

**КОСТАНАЙСКАЯ АКАДЕМИЯ
МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ РЕСПУБЛИКИ КАЗАХСТАН
ИМЕНИ ШРАКБЕКА КАБЫЛБАЕВА**

**ПРЕДУПРЕЖДЕНИЕ ИНТЕРНЕТ-МОШЕННИЧЕСТВ:
ОСНОВЫ ПРАВОВОЙ ГРАМОТНОСТИ
И ЗАЩИТЫ ОТ МОШЕННИКОВ**

Методические рекомендации

Костанай, 2025

УДК 343.2/7:004
ББК 67.408:32.973
П 71

Рекомендованы решением Ученого совета Костанайской академии МВД
Республики Казахстан имени Ширакбека Кабылбаева

Рецензенты:

профессор кафедры уголовного права и криминологии
Костанайской академии МВД Республики Казахстан им. Ш.Кабылбаева,
доктор юридических наук, профессор **Скаков А.Б.**,
профессор кафедры уголовного процесса и криминалистики
Костанайской академии МВД Республики Казахстан им. Ш. Кабылбаева,
кандидат юридических наук **Брылевский А.В.**,
начальник кафедры кибербезопасности и информационных технологий
Карагандинской академии МВД Республики Казахстан им. Б. Бейсенова,
кандидат юридических наук, майор полиции **Шульгин Е.П.**,
начальник Центра по борьбе с киберпреступностью
Департамента криминальной полиции МВД Республики Казахстан,
полковник полиции. **Басыбаев Ж.О.**

П 71 Предупреждение интернет-мошенничеств: основы правовой грамотности
и защиты от мошенников: методические рекомендации / сост.:
Р.Т. Абенов. - Костанай: Костанайская академия МВД Республики
Казахстан им. Ш. Кабылбаева, 2025. - 18 с.
ISBN 978-601-367-052-2

Методические рекомендации основываются на теоретических материалах
и правоприменительной деятельности органов внутренних дел в современных
реалиях.

В процессе подготовки исследованы информационные ресурсы по данной
тематике, рассмотрены современные методы противодействия интернет-
мошенничеству, представляющему угрозу национальной безопасности нашей страны.

Методические рекомендации предназначены для практических сотрудников
ОВД, слушателей, курсантов, профессорско-преподавательского состава,
обучающимся в рамках послевузовской образовательной программы (магистранты,
докторанты) в организациях образовательной системы МВД, а также для широкого
круга лиц из числа читателей, интересующихся современной методикой
противодействия преступности.

УДК 343.2/7:004
ББК 67.408:32.973

ISBN 978-601-367-052-2

© Абенов Р.Т., 2025
© Костанайская академия МВД
Республики Казахстан
им. Ш. Кабылбаева, 2025

СОДЕРЖАНИЕ

Введение	4
Исторический аспект и проблематика развития интернет-мошенничеств	5
Виды интернет-мошенничеств.....	7
Мошенничество, связанное с личными отношениями.....	7
Мошенничество, связанное с авансовым платежом.....	7
Мошенничество, связанное с покупками и сбором пожертвований через Интернет.....	8
Мошенничество, связанное с получением кредитов в банке.	8
Мошенничество, связанное с трудоустройством.....	9
Типы интернет-мошенничеств.....	10
Средства профилактики, применяемые уполномоченными лицами при расследовании интернет-мошенничеств.....	12
Защите себя от интернет-мошенников.....	13
Заключение.....	15
Список литературы.....	17

ВВЕДЕНИЕ

В современном мире онлайн-мошенничество стало глобальным бедствием, затрагивающим людей независимо от географического положения или социального статуса. Казахстан, с ее быстро развивающейся цифровой инфраструктурой и сложной социальной и экономической обстановкой, не является исключением. Фактический, за последние годы в стране значительно увеличилась киберпреступность во многих сферах жизни – от обычного фишинга до сложных банковских афер. Эти виды мошенничеств несут угрозу не только индивидуальной безопасности и благосостоянию людей, но и подрывают экономическую и социальную стабильность государства.

