деанон соцсетей

1

Собираем фотографии анонимов в:

- **аватарках** Telegram, Whatsap, Instagram, FaceBook, Tiktok
- **публикациях** Instagram, FaceBook, Tiktok

2

Сверяем с накопленной базой, где **более 1,2 млрд лиц** из соцсетей:

Instagram	**31 560 864**	WhatsApp	**426 891**
Telegram	**76 859**	Linkedin	**1 123 193**
FaceBook	**11 484 907**	OK	**277 480 366**
VK	**436 596 336**	Twiter	**15 019 472**
TikTok	**176 480 736**		

3

Сверяем с:

980 млн	фотографий из ЕИС «Беркут»/ИС МП
28 млн	фотографий из ГБД «Физлица»

Способ №4

Voice Recognition

Идентификация аудио или видео сообщения по голосу путем сличения с образцами голосов всех абонентов

Деанон соцсетей

1

Сбор **аудио/видео публикаций** анонимного аккаунта

2

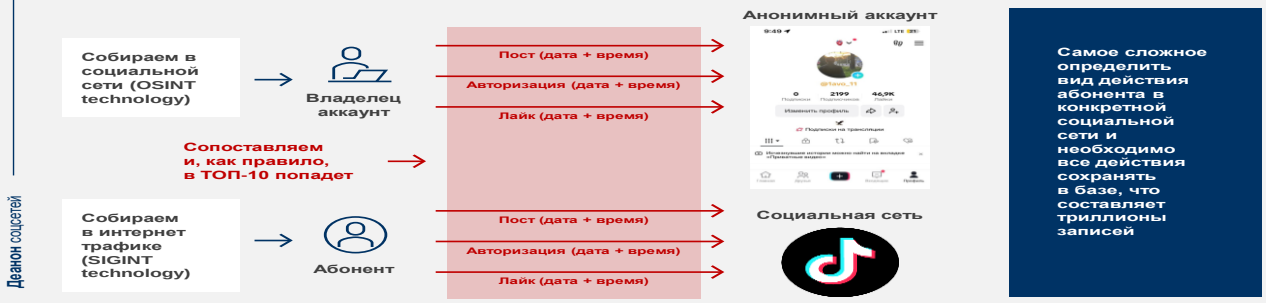
Сравнение с голосовыми отпечатками всех казахстанских абонентов

- Будут сформированы голосовые отпечатки на **30 млн абонентов.** Необходимо **1.92 секунд на 1** голос.
- Размер одного голосового отпечатка составляет **2600 байт**
- В Казахстане база будет сформирована **в первом полугодии 2025 года**
- Данные будут собраны **в 2G, 3G и 4G со всех 3 сотовых операторов**

Способ №5

Matching

Идентификация аудио или видео сообщения по голосу путем сличения с образцами голосов всех абонентов

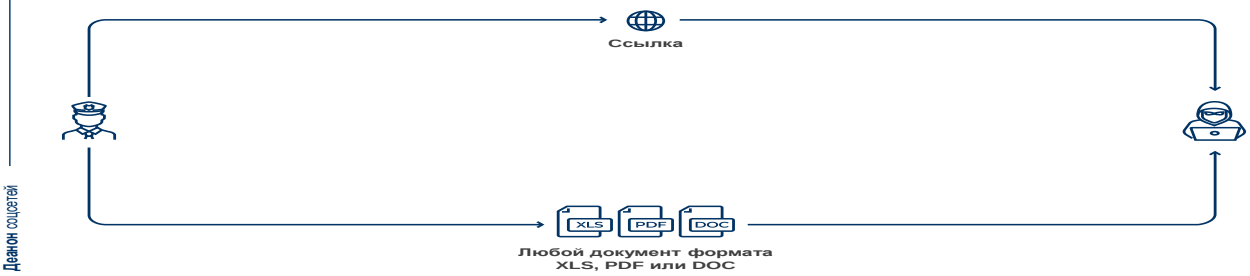


Деанон соцсетей

Способ №6

Phishing

Отправка ссылки или документа для перехвата IP-адреса

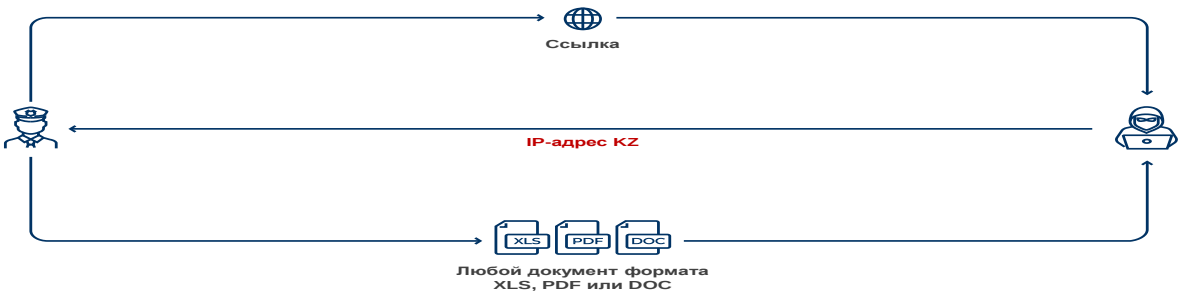


Деанон соцсетей

Способ №6

Phishing

Отправка ссылки или документа для перехвата IP-адреса



Деанон соцсетей

Способ №6

Phishing

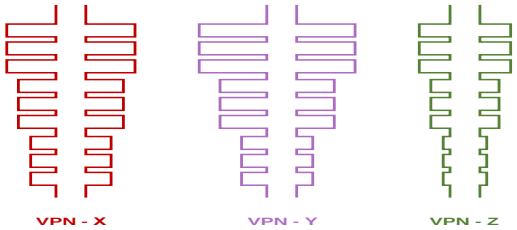
Отправка ссылки или документа для перехвата IP-адреса

Деанон соцсетей

Способ №6

Phishing

Отправка ссылки или документа для перехвата IP-адреса



- Разные VPN по разному реагируют на отправляемые пакеты, но паттерн всегда сохраняется. Всего +- 80 видов VPN, наиболее популярных 10.
- Ведутся работы по фиксации закономерности каждого вида VPN.
- Всего 250 тысяч абонентов используют VPN. Результаты проводимых исследований в разы повысят точность идентификации анонимного аккаунта.

