Дата поступления рукописи в редакцию: 18.06.2026 г.
Дата принятия рукописи в печать: 20.07.2026 г.
DOI: 10.24412/2224-9133-2026-6-365-371

АГАФОНОВ С.Ю.,
кандидат юридических наук,
доцент кафедры криминалистики
Нижегородской академии МВД России;
доцент кафедры общей и клинической психологии
Приволжского исследовательского медицинского университета
Министерства здравоохранения Российской Федерации,
e-mail: agafonov_sergey82@mail.ru

СЕРЕБРОВ Д.О.,
кандидат юридических наук,
доцент кафедры криминалистики
Нижегородской академии МВД России,
e-mail: do.serebrov@gmail.com

ПАВЛОВ Е.Н.,
преподаватель кафедры криминалистики
Нижегородской академии МВД России,
e-mail: mail@law-books.ru

БУРЦЕВ В.А.,
преподаватель кафедры криминалистики
Нижегородской академии МВД России,
e-mail: yakovleva-185@mail.ru

КОВАЛЕНКО О.Н.,
преподаватель кафедры криминалистики
Нижегородской академии МВД России,
e-mail: Oksana-chan@yandex.ru

О ПОЛОЖИТЕЛЬНОМ ОПЫТЕ РАССЛЕДОВАНИЯ УГОЛОВНЫХ ДЕЛ О ПРЕСТУПЛЕНИЯХ, СОВЕРШЕННЫХ В СФЕРЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ, В СОСТАВЕ ОРГАНИЗОВАННОЙ ГРУППЫ

Аннотация. *Преступления в сфере информационно-телекоммуникационных технологий – общественно опасные деяния, запрещенные Уголовным кодексом Российской Федерации под угрозой наказания, совершенные с использованием информационных технологий и информационно-телекоммуникационных сетей в интернет-пространстве. Авторами проанализированы диспозиции статей Уголовного кодекса Российской Федерации, содержащие понятие «информационно-телекоммуникационные технологии». Для изучения данной тематики авторами использованы методы синтеза, анализа, формально-юридический (догматический) и статистический. Рассмотрено действие уголовно-правовых норм в расследовании преступлений данной категории, представлена реализация данных норм на примере конкретного уголовного дела.*

Ключевые слова: *преступления в сфере информационно-телекоммуникационных технологий, уголовный кодекс Российской Федерации.*

AGAFONOV S.YU.,
Candidate of Law, Associate Professor of the Department
of Criminalistics of the Nizhny Novgorod Academy
of the Ministry of Internal Affairs of Russia; Associate Professor,
Department of General and Clinical Psychology,
Volga Research Medical University,
Ministry of Health of the Russian Federation

SEREBROV D.O.,
Candidate of Law, Associate Professor,
Department of Criminalistics,
Nizhny Novgorod Academy of the Ministry
of Internal Affairs of Russia

PAVLOV E.N.,
Lecturer, Department of Forensic Science,
Nizhny Novgorod Academy of the Ministry
of Internal Affairs of Russia

BURTSEV V.A.,
Lecturer, Department of Forensic Science,
Nizhny Novgorod Academy of the Ministry
of Internal Affairs of Russia

KOVALENKO O.N.,
Lecturer, Department of Forensic Science,
Nizhny Novgorod Academy of the Ministry
of Internal Affairs of Russia

ON THE POSITIVE EXPERIENCE OF INVESTIGATING CRIMINAL CASES OF CRIMES COMMITTED IN THE FIELD OF INFORMATION AND TELECOMMUNICATIONS TECHNOLOGIES, AS PART OF AN ORGANIZED GROUP

Annotation. *Crimes in the field of information and telecommunication technologies are socially dangerous acts prohibited by the Criminal Code of the Russian Federation under threat of punishment, committed using information technologies and information and telecommunication networks in the Internet space. The authors analyzed the dispositions of articles of the Criminal Code of the Russian Federation containing the concept of "information and telecommunication technologies". To study this topic, the authors used methods of synthesis, analysis, formal legal (dogmatic) and statistical. The article considers the effect of criminal law norms in the investigation of crimes of this category, and presents the implementation of these norms using the example of a specific criminal case.*

Key words: *Crimes in the field of information and telecommunications technologies, Criminal Code of the Russian Federation.*

