МРНТИ 10.79.51

Н.К. Имангалиев[1]
Л.А. Темиржанова[2]

[1]Академия правоохранительных органов при Генеральной прокуратуре Республики Казахстан, Нур-Султан, Казахстан
[2]Евразийский национальный университет им. Л.Н. Гумилева, Нур-Султан, Казахстан
(E-mail: 7171131@prokuror.kz, lyazzat_1805@mail.ru)

# Актуальные проблемы выявления и раскрытия уголовных правонарушений, совершаемых в сети Интернет

**Аннотация.** *В статье исследуются проблемные вопросы выявления и противодействия уголовным правонарушениям, совершаемым в сети Интернет. Анализ статистических данных свидетельствует о значительном росте данного вида правонарушений. Основная доля преступлений остается не раскрытой по причине отсутствия доступа к хранимым сведениям по использованию информационных систем в базах данных интернет-провайдеров, социальных сетей и других организаций. В большинстве случаев злоумышленники находятся за пределами страны, куда и выводятся похищенные средства. Предъявляемые законодателем процессуальные требования не позволяют оперативного доступа к ним, что влечет собой утрату доказательств, усложняет розыск преступников и похищенных денежных средств. Автором сформулированы предложения по совершенствованию отечественного законодательства, направленного на усиление мер государственной политики в части защиты конституционных прав граждан.*

**Ключевые слова:** *сеть Интернет, киберпреступность, электронные доказательства, вредоносная программа, IP-адрес, информационные системы, раскрытие, социальные сети, международное сотрудничество.*

**DOI: https://doi.org/10.32523/2616-6844-2022-138-1-124-132**

## Введение

Информационно-телекоммуникационная инфраструктура становится важнейшим элементом развития, без доступа к которой существование, как личности, так и государств в мировом информационном пространстве представляется затруднительным [1].

Уголовные правонарушения, совершаемые в сети Интернет, вместе с бурным развитием научно-технического прогресса с каждым днем обретают все более изощренные и опасные формы, в том числе и транснационального характера. Правоохранительные органы все чаще имеют дело с профессиональными преступниками, с высоким уровнем технической подготовленности и упорством в достижении цели.

Будучи осведомленными о формах и методах работы органов, они оказывают активное «интеллектуальное» сопротивление раскрытию преступлений. Наиболее заметную специфику среди таких лиц образуют хакерские сообщества, имеющие особую криминогенную среду, способную продуцировать значительное число латентных преступлений.

**Методы**

Методологической основой настоящей работы являются общенаучные и частно-научные методы, включая формально-логический, сравнительно-правовой анализ, синтез.

**Дискуссия**

В сети Интернет преступники способны дистанционно совершать целый ряд различных незаконных операций одновременно в нескольких операционно-вычислительных системах, перемещаясь в физическом пространстве.

В результате чего «размывается» физическое место совершения преступления и нарушается пространственная локализация. Сложность обнаружения действий компьютерного преступника и его возможности совершать преступления в киберпространстве, не имеющем государственных временных границ, многократно увеличивают степень общественной опасности таких деяний [2].

Так, по данным Министерства информации и общественного развития в период с 2017 года по 2021 года наибольшее количество совершаемых через сеть противоправных деяний были по следующим направлениям:

1. Пропаганда терроризма, экстремизма;
2. Распространение порнографии;
3. Пропаганда наркотических средств, психотропных веществ, их аналогов и прекурсоров;
4. Распространение информации, пропагандирующей суицид. Архив Комитета информации Министерства информации и общественного развития, 2021 год [Таблица 1].

Согласно отчету Международного союза электросвязи ООН, в 2020 году Казахстан по Глобальному индексу кибербезопасности занял 31 место из 193 стран. Данные показатели достигнуты в результате технических, законодательных и корпоративных мер, направленных на создание и укрепление институтов, вовлеченных в обеспечение кибербезопасности, а также благодаря потенциалу развития и сотрудничества с другими государствами.

Эффективность противодействия киберпреступлениям зависит от таких факторов, как уровень развития правовой среды, технические предпосылки, организационные меры, развитие компетенций и кооперация внутри и вне страны [4].

