Темиржанова Ляззат Ахметжановна,
канд. юрид. наук, доцент Евразийского Национального университета им. Л.Н. Гумилева, советник юстиции (подполковник) в отставке, адвокат Коллегии адвокатов г. Нур-Султан, Республика Казахстан
lyazzat_1805@mail.ru

КИБЕРБЕЗОПАСНОСТЬ В РЕСПУБЛИКЕ КАЗАХСТАН: ПРОБЛЕМЫ, РЕКОМЕНДАЦИИ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРХИЩЕНИЯМ

УДК 343.9

Аннотация. В статье автор рассмотрел состояние обеспечения кибербезопасности в Республике Казахстан, попытался объединить имеющиеся проблемные вопросы в сфере обеспечения кибербезопасности, а также в правоприменительной практике при противодействии киберпреступлениям, кибермошенничеству, киберхищениям, фактически осветив две главы Уголовного кодекса Республики Казахстан (главы 6 и 7). Установлено, что в ходе расследования уголовных правонарушений данной категории, следователи ОВД сталкиваются с проблемными вопросами, связанными с получением информации о принадлежности зарубежных IP-адресов, 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. Проанализированы имеющиеся проблемы, предложены рекомендации по противодействию киберхищениям, мошенничеству, киберпреступлениям.

Цель работы — усовершенствовать методы противодействия киберпреступлениям и отдельным формам хищения (мошенничество, киберхищение). Предмет исследования — исследование уголовно-правовой и криминологической характеристики некоторых видов киберпреступлений; обобщение влияния судебно-следственной практики и результатов противодействия киберпреступлениям заинтересованными государственными органами; определение механизма противодействия.

Методологическую основу исследования составляют общенаучные и частнонаучные методы познания правовых явлений в деятельности правоохранительных и иных государственных органов по противодействию киберхищениям, киберпреступлениям (историко-правовой, сравнительно-правовой, системно-аналитический метод, формально-юридический, статистический, изучение правоприменительной практики по конкретным уголовным делам, касающимся киберпреступлений и киберхищений, и др.).

Ключевые слова: противодействие, мошенничество, киберхищение, кибербезопасность, киберпреступления, рекомендации, уголовное право, процесс.

Lyazzat A. Temirzhanova,
Ph.D in Law, Associate Professor of the Eurasian National University named after L.N. Gumilyov, retired counselor of justice (lieutenant colonel), lawyer of the Nur-Sultan Bar Association, The Republic of Kazakhstan
lyazzat_1805@mail.ru

CYBER SECURITY IN THE REPUBLIC OF KAZAKHSTAN: PROBLEMS, RECOMMENDATIONS FOR COUNTERACTION OF CYBER HUNTERS

Abstract. In the article, the author examined the state of cybersecurity provision in the Republic of Kazakhstan. The author tried to combine the existing problematic issues in the field of cybersecurity, as well as in law enforcement practice in countering cybercrime, cyber fraud, cyber theft, in fact, highlighting two chapters of the Criminal Code of the Republic of Kazakhstan (chapters 6 and 7).

It has been established that during the investigation of criminal offenses of this category, investigators of the Internal Affairs Directorate are faced with problematic issues related to obtaining information about the ownership of foreign IP addresses, the ownership of mobile phones and electronic wallet numbers, as well as a qualified inspection of equipment, since even when deleting electronic information certain data may remain on the digital medium.

The existing problems are analyzed, recommendations for countering cyber theft, fraud, and cybercrimes are offered.

The aim of the work is to improve methods of countering cybercrimes and certain forms of theft (fraud, cyber theft). The subject of the research is the study of criminal law and criminological characteristics of some types of cybercrimes; generalization of the impact of forensic practice and the results of countering cybercrimes by interested government agencies; determination of the countermeasure mechanism.