Деанон соцсетей

5 социальных сетей охвачены

Telegram TikTok Instagram Facebook Youtube

Деанон соцсетей

Наша миссия

СОЗДАНИЕ ТЕХНОЛОГИЧЕСКИХ РЕШЕНИЙ, ОБЕСПЕЧИВАЮЩИХ БЕЗОПАСНОСТЬ ЛЮДЕЙ И СПРАВЕДЛИВОСТЬ В ОБЩЕСТВЕ

ЖУБАНДЫКОВ АЙДАР АРГЫНГАЗИЕВИЧ
Аккаунт менеджер по работе с корпоротивными клиентами
ПЕРОВ ВИТАЛИЙ ВИТАЛЬЕВИЧ
Эксперт по кибербезопасности, кибербразведке и Центра анализа и расследования кибератак

ЦИФРОВАЯ ЛАБОРАТОРИЯ, ОПЫТ ГРУЗИИ, КЫРГЫЗСТАНА

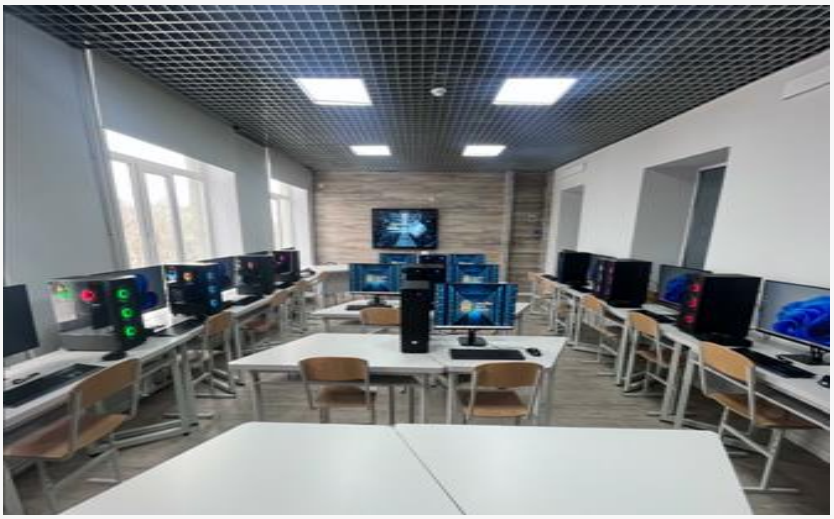
Тема доклада - это наша практика которой мы поделелились с Центрально Азиатскими странами и вы знаете что ЦАРКА сейчас очень усиленно в последние годы взаимдействует и пытается развивать также тематику информбезопасности в области защиты и поиски индификации преступников и взаимдейсвие с ними в Центральных Азиатских странах.

Так вот, один из таких проектов где я участвую ка руководитель и эксперт находится в Кыргызстане при Минюсте это цифровая лаборатория, ведем непосредственно взаимодействие с МВД, с прокураторуй и Минюстиции Кыргызстана. С прошлого года мы провели обучение в Академиях где внедрили систему постоянного по цифровой криминалситике, разработали программы, проводили усиленные тренингы который был ориентирован на специалистов в области цифровой криминалистике, также большей части для оперативных действий по изъятий цифровых доказательств и в том числе для цифровой лаборатории в котором собственно и заключалось цифровая деятельность следователям передаяи цифровых доказательстви и ответов в вопросах следователям. Сейчас данная стадия подходит к завершению, тоесть мы занимаемся поставкой обарудованием, так как мы выбираем обарудование и проводили и сопровождали, практический около года находясь в Кыргызстане в области ментринга.

KAZDREAM GROUP

КАРАГАНДИНСКАЯ АКАДЕМИЯ МВД РК ИМ Б. БЕЙСЕНОВА

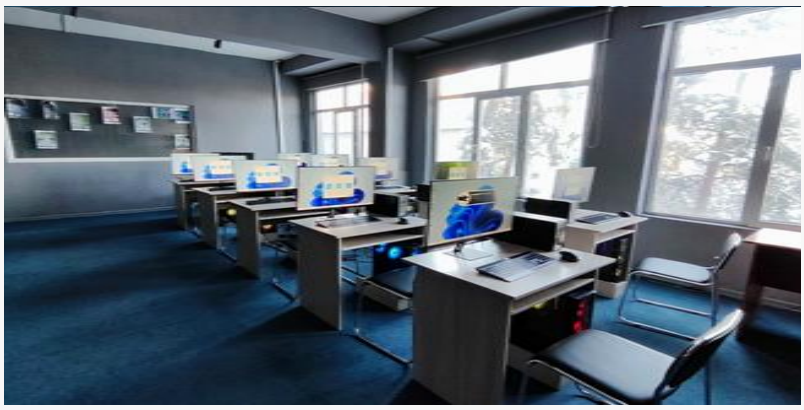
iRPLAB



KAZDREAM GROUP

АЛМАТИНСКАЯ АКАДЕМИЯ МВД РК ИМ М. ЕСБУЛАТОВА

iRPLAB



Криминалистика мобильных устройств

Cellebrite UFED

01
UFED 4PC
PHYSICAL ANALYZER

MKO

MKO Systems 02
Мобильный криминалист Эксперт плюс

GMDSOFT

GMDSOFT 03
MD-NEXT
MD-RED

MAGNET FORENSICS®

MAGNET FORENSICS 04
MAGNET GrayKey
Magnet Axiom

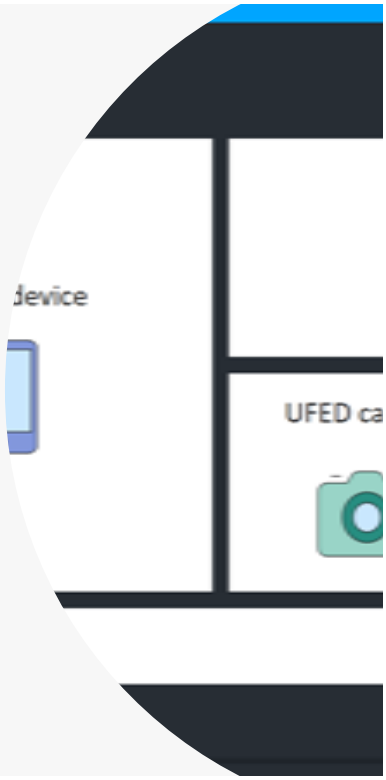
MSAB

MSAB 05
XRY
XRY Pro

МОБИЛЬНАЯ КРИМИНАЛИСТИКА

Cellebrite
UFED
Physical Analyzer

- Извлечение данных с мобильных устройств и дронов
- Работа с microSD картами
- Полное извлечение файловой системы Android
- Восстановление удаленных данных
- Анализ извлеченных данных
- Восстановление удаленных данных
- Исследование на уровне файловой системы
- Поиск по ключевым словам
- Создание детальных отчетов



