UDC: 343.98:343.72(045)(575.1)

ТАКТИЧЕСКИЕ ОСОБЕННОСТИ ДОПРОСА ЛИЦ, ПОДОЗРЕВАЕМЫХ В СОВЕРШЕНИИ КИБЕРМОШЕННИЧЕСТВА (НА ПРИМЕРЕ ФИШИНГА)

Сабырбаева Айнура Бахыт кызы,
доктор философии по юридическим наукам (PhD),
преподаватель кафедры «Уголовно-процессуальное право»
Академии МВД Республики Узбекистан
ORCID: 0000-0002-8364-5319
e-mail: ww.a_sabyrbaeva@inbox.ru

Аннотация. *В статье рассматриваются тактические особенности производства допроса подозреваемых в совершении кибермошенничества, а также разработан примерный перечень вопросов, который необходимо задать подозреваемым в совершении фишинговых атак. В статье описаны виды фишинговых атак, а также наиболее опасные способы его совершения. Описан один из видов кибермошенничества с использованием приложения «Осон кредит», который направлен на захват конфиденциальных данных пользователей, таких как данные банковской карты, получение доступа к аккаунтам в социальных мессенджерах, видео-, фотофайлам, а также документам, находящимся на телефонном устройстве, к которому злоумышленники получили доступ. Рассмотрены наиболее часто встречающиеся в судебно-следственной практике ошибки, допускаемые следователями ввиду незнания специальной терминологии, особенностей расследования новых видов мошеннических посягательств – кибермошенничества. Изучение тенденций развития преступлений в сфере экономики говорит о необходимости разработки новых действенных и эффективных методов по расследованию кибермошенничества. С учетом анализа статистики киберпреступлений за последние несколько лет можно прийти к выводу о необходимости усиления противодействия новым видам киберпреступлений, таким как кибермошенничество, фишинг, смишинг, кардинг и т. д.*

Ключевые слова: *фишинг, допрос, киберпреступления, мошенничество, алгоритм, подозреваемый.*

KIBERFIRIBGARLIKNI SODIR ETISHDA GUMON QILINGAN SHAXSLARNI SO‘ROQ QILISHNING TAKTIK XUSUSIYATLARI (FISHING MISOLIDA)

Sabirbayeva Aynura Baxit qizi,
O‘zbekiston Respublikasi Ichki ishlar vazirligi akademiyasi,
Jinoyat-protsessual huquqi kafedrasi o‘qituvchisi,
yuridik fanlar bo‘yicha falsafa doktori (PhD)

Annotatsiya. *Maqolada kiberfiribgarlikni sodir etishda gumon qilingan shaxslarni so‘roq qilishning taktik xususiyatlari o‘rganilgan, shuningdek, fishing hujumlarida gumon qilinuvchilarga berilishi kerak bo‘lgan savollarning taxminiy ro‘yxati ishlab chiqilgan. Maqolada fishing hujumlarining turlari, shuningdek, uni sodir etishning eng xavfli usullari keltirilgan. “Oson Credit” ilovasidan foydalangan*

holda, kiberfiribgarlik turlaridan biri tavsiflangan bo'lib, bu firibgarlik turi foydalanuvchilarning maxfiy ma'lumotlari, ayniqsa, bank karta ma'lumotlarini egallab olish, ijtimoiy tarmoqlardagi akkauntlarga kirish, jinoyatchilar telefon vositasiga kirish imkoniyatini qo'lga kiritgan va telefonda mavjud bo'lgan video, foto fayllar, hujjatlarni egallashga qaratilgan. Maqolada sud-tergov amaliyotida tergovchilar tomonidan maxsus terminologiya, firibgarlikning yangi turlarini tergov qilish xususiyatlarini bilmaslik tufayli eng ko'p tarqalgan xatolar ko'rib chiqilgan. Iqtisodiy sohadagi jinoyatlarning rivojlanish tendensiyalarini o'rganish natijasida kiberfiribgarliklarni tergov qilishning yangi samarali usullarini ishlab chiqish zarurati aniqlangan. Kiberjinoyatchilikning oxirgi yillardagi statistikasi tahliliga ko'ra, firibgarlikning yangi turlari, ya'ni fishing, smishing, karding va h.k.larga bo'lgan kurashni yanada kuchaytirish zaruriyati to'g'risida fikr yuritilgan.