The methodological basis of the study is made up of general scientific and private scientific methods of cognition of legal phenomena in the activities of law enforcement and other state bodies to counter cyber-robbery, cybercrimes (historical-legal, comparative-legal, system-analytical method, formal legal, statistical, study of law enforcement practice on specific criminal cases related to cybercrimes and cyber-theft, and others).

Keywords: counteraction, fraud, cyber theft, cyber security, cyber crimes, recommendations, criminal law, process.

Обеспечение информационной безопасности государственных органов, физических и юридических лиц, а также выработки механизмов предупреждения и оперативного реагирования на инциденты информационной безопасности наглядно показывает принятие в 2017 г. в Республике Казахстан Концепции кибербезопасности «Киберщит Казахстана». Новизна исследования заключается в том, что в Республике Казахстан проведен ряд исследований отдельно по мошенничеству, хищениям, киберпреступлениям. Однако комплексного исследования противодействия мошенничествам и киберхищениям, кибератакам не проводилось. Соответственно, данные научно обоснованные разработки по совершенствованию методов противодействия мошенничеству и киберхищениям (превентивный механизм, пресечение, раскрытие), в том числе путем межведомственного взаимодействия государственных органов, организаций и гражданского общества являются весьма актуальными и востребованными.

Общеизвестно, что 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.

Существующие проблемы — недостаточный уровень подготовки сотрудников органов, осуществляющих противодействие этим явлениям, в части специальных познаний в сфере информатизации и применения компьютерных технологий; некачественные услуги и приложения egov.kz и в казахстанском высшем образовании, которое не предлагает достаточных знаний в информационно-коммуникационной области; недооценка важности противодействия информационным угрозам; в уголовном законодательстве не определены такие ключевые понятия, как киберпреступность, киберпространство, кибербезопасность, киберзащита, обман.

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. 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 повышение грамотности банковских работников и бухгалтеров, непосредственно занимающихся сопровождением финансовых операций.

По имеющимся сведениям прокуратуры ежемесячно служба ГТС (Государственная техническая служба, находящаяся в структуре Комитета Национальной безопасности Республики Казахстан) фиксирует и направляет о 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.

Необходимо отметить общеизвестные и плодотворные проекты Комитета правовой статистки и специальных учетов Генеральной прокуратуры РК. В период с 2011 по 2012 гг. внедрена электронная регистрация всех заявлений и сообщений о преступлениях — книга учета заявлений (КУЗ). С 2015 г. заработал Единый реестр досудебных расследований (ЕРДР). Сегодня регистрация в нем служит началом уголовного процесса.

Интеграция аналитической информационной системы суда «Төрелік» и органов прокуратуры ЕРДР позволила Верховному суду и Генеральной прокуратуре дать старт новому совместному проекту «Заңдылық».

Интернет-портал «Карта уголовных правонарушений», «Карта ДТП», Е-штрафы, информационный сервис «Централизованный банк данных должников «Шектеу», система «Web-АП», система «Электронное уголовное дело — Заңдылық», проект «Е-уголовное дело», который направлен на упрощение и повышение качества уголовного процесса, позволяют минимизировать ошибки следователей, прокуроров и судей страны. Также существуют много других проектов КПСиСУ, которые значительно упростили и оптимизировали правоприменительные процессы.

Данные успешные проекты показали обширный информационный потенциал КПСиСУ, который может быть использован и в целом при обеспечении кибербезопасности электронных систем не только КПСиСУ, а также и всех органов прокуратуры и для проработки вопроса создания информационной системы на базе КПСиСУ мониторинга и отслеживания состояния и обнаружения критической уязвимости в информационно-аналитических системах правоохранительных органов без каких-либо серьезных финансовых затрат.

Необходима консолидация всех государственных и правоохранительных органов в вопросах обеспечения 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.

В Стратегии «Казахстан-2050»: «Новый политический курс состоявшегося государства» указано, что «государство должно следовать принципу нулевой терпимости к беспорядку. Ощущение беспорядка и вседозволенности создает почву для более серьезных преступлений» [1].

