УДК 343.9

Темиржанова Л.А.
Главный научный сотрудник Центра по исследованию проблем в сфере защиты общественных интересов Межведомственного научно-исследовательского института Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан
к.ю.н., советник юстиции

Абулгазина А.Ж.
Старший прокурор Управления учебно-методического обеспечения Института послевузовского образования и повышения профессионального уровня Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан советник юстиции

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРАВООХРАНИТЕЛЬНЫХ СТРУКТУР И ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПЛЕНИЯМ, КИБЕРХИЩЕНИЯМ (НАЦИОНАЛЬНЫЙ И ЗАРУБЕЖНЫЙ ОПЫТ)

Использование IT-технологий во всех сферах жизнедеятельности граждан, организаций связано напрямую с вопросами повышения уровня кибербезопасности серверов всех государственных и правоохранительных структур, а также непрерывном его совершенствовании.

В этой связи взлом электронных систем любого учреждения обоснованно вызывает вопросы и тревогу по поводу эффективности усилий органов, отвечающих за обеспечение кибербезопасности государства.

Справочно: Казахстан в 2017 году занял 83 место среди 165 стран в Глобальном индексе кибербезопасности (ГИК), составленном международным союзом электросвязи. ГИК демонстрирует, на каком уровне находится способность государства противодействовать кибератакам. Россия заняла второе место среди стран СНГ – первое в рамках региона заняла Грузия [1].

Концепцией «Киберщит» на данном этапе только предусматривается создание Национального оперативного органа нацеленного на обработку данных о состоянии защищенности наиболее важных компонентов национальной информационной инфраструктуры [2].

В МВД имеется управление «К» подразделение по борьбе с высокотехнологичной преступностью. КНБ РК также создал специальный отдел для этих целей: группу по борьбе с компьютерной преступностью.

Справочно: С 2011 года в РК существует KZ-CERT (Служба реагирования на компьютерные инциденты) при Министерстве связи и информатизации. KZ-CERT сотрудничает с коллегами из России, Армении и Индии. Целью CERT является выявление атак на объекты информационные инфраструктуры, обеспечение взаимодействия между экспертами и разработка технических рекомендаций и законодательства по борьбе с киберпреступностью [3].

Соответственно, уже сейчас назрела объективная необходимость совместной и слаженной работы правоохранительных органов по противодействию киберугрозам.

Считаем абсолютно верной точку зрения А.В. Турлаева и А.Б. Шәкіровой о том, что «актуальность проблемы обеспечения информационной безопасности обусловлена, прежде всего, тем, что в современном мире информация стала стратегическим национальным ресурсом» [4].

«В Республике Казахстан за период с 2010 по 2016 год плотность пользователей Интернета увеличилась с 36,1% до 75%, а количество пользователей мобильного Интернета

с 3 миллионов 694 тысяч практически утроилось и достигло 10 миллионов 567 тысяч. Такое увеличение числа пользователей Интернета повышает критичность и делает более ощутимыми последствия в случае отказов или вредоносного воздействия на технические средства» [2].

Согласно Концепции, в нашей стране на ежедневной основе фиксируется и отражается более 180 миллионов атак различного уровня воздействия на электронные информационные ресурсы государственных органов. И это только на электронные информационные ресурсы государственных органов!

Таким образом, возникает проблема, так как контроль динамики киберпреступности и ее распространения зависят не только от органов власти, но и от культуры кибербезопасности каждого пользователя.

При этом отдельные сферы национальной безопасности, такие как оборона, финансирование и банковская деятельность, информационные сети государственных органов требуют повышенных мер по обеспечению их информационной безопасности ввиду важности исполняемых ими задач.

Накопление информации на компьютерах и иных цифровых носителях схоже с накоплением денег на банковских счетах и требует высокоэффективных мер по их сбережению. Вред в масштабах государства от нарушения целостности информационных систем, особенно стратегически значимых, может оказаться катастрофическим.

Основные проблемы в информационной системе:

- безграничность Интернета и несовершенство нормативно-правовой базы в исследуемой сфере;
- невозможность идентификации преступника;
- недостаточный уровень подготовки сотрудников органов, осуществляющих противодействие этим явлениям, в части специальных знаний в сфере информатизации и применения компьютерных технологий;
- некачественные услуги, а также слабые знания IT-выпускников ВУЗов;
- недооценка важности противодействия информационным угрозам;
- низкий уровень оплаты услуг IT-специалистов в государственных органах.