Наряду с этим, реальную угрозу интересам общества несет и размещение в Интернете вредоносных программ, устройств компьютерного взлома, методических рекомендаций по применению хакерского инструментария, а также продажа запрещенных к обороту специальных технических средств.

Росту уголовных правонарушений, совершаемых в сети Интернет, способствуют и такие проблемы, как низкая правовая грамотность населения, работников сферы ИКТ и руководителей организаций по вопросам информационной безопасности и программного обеспечения.

**Таблица 1**

Виды уголовных правонарушений, совершаемых в сети Интернет

| Годы | Пропаганда терроризма, пропаганда экстремизма | Распространение порнографии | Пропаганда наркотических средств, психотропных веществ, их аналогов и прекурсоров | Распространение информации, пропагандирующей суицид |
|---|---|---|---|---|
| 2017 | 79186 | 2562 | 2097 | 923 |
| 2018 | 148998 | 1346 | 945 | 354 |
| 2019 | 56428 | 3779 | 1851 | 133 |
| 2020 | 72025 | 2125 | 1068 | 87 |
| 2021 | 231140 | 6760 | 1754 | 28 |

Безусловно, данные обстоятельства крайне усложняют деятельность правоохранительных органов по выявлению и раскрытию уголовных правонарушений, совершаемых в сети Интернет.

Так, выявление, изучение, фиксация и изъятие в установленном законом порядке цифровых объектов, следов и информации из мобильного устройства позволяют:

- напрямую изобличать лицо в совершении преступления;

- косвенно указывать на линию поведения лица, возможную причастность его к совершенному преступлению;

- способствовать установлению иных обстоятельств, имеющих значение для уголовного дела.

Вместе с тем компьютерная информация может быть как носителем следов совершенного уголовного правонарушения, так и непосредственно являться их следами. В сфере высоких технологий компьютерная информация легко передается, копируется, блокируется или модифицируется с беспрецедентной скоростью и на значительном расстоянии.

По мнению В.А. Мещерякова, под понятием «виртуальные следы» следует понимать «любое изменение состояния автоматизированной информационной системы, связанное с событием преступления и зафиксированное в виде компьютерной информации» [5].

Для обозначения указанного термина отдельными авторами предлагаются схожие и аналогичные предложения как «компьютерно-технические следы» [6]

и «бинарные следы» [7].

Отсутствие прямого или удаленного доступа к устройствам, на которых хранятся данные, и проведение необходимых следственных действий являются актуальной проблемой сотрудников правоохранительных органов при выявлении уголовных правонарушений.

Электронные доказательства, указывающие на совершение уголовных правонарушений, аккумулируются в регистрационных данных и системных журналах, находящихся в распоряжении компании - поставщиков хостинговых услуг. Также имеются сложности при установлении лиц, совершивших уголовные правонарушения в сети Интернет. Зачастую, все, что известно о подозреваемом — это его IP-адрес. Это уникальное число, которое идентифицирует устройство в сети, адрес электронной почты, доменное имя или интернет-псевдоним (ник).

Для идентификации физического лица по IP-адресу специалисту нужны данные, которые находятся в распоряжении поставщика интернет-услуг. Поставщики интернет-услуг (электронной почты, хостинговых услуг) зачастую являются единственным источником информации, которая помогает установить связь между виртуальной личностью правонарушителя и конкретным физическим лицом.

В связи с этим независимые владельцы данных часто оказываются ключевым звеном в расследовании. При установлении IP-адреса и времени его нахождения в сети Интернет следователь может узнать, где находится персональный компьютер или гаджет, с которого работал интернет-мошенник (номер квартиры, дома и т.д.). Имея изначально информацию лишь по одному объявлению интернет-мошенника, с помощью анализа Cookie-файлов возможно получить сведения по всем объявлениям, размещенным интернет- мошенником, так как на территории страны все абонентские устройства сотовой связи, и каждый абонентский номер на конкретное физическое или юридическое лицо подлежат обязательной регистрации [8].

Также компьютерные преступления имеют свои специфические особенности, в числе которых фактическое отсутствие так называемого «бумажного следа». Поэтому с точки зрения незаконного использования виртуальных валют, доказательная база, как правило, состоит из электронных доказательств, что требует от следователя высокой квалификации и специальных познаний.

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.