Kalit so'zlar: *fishing, so'roq, kiberjinoyat, firibgarlik, algoritm, gumon qilinuvchi.*

TACTICAL FEATURES OF THE INTERROGATION OF PERSONS SUSPECTED OF COMMITTING CYBERFRAUD (USING THE EXAMPLE OF PHISHING)

Sabyrbayeva Ainura Bakhyt kyzy,
Lecturer of the Department Criminal Procedural Law,
Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan,
Doctor of Philosophy (PhD) in Law

Abstract. *The article discusses the tactical features of the interrogation of suspects in the commission of cyber fraud, and also developed an approximate list of questions that should be asked to suspects in phishing attacks. The article describes the types of phishing attacks as well as the most dangerous ways to commit them. One of the types of cyber fraud using the Oson Credit application is described, which is aimed at capturing confidential user data, such as bank card data, gaining access to accounts in social messengers, video, photo files and documents located on a telephone device to which the attackers gained access. The article considers the most common mistakes in forensic investigative practice made by investigators due to ignorance of special terminology, and features of the investigation of new types of fraudulent encroachments - cyber fraud. The study of trends in the development of crimes in the economic sphere suggests the need to develop new effective and efficient methods for investigating cyber fraud. Considering the analysis of cybercrime statistics over the past few years, it can be concluded that it is necessary to strengthen counteraction to new types of cybercrime, such as cyberfraud, phishing, smishing, carding, etc.*

Keywords: *phishing, interrogation, cybercrime, fraud, algorithm, suspect.*

Введение

Современные информационно-телекоммуникационные технологии приобрели глобальный трансграничный характер и стали неотъемлемой частью всех сфер деятельности общества. В то же время процесс глобальной цифровизации жизни человечества вызвал стремительный рост масштабов преступности в сфере информационно-телекоммуникационных технологий. Основной тенденцией современной преступности в рассматриваемой сфере является совершение кибермошенничества, которое, согласно статистике, на территории нашей страны увеличилось за последние 3 года в 13 раз [1].

По данным центра жалоб на интернет-преступления ФБР, мошеннические действия типа BEC привели к фактическим потерям в размере более 4,5 млрд долларов, и они представляют собой глобальную проблему [2]. Опасность такого вида кибермошенничества, как фишинг, заключается в призыве незамедлительно ответить на спам-сообщение или перейти по ссылке из-за якобы чрезвычайной

срочности дела, что приводит к утрате бдительности потерпевших и внесению конфиденциальных данных.

К слову, фишинг (от англ. *phishing*, от *fishing* – рыбная ловля, выуживание) – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям [3].

Фишинговые атаки направлены на дезинформацию потенциальной жертвы и побуждение перейти ее по ссылке, базируясь на таких человеческих качествах, как неосторожность, торопливость, невнимательность. Появились рассылки по социальным сетям о возможности выигрыша телефона марки Samsung или iPhone при ответе на поставленные вопросы, в конце потерпевшего объявляют победителем и просят ввести свои конфиденциальные данные и написать код подтверждения, пришедший на телефон, введение их достаточно для получения злоумышленниками доступа к системе онлайн-банкинга жертвы. Ссылка на фишинговое письмо может выглядеть примерно так: go2ere.com/NGF1enV6.

Материалы и методы

В ходе исследования использовались общенаучные и специальные методы научного познания: исторический, системный, сравнительно-правовой, аналитический, логико-юридический и другие, которые позволили в определенной степени обеспечить достоверность и обоснованность результатов настоящего исследования.