МОБИЛЬНАЯ КРИМИНАЛИСТИКА

МКО Системы
МК Эксперт Плюс

- Извлечение и анализ данных
- Восстановление удаленных данных
- Обход парольной защиты
- Анализ на физическом и логическом уровнях

МОБИЛЬНАЯ КРИМИНАЛИСТИКА

GMD SOFT
MD-NEXT
MD-RED
MD-PLUG

- Извлечение данных с Android и iOS устройств
- Специализированный адаптер для получения прав
- Эффективная работа с устройствами корейских и китайских производителей
- Анализ данных мобильных устройств
- Расшифровка и восстановление
- Расширенная фильтрация
- Визуализация данных

МОБИЛЬНАЯ КРИМИНАЛИСТИКА

MAGNET FORENSICS
MAGNET GreyKey
MAGNET Axiom

- Мобильные устройства, компьютеры, облачные данные и автомобильные системы в одном деле
- Интеграция с Magnet Graykey
- Искусственный интеллект
- Использование токенов и связок ключей для доступа к зашифрованным данным
- Совместная работа

МОБИЛЬНАЯ КРИМИНАЛИСТИКА

ELCOMSOFT
DESKTOP, MOBILE & CLOUD FORENSICS

- Научные разработки
- Доступ к защищённым данным за минимальное время
- Мгновенное восстановление доступа
- Инструментарий для мобильной криминалистики
- Оптимальное соотношение цена-качество
- Условия лицензирования

КОМПЬЮТЕРНАЯ КРИМИНАЛИСТИКА

BelkaSoft Evidence Center X

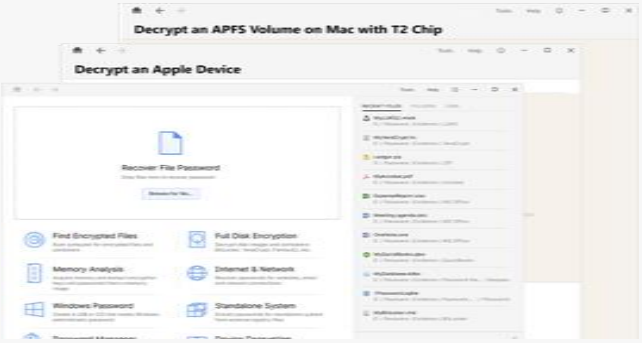
- Универсальное решение для анализа цифровых устройств
- Поддержка всех популярных ОС
- Извлечение данных из мессенджеров и соцсетей
- Анализ метаданных
- Восстановление зашифрованных файлов

КОМПЬЮТЕРНАЯ КРИМИНАЛИСТИКА

ACE Lab PC-3000 Portable

- Восстановление данных с поврежденных накопителей
- Поддержка SATA/PATA/USB
- Работа с SSD и RAID массивами
- Лидер в восстановлении поврежденных устройств

КОМПЬЮТЕРНАЯ КРИМИНАЛИСТИКА



Passware Kit Ultimate

- Восстановление паролей
- Анализ зашифрованных данных
- Поддержка множества форматов (ZIP, PDF, Office)
- Работа с криптоконтейнерами
- Доступ к облачным сервисам

КРИМИНАЛИСТИКА ВИДЕО

GMD SOFT

MD-VIDEO

- Искусственный интеллект для анализа видео
- Автоматическое распознавание объектов
- Реконструкция недостающих фрагментов
- Улучшение качества видео
- Оптимизация процесса анализа

КРИМИНАЛИСТИКА ВИДЕО

MAGNET

Witness

- Работа с видеорегистраторами
- Восстановление удаленных записей
- Извлечение метаданных
- Поддержка различных форматов
- Анализ хронологии событий

Передовые решения

Cellebrite Inseyets

Самые передовые технологии и методы.
Высочайшая скорость работы и достоверность полученных даных

		Входит
1 В 5 раз больше устройств поддерживается чем в UFED	2 Разблокировка устройств через Premium	3 Inseyets.UFED
На 60% больше информации извлекается с устройств		Inseyets.PA
В 2 раза быстрее получение общей картины чем в UFED		Inseyets.CLOUD
Add an insight		Premium

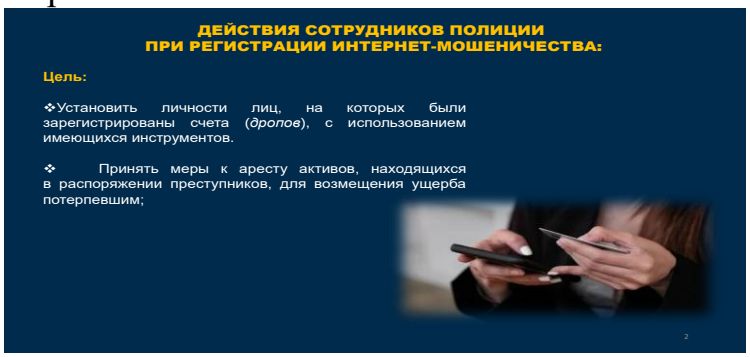
MAGNET GRAYKEY™

- Ускоренный брутфорс доступа к iOS и Android устройствам
- Доступ и извлечение данных независимо от состояния устройства
- Доступ к хранилищам учетных данных (Keychain и Keystore)
- Извлечение данных по категориям
- Извлечение данных на месте в отделе
- Интеграция с существующими криминалистическими инструментами

ЖАНДОС СУЙНБАЙ
начальник Департамента противодействия киберпреступлений

МЕТОДИКА РАСКРЫТИЯ ИНТЕРНЕТ-МОШЕННИЧЕСТВ С УЧЕТОМ НОВЫХ СПОСОБОВ ИХ СОВЕРШЕНИЯ

Сейчас большинство преступлений переходят в цифровую среду. Для реализации своих целей преступники все чаще используют весь потенциал интернет-технологий, социальных сетей, а также различных электронных платежных систем и криптовалюты.