Преступники похищали денежные средства путем неправомерного доступа к компьютерной информации с использованием дистанционного банковского обслуживания системы «Банк-клиент».

Предварительно была создана вредоносная программа (компьютерный вирус - троянский конь), которая прикреплялась к электронному письму, отправленному от имени налогового органа на электронный адрес бухгалтера организации. Электронные адреса (ящики) хакерами выяснялись в социальных сетях, форумах бухгалтеров.

При этом преступник «хакер» получал доступ к управлению информацией, хранящейся на компьютере бухгалера и имел возможность от его имени направлять в банк электронные платежные поручения и производить переводы денежных средств.

В ходе исследования цифровых доказательств установлено, что преступники в целях сокрытия следов преступлений, использовали Интернет-ресурсы зарубежных стран, в т.ч. прокси-сервера, через которые удаленно совершались хищения.

Обналичивание денег производилось известными способами. Организатор (хакер) находил посредников, которые в свою очередь занимались поисками обнальщиков (дропов) путем приобретения их пластиковых карт либо оформления на их имя фиктивных юридических лиц (ТОО, ИП и т.д.) с последующим открытием банковских счетов, на которые перечислялись похищенные денежные средства. В некоторых случаях изготавливались поддельные документы, пластиковые карточки.

По результатам предварительного расследования, преступникам предъявлены обвинения в совершении 16 хищений на общую сумму около 400 млн. тенге (примерно 2,7 млн. долларов США), 13 фактов неправомерного доступа к компьютерной информации путем создания и использования вредоносных программ, а также 2 фактов подделки документов и печатей. Кроме того, учитывая, что преступления носили организованный характер с распределением ролей, преступникам дополнительно предъявлено обвинение в создании, руководстве и участии в организованной группе в целях совершения преступлений.

Ряд уголовных дел по аналогичным преступлениям расследовался в 2015 году в г.Алматы органами прокуратуры. Так, в 2015 году задержан житель г. Петропавловска, который посредством сети Интернет совершил преступление, предусмотренное ст.208 УК РК «неправомерное завладение информацией» в отношении клиентов банков «Евразийский» и «Народный».

Установлено, что он посредством социальной сети осуществил массовую рассылку писем от пенсионного фонда указанных банков с требованием подтверждения идентификационных данных пластиковых карт. После получения необходимой информации им планировалось совершение хищений с карт-счетов клиентов банков.

Известно множество способов хищений, совершаемых с использованием «пробелов» банковской защиты. К ним можно отнести кражи и мошенничества с использованием систем обслуживания клиентов, таких как мобильный банкинг, интернет-банкинг и т.д.

В 2013 году в г. Алматы задержаны граждане Болгарии и Румынии, которые прибыли в Казахстан для совершения краж с использованием «скимминговых устройств» (устройства кустарного производства, устанавливаемые на банкоматы для копирования информации с пластиковых карт держателей) на банкоматы (АО «Народный банк» и по АО «Сбербанк»). Владельцам карточек причинен ущерб на сумму свыше 8 млн. тенге.

Так, в 2015 году задержан житель Акмолинской области, который звонил на номера сотовых телефонов граждан и представлялся сотрудником представительства какой-либо крупной торговой марки. Он сообщал о вымышленном выигрыше и предлагал произвести оплату его денежного эквивалента на карточку, для чего просил подключить услугу мобильный банкинг на свой номер. Таким образом, он получал доступ к деньгам граждан и переводил их с помощью услуги интернет-банкинг.

С учетом изложенного можно сделать вывод, что противодействие киберпреступле-

ниям, 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. В целом борьба с данными преступлениями должна содержать многоплановый характер, поэтому и работа должна вестись по разным направлениям, в первую очередь со стороны банков.

Следует признать необходимость не только оперативного обмена информацией между банками и правоохранительными органами, но и постоянного совершенствования системы безопасности банков и повышения грамотности банковских работников и бухгалтеров, непосредственно занимающихся сопровождением финансовых операций.