Именно поэтому Президент страны Касым-Жомарт Токаев отметил необходимость активизации мер по противодействию интернет-мошенничеству и финансовым пирамидам [1].

Рассматриваемый вид уголовного деяния все чаще приобретает новые свойства и оказывает особую форму информационного воздействия на человеческую психику.

Кроме того, данный вид преступного посягательства по замыслу исполнения имеет технически сложную характеристику. Часто преступники в целях реализации своего умысла объединяются в группы. Здесь в процессе подготовки к преступному деянию важным является четкое распределение ролей. Познания в области психологии, которым обладают организаторы и исполнители нередкость.

Мы подробно рассмотрим историческое развитие, различные виды афер, технологические методы, используемые преступниками, психологические и социальные последствия, а также возможные варианты действий для жертв. Цель состоит в том, чтобы всесторонне описать схему мошенничеств и одновременно предложить эффективные практические шаги для защиты физических и юридических лиц в случае необходимости.

В настоящих методических рекомендациях мы делаем объемный обзор различных схем онлайн-мошенничеств в Казахстане. В эпоху, когда границы между цифровым и реальным миром все больше стираются, осознание угроз, исходящих от цифрового мира, и владение инструментами защиты важнее, чем когда-либо. Подготовленными методическими рекомендациями мы хотим способствовать осведомленности людей, тем самым укрепить их самосознание против темной стороны цифровизации.

ИСТОРИЧЕСКИЙ АСПЕКТ И ПРОБЛЕМАТИКА РАЗВИТИЯ ИНТЕРНЕТ-МОШЕННИЧЕСТВ

История интернет-мошенничеств в Казахстане тесно связана с быстрыми технологическими и политическими изменениями последних десятилетий. С момента обретения независимости Казахстан пережил динамичное развитие, в том числе, охватившее сферу информационных технологий. Однако это развитие предоставило не только возможности для экономического роста и инноваций, но и для преступной деятельности.

В начале 2000-х годов интернет начал играть значительную роль в мире информации. С увеличением доступности онлайн-услуг и ростом числа интернет-пользователей выросли возможности для такого вида преступления как интернет-мошенничество. В то время наиболее распространенными были относительно простые виды мошенничества, такие как классические фишинговые атаки, при которых пользователи были склонны раскрывать личную информацию.

Как свидетельствует правоприменительная практика большая часть преступлений рассматриваемой категории совершаются правонарушителями из зарубежа, а именно из Украины. Как полагают эксперты, что «Украина - очень важный центр хакерства, наряду с Россией, Бразилией, Китаем и, в меньшей степени, – Индией. В этих странах довольно образованное молодое население, высокий уровень безработицы и ограниченные возможности трудоустройства» [2, с. 133]. Так, например, в 2022 году был ликвидирован call-центр мошенников в украинском городе Днепр и задержано 32 жителя Украины [3], которые выдавали себя за сотрудников службы безопасности казахстанских банков и правоохранительных органов. В 2023 году зарегистрировано 13746 фактов интернет-мошенничества, от которых пострадали 13500 тысяч граждан, и общий нанесённый гражданам ущерб составляет 11 млрд 355 млн тенге [4]. Только в текущем 2024 году полицейские из трех стран (Казахстан, Чехия, Украина) задержали две группы интернет-мошенников, изъяли их технику на территории Украины [5].

Учитывая изложенное, уместно обратить внимание на исторический аспект развития рассматриваемого вида преступления на территории Украины. На постсоветском пространстве «оранжевая революция» в Украине 2004 года и последующие политические потрясения оказали значительное влияние на все сферы жизни, что безусловно отразилось и на киберпреступности. Политическая нестабильность привела к ослаблению судебного преследования и контроля, что открыло новые возможности для правонарушителей (киберпреступников). Именно в тот период времени Украина стала центром различных видов онлайн-мошенничества, включая более сложные схемы, такие как продажа несуществующих товаров и услуг через поддельные веб-сайты.