На сегодняшний день в Казахстане, впрочем, как и во всем мире, самым распространенным и актуальным видом киберпреступлений являются интернет-мошенничества .

Хотелось бы отметить, что для эффективного раскрытия и расследования таких преступлений необходимо тесное взаимодействие следственных подразделений с оперативными службами, а также учитывать ряд особенностей, присущих именно интернет-мошенничествам.

Так, самая большая регистрация приходится на:

-Размещение онлайн объявлений. Мошенники размещают на сайтах либо в социальных сетях заведомо ложные объявления о продаже товаров, либо оказании услуг по заниженной цене;

-Распространены мошенничества, совершенные под предлогом выгодных вложений денег в различные инвестиционные проекты, раскрутки денег в "Ватсап" и "Телеграмм" группах, а также ставок на спортивные события и т.д.

-Особую тревогу сейчас вызывают мошенничества, совершаемые путем обзвона граждан от имени сотрудников специальных и правоохранительных органов, финрегуляторов и банков второго уровня.

Здесь мошенники используют различные уловки для убеждения граждан. Это могут быть звонки от сотрудников банков и правоохранительных органов:

-о якобы оформляемом мошенникам кредите;

-проведении полицией спецоперации по поимке мошенников;

-подозрении на перевод денег для финансирования террористических групп и т.д.

Во всех случаях опустошаются депозиты, оформляются кредиты, а в некоторых случаях продается имущество.

САМАЯ БОЛЬШАЯ РЕГИСТРАЦИЯ ПРИХОДИТСЯ НА СЛЕДУЮЩИЕ ВИДЫ МОШЕННИЧЕСТВА:

- РАЗМЕЩЕНИЕ ОНЛАЙН ОБЪЯВЛЕНИЙ

- «ВЫГОДНОЕ» ВЛОЖЕНИЕ ДЕНЕГ

- ОБЗВОН ГРАЖДАН ОТ ИМЕНИ СОТРУДНИКОВ СПЕЦИАЛЬНЫХ И ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ, ФИНРЕГУЛЯТОРОВ И БАНКОВ ВТОРОГО УРОВНЯ

ЗАЧАСТУЮ ЗВОНКИ ОСУЩЕСТВЛЯЮТ ПО СЛЕДУЮЩИМ ТЕМАМ:

- о якобы оформляемом мошенниками кредите;
- проведении полицией спецоперации по поимке мошенников;
- подозрении на перевод денег для финансирования террористических групп и т.д.

Практически все интернет-мошенничества, связанные с оформлением на доверчивых граждан онлайн-кредитов и займов, а также хищением их банковских накоплений, совершаются преступниками из-за рубежа

В некоторых случаях мошенники просили граждан установить на мобильные устройства программы, обеспечивающие доступ ко всем приложениям, соответственно к банковским счетам и депозитам

ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПНОСТИ

Совместно с Нацбанком запустили работу **«Антифрод-центра»** для оперативного реагирования на мошеннические операции.

По состоянию на 1 января т.г. на платформе создано **15184 инцидентов**, из них **5214** созданы банками второго уровня *(далее –– БВУ)* и **9970** – правоохранительными органами

ANTIFRAUD

Благодаря электронной платформе «Антифрод-центра» имеется возможность установить маршрут движения денежных средств и конечного получателя, в т.ч. лиц, производивших обмен денежных средств и их обналичивание *(номер конечного счета или криптокошелька)*. Блокировать их передвижение. Зафиксировать данные об участниках финансовой «цепочки».

Основная задача функционала системы "Антифорд" - блокирование подозрительных транзакций *(предупреждение мошеннических действий)* и незамедлительное уведомление как клиентов, так и полиции.

В связи с чем, в ходе опроса потерпевшего установлению подлежит следующая информация:

-Кто звонил? Как представился? Какой номер телефона был использован?

-Были ли переданы данные банковские карты (номер, CVV - код, срок действия)?

-Выполнял ли потерпевший переводы? Если да, то уточните реквизиты счетов.

-Получал ли потерпевший коды из СМС и передавал их?

ДЛЯ ИСПОЛЬЗОВАНИЯ АНТИФРОД-ЦЕНТРА В ПОЛНОЙ МЕРЕ ПО ВСЕМ ФАКТАМ ИНТЕРНЕТ-МОШЕНИЧЕСТВ, НЕОБХОДИМО:

- С использованием учетной записи создать инцидент в интернет-платформе «Антифрод-центр» согласно установленного алгоритма.

На основании созданного обращения *(инцидента)*, при наличии денежных средств на счете, принять меры к их блокированию.

- Если использовались электронные кошельки, запросите информацию о зарегистрированных пользователях.

7

ДЕЙСТВИЯ СОТРУДНИКОВ ПОЛИЦИИ ПРИ РЕГИСТРАЦИИ ИНТЕРНЕТ-МОШЕНИЧЕСТВА:

❖Идентифицировать и отследить номера, использованные в мошеннической схеме.

❖Если звонок совершён с подменой номера, запросить данные о маршрутизации вызова.

❖Для этого необходимо направить запрос в АО «Қазақтелеком» или другие юридические лица, оказывающие услуги телекоммуникаций.

❖Отследить, с каких устройств и из каких локаций совершались звонки или фишинговые действия.

❖Запросить у провайдера информацию о подключениях в момент совершения действий. Для этого необходима информация полученная при опросе потерпевшего *(дата, время, устройство с которого производилось соединение)*.

8

ДЕЙСТВИЯ СОТРУДНИКОВ ПОЛИЦИИ ПРИ РЕГИСТРАЦИИ ИНТЕРНЕТ-МОШЕНИЧЕСТВА:

❖ Выявить IP-адреса при наличии связи с преступником *(путем переписки или совершения звонка)*.