Общие рекомендации по защите от кибермошенничества, киберпреступлений:

- не использовать в качестве паролей или слов доступа информацию, которую можно почерпнуть о вас в интернете;

- не указывать свои данные на подозрительных сайтах, нужно иметь отдельные (не привязанные к карточкам) счета в банках для хранения сбережений, использовать усовершенствованные системы оплаты, создавать виртуальные карты или иметь специальную отдельную карту с функцией 3D-secure для платежей в интернете;

- использовать антивирусные программы;

- повышать компьютерно-информационную грамотность населения;

- в программу школьного и вузовского обучения внедрить учебные занятия по кибербезопасности, киберграмотности, с разъяснением видов кибермошенничества в интернет-сети и способов предостережения (по опыту США, ФБР проводит специальные программы в школьных учреждения «Безопасный интернет-серфинг»).

**Результаты**

Наиболее распространенным способом совершения уголовных правонарушений в сети Интернет являются такие виды как:

- получение частичной или полной предоплаты за товар или услугу по объявлениям, размещенным на торговых интернет-площадках (OLX, Kolesa.kz, Krisha.kz и т.д.) и в социальных сетях (Instagram, Facebook, VKontakte и т.д.);

- оформление фиктивных онлайн-займов через сайты микрокредитных организаций («Деньги-населению», «Займер», «Тенго», «Финкап», «Смарт-Финанс» и др.).

В одном случае после обманного завладения персональными данными, преступники оформляют онлайн-кредит и получают полный доступ к управлению банковской картой и депозитами. Далее деньги через банкинг переводятся на сторонние счета, в т.ч. за рубеж.

В большинстве случаев преступники представляются сотрудниками служб безопасности банков и похищают деньги со счетов граждан путем подключения к мобильному банкингу с последующим переводом на счета зарубежных банков, в т.ч. российских, белорусских, украинских и др.

Почти треть (2822) оставшихся в 2020 году нераскрытыми интернет-мошенничеств совершены с территорий государств постсоветского пространства (Россия, Беларусь, Украина) [9].

Так, выявление уголовных дел по фактам интернет-мошенничеств осложнено продолжительными поисковыми мероприятиями владельцев сим-карт, с которых произведен звонок, а также «интернет-адресов» подозреваемых. В большинстве случаев для совершения уголовных правонарушений данной категории используются «сайты-однодневки», при регистрации доменного имени вносятся вымышленные данные.

Также направляются санкционированные постановления в банки второго уровня о выемке транзакции по банковским счетам, на которые потерпевшими перечисляются денежные средства.

Здесь проблема заключается в том, что в предоставляемых ответах на постановления практически все банки дают не полные ответы, что создает дополнительные трудности в расследовании, а именно:

- сообщается о перечислении денежных средств на другие карты банка или счета, при этом полные номера счетов и карт не указываются;

- сообщается о перечислении денежных средств на номера телефонов сотовых компаний, однако номера и данные сотовых компании не предоставляются;

- денежные средства перечисляются на счета зарубежных банков, установить принадлежность которых также не представляется возможным.

При этом для получения исходных данных подозреваемых затрачивается много времени, за которое последние успевают поменять платежные карты, мобильные устройства, создать новые сайты и т.д.

После получения необходимых сведений (посредством запроса, санкционированного прокурором) требуется выемка документов (договоров банковского займа, залога недвижимого имущества, кредитного досье и т.д.), содержащих банковскую тайну.

Также в ряде случаев возникает необходимость в получении из банков второго уровня информации о передвижении денежных средств (по одному или нескольким банковским счетам), IP-адресах (при online-переводах), абонентских номерах (привязанных к банковским счетам), местонахождении банкоматов, через которые обналичены похищенные денежные средства, а также фото и видеоизображений с камер банкоматов.

Вместе с тем имеются проблемы в получении санкций о выемке сведений с банков второго уровня и вопросы взаимодействия с администрациями интернет-сайтов, социальных сетей, мессенджеров (ВКонтакте, Facebook, Watsapp, Одноклассники, Инстаграмм, Mail.ru), находящихся за пределами страны, которые не имеют своих представительств в РК.

- администрированием чатов в социальных сетях, через которые осуществляется сбыт, занимаются «боты», то есть фактически чаты страницы не зарегистрированы на конкретных лиц, которых можно установить (в основном в социальной сети «Телеграмм»);

- использование прокси-серверов не позволяет установить IP-адреса возможных создателей чатов, через которых осуществляется сбыт наркотических средств.