Преступления в сфере информационно-телекоммуникационных технологий (далее – ИТТ) – общественно опасные деяния, запрещенные Уголовным кодексом Российской Федерации (далее – УК РФ) под угрозой наказания, совершенные с использованием информационных технологий и информационно-телекоммуникационных сетей в интернет-пространстве [1]. Анализируя диспозиции статей УК РФ, ссылаясь на указание Генеральной прокуратуры Российской Федерации № 11/11, МВД России № 1 от 17 января 2023 года «О введение в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности» (Перечень № 25), а также исследование статистической отчетности, можно выделить ряд статей Уголовного закона, являющихся наиболее распространенными в рамках исследования рассматриваемого вида преступных деяний. Так, например, пункт «г» части 3 статьи 158 – кража (тайное хищение чужого имущества), совершенная с банковского счета, а равно в отношении электронных денежных средств [2]. Наиболее распространенными примерами указанного вида преступлений являются: использование виновным лицом похищенной банковской карты путем оплаты товаров и услуг, снятия наличных денежных средств через банкомат, перевода денежных средств на личный расчетный счет; использование мобильного телефона потерпевшего с привязанными банковскими счетами к определенным приложениям;

– статья 159.3 УК РФ – мошенничество (хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием), совершенное с использованием электронных средств платежа;

– статья 159.6 УК РФ – мошенничество (хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием) в сфере компьютерной информации путем ввода, удаления, блокирования, модификации либо иного вмешательства в функционирование средств хранения, обработки или передачи указанной информации [3].

Использование информационно-коммуникационных сетей, включая сеть «Интернет», является квалифицирующим признаком преступлений, не связанных с хищением чужого имущества (например, доведение до самоубийства (п. «д» ч. 2 ст. 110 УК РФ); незаконные производство, сбыт или пересылка наркотических средств, психотропных веществ или их аналогов, а также незаконные сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества (п. «б» ч. 2 ст. 228.1 УК РФ).

На основании вышеизложенного мы можем сделать вывод о том, что преступления, совершаемые с использованием ИКТ, имеют под собой довольно прочный фундамент и нашли свое активное распространение среди всего спектра преступлений, совершаемых на территории Российской Федерации, что является негативной тенденцией и требует введение наиболее эффективных средств и методов для искоренения данной категории преступлений.

Обращаясь к криминологическому аспекту [4], а также изучив статистическую базу, авторами установлено, что за 2024 год на территории Российской Федерации зарегистрировано около 2 000 преступлений, из которых 40 % совершены с использование информационно-коммуникационных технологий, что выше на 13, 1% по сравнению с 2023 годом. Согласно статистическим данным, представленным МВД России за 2025 год, ущерб от IT-преступлений вырос на 16 % и составил почти 120 млрд рублей [5]. Данная тенденция обусловлена некоторыми объективными факторами:

Доверчивость и низкая правовая грамотность граждан. Наряду с активной цифровизацией современного общества возникает проблема, связанная с использованием мошенниками различных методов и способов обмана посредством использования мобильных средств связи и социальных сетей. С учетом того, что в средствах массовой информации скоплен и раскрыт обширный перечень способов обмана, используемых мошенниками, а также профилактической информации, граждане зачастую это игнорируют или даже не обращают внимание, предполагая, что не станут жертвами мошеннических действий. Это является заблуждением и одной из основных причин увеличения количества рассматриваемого вида преступлений.

Низкий уровень взаимодействия правоохранительных органов с кредитными организациями, сотовыми операторами и иными службами, имеющими прямую или косвенную связь с киберпреступностью. В настоящее время данная причина постепенно искореняется с учетом обновления и совершенствования нормативной правовой базы как на общеправовом, так и на частном уровне путем внесения изменений во внутриведомственные приказы. По нашему мнению, в данном случае необходимо обратить внимание на наиболее детальные аспекты (например, на временные промежутки, в частности, сокращение сроков, предоставляемых коммерческим организациям при подготовке ответов на запросы правоохранительных органов).

Не маловажной причиной выступает сама цифровизация гражданского общества. В основном граждане используют сеть «Интернет» в различных сферах своей жизни: при хранении и обмене денежными средствами, используя электронные средства платежа, инвестиционные платформы; при получении и использовании товаров и услуг, располагаемых на цифровых платформах; при хранении, редактировании, модификации частной информации на электронных носителях. С одной стороны, это указывает на развитие современного общества, а с другой – на становление фундамента преступной деятельности, связанной с хищением денежных средств с использованием сети «Интернет».