В соответствии с уголовным законодательством киберпреступления отнесены к главе 7 «Уголовные правонарушения в сфере информатизации и связи» УК РК. Кроме того, в главе 6 «Уголовные правонарушения против собственности» УК РК указаны деяния, предусмотренные ст.190 ч.2 п.4 УК РК, а именно «мошенничество, то есть хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием», совершенное «путем обмана или злоупотребления доверием пользователя информационной системы» и ст.188 ч.2 п.4 УК РК – «кража, то есть тайное хищение чужого имущества, совершенное «путем незаконного доступа в информационную систему либо изменения информации, передаваемой по сетям телекоммуникаций» [5].

При этом, в ряде статей кодекса *(147 – «Нарушение неприкосновенности частной жизни и законодательства Республики Казахстан о персональных данных и их защите»; 148 – «Незаконное нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений»; 159 – «Незаконное ограничение права на доступ к информационным ресурсам»; 161 – «Пропаганда или публичные призывы к развязыванию агрессивной войны»; 174 – «Возбуждение социальной, национальной, родовой, расовой, сословной или религиозной розни»; 179 - «Пропаганда или публичные призывы к захвату или удержанию власти, а равно захват или удержание власти либо насильственное изменение конституционного строя Республики Казахстан»; 180 - «Сепаратистская деятельность»; 188 – «Кража»; 190 – «Мошенничество»; 256 - «Пропаганда терроризма или публичные призывы к совершению акта терроризма и другие»*) также содержатся квалифицирующие признаки, где высокие технологии выступают в роли объекта, орудия преступления или способа совершения незаконного деяния.

Наиболее опасными видами угроз, отмечаемых специалистами, являются сети ботов; атаки на правительственные сайты, частные предприятия, и конечных пользователей; финансовое мошенничество, потерпевшими от которого являются банки, частные предприятия и их клиенты; мошенничество с личными данными людей.

Всецело разделяем точку зрения д.ю.н. Н.А. Биекенова о том, что «государственные органы и электронное правительство пользуются иностранными антивирусными продуктами,

что также не способствует обеспечению безопасности. Кроме того, следует разрабатывать собственные криптографические программы» [6].

Согласно статистическим данным количество кибермошенничеств в прошлом году возросло в 23 раза *(с 45 в 2015 году до 1047 в 2016 году)*, по итогам 9 месяцев т.г. уже зарегистрировано 1,5 тыс. таких преступлений [7].

На сегодня судом рассмотрено всего 3% или 83 уголовных дела *(2015 год – 6, 2016 год – 3, 9 мес. т.г. – 74)*. Из-за неустановления виновного лица прерваны сроки по 1800 кибермошенничествам *(2015 год – 24, 2016 год – 876, 9 мес. т.г. – 900)*.

Проведенный анализ показал о недостаточной практике расследования дел данной категории. Так, за 2,5 года (с 2015-2016 гг. и 6 месяцев 2017 г.) было прекращено производство по 274 уголовным делам, возбужденным по ст.ст.205-208 и 210 УК РК. Из них, более 90% прекращаются на основании п.1 и 2 ч.1 ст.35 УПК РК.

Справочно: К примеру, приговором районного суда № 2 Бостандыкского района города Алматы от 24 января 2017 года осуждено 20 человек за совершение более 40 эпизодов преступлений, хищений по совокупности статей, в том числе за кражу с использованием информационных технологий (осуждены к различным срокам наказаний – лишение свободы, либо условное). О., работающий системным администратором на предприятии, имеющий большой опыт работы в сфере информационных технологий, и Д., имеющий опыт работы в сфере информационных технологий и бухгалтерского учета, онлайн-платежей, находясь в городе Алматы, создали устойчивую организованную группу, в состав которой вовлекли 20 человек, распределили роли, открыли счета на себя и на подставных физических и юридических лиц в банках второго уровня и совершили ряд преступлений. Этих людей О. и Д. посвятили в свои преступные планы и при этом раскрыли механизм совершения хищения денежных средств со счетов юридических и физических лиц, основным способом, которого являлось создание, использование и распространение вредоносных программных продуктов. Путем умышленного неправомерного доступа и неправомерного завладения охраняемой законом информацией, содержащейся на электронных носителях, согласно распределенным им ролям, они осуществляли открытие счетов на себя и на подставных физических и юридических лиц в банках второго уровня. Далее, после незаконных перечислений денежных средств на расчетные счета физических и юридических лиц, открытых пособниками и участниками организованной преступной группы, организовывали последующее снятие незаконно перечисленных денежных средств с указанных счетов и в дальнейшем распределяли их между участниками преступной группы.