Результаты исследования

Ошибки в практической деятельности следственных подразделений указывают на необходимость разработки новой методики по расследованию кибермошенничества, так как традиционная методика не предусматривает тактику проведения следственных действий по выявлению и расследованию новых видов мошенничества, привлечение при расследовании фишинга IT-специалистов, назначение судебной компьютерно-технической экспертизы и т. д. Также необходимо расширить штатные подразделения следственных органов с повсеместным повышением квалификации специалистов, расследующих кибермошенничество и прохождением ими переподготовки за рубежом, а также налаживанием тесного сотрудничества с правоохранительными органами зарубежных стран и обмена опытом по противодействию новым проявлениям кибермошенничества.

Одной из ключевых особенностей расследования кибермошенничества является производство допроса подозреваемого лица. Проблемой при допросе подозреваемых в совершении новых видов мошенничества, таких как мошенничество с использованием информационно-коммуникационных сетей, систем или программ обеспечения (кибермошенничество), является наличие специальной терминологии, требующей более тщательного и углубленного изучения и осмысления со стороны допрашивающего.

Основаниями для привлечения лица к участию в уголовном деле в качестве подозреваемого по делам о кибермошенничестве могут быть:

- показания потерпевшего лица, указывающие на его причастность к совершению мошенничества (переписка в социальных мессенджерах);

- представление потерпевшим лицом документов, подтверждающих вину лица (звукозапись переговоров по телефону);

- показания свидетелей (показания от представителя администрации торговых онлайн-площадок со сведениями об аккаунте и прикрепленном к нему номере);

- справка о банковских операциях (перевод денежных средств потерпевшего на счет подозреваемого лица);

E-ISSN 2181-1148
ISSN 2181-919X

- справка от администрации электронных систем платежа о денежных переводах, осуществленных с банковской карты посредством системы онлайн-банкинга;

- справка о владельце телефонного средства, с которого велись переговоры с потерпевшим лицом;

- ответ на оперативное задание о причастности лица к совершению мошенничества;

- показание других подозреваемых о совершении мошенничества в преступном сговоре;

- протокол осмотра и изъятия электронных, вещественных или письменных доказательств (наличие на телефонном устройстве, в средствах компьютерной техники: переписки в социальных мессенджерах, отчета в программах онлайн-банкинга о пополнении счета, следов программ для создания фишингового письма).

Данный перечень не является исчерпывающим и в зависимости от ситуации может варьироваться. Иногда достаточно и свидетельских показаний для привлечения лица к участию в деле в качестве подозреваемого.

В случае установления личности преступника либо лица, на чей счет поступили денежные средства (стоит отметить, что не всегда это лицо может быть преступником или пособником), то следует незамедлительно провести его допрос с привлечением его к участию в деле в качестве подозреваемого.

В случаях когда подозреваемое лицо было заранее известно, и в ходе доследственной проверки были получены первичные показания в виде объяснительных, то допрос фактически будет являться повторным изложением ранее данных показаний, что позволяет более тщательно подготовиться к допросу лица в связи с наличием предварительной информации о занимаемой им позиции, в особенности к допросу лиц, изначально выбравших позицию дачи заведомо ложных показаний (в данной ситуации необходимо тщательно подготовиться к допросу путем составления предварительных вопросов, изучения анкетных данных).

Список вопросов может варьироваться в зависимости от сложившейся следственной ситуации, личности преступника или жертвы, имеющихся противоречий, занимаемой позиции подозреваемого (отрицание или признание вины), способа совершения мошенничества. Однако существуют некоторые обстоятельства, подлежащие доказыванию (к примеру, время, место, способ совершения мошенничества, сумма причиненного ущерба), и установление их в ходе допроса является важным. Доказательственное значение могут иметь мельчайшие детали, которые на взгляд подозреваемого лица могут быть маловажными.

По мнению С.Н. Казинской, «в условиях отсутствия явных следов преступной деятельности необходимо предъявлять подозрения в совершении преступления при осуществлении следственных и иных процессуальных действий, направленных на сбор доказательств, с учетом фактора внезапности» [4]. Это касается случаев, когда мошенник не уверен в наличии доказательств у следственных органов, а по материалам уголовного дела фактически нет весомых доказательств. В таком случае необходимо использовать имеющиеся в материалах уголовного дела доказательства таким образом, чтобы у мошенника возникло преувеличенное представление об имеющихся в отношении него доказательств.