В «Плане нации — 100 конкретных шагов по реализации пяти конституциональных реформ» отмечено, что «независимое правосудие и вся правоохранительная система Казахстана должны быть нацелены исключительно на обеспечение прав и свобод граждан, строгое исполнение законов и укрепление правопорядка» [2].

Мошенничество, по сравнению с другими формами хищения, не имеет широкого распространения, но охватывает социально уязвимые слои населения и отличается размерами причиненного ущерба.

Всецело разделяем мнение д-ра юрид. наук, профессора Е.И. Каиржанова, который полагал, что «..на динамику преступности влияют многие факторы, самые важные из них — социальные и юридические. Социальные факторы — это причины и условия преступности, демографическая структура населения, миграция и др. Юридические — это изменения и дополнения в уголовное и административное законодательства, сужающие либо расширяющие сферу преступности» [3]. Для полноты картины выявления имеющихся причин роста мошенничества были изучены статистические данные КПСиСУ РК, аналитические материалы, справки 2-го, 4-го, 10-го Департаментов Генеральной прокуратуры.

Основные проблемные моменты досудебной и судебной практики по делам о мошенничестве.

1. В УК РК нет понятия слова «обман», в этой связи возникают различные толкования обманных действий.

2. В связи с расширением способов, разновидностей мошеннических действий, в том числе с использованием информационных технологий, имеются объективные основания для заимствования Республикой Казахстан, к примеру, опыта России и Германии по введению уголовной ответственности за определенные виды совершения мошеннических действий (например, в сфере страхования, капиталовложения и т.д.).

Одной из проблем являются рост и низкая раскрываемость интернет-мошенничеств, так как сервера и системные администраторы, которые используют преступники, либо данные счета, к примеру «QIWI-кошелька», в основном находятся за пределами страны (аналитические справки 2-го Департамента ГП) [4].

3. Отсутствие нормативного закрепления разграничения уголовно-наказуемых деяний от гражданско-правовых отношений, в связи с этим неоднозначная судебная практика назначения наказаний за мошенничество (аналитические материалы 10-Департамента ГП) [5].

Предлагаемые рекомендации по противодействию киберпреступлениям:

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) (режим работы Центра — круглосуточно, расширить штатную численность группы до 4-х штатных специалистов КПСиСУ и 13 работников подрядной организации, т.е. 17 высококвалифицированных специалистов по кибербезопасности).

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 кибератакам, в том числе и проведения занятий, повышающих уровень компьютерной грамотности в сфере кибербезопасности сотрудников правоохранительных органов.

4. Дополнить ст. 3 УК РК понятиями, касающимися кибербезопасности (перечень которых взять из Концепции «Киберщит», утвержденной Постановлением Правительства РК № 30 от 30 июня 2017 г.).

5. Ужесточить санкцию статей киберпреступлений, которые совершены в отношении информационных систем государственных органов (по опыту США), это послужит эффективной мерой противодействия.

Рекомендации по противодействию киберхищениям, мошенничеству:

1. Диспозицию статьи 190 УК Республики Казахстан дополнить понятием «Обман» на примере УК Франции.

Часть 1 статьи 190 (мошенничество) УК РК изложить в следующем виде: мошенничество, т.е. хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием либо иным противоправным путем, при этом под обманом понимать — обман (введение в заблуждение, злоупотребление доверием, иной противоправный способ) физического или юридического лица, совершенный путем использования ложного имени, должности или положения, а также злоупотребления служебным положением либо путем использования обманных действий в целях побуждения лица к передаче денежных средств, ценностей или иного имущества, оказанию услуг или предоставлению документа, содержащего обязательство или освобождение от обязательства в ущерб себе или третьим лицам.