Активное развитие и использование иностранных цифровых платформ (VPN, Bitcoin), что в значительной мере затрудняет не только контроль со стороны государственных органов за сохранностью и безопасностью личных данных граждан, а также процесс раскрытия указанных преступлений с учетом проблем, возникающих в рамках международного сотрудничества, с учетом внешнеполитической обстановки.

По нашему мнению, данный перечень причин является наиболее распространенным, однако их спектр намного шире.

Кроме того, важно обратить внимание не только на момент производства предварительного следствия, но и этап доследственной проверки материалов. Процесс проверки сообщения о преступлении, совершенного с использованием ИТТ, является наиболее важным, так как именно в течение данного периода времени возможно провести ряд процессуальных действий до возбуждения уголовного дела, направленных на сохранение денежных средств потерпевших и установления правонарушителей. В процессе доследственной проверки необходимо установить сам

факт хищения денежных средств, сумму похищенного и способ совершенного деяния. В случае установления достаточных данных, указывающих на признаки состава преступления, следователем возбуждается уголовное дело, и дальнейшее расследование производится по разработанному алгоритму. Так, согласно статьям 145–146 Уголовно-процессуального кодекса Российской Федерации (далее — УПК РФ) первоначальным этапом производства по сообщению о преступлении является уведомление потерпевшего о возбуждении уголовного дела, признание его таковым соответствующим постановлением и допрос лица, которому причинен имущественный вред, в качестве потерпевшего [6].

В протоколе допроса должны быть отражены сведения об имущественном положении лица, о периоде совершенного хищения с указанием точных даты и времени. В случае поступления звонков и смс-сообщений время должно быть указанно поминутно. Кроме того, должна быть отражена полная информация о расчетном счете потерпевшего и, по возможности, виновного лица, включая все операции, производимые с денежными средствами потерпевшего. Также необходимо установить способ совершения хищения путем предоставления потерпевшим подробной информации о происходящих событиях. По окончании допроса необходимо провести профилактические мероприятия с потерпевшим в целях недопущения повторения виктимологической составляющей.

После производства вышеуказанных следственных действий необходимо провести выемку сотового телефона, документов, скриншотов смс-сообщений, переводов, выписок с расчетных счетов, детализации телефонных соединений у потерпевшего в случае, если данная информация в наличии. В противном случае необходимо подготовить и направить запросы в банки или сотовые организации для установления данной информации. Далее необходимо осмотреть изъятое и приобщить к материалам уголовного дела.

Следующим этапом является направление официальных зарегистрированных запросов посредством электронного документооборота, почтовой связи в кредитные организации, иные интернет-сервисы, с использованием которых было совершено хищение. Далее на основании полученной информации органом дознания или следствия необходимо подготовить ходатайство в суд на разрешение получения у оператора связи сведений о соединениях между абонентами и абонентскими устройствами о наложении ареста на денежные средства, находящиеся на расчетных счетах.

Данные процессуальные действия необходимо произвести в течение первых суток после регистрации сообщения о преступлении в целях минимизации имущественного вреда и своевременного получения информации для установления лица, совершившего преступление.

В дальнейшем при установлении лиц, их персональных данных, местонахождения, на расчетные счета которых поступили денежные средства потерпевшего, необходимо направить поручения в определенные регионы Российской Федерации на проведение необходимых процессуальных действий.

Но важно помнить, что до производства указанных следственных и процессуальных действий важно внести информацию о полученном сообщении в систему ИБД-Ф «Дистанционное мошенничество». Данная система содержит в себе базу по всем преступлениям, совершаемым с использованием цифровых технологий на территории Российской Федерации. При внесении полного объема информации, включая расчетные счета, абонентские номера, полные сведения о потерпевшем, имеется возможность установления совпадений и получения определенной «линии» уголовного преследования. Также необходимо осуществить звонок в кредитную организацию, направленный на блокировку «сомнительной» операции, то есть предполагается, что банк отменит операцию перевода денежных средств на счет правонарушителя, тем самым денежные средства будут возвращены, соответственно, одна из основополагающих целей уголовного судопроизводства будет выполнена.