В случае отрицания причастности подозреваемого к совершенному преступлению необходимо установить его местонахождение в момент совершения преступления, имеется ли алиби у него, есть ли лица, которые могут подтвердить его

присутствие. Нельзя применять по отношению к нему пытки либо иные унижающие его честь и достоинство действия и стараться заставить его «взять на себя вину», так как если даже под таким давлением он признается, то в суде, возможно, все равно будет говорить «свою правду».

В первом случае, когда подозреваемый признает свою вину полностью, то необходимо задать следующие вопросы: когда он зарегистрировался на торговой онлайн-платформе, социальном мессенджере либо когда создал электронную почту; степень его образования; имеет ли какие-либо навыки по созданию фишинговых сайтов, образование в IT-сфере; когда возник умысел создания фишингового сайта либо письма; с помощью какой программы он создавал фишинговое письмо или сайт, обучался ли он этому у кого-то, какую компьютерную технику он использовал, чтобы войти в систему; как он выбирал жертву, скольким жертвам направили фишинговое письмо и сколько из них стали жертвами, как он понимал, что жертва «попалась на крючок»; на что ориентировался при пересылке данных писем, была ли у него программа по автоматической рассылке писем (название программы) либо он все делал вручную; были ли у него подельники (при утверждении, что он сам все создал можно провести эксперимент – сможет ли он сам создать такое письмо или сайт); схема совершенного мошенничества, как он выуживал конфиденциальные данные и какие именно (логин, пароль к аккаунту или электронной почте, номер банковской карты, пин-код и т. д.); какие действия предполагалось провести самой жертве, как работал данный механизм, сколько процессов необходимо было пройти жертве, что обещалось жертве (получение выигрыша в лотерее, подарок, скидки, купоны); какова была мотивация; название сайта или фишингового письма, от чьего имени оно приходило; как приходило уведомление о введенных данных жертвы, с помощью какой компьютерной техники производились все операции, где она находится, марка, модель, наименование компьютерной техники либо другого устройства (ноутбук, планшет, телефон), с которого производилась фишинговая атака, кому она принадлежит, сколько средств техники было задействовано в ходе фишинговой атаки, какая программа обеспечения функционировала на компьютере; в течение какого периода времени рассылались данные письма; кто писал содержание фишингового письма (сам или скачал готовый образец письма через сеть Интернет), если скачал, то когда и с какого сайта, была ли произведена оплата деньгами (на банковский счет или электронными деньгами); когда и кем был зарегистрирован фишинговый сайт, период его действия (до какого числа оплачено); учитывались ли особенности определенного круга жертв либо письмо было шаблонное; со скольких аккаунтов пересылались письма, на какой телефонный номер они были зарегистрированы; как создавался фишинговый сайт, какой сайт служил основой для его фальсификации (так как в основном подделывается реальный узнаваемый большинством сайт, такие как Olx, Adidas, AliExpress и др.); какие способы использовались для получения денежных средств со счетов потерпевших; как они использовали данные, полученные у потерпевших (электронная почта, аккаунт в торговой онлайн-площадке, банковская платежная карта), ведь даже при завладении номером банковской карты без пароля доступа снятие с нее денежных средств невозможно (может быть, на сайте необходимо подтвердить банковскую платежную карту специальным кодом, направленным на телефонный номер, к которому прикреплена платежная карта), использовалась ли специальная программа для автомати-

E-ISSN 2181-1148
ISSN 2181-919X

ческого подключения номера банковской карты к приложению для дальнейшего снятия либо перенаправления денежных средств, создавалась ли копия банковских платежных карт, в общем весь процесс завладения денежными средствами потерпевших; как осуществлялось завладение денежными средствами, на какую платежную карту (Ф.И.О. владельца карты) были переведены средства, к какой международной онлайн-платформе купли-продажи типа Olx или AliExpress подключены; какая сумма была снята, где были обналичены денежные средства, в каких целях были растрачены; общее количество жертв преступлений и общий объем нанесенного им урона.