С дальнейшим развитием цифровой инфраструктуры и распространением широкополосного интернета методы киберпреступников также эволюционировали. Экономические трудности и социальные волнения упростили мошенникам задачу эксплуатации уязвимых групп населения,

особенно в периоды, когда люди более восприимчивы к обещаниям быстрой прибыли или эмоциональной поддержки. Именно это время (этот период) можно назвать «расцветом» интернет-мошенничества в Казахстане. В «постковидный» период данный вид преступления возрос до масштабов угрозы национальной безопасности.

Исходя из сути интернет-мошенничеств, определяют следующие угрозы обществу и государству:

«- открытость общества и государства. Создана на основе компьютерных сетей и информационных технологий удобная инфраструктура для международных поставок товаров, предоставления услуг, перевода средств между физическими и юридическими лицами, хранения информации в сети Интернет и подключение к ней каждого компьютера, предоставляет одновременно широкие возможности как собственно киберпреступлений с помощью компьютерных технологий;

- высокая технологичность. Чрезвычайно быстрое развитие информационных технологий и сложность этой области наряду с относительно длительным и бюрократическим подходом к развитию нормативных правовых баз приводит к значительному отставанию мер по предубеждению и борьбе с интернет-мошенничеством;

- сложный характер преступления. Интернет-мошенники используют компьютерные технологии, информационные сети по социально-психологическим соображениям, в частности дискредитации правительств и государств, размещение сайтов террористической направленности, порча и разрушение ключевых систем, вывод этих систем из рабочего состояния (что является своего рода дополнением к традиционному виду терроризма);

- анонимность преступления. Мошенников привлекает отсутствие физического контакта с жертвой и, бесспорно, сложность выявления, фиксирования и извлечения криминалистически-значимой информации в виртуальном пространстве;

- транснациональный и популярный характер мошенничества. Особенностью данного вида преступности является то, что подготовка и совершение преступления, при наличии доступа к сети Интернет, может осуществляться практически из любого места. А учитывая, что компьютерная техника и интернет-услуги становятся более доступным для все более широкого круга лиц, киберпреступность становится все более популярной.

В последние годы правоохранные органы активизировали усилия по борьбе с киберпреступностью, включая улучшение законодательной базы и укрепление киберполиции» [6].

Однако несмотря на указанные выше усилия, стремительное развитие современных технологий создают проблему защиты граждан и бизнеса от новых форм интернет-мошенничеств.

ВИДЫ ИНТЕРНЕТ-МОШЕННИЧЕСТВ

Мошенничество, связанное с личными отношениями.

Мошенники связываются со своими жертвами в интернете и завоевывают их доверие, строя неискренние отношения. Втершись в доверие, мошенники просят у своих жертв деньги на проезд, выплату штрафов, непредвиденные экстренные расходы и тому подобное. Ища в Интернете пару для отношений, учитывайте признаки, которые могут указывать на то, что ваши собеседники являются не теми, за кого себя выдают.



Мошенничество, связанное с авансовым платежом.

Мошенники выдают себя за настоящие компании и обманывают жертв, убеждая жертв внести предоплату, чтобы получить что-то более ценное, например, ссуду, кредитную карту, грант, инвестиции или наследственные деньги. Жертва направляет средства мошеннику денежным переводом, но ничего за это не получает. Этих кредитов, кредитных карт, инвестиций или наследства никогда не существовало. Получив ваши деньги, мошенники больше не будут выходить с вами на связь.



Мошенничество, связанное с покупками и сбором пожертвований через Интернет.

Мошенники используют сайты и объявления в Интернете для рекламирования товаров вроде мобильных телефонов, билетов на мероприятия или машин, которые на самом деле не существуют. Кроме того, мошенники через социальные сети создают фейковые аккаунты и осуществляют сбор пожертвований для тяжелобольных, нуждающихся в материальной помощи лиц.