В распоряжении территориальных имеются автоматизированные программные комплексы, такие как:
- ➢Iris;
- ➢Blure;
- ➢Argus;
- ➢Cross 2.0;
- ➢Foxy;
- ➢Altair Analytics;
- ➢Sniff;

9

ДЕЙСТВИЯ СОТРУДНИКОВ ПОЛИЦИИ ПРИ РЕГИСТРАЦИИ ИНТЕРНЕТ-МОШЕНИЧЕСТВА:

❖ Провести финансовый анализ, который позволит определить, на какой стадии были обналичены деньги, в том числе с использованием виртуальных активов.

❖ Только по результатам финансового анализа возможно установление конечного получателя.

❖ Необходимо направить санкционированный запрос в банк для получения информации о владельце счета, с которого были сняты деньги.

❖ При использовании криптовалютной биржи «**Binance**» направить запрос через платформу «Kodex».

10

ДЕЙСТВИЯ СОТРУДНИКОВ ПОЛИЦИИ ПРИ РЕГИСТРАЦИИ ИНТЕРНЕТ-МОШЕНИЧЕСТВА:

❖Если преступление совершено из-за рубежа и его следы находятся за пределами страны, необходимо принять меры по направлению международного следственного поручения для производства следственных действий на территории другой страны.

❖В целях недопущения повторного обращения потерпевших по фактам мошенничества, прошу Вас обратить внимание на профилактическую работу с потерпевшими.

❖Так, под предлогом возврата похищенных денежных средств, потерпевшие могут быть склонены к совершению иных противоправных действий (*поджоги, уничтожение имущества и т.п.*).

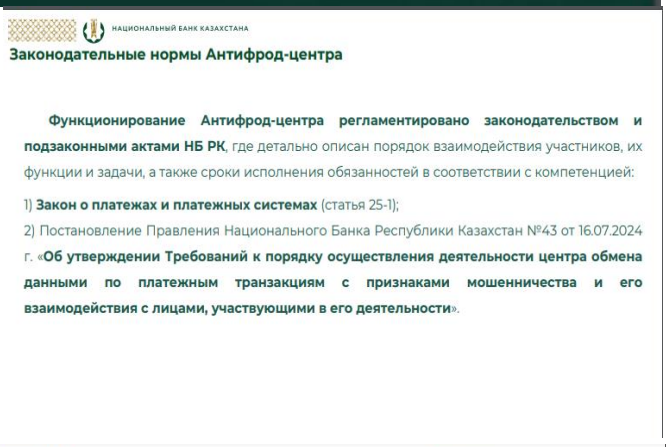
11

Уважаемые коллеги, борьба с киберпреступностью требуют слаженной совместной работы, только при объединении усилий возможно достижение положительных результатов.

ИЗМАЙЛОВА АЙНУРА ЖУМАБЕКОВНА

Руководитель Антифрод-Центра Национального банка РК

О РАБОТЕ АНТИФРОД-ЦЕНТРА



НАЦИОНАЛЬНЫЙ БАНК КАЗАХСТАНА

Основные атрибуты Антифрод-центра

Портал Антифрод-центра

1. **площадка взаимодействия** между финансовыми организациями и органами уголовного преследования;

Для обеспечения деятельности антифрод-центра, формируются следующие **базы данных**:

1. **о событиях** осуществления платежной транзакции с признаками мошенничества, подтвержденных органами уголовного преследования (далее - **база о событиях**);
2. **о попытках** осуществления платежной транзакции с признаками мошенничества (далее – **база о попытках**);

→ Базы данных хранят в себе **список транзакций** с мошенническими признаками

Дополнительно формируются **списки**:

1. о контрагентах, подтвержденных органами уголовного преследования в участии в платежной транзакции с признаками мошенничества;
2. о контрагентах, подозреваемых в участии в платежной транзакции с признаками мошенничества.

→ Списки привязаны **к конкретному контрагенту** осуществлявшему мошеннические транзакции

НАЦИОНАЛЬНЫЙ БАНК КАЗАХСТАНА

В рамках создания инцидентов, имеются 4 основания для создания инцидента в Антифрод-центре:

Инцидент

Заявление клиента
В случае, если **клиент самостоятельно обратился** с организацию с событием или попыткой совершения мошенником инцидента

В соответствии с внутренними документами Финансовой организации
В случае, если **финансовая организация на своем уровне установила попытку осуществления мошеннической операции** и в соответствии с внутренними документами имеются такие основания

От органа уголовного преследования
В случае, если имеется подтвержденная информация от органа уголовного преследования, **орган уголовного преследования заводит инцидент в системе**

Если имеется совпадение со списками Антифрод-центра
В случае, если **контрагент находится в базе данных о событиях и попытках и списках** осуществления платежной транзакции с признаками мошенничества

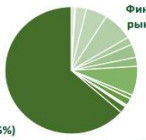
НАЦИОНАЛЬНЫЙ БАНК КАЗАХСТАНА

БИЗНЕС-ПРОЦЕСС ВЗАИМОДЕЙСТВИЯ УЧАСТНИКОВ В РАМКАХ ЗАВЕДЕНИЯ И РАССЛЕДОВАНИЯ ИНЦИДЕНТА

НАЦИОНАЛЬНЫЙ БАНК КАЗАХСТАНА

Первые результаты Антифрод-центра

Всего – 19 927 инцидентов



155 участников Антифрод-центра

~ 987 млн Своевременно заблокировано (на уровне Банка отправителя)

~ 312 млн Своевременно заблокировано (на уровне Банка получателя)

~ 83 млн Возвращено добровольно

Топ-3 вида мошенничества

Ложный звонок от КНБ, полиции, НБ, сотовых операторов

Мошенничество в **социальных сетях и мессенджерах**

Лжеинвестирование денежных средств *(брокеры, инвестиционные компании, финансовые пирамиды)*

5 *По состоянию на 09.01.2025*

НАЦИОНАЛЬНЫЙ БАНК КАЗАХСТАНА

Развитие Антифрод-центра в 2025 году

01 Усовершенствование законодательной базы (оперативный возврат средств, работа с дропперами)