Большинство киберхищений остается вне поля зрения правоохранительных органов Республики Казахстан.

Одной из причин сложившейся ситуации является недостаточный уровень подготовки сотрудников органов, осуществляющих противодействие этим явлениям, в части специальных познаний в сфере информатизации и применения компьютерных технологий.

Общий обзор зарегистрированных преступлений с использованием IT-технологий показал рост за 5 лет более чем в 22 раза *(с 2012 по 2017 годы)* [7].

Так, согласно статистическим данным за 6 месяцев т.г. зарегистрировано 1013 киберпреступления *(за 2012 г. - 54, за 2013 г. - 75, за 2014 г. - 95, за 2015 г. - 357, 2016 г. - 1234)*, из них в разрезе статей УК РК [8].

- по ст.205 УК (неправомерный доступ к информации, в информационную систему или информационно-коммуникационную сеть - нарушение конфиденциальности информации) – 26 (в 2015 г. - 50, 2016 г. - 44);

- по ст.206 УК (неправомерные уничтожение или модификация информации – уничтожение или изменение данных) – 10 (в 2015 г. - 14, 2016 г. - 9) и т.д;

- по ст.207 УК (нарушение работы информационной системы или информационно-коммуникационной сети – взлом компьютера) – 4 (в 2015г. - 9, 2016г. - 11);

- по ст.208 УК (неправомерное завладение информацией – кража данных) - 2 (в 2015 г. - 14, 2016 г. - 44);

- по ст.210 УК (создание, использование или распространение вредоносных компьютерных программ и программных продуктов – компьютерный вирус) – 3 (в 2015 г. - 61, 2016 г. - 24);

- по ст.211 УК (неправомерное распространение электронных информационных ресурсов ограниченного доступа – распространение служебных информсистем) – 4 (в 2015 г. - 19, 2016 г. - 17);

- по ст.212 УК (предоставление услуг для размещения интернет-ресурсов, преследующих противоправные цели – предоставление сервера для установки незаконных сайтов) – 1 (в 2015 г. - 4, 2016 г. - 2);

- по ст.213 УК - ст.227-1 старого УК (неправомерные изменение идентификационного кода абонентского устройства сотовой связи, устройства идентификации абонента, а также

создание, использование, распространение программ для изменения идентификационного кода абонентского устройства – перепрошивка ИМЕЙ кода сотового телефона) – 2 (в 2012 г. - 0, в 2013 г. - 1, в 2014 г. - 8, в 2015 г. - 4, 2016 г. - 5);

- по ст.227 старого УК (неправомерный доступ к компьютерной информации, создание, использование и распространение вредоносных программ для ЭВМ – нарушение конфиденциальности информации, компьютерный вирус) – (за 2012г. – 54, за 2013г. – 74, за 2014г. – 87);

- по п.4 ч.2 ст.188 УК (кража, совершенная путем незаконного доступа в информационную систему либо изменения информации, передаваемой по сетям телекоммуникаций – кража путем незаконного доступа на компьютер) – 58 (2015г. – 135, 2016г. - 31);

- по п.4 ч.2 ст.190 УК (мошенничество, совершенное путем обмана или злоупотребления доверием пользователя информационной системы – Интернет-мошенничество) – 888 (2015 г. – 45, 2016 г. - 1047);

- по ст.217 УК (создание и руководство финансовой (инвестиционной) пирамидой – финансовая пирамида) – 15 (за 2015г. – 2, за 2016г. - 0).

Пример - финпирамиды - Questra World. Представлена испанской компанией, при этом зарегистрирована в оффшоре – Британские Виргинские острова. Владельцем оффшорного счета, открытого в Кипре, является Украина. Деятельность фиксируется с середины 2016 года и только в пределах стран СНГ.