Мошенничество, связанное с получением кредитов в банке.

Данный тип мошенников можно именовать как «кредитные помогайки», которые предлагают посреднические услуги в оформлении займов, обналичивании товарных кредитов. Их схемы обмана основываются на доверии граждан, которые добровольно передают мошенникам свои персональные данные. При этом взаимодействуют злоумышленники со своими жертвами исключительно онлайн, чтобы вовремя замести свои следы. Взаимодействие мошенников с пользователями, которые откликнулись на объявления, происходит через мессенджеры. При этом злоумышленники предпочитают вести переписку посредством WhatsApp, в котором имеется режим исчезающих сообщений, и действуют по одной из двух схем: оформление кредита наличными; оформление товарных кредитов.



Мошенничество, связанное с трудоустройством.

Жертва отвечает на вакансию, ее нанимают на фиктивную должность и отправляют поддельные чеки для покрытия расходов, связанных с трудоустройством. Сумма в чеке превышает расходы жертвы, поэтому остаток нужно вернуть денежным переводом. Банк отказывается принять чек из-за недостатка средств на счете чекодателя, поэтому у жертвы остается задолженность перед банком на всю сумму.



ТИПЫ ИНТЕРНЕТ-МОШЕННИЧЕСТВ

Спектр схем киберпреступности в Казахстане разнообразен и включает множество видов мошенничества, которые несут угрозу как гражданам страны, так и иностранцам. В этом разделе мы рассмотрим наиболее распространенные виды мошенничества, чтобы наглядно показать развитие преступной деятельности.

Фишинг

Фишинг - вид мошенничества, в соответствии с которым клиентам платежных систем присылают уведомление по электронной почте якобы от администрации или службы безопасности этой системы с просьбой указать свои счета и пароли [7]. Фишинг остается одной из самых частых форм киберпреступности. Также, этот метод включает отправку поддельных электронных писем или создание поддельных веб-страниц с целью незаконной получения личной информации, такой как пароли и данные кредитных карт.

Вишинг (голосовой фишинг)

Вишинг - вид киберпреступлений, в котором в сообщениях содержится просьба позвонить на определенный городской номер, а при разговоре запрашиваются конфиденциальные данные владельца карты [7]. Вишинг, разновидность фишинга, при которой мошенники связываются с жертвами по телефону, также увеличилась в последние годы. Преступники часто выдают себя за сотрудников банков или представителей доверенных организаций.

Кардинг

Кардинг-использование в операциях реквизитов платежных карт, полученных со взломанных серверов интернет-магазинов, платежных и расчетных систем, а также с персональных компьютеров (либо напрямую, либо через программы удаленного доступа, «трояны», «боты») [7].

Другие виды мошенничества

Помимо упомянутых видов мошенничества существует множество других схем, включая фальшивые выигрыши в лотерею, предложения о работе и инвестиционное мошенничество. Эти методы постоянно меняются, чтобы адаптироваться к технологическим разработкам и изменениям в поведении потребителей. К ним можно отнести:

- «1. *Онлайн-мошенничество* - ненастоящие интернет-аукционы, интернет-магазины, сайты и телекоммуникационные средства связи;
2. *пиратство* - незаконное распространение интеллектуальной собственности в Интернете;
3. *кард-шаринг* - предоставление незаконного доступа к просмотру спутникового и кабельного TV;
4. *социальная инженерия* - технология управления людьми в Интернет-пространстве;

5. *малваре* - создание и распространение вирусов и вредоносного программного обеспечения;

6. *противоправный контент* - контент, пропагандирующий экстремизм, терроризм, наркоманию, порнографию, культ жестокости и насилия;

7. *рефайлинг* - незаконная подмена телефонного трафика» [7].