Отличительной особенностью преступлений, связанных с незаконным сбытом наркотических средств, совершаемых с использованием сети Интернет, является отсутствие личности потерпевшего. При покупке и других незаконных действиях с наркотиками лицо само нарушает соответствующие нормы права и становится преступником. Правоохранительными органами в настоящее время устанавливаются и привлекаются к уголовной ответственности только исполнители (закладчики). Организаторы сбыта продолжают свою преступную деятельность, привлекая новых участников в виде исполнителей.

Указанные проблемы создают определенные сложности и при проведении профилактики преступлений данной категории.

Не менее важна проблема недостаточной эффективности системы международной взаимной правовой помощи для решения вопросов, связанных с киберпространством, в частности, ввиду ее медлительности.

Средний срок обработки запроса об оказании взаимной правовой помощи в связи с вопросами кибербезопасности составляет от 6 месяцев (по информации Республики Чехия средний срок среди государств-членов Совета Европы составил 21 месяц) [10].

В связи с чем для решения указанных проблем необходимо:

- внести предложения об изменении порядка регистрации пользователей в платежной системе Киви-кошелек (Казахстан), где обязательным условием для создания кошелька определить регистрацию пользователя (для всех регистрирующихся) путем внесения данных ИИН и др.

- упрощение процедуры получения информации о транзакциях через Киви-кошелек, без санкционирования постановления в следственном суде, а по запросам в рамках уголовного дела.

В целях минимизации рисков хищения денежных средств (правовые и технические аспекты) компетентным государственным ор-

ганам (АРРФР, МТ) совместно с Ассоциацией «Цифровой Казахстан» необходимо принять дополнительный комплекс мер по урегулированию интернет-торговли.

Кроме того, ввиду трансграничности, а также малоэффективности существующих механизмов международного обмена оперативной информацией и международными запросами, дела о хищениях с использованием сети Интернет остаются нераскрытыми.

В этой связи необходима проработка вопроса взаимодействия органов внутренних дел (полиции) государств-участников СНГ по раскрытию преступлений в сфере информационных технологий, в том числе интернет-мошенничеств.

Сходные проблемы существуют при использовании зарубежных социальных сетей и мессенджеров, которые находятся вне юрисдикции РК и информация об интересующих пользователях может быть получена на основании международного следственного поручения.

Также имеются проблемы и в том, что следователи и прокуроры не знают как правильно и грамотно работать за рубежом. Не учитываются мировые стандарты и требования других стран (ЕС, Великобритания, США и т.д.). Нет должного взаимодействия правоохранительных органов и судов РК с международными организациями и зарубежными правоохранительными органами и судами.

**Вывод**

На данном этапе своего развития правоприменительная практика остро нуждается в совершенствовании оперативно-розыскных, криминалистических приёмов и способов выявления и раскрытия преступлений, совершаемых посредством интернет-ресурсов. В целях создания эффективного механизма противодействия теневому обороту наркодоходов посредством «электронных кошельков» и пресечения распространения новых психоактивных веществ с использованием виртуальных платежных систем предлагается поручить Национальному банку внести изменения в Закон РК «О платежах и платежных системах» в части отказа в оказании услуг неидентифицированным пользователям электронных платежных систем.

Процесс идентификации пользователей предлагается осуществлять по аналогии с процедурой прохождения регистрации в онлайн-режиме в банковских и сервисных мобильных приложениях («Каспи», «InDriver» и др.).

Таким образом, в целях совершенствования правоприменительной практики расследования уголовных правонарушений, совершаемых в сети, предлагается активизировать деятельность по ратификации Конвенции Совета Европы «О компьютерных преступлениях» [11].

Имплементация положений Конвенции и приведение национального законодательства в соответствие с международными нормами позволит расширить сферы взаимодействия правоохранительных органов Казахстана с зарубежными коллегами по раскрытию уголовных правонарушений, совершаемых в сети Интернет.

Полагаем, что указанные меры позволят усилить меры государственной политики в части защиты конституционных прав граждан и повышения осведомленности населения о совершаемых уголовных правонарушениях.

**Список литературы**

1. Постановление Правительства Республики Казахстан от 12 декабря 2017 года №827 «Об утверждении Государственной программы «Цифровой Казахстан»»// https://adilet.zan.kz/rus/docs/P1700000827.

2. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий. Учебное пособие: в 2 ч. / А.В. Аносов и др. – М.: Академия управления МВД России, 2019. – Ч. 1 – 208 с.

3. Архив Комитета информации Министерства информации и общественного развития Республики Казахстан, 2021.

4. Global Cybersecurity Index 2020//https://www.itu.int/en/myitu /Publications /2021/06/28/13/22/Global-Cybersecurity-Index-2020.

5. Мещеряков В.А. «Виртуальные следы под скальпелем Оккама» // Информационная безопасность регионов. 2009. №1(4). С. 28-33.

6. Лыткин Н.Н. Использование компьютерно-технических следов в расследовании преступлений против собственности// - автореф. дис…канд. юрид. наук. М., 2007. 24 с.

7. Милашев В.А. Проблемы тактики поиска, фиксации и изъятия следов при неправомерном доступе к компьютерной информации в сетях ЭВМ: автореф. дис…канд. юрид. наук. 2004. 24 с.

8. Приказ и.о. Министра информации и коммуникаций Республики Казахстан от 23 мая 2018 года № 226 «Об утверждении Правил регистрации абонентских устройств сотовой связи». Зарегистрирован в Министерстве юстиции Республики Казахстан 11 июня 2018 года № 17028.

9. Архив Департамента криминальной полиции МВД Республики Казахстан, 2021.

10. Доклад Генерального секретаря ГА ООН «Противодействие использованию информационно-коммуникационных технологий в преступных целях» С.26-27. https://www.unodc.org/documents/Cybercrimer /SG_report/V1908184_R.

11. «Конвенция о преступности в сфере компьютерной информации» (ETS №185) (Заключена в г.Будапеште 23.11.2001).

**Н.Қ. Иманғалиев[1], Л.А. Теміржанова[2]**

*[1]Қазақстан Республикасы Бас Прокуратурасының жанындағы*
*Құқық қорғау органдарының академиясы, Нұр-Сұлтан, Қазақстан*
*[2] Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Нұр-Сұлтан, Қазақстан*

**Интернет жеріндегі қылмыстық құқық бұзушылықты анықтау және қарсы жасау туралы мәселелер**

**Аңдатпа.** Мақалада Интернетте жасалған қылмыстық құқық бұзушылықтарды анықтау және оларға қарсы тұрудың проблемалық мәселелері қарастырылады. Статистикалық мәліметтерді талдау құқық бұзушылықтың бұл түрінің айтарлықтай өскенін көрсетеді. Қылмыстың негізгі үлесі интернет-провайдерлердің, әлеуметтік желілердің және басқа да ұйымдардың дерекқорларындағы ақпараттық жүйелерді пайдалану туралы сақталған ақпаратқа қолжетімділіктің болмауына байланысты ашылмаған күйде қалып отыр. Көп жағдайда шабуылдаушылар ұрланған қаражат аударылатын елден тыс жерде орналасқан. Заң шығарушы қойған процессуалдық талаптар оларға жедел қол жеткізуге мүмкіндік бермейді, бұл дәлелдемелердің жоғалуына әкеп соғады, қылмыскерлерді және ұрланған қаражатты іздеуді қиындатады. Автор азаматтардың конституциялық құқықтарын қорғау бөлігінде мемлекеттік саясат шараларын күшейтуге бағытталған отандық заңнаманы жетілдіру бойынша ұсыныстарды тұжырымдаған.

**Түйін сөздер:** интернет желісі, киберқылмыс, электрондық дәлелдер, зиянды бағдарлама, IP-мекенжайы, ақпараттық жүйелер, ашу, әлеуметтік желілер, халықаралық ынтымақтастық.