Противодействие киберпреступлениям, киберхищениям с использованием информационных технологий, в том числе и в финансовой сфере, должно предусматривать не только комплекс мер, предпринимаемых правоохранительными органами либо их скоординированные действия. Следует признать необходимость не только оперативного обмена информацией между банками и правоохранительными органами, но и постоянного совершенствования системы безопасности банков и повышение грамотности банковских работников и бухгалтеров, непосредственно занимающихся сопровождением финансовых операций.

Так, в декабре 2013 года в городе Алматы сотрудниками Управления «К» МВД и ДВД г.Алматы задержана организованная преступная группа, которая на протяжении нескольких лет занималась совершением хищений крупных сумм денег с банковских счетов организаций [8].

Преступники похищали денежные средства через систему «Банк-клиент». Предварительно создали вредоносную программу (компьютерный вирус - троянский конь), которая прикреплялась к электронному письму, отправленного от имени налогового органа на электронный адрес бухгалтера организации. Электронные адреса (ящики) хакерами выяснялись в социальных сетях, форумах бухгалтеров.

Ряд уголовных дел по аналогичным преступлениям расследовался в 2015 году в г.Алматы органами прокуратуры.

В ходе расследования уголовных правонарушений данной категории, следователи ОВД сталкиваются с проблемными вопросами, связанными с получением информации о принадлежности зарубежных IP-адресов, принадлежности мобильных телефонов и номеров электронных кошельков, а также квалифицированного осмотра техники, так как даже при удалении электронной информации на цифровом носителе могут оставаться определенные данные.

Приобретает особое значение заявление Президента Республики Казахстан Н.А. Назарбаева, отметившего целесообразность создания «глобальной валюты» в виде криптовалюты, которая бы основывалась на реальных активах [9].

Справочно: Криптовалюта – это цифровая (виртуальная) валюта, единица которой – монета (англ. -coin). Монета защищена от подделки, т.к. представляет собой зашифрованную информацию, скопировать которую невозможно (пользование криптографии и определило приставку «крипто» в названии). Заниматься ее добычей в сети (так называемым майнингом) может каждый желающий, обладающий компьютерным оборудованием необходимой мощности и специальным программным обеспечением. В процессе майнинга вычислительные мощности оборудования решают алгоритмы, сложность которых постепенно растет и, решив, добывают монету – набор зашифрованной информации. Доказательством наличия монеты в сети служит блокчейн – своего рода учетная запись. Хранится данная валюта децентрализовано, распределенной по электронным криптокошелькам пользователей.

Майнинг (добыча криптовалюты) становится всё более удобной платформой для мошенников и всё менее удобной для честного заработка. Мошенники вначале узнают номер телефона владельца кошелька. После этого они звонят в службу поддержки и говорят, что хотят перенести номер к другому оператору. Для этого достаточно выведать у сотрудника службы поддержки пин-код и потом назвать его новому оператору. Поскольку для такой операции нужно

подтвердить личность звонящего, мошенники либо используют какие-то сведения (например, дату рождения), полученные из социальных сетей, либо им приходится звонить много раз, пока не попадется сговорчивый сотрудник службы поддержки.

Национальный Банк РК неоднократно предупреждал об опасности проведения операций и вложения инвестиций в биткоины и другие виды криптовалют. Несмотря на это, за год курс криптовалюты «биткоин» в Казахстане вырос в 6 раз, на 4 октября т.г. на бирже «The Rock Trading Compani» продавался за 4 465 доллара *(на сегодня стоимость одного биткоина уже 7 000 долларов США).*

Отсутствие законодательного регламентирования оборота криптовалют создает благоприятные условия для отмывания и выводу финансовых средств за рубеж, незаконному обороту запрещенных предметов *(оружия, наркотических и психотропных веществ, детской порнографии)* и финансированию терроризма.

Указанные вопросы также коррелируются с разрабатываемой Министерством информации и коммуникаций РК Государственной программой «Информационный Казахстан - 2020», утверждённой 08.01.2013 г. Указом Президента РК № 464. Учитывая изложенное в РК необходимо разработать законодательство, регулирующее рынок криптовалют.

Многие зарубежные государства серьезно подходят к проблемам кибербезопасности, в том числе к организации расследования правонарушений, совершаемых с использованием информационных систем.

В Израиле при Общей службе безопасности *(ШАБАК)* был создан отдел по информационной безопасности. В 2011 году было создано Национального бюро израильской кибербезопасности.