СРЕДСТВА ПРОФИЛАКТИКИ, ПРИМЕНЯЕМЫЕ УПОЛНОМОЧЕННЫМИ ЛИЦАМИ ПРИ РАССЛЕДОВАНИИ ИНТЕРНЕТ-МОШЕННИЧЕСТВ

Средства профилактики, применяемые уполномоченными лицами при расследовании интернет-мошенничеств имеют широкий спектр предупредительных мер. Здесь следует отметить, что «предупреждение интернет-мошенничеств основано на мерах, направленных на снижение риска совершения таких уголовных правонарушений и нейтрализация - этих вредных последствий для общества» [6].

По мнению некоторых авторов в организационном аспекте «основной проблемой профилактики данного вида мошенничества является отсутствие необходимой специализации подразделений киберполиции при организации и осуществлении профилактики таких уголовных правонарушений и слабое взаимодействие между субъектами профилактики, а также отсутствие единого координирующего органа и эффективной системы контроля за выявлением и расследованием уголовных правонарушений» [8].

Следует отметить, что Г.В. Недзельская среди мер предотвращения интернет-мошенничеств выделяет следующие аспекты:

- «- создание специализированных центров сбора и анализа информации о фактах мошенничества в сети Интернет. Деятельность подобных организаций должна быть ориентирована не столько на констатацию преступных посягательств, сколько на выработку действенных профилактических мер. Одним из направлений деятельности этих центров имеют стать сбор информации о потенциально опасных объектах и их блокировка; организация подбора, обучения и инструктажа работников служб компьютерной (информационной) безопасности субъектов хозяйствования;

- внедрение программы обучения граждан основам компьютерной безопасности во время производства финансовых операций через информационные сети, общение в социальных сетях и др., информирование через СМИ о новых видах компьютерного мошенничества;

- разработка и использование специального программного обеспечения, в том числе антивирусных программ или программ идентификации пользователя;

- расширение системы специализированных отделов, занимающихся компьютерными преступлениями, и формирование единой государственной базы интернет-мошенников» [9, с. 212].

Не следует оставлять без внимания и профилактические меры информационно-воспитательного и виктимологического характера.

Путем задействования средств массовой информации (газеты, журналы, телевидение, интернет, информационные ресурсы, официальные web-страницы государственных органов власти и предприятий) осуществляется реализация метода распространения информационного контента. Правоохранительные органы также могут принимать участие в подобных мероприятиях через специализированные подразделения и пресс-центры органов внутренних дел [10, с. 97].

ЗАЩИТИТЕ СЕБЯ ОТ ИНТЕРНЕТ-МОШЕННИКОВ

Не передавайте никому свои личные данные, пароли, СМС-коды;

Не отправляйте деньги для получения кредита, например, взнос по кредитной карте, таможенные пошлины или расходы на доставку.

Не отправляйте деньги людям, с которыми вы не встречались лицом к лицу.

Не скачивайте незнакомые мобильные приложения по просьбе третьих лиц;

Не вкладывайте свои сбережения в сомнительные инвестиционные проекты.

Проверьте предприятия, у которых нет подтвержденного адреса.

Не оплачивайте товары или услуги денежными переводами на имя человека.

Создайте надежные пароли, что позволит обеспечить защиту информации и периодическое их изменение;

Осведомляйтесь о распространенных приемах, которые используют преступники для того, чтобы распознавать их;

Защитите устройства, путем установки антивирусных программ;

Используйте защищенные сети;

Проверяйте ваши учетные записи;

Не проходите по незнакомым ссылкам в мессенджерах и соцсетях;

Используйте инструменты конфиденциальности и безопасности Google или других браузеров;

Правила, чтобы не стать жертвой интернет-мошенников:

«- ни в коем случае не доверяйте телефонным звонкам (якобы родственникам, совершившим ДТП, или задержанным полицией и т.д.) с просьбой о материальной помощи. Выясните, кто находится с вами на связи, как его фамилия, имя, сколько ему лет, откуда он родом, где находится, знает ли он хорошо Ваших родственников и друзей, в том числе как он выглядит. Конкретные вопросы поставят мошенника в тупик, он начнет врать или прервет звонок» [11]. Кроме того, следует:

«- игнорировать звонки с информацией о том, что вам положена любая денежная компенсация в обмен на перевод денежных средств на расчетные счета.