Данные вопросы являются далеко не исчерпывающими, и в зависимости от обстоятельств могут быть заданы дополнительные вопросы. Данные моменты должны быть уточнены в ходе самого процесса допроса, если что-то упущено в ходе свободного рассказа – выяснить путем дополнительных вопросов.

Говоря о международном опыте расследования современных способов мошенничества, Ассоциация сертифицированных специалистов по расследованию мошенничества (ACFE) рекомендует проводить допрос в прямой, непрямой либо комбинированной форме. Они различают два порядка последовательности задавания вопросов. Первый – последовательность конусов, то есть порядок направлен на эмоционально раздражительных и вспыльчивых допрашиваемых – метод от общего к частному. Второй – последовательность перевернутых конусов – направлен на разговорчивых допрашиваемых – метод от частного к общему. Но считаем не совсем уместными некоторые из их методов производства допроса. Так, к примеру, они различают два вида задавания дополнительных вопросов: подтверждающие или нет вопросы, то есть допрашивающий задает вопросы с целью получения одобрения и подтверждения. Например, вы отправили фишинговое письмо гражданину Н., не так ли? Это один из видов наводящего вопроса. Второй способ допроса: прямо задаются наводящие вопросы. Допрашиваемый направляет допрашиваемого по одному направлению, а сам идет по-другому. Во время допроса допрашиваемый сам рассказывает, что, якобы, по его мнению, произошло, убеждая в этом допрашиваемого, а потом сам подходит с противоположной, опровергающей данную гипотезу стороны. В соответствии с национальным законодательством данный принцип противоречит закону и категорически запрещен. Это банальное введение в заблуждение лица, пользуясь его доверчивостью, страхом либо податливостью.

В случае частичного признания вины необходимо установить, в какой мере и части он признает и отрицает свою вину, что именно в материалах уголовного дела, по его мнению, не совпадает с «реальным» событием. Важно помнить, что следствие должно опираться на имеющиеся доказательства и никак не привязывать ход следствия к установившейся гипотезе или следственной версии (в противном случае теряется объективность хода расследования).

Анализ результатов исследования

Изменения, внесенные в УПК 18 февраля 2021 года, касающиеся введения нового института – «соглашения о признании вины», явились новшеством. На практике следователи и дознаватели начали пользоваться возможностями данного института, так как он обладает рядом преимуществ, одним из которых является упрощение механизма производства предварительного расследования, экономия временных и материальных затрат, «бумажной» волокиты, необходимости поиска новых доказательств, производства следственных действий и т. д. Дан-

ная возможность «заключения сделки» разъясняется подозреваемым или обвиняемым лицам. С одной стороны, данный институт обладает рядом преимуществ, но все же необходимо акцентировать внимание и на другую сторону медали, когда в некоторых случаях, не желая вдаваться в подробности, искать улики, следователи и дознаватели могут добиться «признания вины и заключения сделки» с невиновным лицом, что приведет к осуждению невиновного и оставлению истинно виновного безнаказанным, либо к осуждению лица по статье менее тяжкой, нежели ему инкриминируется.

Как отметил Р.В. Новак, «процедура заключения соглашения о признании вины подробно регламентируется Федеральными правилами уголовного процесса в окружных судах США (1997 г.), в соответствии с п. 11 которых соглашение о признании вины является письменным соглашением обвиняемого и защитника, с одной стороны, и стороны обвинения – с другой, в котором стороны договариваются о конкретном разрешении уголовного дела, включая все пункты обвинения и наказания обвиняемого. Суть этого соглашения заключается в том, что обвиняемый признает себя виновным в менее тяжком преступлении, чем фактически сделал, а в обмен на это лицо, которое поддерживает обвинение, требует назначения более мягкого наказания, чем то, которое могло бы быть» [5].

Как бы уголовно-процессуальное законодательство не стремилось к принципу «непредвзятости и объективности», нельзя исключить человеческий фактор, который может привести к должностным преступлениям. Есть опасность, что защитники вместо осуществления защиты своих подопечных могут перейти на сторону следователей или дознавателей и уговорить подзащитных на заключение «сделки» во избежание волокиты.