Очень интересен опыт Республики Корея, там Центр кибербезопасности прокуратуры Республики Корея *(далее – ЦКБП)* создан в феврале 2012 года (Prosecutor'sCybersecurityCenter). Способ организации службы кибербезопасности в Генеральной прокуратуре Республики Корея на деле доказал свою эффективность, т.к. с момента создания ЦКБП не отмечено ни одного значительного инцидента кибербезопасности.

ЦКБП представляет собой центр мониторинга информационных систем и систем кибербезопасности *(анализ электронных журналов и корреляция событий, анализ вирусной активности, средств предотвращения утечек информации и других источников событий).*

Подобные национальные центры кибербезопасности, также имеются и в других странах, например в Германии (NCAZ), США (NCSC), Великобритании (NISCC).

В рамках СНГ утверждена Программа сотрудничества государств – участников Содружества Независимых Государств в борьбе с преступлениями, совершаемыми с использованием информационных технологий, на 2016-2020 годы [10].

В этой связи знакомство с опытом противодействия кибератакам, киберпреступлениям, компьютерной криминалистики лучших мировых практик интересно и полезно для сотрудников правоохранительных органов. Данные презентации – это стартовая площадка для дальнейшего возможного сотрудничества по практическим вопросам киберрасследований и информационной безопасности.

Генеральная прокуратура РК активно изучает международный опыт по противодействию киберугрозам, направляет своих сотрудников в командировки для обучения и участия в зарубежных семинарах.

Так, в период с 1 по 2 октября 2013 года сотрудники главного надзорного органа нашей страны приняли участие в 8-ом Московском Международном Форуме по вопросам безопасности «InterSecurityForum-2013» [11].

В период с 22-го по 25-ое июня 2014 года, делегацией во главе с заместителем Генерального Прокурора с целью изучения опыта, в том числе в сфере кибербезопасности и противодействию киберпреступности, была посещена Генеральная прокуратура Республики Корея [11].

25.10.2017 г. в здании ГП сотрудники межведомственной рабочей группы в рамках проведения Академией в текущем году межведомственного научного исследования на тему «Совершенствование методов противодействия отдельным формам хищения» организовали проведение on-line презентации компании Group-IB (г.Москва, РФ) на тему: «Особенности предотвращения и расследования киберхищений и мошенничества с использованием информационных технологий» (пункт 14-1 Оперативного плана ГП) (приняли участие сотрудники

1, 2 службы, Департамента международного сотрудничества, представители Управления «К» МВД РК и СЭР КГД МФ).

Справочно: В 2015 году Group-IB (г.Москва, РФ) по версии британского издания Business Insider была названа в числе семи самых влиятельных игроков в сфере информационной безопасности. Компания имеет крупнейшую криминалистическую лабораторию в Восточной Европе, а также центр оперативного реагирования CERT-GiB. Для выявления и предотвращения киберугроз Group-IB поставляет решения из линейки продуктов на базе системы киберразведки, сотрудничает с ФСБ, МВД РФ.

07.10.2017 г. директором Департамента защиты информационных услуг Цеснабанка проведена презентация в здании Академии для авторского коллектива по предупреждению кибератак, информационной безопасности;

*27.10.2017 г. членами МВРГ принято участие на практической конференции (хакерская конференция) по актуальным проблемам информационной безопасности «Kaz*Hack*Stan» (г.Алматы). Организаторы конференции – ОЮЛ «Центр анализа и расследования кибератак» (ЦАРКА) совместно с «Казахстан ГИС Центр» Министерства обороны РК.*

2 ноября 2017 г. членами МВРГ принято участие в круглом столе на тему «Киберпреступность и информационная безопасность: современное состояние, проблемы и перспективы развития» (г.Астана).

16-17 ноября 2017 г. (г.Астана-г.Алматы) членами МВРГ принято участие на международной научно-практической конференции на тему: «Актуальные вопросы обеспечения общественной безопасности и противодействия преступности, посвященной 90-летию со дня рождения д.ю.н., профессора, государственного советника юстиции 3-го класса Бегалиева Калауши Адильхановича (1927-2006) (г.Алматы, г.Астана).

В связи участившимися кибератаками на ведущие информационные системы, начавшейся эпидемии опасного компьютерного вируса-шифровальщика и заражения персональных компьютеров существует опасность взлома программного обеспечения Генеральной прокуратуры [12].