Одной из главных проблем расследования исследуемой категорий преступлений является их низкая раскрываемость [7]. Связано это с тем, что преступные связи мошенников довольно обширны, зачастую данные преступления совершаются организованными группами, и для установления организатора необходимы крупные и разработанные материально-технические ресурсы и высококвалифицированная профессиональная подготовка сотрудников. Авторами статьи проанализирован процесс эффективного уголовного преследования данного вида преступления на примере уголовного дела, находящего в производстве СЧ ГСУ ГУ МВД России по Нижегородской области, возбужденного по 124 эпизодам деятельности по признакам преступления, предусмотренного частью 2 статьи 210 УК РФ, части 4 статьи 159 УК РФ, п.п. «а, б» части 4 статьи 1741 УК РФ по факту того, что не позднее 1 декабря 2016 года более точное дата и время следствием не установлены, гр. Р. и гр. Ш., находясь на территории г. Нижнего Новгорода, действуя умышленно, из корыстных побуждений, с целью личного незаконного материального обогащения, имея единый преступный умысел, заранее объединились в устойчивую группу для

совершения хищений денежных средств физических лиц путем обмана. Для реализации своего преступного умысла гр. Р. и гр. Ш., имея достаточные познания в сфере информационных технологий и маркетинга, избрали способ совершения систематических преступных действий в отношении заранее неопределенного круга физических лиц и в дальнейшем постоянно корректировали план их совершения.

Обвиняемые при реализации своего преступного умысла выбрали наиболее распространенный и удобный метод обмана – «вишинг», представляющий собой одну из форму социальной инженерии, при которой мошенники, используя средства мобильной связи, а именно звонки, представляясь сотрудниками кредитных организаций, ведомственных структур, службы безопасности, вынуждают абонентов добровольно передать конфиденциальную информацию либо же в целом денежные средства виновным. В данном случае гр. Р. и гр. Ш., используя иных лиц, являющихся соучастниками их преступной деятельности, представлялись жертвам мошеннических действий сотрудниками кредитных организаций (различных банков), предоставляли документы, содержащие ложную и сфабрикованную информацию, убеждали физических лиц производить перечисления денежных средств на указанные ими расчетные счета под предлогом оплаты оказания различного вида услуг, якобы необходимых для успешного прохождения процедуры одобрения банковского кредита. Жертвами их действий являлись физические лица, проживающие за пределами Нижегородской области, имеющие своей целью получение кредитных продуктов при низком кредитном рейтинге и неодобрения их банками при обращении.

В рамках дальнейшей реализации своего преступного умысла и создания преступного сообщества гр. Р. и гр. Ш. создан контактный центр, сотрудниками которого являлись члены преступного сообщества. Основная цель деятельности данного контактного центра заключалась в выстраивании телефонно-коммуникационных связей с физическими лицами, обратившимися для получения кредитного продукта. Данная организация преступной деятельности основана на структуризации преступной организации, построение линии взаимодействия между структурными подразделениями, распределении материальной доли денежных средств, получаемых преступным путем, в зависимости от индивидуального вклада, вносимого участниками в достижении преступной цели.

Каждое структурное подразделение имело сою функциональную базу, руководящий состав, специализацию, особое внимание обращалось именно на взаимодействие между подразделениями, что способствовало построению обособленности, стабильности и согласованности в действиях.

1. В функции членов первого структурного подразделения входило техническое и информационное обеспечение преступной деятельности, а именно:

– контроль работоспособности одностраничных сайтов в сети «Интернет» («лендингов»), предназначенных для информирования неограниченного круга лиц об оказании подставным юридическим лицом комплекса услуг, связанных с содействием в получении кредита, а также для сбора первичной информации о лицах, заинтересованных в получении кредита;
– техническое обеспечение деятельности контактного центра, то есть установка, настройка и контроль за бесперебойной работой технического оборудования, предназначенного для ведения переговоров с лицами, обратившимися за содействием в получении кредита, в том числе его подключение к сети «Интернет», обеспечение доступа к программам для обмена мгновенными сообщениями (мессенджерам) и электронной почте, используемым для обмена информацией между соучастниками преступной деятельности и потерпевшими, обеспечение доступа к средствам ip-телефонии, позволяющей участникам преступного сообщества создавать зашифрованные сеансы связи с использованием подменных абонентских номеров, недоступных для внешнего прослушивания;
– оформление подложных документов, якобы выданных подставными юридическими лицами либо кредитно-финансовыми учреждениями (банками) в ходе исполнения договоров оказания услуг посредничества, которые предоставлялись потерпевшим с целью убеждения в результативности проводимой работы и необходимости оплаты оказанных услуг.

2. Второе структурное подразделение – контактный центр, в функции членов которого входили все аспекты взаимодействия с потерпевшими, обратившимися за оказанием услуг по содействию в получении кредита по телефонам горячих линий либо через формы заявок, размещенных в сети «Интернет» членами первого структурного подразделения, в том числе устное общение, переписка с использованием электронной почты, предоставление документов, содержащих заведомо ложные сведения.