В.Н. Махов и М.А. Пешков объясняют, что более 90 % уголовных дел в США не проходят через процедуру судебного разбирательства в связи с тем, что в одних случаях признание вины влечет за собой упрощенную процедуру в суде, а в других – органы предварительного расследования без признания обвиняемым вины не в состоянии обеспечить сбор доказательств, изобличающих обвиняемого, поэтому заключается так называемая сделка о признании вины [6]. Поэтому необходимо во всех случаях тщательно производить проверки по фактам применения данного института, чтобы избежать привлечения невиновных, которые соглашаются только из-за оказания психического или иного давления, угроз, убеждения, что он якобы «будет осужден в любом случае».

Как справедливо отметила А.А. Прокопенко: «Ускорение судопроизводства за счет исключения процессуальных гарантий тем более опасно, поскольку весьма затруднительно определить предел, за которым искоренение гарантий из процессуальной формы следует остановить» [7]. Ряд ученых высказались против данного института, полагая: «Признание подозреваемым своей вины тут может быть положено в основу обвинения, а полнота доказывания не обеспечивается в полной мере. Факт признания лицом своей вины создает границы, за пределами которых остается принцип всестороннего, полного и объективного исследования обстоятельств дела» [8].

Правоведы в области уголовного судопроизводства США считают, что большинство подсудимых, заключивших сделку о признании вины, поступают невольно, что приводит в итоге к значительному росту числа невиновных. Данный факт вызывает озабоченность в обществе по поводу конституционности [9].

Хотелось бы отметить необходимость соблюдать требования закона при приня-

E-ISSN 2181-1148
ISSN 2181-919X

тии решения о признании вины, взвесить все «за» и «против» во избежание привлечения к уголовной ответственности невиновного лица, а также инкриминирования вины намного меньшей, чем действительно совершенной. Хотя данный тактический подход может принести положительные результаты, но существует риск нарушения норм закона.

При отрицании вины подозреваемым необходимо направить все силы и средства на сбор доказательственной информации посредством проведения следственных действий: допроса потерпевшего, свидетелей, назначения экспертиз, обыска, направления соответствующих запросов. И, получив достаточно весомые доказательства, следует, воспользовавшись тем, что мошенник знает только ту информацию, которая имелась в материалах доследственной проверки, провести допрос, выслушивая его показания и делая заметки, после чего представлять ему доказательства по мере возрастания доказательственного значения, не давая времени для обдумывания новой тактики для обмана, чтобы мошенник, осознав, что его вина доказана, начал давать правдивые показания.

Необходимо установить наличие образования в IT-сфере и технологиях, его алиби с предупреждением, что новые технологии и привлечение IT-специалистов, распечатки с банковских учреждений, возможности камер видеонаблюдения позволяют раскрыть любое преступление. При этом не оказывая какого-либо давления на подозреваемое лицо.

При даче ложных показаний допрашиваемые подозреваемые от неестественно построенных «вариантов случившегося» «загромождают» свою память, соотнося это с действительностью и, в конце концов, сами запутываются в сетях лжи. Чем больше человек говорит неправду, тем больше вероятность оговориться. Следует применить тактику задавания прямых вопросов касательно начала, середины или конца рассказа, чтобы ввести допрашиваемого в тупик и подвести к даче правдивых показаний. Эффективным методом разоблачения ложных показаний является «рассказ в обратной последовательности». Даже в случае усиленной подготовки повторить все до «мельчайших подробностей» затруднительно.