По мнению Генеральной прокуратуры РК, имеется потребность в кадрах для организации круглосуточно функционирующего центра кибербезопасности Генеральной прокуратуры *(по опыту Кореи)* в том числе с подготовкой специалиста по сбору и анализу цифровых улик и выделению аналитика для работы с системой предотвращения утечек информации.

В тоже время Департамент финансов, информатизации и защиты информационных ресурсов Генеральной прокуратуры, в качестве объективных обстоятельств, препятствующих кадровому обеспечению государственных органов квалифицированными специалистами по кибербезопасности указывает: значительную разницу в размере заработной платы специалистам по кибербезопасности *(в государственных органах не установлен конкурентоспособный размер заработных плат для специалистов по кибербезопасности);* действующие процедуры приема на государственную службу; поручение об установлении моратория до конца 2018 года на расширение штатов и увеличение заработной платы, а также на выделение средств из государственного бюджета на новые инициативы [13].

В целом, в структуре Генеральной прокуратуры имеется Управление информационной безопасности *(Управление),* которое обеспечивает информационную безопасность органов Генеральной прокуратуры, однако надзорными функциями данное Управление не обладает.

По сведениям Управления ежемесячно служба Государственная техническая служба, находящаяся в структуре КНБ РК фиксирует и направляет им отчет об имеющихся, как минимум, 100 000 событий, в том числе критических угрозах. В дальнейшем подрядная организация «Логитекс» изучает и принимает соответствующие меры по устранению данных угроз.

В тоже время недавно в Комитете правовой статистики и специальных учетов Генеральной прокуратуры Республики Казахстан *(далее - КПСиСУ)* создана Группа по информационной безопасности Управления аналитической работы и правового регулирования, которая обеспечивает информационную безопасность КПСиСУ [14].

Необходимо отметить общеизвестные и плодотворные проекты КПСиСУ - Единый реестр досудебных расследований; аналитические информационные системы - «Төрелік»; «Заңдылық»; интернет-портал «Карта уголовных правонарушений»; «Карта ДТП»; Е-штрафы; единый шлюз «Система информационного обмена правоохранительных и специальных органов»; информационный сервис «Централизованный банк данных должников «Шектеу»; «Единый реестр субъектов и объектов проверок»; проект «Е-уголовное дело» и т.д.[15].

Данные успешные проекты показали обширный информационный потенциал КПСиСУ, который может быть использован в обеспечении кибербезопасности электронных систем не только КПСиСУ, а также и всех органов прокуратуры.

Имеющиеся в целом в правоприменительной практике общие проблемы по мошенничеству, киберхищениям, мошенничеству с криптовалютами:

1**.** В Комплексном плане МВД по профилактике правонарушений на 2017-2019 годы мер противодействия мошенничеству нет.

2. Высокий уровень латентности. Мало рассмотренных судом дел по киберхищениям. Мошенничество умышленно завуалировано под гражданско-правовые сделки, что влечет отказ их в регистрации в ЕРДР либо вызывает сложности в квалификации *(за 2016 год 20 тыс. дел о мошенничестве прекращены по реабилитирующим основаниям, тогда как в производстве находилось 37 тыс дел).*

- неправильная квалификация при регистрации в ЕРДР. Так, имеются случаи несоответствия частей ст.УК РК в стадии регистрации ЕРДР и по ч.ст.УК «на выходе» (прекращено и осуждено – разные части, к примеру, приговор в отн.Аскарбекова С.Т. осужден по ч.3 п.1 ст.190 мошенничество (*крупно-рогатый скот)* УК, а регистрация по 190 ч.2 п.4 *(с использованием информационных технологий).*

- низкий уровень либо отсутствие у сотрудников полиции, занимающихся борьбой с киберхищениями, IT-образования;

- проблемы выявления, предупреждения пресечения и расследования таких преступлений, *в частности, сбора и оценки доказательств, возможности использования электронных документов, электронных сообщений, информации сети Интернет в доказывании по ним;*

- проблемы изъятия и правил осмотра электронных носителей информации, назначение экспертиз (постановки вопросов) и оценки их результатов;

- проблемы получения сведений о регистрации пользователей социальный сетей и интернет-ресурсов, в том числе зарубежных

- проблемы международного сотрудничества по делам о преступлениях, подозреваемые в совершении которых находятся за рубежом или являются иностранными гражданами.