02 Интеграция с базами данных иных операторов Антифрод-центра

03 Выявление новых паттернов мошенничества на базе искусственного интеллекта

04 Построение аналитической и статистической отчетности

ТАЖМАГАНБЕТОВ ОМИРСЕРИК САЙЛАУБАЕВИЧ
руководитель 1-госледственного управления
Следственного департамента АФМ
полковник СЭР

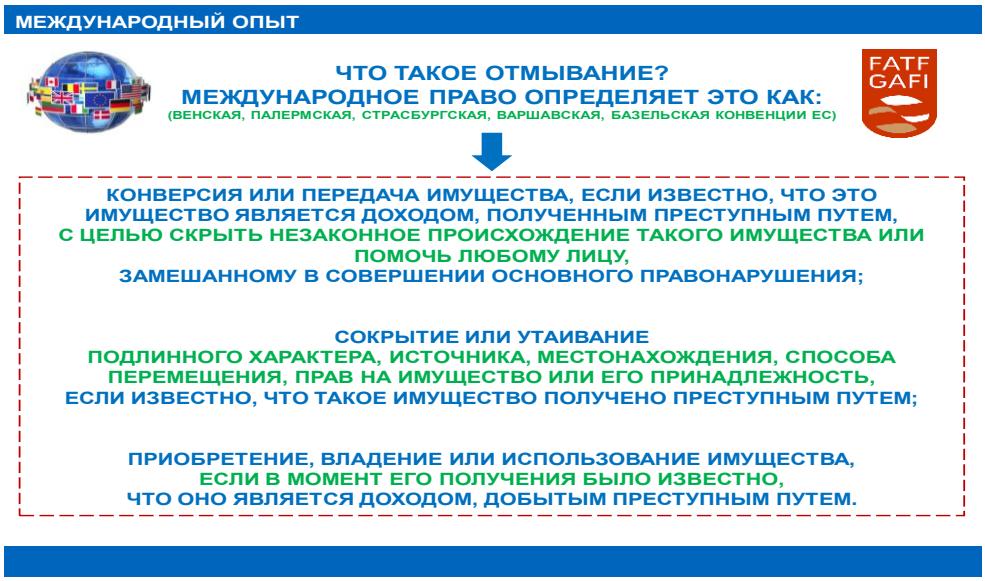
О ТАКТИКЕ РАСКРЫТИЯ И РАССЛЕДОВАНИЯ КИБЕРПРЕСТУПЛЕНИЙ

(Об основных схемах отмывания преступных доходов)

Слайд № 1

Легализация преступных доходов представляет собой сложный процесс, включающий множество разнообразных элементов. Знание процесса отмывания необходимо для правильной квалификации и отражение всех признаков легализации в обвинительном акте.

Слайд № 2



Международное законодательство(Венская, Страсбургская, Палермская, Варшавская, Базельская конвенции ЕС, Конвенция ООН против коррупции) определяет **отмывание** как:

❖ **конверсия** или **передача имущества**, если известно, что это имущество является доходом, полученным преступным путем, **с целью скрыть незаконное происхождение такого имущества или помочь любому лицу,** замешанному в совершении основного правонарушения;

❖ сокрытие или утаивание **подлинного характера, источника, местонахождения, способа перемещения, прав на имущество или его принадлежность,** если известно, что такое имущество получено преступным путем;

❖ приобретение, владение или использование имущества, **если в момент его получения было известно,** что оно является доходом, добытым преступным путем.

Слайд № 3

FATF сложный процесс легализации преступных доходов подразделяет на стадии **размещения**, **расслоения** и **интеграции**.

Если коротко, то:

РАЗМЕЩЕНИЕ – денежные средства, полученные преступным путем, вводятся в финансовую систему;

РАССЛОЕНИЕ – проведение финансовых операций для маскировки источников дохода или их сокрытия

ИНТЕГРАЦИЯ – конечный этап, когда отмытые деньги или имущество вводятся в легальный оборот.

При этом обязательными стадиями для квалификации деяний по ст.218 УК являются **расслоение** и **интеграция**.

Стадия размещения

На данной **стадии** преступные доходы, вводятся в финансовую систему путемразмещения на счетах в банке или других организациях (внесение денег на банковский счет, в том числе подконтрольных лиц и организаций, электронные кошельки, букмекерские конторы, казино и т.д.).

Преступные доходы могут вводиться в финансовую систему, в том числе и с привлечением третьих лиц.

Слайд № 5

Стадия размещения характерна для легализации доходов от теневого бизнеса, где преобладает «серая наличность».

Например, деньги от продажи наркотиков переводятся на KIWI-кошельки подставных лиц либо дропперов.

При сбыте фальшивых долларов и евро пополняются счета в игровом заведении (Лото клуб) и забирается выигрыш в тенге.

Таким образом, наркодоходы и фальшивые деньги поступили в финансовую систему. На этом этап размещения преступных доходов завершен.

Слайд №6

Этап размещения может **отсутствовать,** если денежные средства, полученные преступным путем, уже находятся в финансовой системе.

К примеру, по делам о хищениях, бюджетные деньги от заказчика после подписания фиктивных актов выполненных работ, **находясь в финансовой системе**, поступают на счет подрядчика.

Слайд №7

Стадия расслоения

Целью данной **стадии** является – оторвать незаконные денежные средства от источника происхождения и скрыть их от правоохранительных органов во избежание конфискации.