Целесообразно детально уточнить его «алиби», место его пребывания в момент совершения преступления, имеется ли платежная карта, на чье имя открыта и когда, в каком банке, наличие смс-информирования о транзакциях банковского счета, кто имеет доступ к данной карте, к какому номеру телефона она прикреплена, какая сумма денег поступает ему ежемесячно (заработная плата), сколько денежных средств поступило в определенный период времени, источник их поступления, сколько он истратил, имеется ли у него аккаунт в социальных сетях, если да, то когда он зарегистрировался, в каком социальном мессенджере, когда заходил в последний раз, с какого технического средства (личный компьютер или рабочий, личный телефон или членов семьи, личный планшет или друга), кто еще имеет доступ к аккаунту, со скольких технических средств осуществлялся вход в данный аккаунт (к примеру, из рабочего компьютера, личного телефона и планшета члена семьи), когда он в последний раз заходил в свой аккаунт, с кем переписывался, не было ли странных переписок, о которых он сам не знал, осуществлял ли он выход после использования данными аккаунтами с чужих технических средств (компьютер или планшет). Вопросы должны быть составлены не с позиции доказывания вины, а установления истины, действительной причастности к преступлению, и варьироваться исходя из имеющихся в деле доказательств.

Выводы

Таким образом, в зависимости от следственной ситуации необходимо подобрать соответствующую тактику допроса подозреваемого и направить все действия на установление всей логической последовательности совершения преступления – с момента возникновения умысла завладения денежными средствами до момента их растраты, снятия либо перевода. Особую трудность в данном случае представляет перевод денежных средств в офшорные счета другой страны типа Бангладеш, Таиланд и т. д. Так как с этими странами не подписаны соответствующие договора, и получить сведения о данных транзакциях представляется затруднительным, что приводит в большинстве случаев к приостановлению уголовного дела по пункту 1 части 1 статьи 364 УПК Республики Узбекистан, на что и рассчитывают мошенники. Данная проблема существует ввиду отсутствия единого международного механизма, системы и договоров для урегулирования вопросов оказания сотрудничества для борьбы с данным видом преступлений, что предполагает необходимость разработки единого международного документа на базе ООН «О противодействии кибермошенничеству», обязательного для исполнения всеми странами-членами ООН.

От правильного выбора тактики производства допроса подозреваемого лица и последовательности задаваемых вопросов зависит ход расследования в целом, что позволит получить необходимую информацию касательно фактов кибермошенничества, а также всесторонне и тщательно проверить, сопоставить имеющиеся факты, установить истину и привлечь виновных лиц к ответственности.

REFERENCES

1. Statistika Tsentra kiberbezopasnosti MVD Respubliki Uzbekistan [Statistics of the Cybersecurity Center of the Ministry of Internal Affairs of the Republic of Uzbekistan]. International Scientific and Practical Conference of the Academy of the Ministry of Internal Affairs. 2022, February 23.

2. Bezmaly V. Tipy fishingovykh atak i sposoby ikh vyyavleniya [Types of Phishing attacks and how to detect them]. 2019, April, 19. Available at: https://www.osp.ru/winitpro/2019/03/13054903/.

3. Phishing. From Wikipedia, the free encyclopedia. Available at: https://ru.wikipedia.org/wiki/%D0%A4%D0%B8%D1%88%D0%B8%D0%BD%D0%B3/.

4. Kazinskaya S.N. Metodika rassledovaniya moshennichestva v sfere potrebitel'skogo rynka v otnoshenii predprinimateley [Methodology for investigating fraud in the consumer market in relation to entrepreneurs]. Abstract of PhD thesis. Moscow, 2011. Available at: https://www.dissercat.com/content/metodika-rassledovaniya-moshennichestva-v-sfere-potrebitelskogo-rynka-v-otnoshenii-predprini/.

5. Novak R.V. Institut sdelok o priznanii viny v zarubezhnykh stranakh: sravnitel'no-pravovoy aspect [The institution of plea bargains in foreign countries: a comparative legal aspect]. *Chelovek: prestupleniye i nakazaniye – MAN: crime and punishment*, 2013, no. 4 (83), p. 147.