При этом фактической целью членов второго структурного подразделения, заведомо знавших, что никаких услуг в интересах потерпевших они не совершат, являлось введение потерпевших в заблуждение относительно необходимости перечисления денежных средств на расчетные счета, контролируемые членами четвертого структурного подразделения, в счет оплаты различных услуг, связанных с получением кредита, таких как страхование, открытие банковского счета, улучшение кредитной истории.

Характерной особенностью функционирования второго структурного подразделения являлось систематическое совершение преступных действий в формах, внешне не отличимых от обычной деятельности коммерческой организации, направленной на извлечение прибыли, в том числе:

– выполнение его членами своих преступных ролей в рабочее время, то есть, как правило, ежедневно с понедельника по пятницу, в период времени с 09 часов утра до 18 часов вечера, что создавало у потерпевших видимость осуществления законной предпринимательской деятельности;
– выполнение его членами своих преступных ролей в специально подысканных офисных помещениях, в которых гр. Р. и гр. Ш., исполняя свою преступную роль руководителей преступного сообщества (преступной организации), оборудовали рабочие места операторов контактного центра, отдельный кабинет для себя, как его руководителей, а также разместили техническое оборудование, предназначенное для обмена информацией между участниками преступного сообщества (преступной организации) и ведения переговоров с потерпевшими.

3. Третье структурное подразделение, в функции членов которого входили переговоры с потерпевшими, обратившимися за оказанием услуг по содействию в получении кредита от имени сотрудников различных подразделений кредитных организаций АО «Россельхозбанк», ПАО «Сбербанк», АО «Райффайзенбанк», таких как кредитный отдел, принимающий решение о предоставлении кредита, либо служба безопасности, контролирующая правомерность его предоставления. При этом в действительности никаких договорных либо трудовых отношений между указанными кредитными организациями и членами третьего структурного подразделения не имелось, а их фактической целью являлось убеждение потерпевших в том, что заключение договора оказания услуг посредничества либо оплата услуг, связанных с получением кредита, послужило основанием для принятия положительного решения о выдаче банком кредита.

Характерной особенностью функционирования третьего структурного подразделения являлось выполнение его членами своих преступных ролей удаленно, то есть при нахождении по фактическому месту жительства без личного посещения вышеуказанных офисных помещений.

4. Четвертое структурное подразделение, в функции членов которого входило создание условий для завладения похищенными у потерпевших денежными средствами, дальнейшее распоряжение ими по своему усмотрению и придание законного вида владению, пользованию и распоряжению ими, а именно:

– подыскание банковских карт, оформленных на подставных физических лиц;
– передача сведений об этих картах членам иных структурных подразделений преступного сообщества, а в дальнейшем и потерпевшим, которые под влиянием обмана осуществляли переводы принадлежащих им денежных средств на указанные банковские карты;
– перевод безналичных денежных средств, перечисленных потерпевшими на указанные банковские карты, в наличную форму, в том числе с использованием банкоматов, расположенных на территории г. Нижнего Новгорода и Нижегородской области.

В целях конспирации и сокрытия своих личных данных гр. Р. и гр. Ш. оснастили деятельность преступного сообщества (преступной организации) оборудованием, предназначенным для реализации общего преступного замысла: использовались услуги компании, предоставляющие возможность связи посредством ip-телефонии, позволяющей участникам преступного сообщества создавать зашифрованные сеансы связи с использованием подменных абонентских номеров, недоступных для внешнего прослушивания; регулярно менялись интернет-сайты и наименования организаций, использовавшихся при оказании предлагаемых услуг; неоднократно менялись адреса расположения офисов контактных центров; при производстве телефонных переговоров с потенциальными заемщиками использовались вымышленные имена; использовались фиктивные договоры, составленные от имени третьих лиц.

Рассматриваемое уголовное дело было направлено в Нижегородский районный суд г. Нижнего Новгорода для судебного производства. 23 октября 2024 года Нижегородским районным судом г. Нижнего Новгорода вынесен обвинительный приговор в отношении вышеуказанных

лиц, однако вмененная частями 1 и 2 статьи 210 УПК РФ (организация и участие в деятельности преступного сообщества) не устоялась. Данный факт регламентирован тем, что вся расписанная в диспозиции обвинения структура относится к одной сплоченной организованной группе, имеющей одну цель – двух прямых руководителей, тесно взаимодействующих в рамках внутриорганизационной составляющей. Преступное сообщество характеризуется наличием отдельных обособленных структурных подразделений.