Основные механизмы расслоения включают:

- запутывание следов путем совершения множественных переводов между физическими, юридическими лицами и обналичивания (в т.ч. вывод за границу);

- смешивание преступных денег с легальными путем введения в финансовый оборот действующего бизнеса (финансовая помощь, приобретение ценных бумаг, ставки в казино);

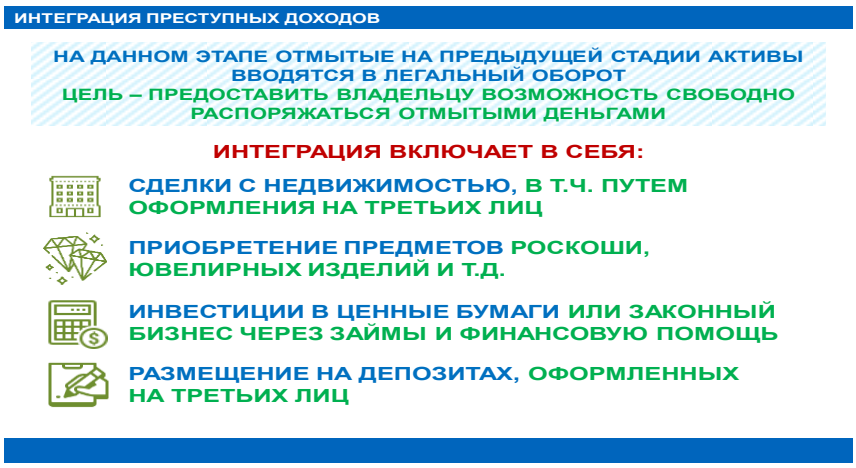
- вывод в крипто валюты (покупка цифровых активов и дальнейший перевод их в криптомиксеры).

Таким образом, в процессе расслоения совершается множество финансовых операций, усложняющих процесс доказывания их преступного происхождения и установления бенефициарных собственников.

Слайд № 8

На примере все тех же сбытов наркотиков и фальшивок, денежные средства, полученные преступным путем, размещались на счетах в игровых заведениях, где использовались на ставках с низким коэффициентом выигрыша для смешивания, обналичивания и сокрытия их преступного происхождения.

Слайд № 9



Стадия интеграции

На данной **стадии,** отмытые на предыдущем этапе, активы вводятся в легальный оборот для свободного распоряжения конечным бенефициаром.

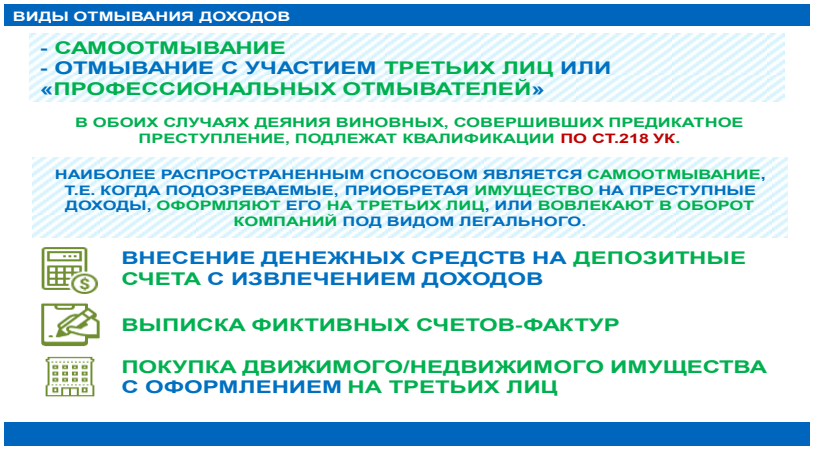
Интеграция заключается в совершении сделок с имуществом, полученным преступным путем, в т.ч. с оформлением на третьих лиц.

Если отмывание не выявлено на двух предыдущих этапах, доказать преступное происхождение имущества на стадии интеграции сложно.

Этапы расслоения и интеграции в совокупности образуют состав преступления, предусмотренный ст.218 УК.

При этом, каждый из этапов подлежит доказыванию в соответствии со ст.113 УПК.

Слайд № 10



С учетом практики и международного опыта на сегодняшний день в Казахстане мы выделяем два основных вида отмывания доходов:

-самоотмывание;

-отмывание **с участием третьих лиц** или **профессиональных отмывателей**.

В обоих случаях деяния виновных, совершивших предикатное преступление, подлежат квалификации по ст.218 УК.

Наиболее распространенным способом ОДу нас является самоотмывание, т.е. когда подозреваемые, приобретая имущество на преступные доходы, оформляют его на третьих лиц, или вовлекают в оборот компаний под видом легального.

Так, основные виды отмывания совершаются:

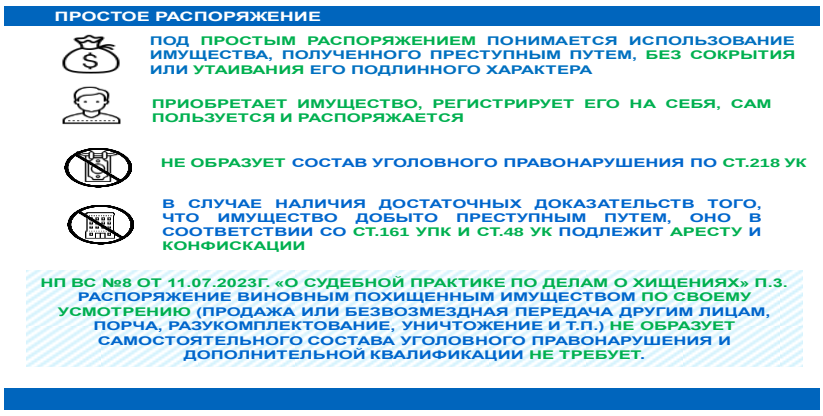
-путем внесения денежных средств на депозитные счета с извлечением доходов;

-путем **выписки фиктивных счетов-фактур**;

-путем покупки движимого/недвижимого имущества с оформлением на третьих лиц.

Особенностью нашей правоприменительной практики является то, что преступники не используют сложные и замысловатые схемы ОД, за редким исключением.

Слайд № 11



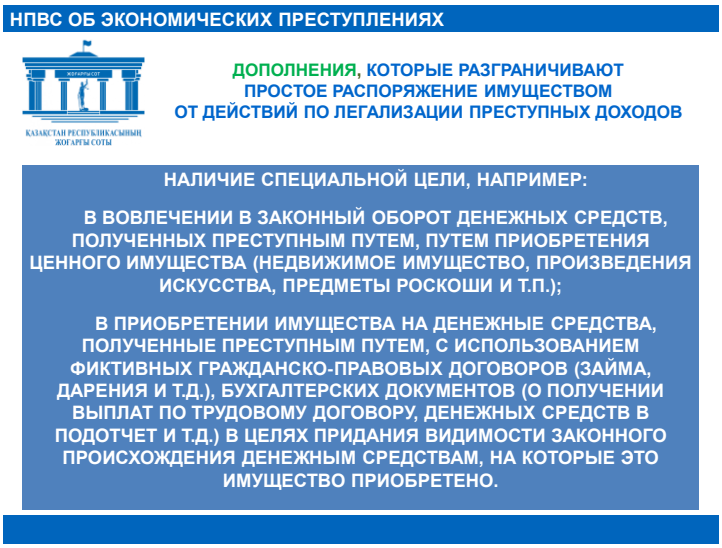
Важно разграничивать **самоотмывание** от **простого распоряжения** имуществом, полученного преступным путем.