3. Самостоятельный гражданско-правовой способ защиты жертв мошенников не эффективен, не все мошенники несут наказание из-за неоднозначной судебно-следственной практики.

4. Необходимо расширить квалифицирующие признаки ст.190 УК, проработать вопрос целесообразности дополнения УК определением «обман», либо постановления ВС РК № 6 от 29.06.2017 года «О судебной практике по делам о мошенничестве».

5. Отдельной методики по расследованию уголовных дел о киберхищениях в Казахстане нет.

6. Законодательно не урегулировано понятие криптовалют, ответственности за мошенничество с использованием криптовалют и операций с криптовалютами.

7. Не урегулированы соответственно и виды ответственности с возможным мошенничеством с использованием криптовалют.

Таким образом, резюмируя вышеизложенное, приходим к следующим выводам:

1. Имеется актуальная проблема безопасности электронных сетей правоохранительных органов;

2. Недооценивается важность противодействия информационным угрозам;

3. Необходима организация качественной подготовки высококвалифицированных специалистов для нужд государственных органов, начиная с ВУЗов:

3.1. Систематически повышать компьютерно-информационную грамотность населения;

3.2. Внедрить учебные занятия по кибербезопасности, киберграмотности в программу школьного и ВУЗовского обучения, с разъяснением видов кибермошенничества в сети Интернет и способах предостережения *(по опыту США: ФБР проводит специальные программы в школьных учреждениях «Безопасный интернет серфинг»).*

4. Правоохранительным органам необходимо сделать упор на предупреждение правонарушений и преступлений, совершаемых посредством сети Интернет;

5. Необходима консолидация всех государственных и правоохранительных органов в сфере кибербезопасности. К примеру, со стороны Генеральной прокуратуры имеется объективная возможность использовать информационный потенциал КПСиСУ и уже сейчас создать свою базу мониторинга и отслеживания состояния имеющихся киберугроз.

6. Нет правовых актов, регулирующих понятие, порядок и движение криптовалют, соответственно не урегулированы и виды ответственности с возможным мошенничеством с использованием криптовалют.

В этой связи предлагаем следующее:

1. Создать Центр мониторинга информационных систем *(далее Центр)* на базе Группы по информационной безопасности Управления аналитической работы и правового регулирования КПСиСУ *(по опыту Республики Корея);*

2. Разработать информационно-аналитическую систему *(ИАС):* «Единый центр мониторинга и реагирования на кибератаки», интегрированную во все правоохранительные органы;

3. Использовать информационные возможности КПСиСУ, Регионального Хаба Академии по противодействию глобальным угрозам, в том числе и проведения занятий, повышающих уровень компьютерной грамотности в сфере кибербезопасности сотрудников правоохранительных органов.

При составлении технического задания по ИАС предусмотреть:

- разработку своих программ *(по опыту Кореи, РФ, США);*
- разделы с анализом нормативной правовой базы в области информационной безопасности на предмет ее актуальности текущим вызовам;
- раздел, информирующий и повышающий компьютерно-информационную грамотность пользователя (сотрудника правоохранительных органов) о кибербезопасности, с разъяснением видов кибермошенничества в сети Интернет и способах предостережения *(по опыту США);*
- проведение автоматического единого мониторинга реагирования на компьютерные атаки, киберугрозы*;*
- проведение единого стандарта обмена информацией;
- раздел по международному опыту *(выработка и распространение защитных и превентивных мер);*
- унификация национального законодательства с международным;

4. Дополнить ст.3 УК понятиями, касающимися кибербезопасности *(перечень которых взять из Концепции «Киберщит», утвержденной Постановлением Правительства РК №30 от 30 июня 2017 года, а также использовать определения из международного зарубежного опыта, к примеру РФ, США и т.д.)* в том числе: кибератака (нападение), кибервторжение (проникновение), кибероперация, киберзащита (оборона), понятие он-лайн обыск *(по примеру Германии, также и внести в УПК соответствующие дополнения и изменения).*

5. Ужесточить санкцию статей киберпреступлений, которые совершены в отношении информационных систем государственных органов *(по опыту США),* это послужит эффективной мерой противодействия. Например, увеличить штраф до 700 МРП, предусмотреть в санкции лишение свободы сроком до 7 лет в ч.2 ст.ст.205, 206, 207, 208 УК главы 7 УК.