Таким образом, положительная тенденция развития преступности в сфере ИТТ характеризуется наличием объективных и социально значимых причин, борьба с которыми позволит искоренить данную категорию преступлений [4]. В рамках досудебного производства по уголовному делу наиболее важным фактором является установление взаимодействия среди структурных подразделений, совершенствование и развития материально-технической базы и оснащенности, повышение квалификационного уровня сотрудников правоохранительных органов, направленное на получение образования, связанного с цифровизацией общества, обновление и совершенствование уголовного законодательства наряду с появлением иных способов и форм хищения чужого имущества, криминализация санкций за нарушение данных категорий преступлений и, безусловно, активная профилактическая работа с гражданами не только на базе общероссийского уровня, но и, охватывая все сфера индивидуальной жизнедеятельности.

Список литературы:

[1] Карабеков К. О. Киберпреступность в Российской Федерации и Республике Казахстан: состояние и меры предупреждения: дис. ... канд. юрид. наук. Омск, 2025. 26 с.

[2] Уголовный кодекс Российской Федерации от 13 июня 1996 года № 63-ФЗ. Доступ из СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_34661/ (дата обращения: 23.04.2026).

[3] Овсюков Д. А. Корыстные преступления против собственности с использованием информационно-телекоммуникационных сетей: вопросы квалификации: автореф. дис. … канд. юрид наук. Москва, 2023. 34 с.

[4] Елин В. М. О подходах к криминологической характеристике лиц, совершающих преступления в сфере компьютерной информации // Российский следователь. 2022. № 7. С. 61–65. DOI:https://doi.org/10.18572/1812-3783-2022-7-61-65.

[5] В. Гердо В России за январь–июль 2025 года ущерб от IT-преступлений вырос на 16 % и составил почти 120 млрд рублей // ТАСС: офиц. сайт. URL: https://alrf.ru/news/v-rossi-za-yanvar-iyul-2025-goda-ushcherb-ot-it-prestupleniy-vyrosna-16-i-sostavil-pochti-120-mlrd/?ysclid=mokdyv60n5554805263 (дата обращения: 20.05.2026).

[6] Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 года № 174-ФЗ (ред. от 18 марта 2023). Доступ из СПС «КонсультантПлюс».

URL: https://www.consultant.ru/document/cons_doc_LAW_34481/ (дата обращения: 12.04.2026).

[7] Лебедева А. А. Особенности расследования киберпреступлений // Безопасность бизнеса. 2021. № 6. С. 48–56. DOI: https://doi.org/10.18572/2072-3644-2021-6-48-56.

References:

[1] Karabekov K. O. Cybercrime in the Russian Federation and the Republic of Kazakhstan: status and preventive measures: dis.... cand. jurid. sciences. Omsk, 2025. 26 pp.

[2] Criminal Code of the Russian Federation of June 13, 1996 No. 63-FZ. Access from SPS “ConsultantPlus.” URL: https://www.consultant.ru/document/cons_doc_LAW_34661/ (access date: 23.04.2026).

[3] Ovsyukov D.A. Mercenary crimes against property using information and telecommunication networks: qualification issues: abstract. dis.... cand. jurid of sciences. Moscow, 2023. 34 pp.

[4] Elin V. M. On approaches to criminological characterization of persons committing crimes in the field of computer information//Russian investigator. 2022. № 7. S. 61-65. DOI:https://doi.org/10.18572/1812-3783-2022-7-61-65.

[5] V. Gerdo In Russia in January-July 2025, the damage from IT crimes increased by 16% and amounted to almost 120 billion rubles//TASS: official. site. URL: https://alrf.ru/news/v-rossi-za-yanvar-iyul-2025-goda-ushcherb-ot-it-prestupleniy-vyrosna-16-i-sostavil-pochti-120-mlrd/?ysclid=mokdyv60n5554805263 (дата обращения: 20.05.2026).

[6] Code of Criminal Procedure of the Russian Federation of December 18, 2001 No. 174-FZ (as amended on March 18, 2023). Access from SPS “ConsultantPlus.”

URL: https://www.consultant.ru/document/cons_doc_LAW_34481/ (access date: 12.04.2026).

[7] A. Lebedeva. Features of cybercrime investigation//Business security. 2021. № 6. S. 48-56. DOI: https://doi.org/10.18572/2072-3644-2021-6-48-56.