Под простым распоряжением понимается использование имущества **без сокрытия** или **утаивания** его преступного происхождения или не предполагает придания ему законного вида.

НП ВС №8 от 11.07.2023г. «О судебной практике по делам о хищениях» п.3. **Распоряжение** виновным похищенным имуществом **по своему усмотрению** (продажа или безвозмездная передача другим лицам, порча, разукомплектование, уничтожение и т.п.) **не образует** самостоятельного состава уголовного правонарушения и дополнительной квалификации **не требует**.

Следовательно, если лицо, совершившее правонарушение, на преступные доходы приобретает имущество, регистрирует его на себя, сам пользуется и распоряжается (продажа, дарение и т.д.), то в данном случае будет иметь место **простое распоряжение** имуществом, что **не образует** состав по ст.218 УК.

Слайд № 12



По нашей инициативе Верховным судом внесены **дополнения** в Нормативное постановление «Об экономических преступлениях», которые разграничивают простое распоряжение имуществом от действий по легализации преступных доходов.

Теперь НПВС под легализацией подразумевает любое вовлечение в законный оборот денежных средств, полученных преступным путем, в т.ч. путем приобретения недвижимости, произведений искусства, предметов роскоши и т.д.

Слайд № 13

Дополнительно направили в суд **проект** отдельного нормативного постановления по делам о легализации, где определены этапы отмывания, виды соучастия и другие аспекты.

Слайд № 14

Профессиональный отмыватель – это лицо, не участвующее в предикатном преступлении, но оказывающее услуги по легализации имущества, добытого преступным путем, за вознаграждение.

Они могут действовать как индивидуально, так и в составе преступных групп.

Их роль заключается в вовлечении преступного имуществав законный оборот с использованием специальных познаний, организаций (фиктивно созданные юр.лица) и инфраструктуры (офис, оргтехника, ИС, специалисты и т.д.).

Деяния проф.отмывателей, наряду с лицом, которому они оказывают свои услуги, подлежат квалификации по ст.218 УК, поскольку они в силу специальных познаний осознают последствия своих действий.

Их цель – скрыть источник, местонахождение, принадлежность имущества и конечного бенефициара.

Слайд № 15

Например, проф.отмыватель Ахметова для осуществления деятельности по ОД –имеет:

-высшее экономическое образование;

-специальные познания в области бухгалтерского учета и налоговой отчетности;

-опыт совершения банковских операций;

-офис, оргтехнику, ИС 1С-Бухгалтерия;

-штат бухгалтеров для сопровождения документов, денежных переводов, налоговых отчетов и тд.;

-предприятия, зарегистрированные на подконтрольных ей лиц.

Аманов с целью отмывания преступных доходов, похищенных путем мошенничества с целью сокрытия следов хищения, привлек проф.отмывателя Ахметову, которая за вознаграждение, используя подконтрольные предприятия обналичила их и передала Аманову.

В итоге Аманов при пособничестве Ахметовой разорвал связь между похищенными средствами и их источником происхождения, легализовав денежные средства, добытые преступным путем, и интегрировал их в имущество стоимостью свыше **1 млрд** тенге.

В таких случаях действия проф. отмывателя подлежат квалификации как соучастие в ОД.

Слайд № 16

Основные причины **оправдательных приговоров** по *ст.218 УК РК:*

1) **отсутствие доказательной базы, подтверждающей этапы** расслоения и интеграции преступных доходов. Подробное описание указанных этапов, позволит разграничить простое распоряжение преступно нажитым имуществом от отмывания.

2) в процессуальных документах **не отражены этапы, характеризующие процесс отмывания:**

Расслоение: каким образом осуществлялось сокрытие следов, маскировались финансовые транзакции, привлекались подставные лица или профессиональные отмыватели?

Интеграция: как производился ввод преступных денег в легальный оборот, при каких обстоятельствах совершены сделки с имуществом, знали ли лица об источниках доходов?

Доказательства преступного характера происхождения имущества станут основанием для его конфискации.

Слайд № 17

Необходимо отметить, что в выявлении схем ОД **ключевым** фактором является принцип **«следуй за деньгами»**, а именно проведение кропотливого анализа поступающих денежных средств на счета и распоряжение ими.

Это позволит раскрыть этапы и доказать факт отмывания.

В процессуальных документах **необходимо**:

❖ четкое поэтапное описание стадий отмывания доходов;

❖ роль каждого – отлица, совершившего предикатное преступление, до действий профессиональных отмывателей или третьих лиц (в случаях, если они привлекались).

Сбор доказательств должен осуществляться **поэтапно** (размещение, расслоение, интеграция).

Важно помнить, что только в случае наличия **достаточных доказательств** того, что имущество **добыто преступным путем**, оно в соответствии со ст.161 УПК и ст.48 УК подлежит **аресту** и **конфискации**.

Основные способы доказывания преступного происхождения имущества изложены в Методике ПФР и учебном курсе по его проведению.

Остановлюсь на практике, которая наработана **ДЭР по ВКО,** где путем анализа банковского счёта установлены факты регулярного поступления по 150 и 180 тыс. тенге супруге подозреваемого от сдачи в аренду двух квартир, оформленных на третьих лиц.

В другом случае ими установлена квартира подозреваемого, оформленная на третьих лиц, путем запроса в маркет – плейс «Крыша» о подаче объявления с номеров телефонов и адресов электронной почты фигурантов и их доверенных лиц.

Подобные положительные примеры **масштабируем** по принципу «1-10» и допоняем существующую методику ПФР и учебные материалы.

Мазмұны