6. Ввести публичный реестр мошенников, в том числе кибермошенников. Данный реестр создать на базе МВД и КПСиСУ, с их фотопортретами, адресами проживания и иной информацией. В базу вносить сведения по всем мошенникам, в отношении которых состоялся судебный акт, вступивший в законную силу и с кратким описанием способа мошенничества *(по примеру США, но в РК не только в отношении половых насильников, но и в отношении мошенников. 26 июня 2006 года был введен в действие Национальный публичный реестр сексуальных преступников – общеамериканская онлайновая база данных лиц, совершивших сексуальные преступления, к которой присоединились 50 штатов).*

Данный список лиц, с фото, следует транслировать постоянно на билбордах всей страны и во всех общественных местах, учебных заведениях, государственных органах, частных структурах, чтобы мошенников население РК знало в лицо.

Ожидаемый эффект: Мощная и эффективная предупредительная мера. Усилится взаимодействие правоохранительных органов в работе по раскрываемости преступлений и розыску мошенников. Снизится уровень рецидивной преступности.

7. Необходимо разработать и принять самостоятельный законодательный акт, как на национальном, так и на международном уровне, который бы вобрал в себя все правовые механизмы регулирования криптовалюты *(понятие, порядок движения, рынок криптовалют, ответственность и т.д.).*

Предлагаемый Центр и ИАС, по нашему мнению, позволит обеспечить кибербезопасность, сформировать необходимую законодательную базу и выстроить процессы и технологии информационного обмена между государственными, правоохранительными службами на основе лучших мировых практик.

Считаю, что данная международная научно-практическая конференция предоставила нам всем прекрасную возможность совместно обсудить имеющиеся актуальные проблемы правоприменительной практики, детально ознакомиться с передовым зарубежным опытом и выработать совместные рекомендации по совершенствованию обеспечения кибербезопасности, противодействия хищениям, киберхищениям.

Список использованных источников:

1. Журнал «Blog Arhive» Глобальный индекс кибербезопасности 2017. 19 июня 2017 г. /http://j-times.ru/rejting/globalnyj-indeks-kiberbezopasnosti-2017.html.

2. Концепция кибербезопасности («Киберщит Казахстана»), утвержденная Постановлением Правительства РК №30 от 30 июня 2017 года /http://adilet.zan.kz

3. В Казахстане создана Служба реагирования на компьютерные инциденты /https://www.nur.kz/200694-v-kazahstane-sozdana-sluzhba-reagirovaniya-na-kompyuternye-inczidenty.html.

4. Турлаев А.В., Шәкірова А.Б. Правовое обеспечение информационной безопасности в Республике Казахстан /https://articlekz.com/article/6210

5. Уголовный кодекс РК от 3 июля 2014 года /http://adilet.zan.kz

6. Биекенов Н.А. Некоторые проблемы обеспечения кибербезопасности в Республике Казахстан /http://online.zakon.kz/Document

7. Аналитические материалы Управления «К» МВД РК.

8. Аналитические материалы ДКП МВД РК, Управления «К» МВД РК.

9. Назарбаев хочет создать «глобальную криптовалюту» //Информационный портал ««TodayNews» /http://today-news.com/News/cryptocurrency/Nazarbaev-hochet-sozdat-globalnuyu-kriptovalyutu-83069.html

10. Программа разработана во исполнение Решения Совета глав государств Содружества Независимых Государств о Концепции сотрудничества государств – участников Содружества Независимых Государств в борьбе с преступлениями, совершаемыми с использованием информационных технологий от 25 октября 2013 года (утверждена 16.09.2016г.).

11. Аналитические материалы Генеральной прокуратуры РК по вопросам информационной безопасности.

12. Письма Генеральной прокуратуры от 15.05.2017 г. за исх.№2-011000-17-35103, 20.07.2017 г. за исх.№2-011000-17-52782.

13. Мораторий до конца 2018 года установлен Подпунктом 2) пункта 1 протокола совещаний по системным мерам экономической политики от 19-20 августа 2015 года под председательством Главы государства.

14. Приказ Председателя КПСиСУ № 64 о/д от 19.07.2017 года /http://adilet.zan.kz

15. Развитие органов правовой статистики и специальных учетов //Закон и время. 2017. № 4/196. С.54-55.