- игнорировать SMS сообщения от неизвестных вам абонентов с просьбой перезвонить на данный абонентский номер. С вашего счета может быть автоматически снята значительная сумма денег.

- провести беседу с детьми о том, чтобы они не вели телефонных разговоров с незнакомыми людьми, не называли персональных данных и адреса проживания неизвестным лицам.

- получив уведомление о блокировке банковской карты не звонить на номера, указанные в смс-сообщении, а связаться с банком по телефону «горячей линии» как правило, он указан на обратной стороне банковской карты. При разговоре с «операторами» не называть пароль карты, ее реквизиты,

свои персональные данные: вся необходимая информация у банковских работников есть, и она сообщается при открытии счета» [12].

ЗАКЛЮЧЕНИЕ

На сегодня мошенничество с использованием интернет сетей – это одна из самых стремительно развивающихся видов общественно опасных преступных посягательств. Такое обстоятельство связано с быстрыми темпами развития информационных технологий, в том числе стремительным и постоянным расширением области применения электронно-вычислительной техники.

Мошенничество с использованием интернет сетей, несмотря на эволюционные процессы, остается преступлением против собственности, совершаемым с использованием обмана или злоупотребления доверием. Разница лишь в том, что обман происходит не во время непосредственного физического вербального или невербального контакта с жертвой, а дистанционно, то есть с использованием возможностей компьютерно-телекоммуникационных устройств, систем или сетей.

Чрезвычайно стремительное развитие информационных технологий в последние годы служит условием к быстрому распространению интернет-мошенничеств. В свете сказанного, актуальность в вопросах предупреждения и противодействия рассматриваемого вида преступления в киберпространстве, не вызывает сомнения.

Предупреждение интернет-мошенничеств основывается на мерах направленных по уменьшению риска их совершения, в том числе нейтрализации преступных последствий для общества. Одной из причин высокой латентности подобных преступлений является отсутствие государственных границ, если преступление совершается с помощью интернета, несовершенство законодательства и, соответственно, невозможность сотрудничать с другими странами при расследовании этих преступлений в связи со значительными различиями в законодательстве разных стран в отношении такого преступления.

Важным для борьбы с угрозой интернет-мошенничества выступает постоянное международное сотрудничество. Здесь следует отметить, что на уровне отдельного государства контролировать и бороться с кибермошенничеством практически невозможно. При этом, принятие международных норм и стандартов должно сопровождаться внесением изменений и дополнений в национальное законодательства государств.

Главная же задача состоит в том, чтобы на международном уровне, например, в рамках ООН, разработать комплексную программу, включающую в себя все возможные формы и методы борьбы с интернет-мошенничеством. Эти действия будут иметь успех только в том случае, если будут опираться на систему постоянного мониторинга интернет-пространства на международном и национальном уровнях. Соответственно, правоохранительные органы всех государств должны параллельно осуществлять мероприятия по пресечению и предупреждению таких преступлений. Если стираются рамки места совершения таких преступлений-должны стираться рамки места проведения расследования. Производство должно происходить в рамках совместного расследования таких

преступлений правоохрательными органами государств.

Соответственно, для комплексного противодействия интернет-мошенничеству необходимы:

- Гармонизация уголовного законодательства об интернет-мошенничестве на международном уровне;

- Разработка на международном уровне и реализация в национальное законодательство стандартов, что позволяют эффективно расследовать преступления в глобальных информационных сетях, получать, исследовать и представлять электронные доказательства;

- Налаженное сотрудничество правоохрательных органов при расследовании интернет-мошенничеств на оперативном уровне.

Кроме того, в целях предупреждения киберпреступности в нашей стране предлагается:

- ✓ Создать специальную техническую службу в составе МВД с наделением необходимых полномочий;

- ✓ Разработать подзаконный нормативный акт с предоставлением субъекту оперативно-розыскной деятельности по киберпреступности разведывательных и контразведывательных функций;

- ✓ Повысить материально-техническое обеспечение киберполиции;

- ✓ Обеспечить повышение заработной платы указанного выше подразделения путем выделения средств из суммы выявленных ими уголовных преступлений (в процентном эквиваленте).