2. Дополнить ч. 2 ст. 190 УК РК (мошенничество) следующими квалифицирующими признаками (по примеру УК РФ), пунктами 6, 7, 8, 9, 10, 11, 12:

П. 6) в сфере дистанционного банковского обслуживания, в предоставлении банковских услуг;

П. 7) в сфере страховой деятельности;

П. 8) в сфере кредитования;

П. 9) при получении выплат;

П. 10) в сфере предпринимательской деятельности;

П. 11) в сфере компьютерной информации;

П. 12) при капиталовложении.

3. Увеличить санкцию ч. 2 ст. 190 УК — штраф до 6000 МРП, ограничение свободы увеличить до 7 лет, лишение свободы — до 7 лет.

4. С целью правильности формирования практики рассмотрения дел по мошенничеству Верховному Суду РК разработать новое Нормативное постановление Верховного Суда РК «О судебной практике по делам о мошенничестве», разъясняющего сложные вопросы квалификации мошеннических деяний против собственности и в сфере экономической деятельности, а также в практике назначения судами наказаний за деяния этого вида.

Также необходимо в нем более подробно изложить признаки мошенничества с учетом возникающих договорных отношений. Кроме того, разграничить, регламентировать, какие действия являются гражданско-правовыми отношениями, а какие имеют признаки состава преступления.

Следует создать единый электронный реестр на платформе технологий блокчейн (блокчейн-транзакций) и внедрить его в электронное правительство, которое исключит факты, способствующие мошенничеству в сфере государственных услуг, сделок с недвижимостью, долевого строительства, страховой деятельности и т.д. Предоставить доступ к базам, на основе технологий блокчейн (блокчейн-транзакций) нотариусам.

Ожидаемый эффект по предлагаемым нормам:

1. Сформулированная содержательная и объемная дефиниция «обман», которая, будучи законодательно закрепленной в ст. 190 УК, дополнит диспозицию статьи, соответственно уточнит и разъяснит саму статью и снимет проблемы правоприменительной практики, устранит коллизии в законодательстве.

2. Увеличение квалифицирующих признаков и верхнего предела санкции части 2 статьи 190 УК РК позволит расширить спектр карательного воздействия на лиц, изобретающих новые виды мошенничества. Позволит в правоприменительной практике пресекать мошенническую деятельность в различных сферах правоотношений (в страховании, сфере финансово-кредитных отношений и пр.).

3. Законодательное регулирование договора условного депонирования (эскроу) и новая разновидность банковского счета — эскроу-счет, обеспечит исполнение обязательств и максимальное снижение возможных рисков подлога и мошенничества.

Вносимые нами предложения всецело имеют профилактическую направленность, нацелены на борьбу с мошенничеством, кибермошенничеством, киберхищениями, киберпреступлениями, а также имеют и социальную направленность — быть бдительными, чтобы не стать жертвой мошенников, а также, чтобы и потенциальные мошенники, прежде чем совершить преступление, задумались — стоит ли оно того.

СПИСОК ЛИТЕРАТУРЫ

1. Стратегия «Казахстан-2050»: «Новый политический курс состоявшегося государства»: Послание Президента Республики Казахстан — Лидера нации Н.А. Назарбаева народу Казахстана, г. Астана, 14 декабря 2012 г. [Электронный ресурс]. URL: https://www.akorda.kz/ru/events/astana_kazakhstan/participation_in_events/poslanie-prezidenta-respubliki-kazahstan-lidera-nacii-nursultana-nazarbaeva-narodu-kazahstana-strategiya-kaz...
2. «План нации — 100 конкретных шагов по реализации пяти конституциональных реформ» от 6 мая 2015 [Электронный ресурс]. URL: https://online.zakon.kz/Document/?doc_id=31977084
3. Каиржанов Е.И. Криминология. Общая часть. Алматы: Рик, 1995. С. 41.
4. Аналитические материалы 2-го Департамента ГП РК.
5. Аналитические материалы 10-го Департамента ГП РК.
6. Аналитические материалы 4-го Департамента ГП РК.