6. Makhov V., Peshkov M. Sdelka o priznanii viny [Plea deal]. *Russian justice*, 1998, no. 7, p. 17.

7. Prokopova A.A. Protsessual'noye soglasheniye o priznanii viny v ugolovnom sudoproizvodstve Respubliki Kazakhstan: kakikh tseley ono dostigayet? [Procedural agreement on recognition of guilt in criminal proceedings of the Republic of Kazakhstan: what goals does it achieve?]. *Bulletin of the Ufa Law Institute of the Ministry of Internal Affairs of Russia,* 2019, p. 65. Available at: https://cyberleninka.

ru/article/n/protsessualnoe-soglashenie-o-priznanii-viny-v-ugolovnom-sudoproizvodstve-respubliki-kazahstan-kakih-tseley-ono-dostigaet/.

8. Toleubekova B.Kh., Khvedelidze T.B. Alogizmy novogo ugolovno-protsessual'nogo kodeksa Respubliki Kazakhstan [Alogisms of the new criminal procedure code of the Republic of Kazakhstan]. *Bulletin of KazNPU named after Abay*, 2017, no. 4 (50), p. 130. Available at: https://kaznpu.kz/docs/vestnik/urisprudensia_/4_2017.pdf/.

9. Fisher G. Plea Bargaining's Triumph: A History of Plea Bargaining in America. Stanford University Press, 2003, p. 300. Available at: https://core.ac.uk/download/pdf/215559239.pdf/.

10. Chernyakova A.V. Mezhdunarodnyy i zarubezhnyy opyt ugolovno-pravovogo protivodeystviya khishcheniyam, sovershayemym s ispol'zovaniyem komp'yuternoy informatsii [International and foreign experience of criminal law counteraction to theft committed with the use of computer information]. *Yuridicheskaya nauka i pravookhranitel'naya praktika – Legal Science and Law Enforcement Practice,* 2018, no. 4 (46), p. 170.

11. Mikhaylenko I.A. K voprosu o sposobakh moshennichestva v seti Internet [To the question of methods of fraud on the Internet]. Available at: https://cyberleninka.ru/article/n/k-voprosu-o-sposobah-moshennichestva-v-seti-internet/.

12. Khachaturova S.S., Zhikhareva Yu. P. Ostorozhno, fishing! [Beware of phishing!]. *International Journal of Applied and Fundamental Research,* 2016, no. 4-4, pp. 793–795.

13. Karpova D.N. Kiberprestupnost': global'naya problema i yeyo resheniye [Cybercrime: a global problem and its solution]. *Vlast' – Power,* 2014, no. 8, p. 47.

14. Dombrovskaya L.A., Yakovleva N.A., Stakhno R.Ye. Sovremennyye podkhody k zashchite informatsii, metody, sredstva i instrumenty zashchity [Modern approaches to information security, methods, means and tools of protection]. *Nauka, tekhnika i obrazovaniye – Science, technology and education*, 2016, no. 4 (22), pp. 16-19.

15. Kharina E.N. Kiberprestupleniya: ugolovno–pravovoy i kriminalisticheskiy aspekt [Cybercrime: criminal law and forensic aspect]. *Bulletin of the University named after O.E. Kutafin (MGYuA),* 2017, no. 5, p. 169.

16. Shaposhnikov A.Yu. Kriminalisticheskiy i ugolovno-pravovoy analiz moshennichestv, sovershayemykh s ispol'zovaniyem komp'yuternykh virusov [Forensic and criminal law analysis of fraud committed using computer viruses]. *Actual problems of economics and law,* 2014, no. 4 (32), p. 296.

YURIDIK FANLAR AXBOROTNOMASI
ВЕСТНИК ЮРИДИЧЕСКИХ НАУК
REVIEW OF LAW SCIENCES

Huquqiy ilmiy-amaliy jurnal

Правовой научно-практический журнал

Legal scientific-practical journal

3 / 2022

Tahririyat manzili:
100047. Toshkent shahar, Sayilgoh ko‘chasi, 35.
Tel.: (0371) 233-66-36 (1169)

Web-sayt: www.tsul.uz
E-mail: lawjournal@tsul.uz
Obuna indeksi: 1387.

Jurnal 10.10.2022-yilda tipografiyaga topshirildi. Qog‘oz bichimi: A4.
Shartli 16,50 b.t. Adadi: 100. Buyurtma raqami: 163.
TDYU tipografiyasida chop etildi.