Таким образом, международное сотрудничество является ключевым моментом в ликвидации правовой пропасти, существующей между развитием информационных технологий и реагированием на них законодательства. Это единственный путь обеспечить безопасность пользователей и государства от электронных посягательств, а также эффективно расследовать интернет-мошенничества.

СПИСОК ЛИТЕРАТУРЫ

1. Токаев поручил усилить борьбу с интернет-мошенниками. [Электронный ресурс] – Режим доступа: <https://informburo.kz/novosti/tokaev-poruchil-usilit-borbu-s-internet-moshennikami>
2. Гурина Д. П. задачи экспертной профилактики. //Актуальные проблемы государства и правая. - 2008. - Вып. 44. - С. 233.
3. 32 жителя Украины задержали за телефонное мошенничество в Казахстане. [Электронный ресурс] – Режим доступа: <https://mgorod.kz/news/32-zhitelya-ukrainy-zaderzhali-za-telefonnoe-moshennichestvo-v-kazaxstane>
4. Казахстанские правоохранители провели полицейскую операцию в Украине. [Электронный ресурс] – Режим доступа: <https://orda.kz/kazahstanskije-pravoohraniteli-proveli-policejskuju-operaciju-v-ukraine-377978/>
5. Обманывали казахстанцев: транснациональных мошенников задержали на Украине. [Электронный ресурс] – Режим доступа: <https://ru.sputnik.kz/20240429/obmanyvali-kazakhstantsev-transnatsionalnykh-moshennikov-zaderzhali-na-ukraine--43974607.html>
6. Типология киберпреступности. [Электронный ресурс] – Режим доступа: https://www.cbr.ru/today/anti_legalisation/evraz/Tipologiya_kiber_EAG_2014.pdf
7. Сардак Д.Б. Использование сети интернет для предотвращения преступлений. Теория и практика расследования преступлений. Э[Электронный ресурс] – Режим доступа: <https://elibrary.ru/item.asp?id=49712484>
8. Теплова Д.О. Криминологическая характеристика и предупреждение организованного мошенничества. [Электронный ресурс] – Режим доступа: <https://repository.rudn.ru/ru/records/dissertation/record/42062/>
9. Недзельская Г.В. специально-криминологические меры предотвращения мошенничества, что совершается организованной группой. //Юридический научный электронный журнал. - 2022. - № 3. - С. 211-213.
10. Лефтеров Л.В. общесоциальные мероприятия предупреждение мошенничества путем применения средств электронных коммуникаций. Публично-правовой дискурс в контексте глобализации. - 2019. - № 1 (15). - С. 89-101.
11. Полиция Талицы продолжает профилактику мошенничества. [Электронный ресурс] – Режим доступа: <https://talisa.bezformata.com/listnews/politciya-talitci-prodolzhaet-profilaktiku/73856138/>
12. Профилактика мошенничества. [Электронный ресурс] – Режим доступа: <https://petrovskoe.bezformata.com/listnews/profilaktika-moshennichestva/43735921/>

Учебно-методическое издание

**ПРЕДУПРЕЖДЕНИЕ ИНТЕРНЕТ-МОШЕННИЧЕСТВ:
ОСНОВЫ ПРАВОВОЙ ГРАМОТНОСТИ
И ЗАЩИТЫ ОТ МОШЕННИКОВ**

Методические рекомендации



Печатается в авторской редакции

Подписано в печать 27.02.2025 г. Формат 60x84 ¹/₁₆

Печать ризография. Объем 1,2 п.л.

Тираж 30 экз. Заказ № 5.

Отпечатано в типографии
Костанайской академии МВД РК им. Ш. Кабылбаева
г. Костанай, пр. Абая, 11.