**N.K. Imangaliyev[1], L.A. Temirzhanova[2]**

*[1]Academy of law enforcement agencies under the General Prosecutor's Office of the*
*Republic of Kazakhstan, Nur-Sultan, Kazakhstan*
*[2]L.N. Gumilyev Eurasian National University, Nur-Sultan, Kazakhstan*

**Actual problems of detection and disclosure of criminal offenses committed on the Internet**

**Abstract.** The article examines the problematic issues of identifying and countering criminal offenses committed on the Internet. Analysis of statistical data indicates a significant increase in this type of offenses. The

main share of crimes remains unsolved due to the lack of access to stored information on the use of information systems in the databases of Internet providers, social networks and other organizations. In most cases, the attackers are located outside the country where the stolen funds are transferred. The procedural requirements imposed by the legislator do not allow prompt access to them, which entails the loss of evidence, complicates the search for criminals and stolen funds. The author formulated proposals for improving domestic legislation aimed at strengthening public policy measures in terms of protecting the constitutional rights of citizens.

**Keywords:** Internet, cybercrime, electronic evidence, malware, IP-adress, information systems, disclosure, social networks, international cooperation.

**References**

1. Postanovlenie Pravitel'stva Respubliki Kazahstan ot 12 dekabrya 2017 goda №827 «Ob utverzhdenii Gosudarstvennoj programmy «Cifrovoj Kazahstan»»// https://adilet.zan.kz/rus/docs/P1700000827.

2. Deyatel'nost' organov vnutrennih del po bor'be s prestupleniyami, sovershennymi s ispol'zovaniem informacionnyh, kommunikacionnyh i vysokih tekhnologij. Uchebnoe posobie: v 2 ch. / A.V. Anosov i dr. – M.: Akademiya upravleniya MVD Rossii, 2019. – CH. 1 – 208 s.

3. Arhiv Komiteta informacii Ministerstva informacii i obshchestvennogo razvitiya Respubliki Kazahstan, 2021.

4. Global Cybersecurity Index 2020//https://www.itu.int/en/myitu /Publications /2021/06/28/13/22/Global-Cybersecurity-Index-2020.

5. Meshcheryakov V.A. «Virtual'nye sledy pod skal'pelem Okkama» // Informacionnaya bezopasnost' regionov. 2009. №1(4). S. 28-33.

6. Lytkin N.N. Ispol'zovanie komp'yuterno-tekhnicheskih sledov v rassledovanij prestuplenij protiv sobstvennosti// - avtoref. dis…kand. yurid. nauk. M., 2007. 24 s.

7. Milashev V.A. Problemy taktiki poiska, fiksacii i iz»yatiya sledov pri nepravomernom dostupe k komp'yuternoj informacii v setyah EVM: avtoref. dis…kand. yurid. nauk. 2004. 24 s.

8. Prikaz i.o. Ministra informacii i kommunikacij Respubliki Kazahstan ot 23 maya 2018 goda № 226 «Ob utverzhdenii Pravil registracii abonentskih ustrojstv sotovoj svyazi». Zaregistrirovan v Ministerstve yusticii Respubliki Kazahstan 11 iyunya 2018 goda № 17028.

9. Arhiv Departamenta kriminal'noj policii MVD Respubliki Kazahstan, 2021.

10. Doklad General'nogo sekretarya GA OON «Protivodejstvie ispol'zovaniyu informacionno-kommunikacionnyh tekhnologij v prestupnyh celyah» S.26-27. https://www.unodc.org/documents/Cybercrimer /SG_report/V1908184_R.

11. «Konvenciya o prestupnosti v sfere komp'yuternoj informacii» (ETS №185) (Zaklyuchena v g.Budapeshte 23.11.2001).

**Сведения об авторах:**

***Имангалиев Н.К.*** – главный научный сотрудник Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан, к.ю.н., ассоциированный профессор, старший советник юстиции, Нур-Султан, Казахстан.

***Темиржанова Л.А.*** – к.ю.н., доцент кафедры Евразийского национального университета им. Л.Н. Гумилева, советник юстиции в отставке, адвокат Коллегии адвокатов, Нур-Султан, Казахстан.

***Imangaliev N.K.*** – Chief Researcher of the Academy of Law Enforcement Agencies under the General Prosecutor's Office of the Republic of Kazakhstan, Ph.D. in Law, Associate Professor, Senior Counselor of Justice; Nur-Sultan, Kazakhstan.

***Temirzhanova L.A.*** – Ph.D. in Law, Associate Professor of the Department of the Eurasian National University. L.N. Gumilyova, retired Counselor of Justice, lawyer of the Nur-Sultan Bar Association; Nur-Sultan, Kazakhstan.