Научная статья
Научная специальность
5.1.4 «Уголовно-правовые науки»

УДК 343.9
DOI https://doi.org/10.26516/2071-8136.2024.3.81

ЦИФРОВАЯ ПРЕСТУПНОСТЬ: ПОНЯТИЕ, КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА, ПРЕДУПРЕЖДЕНИЕ (ЧАСТЬ 2)

© Сидорова Е. З.[1], Усов Е. Г.[2], 2024
[1] Восточно-Сибирский институт МВД России, г. Иркутск, Россия
[2] Иркутский национальный исследовательский технический университет, г. Иркутск, Россия

Настоящая работа является продолжением ранее опубликованной научной статьи: если в первой части проведенного исследования раскрывались понятие и криминологическая характеристика цифровой преступности, то вторая часть работы посвящена в большей степени вопросам предупреждения цифровой преступности. Произведен анализ такого понятия, как преступление, совершенное с использованием информационных (цифровых) технологий, который показывает, что в научной литературе существуют различные точки зрения относительно содержания указанного понятия, однако каждое из определений в той или иной степени опирается на нормы действующего законодательства в сфере информации. Ключевая цель настоящего научного изыскания и вытекающие из поставленной цели задачи сформулированы как раскрытие определения цифрового преступления, описание его видов и представление общих позиций относительно вопроса предупреждения цифровой преступности. Методология исследования строится на использовании общенаучных и частнонаучных методов познания, в частности метода индукции, дедукции, обобщения, анализа, исследования официальных информационных источников, метода экспертных оценок и др. Утверждается, что наибольшим практическим значением обладает разрешение вопроса о профилактике подобных преступлений и максимальным объемом полномочий в вопросах борьбы с цифровыми преступлениями наделены специализированные субъекты профилактики цифровых преступлений. Сделан вывод о том, что обеспечить системную реализацию всех мер превенции могут только все субъекты вместе, в вопросах борьбы с цифровыми преступлениями субъекты профилактики должны действовать сообща и выстраивать эффективный механизм взаимодействия и обмена необходимой информацией. Отмечается, что противодействие рассматриваемым преступлениям включает в себя полный комплекс мер оперативно-технических, поисковых, оперативно-разыскных действий, включая разъяснительные и профилактические средства общей и индивидуальной профилактики правонарушений, которые предусмотрены действующим законодательством.

Ключевые слова: цифровые преступления, киберпреступность, информационные технологии, цифровизация, профилактика цифровых преступлений.

DIGITAL CRIME: CONCEPT, CRIMINOLOGICAL CHARACTERISTICS, PREVENTION (PART 2)

© Sidorova E. Z.[1], Usov E. G.[2], 2024
[1] East Siberian Institute of the Ministry of Internal Affairs of Russia, Irkutsk, Russian Federation
[2] Irkutsk National Research Technical University, Irkutsk, Russian Federation

This scientific work is a continuation of a previously published scientific article: if the first part of the study revealed the concept and criminological characteristics of digital crime, then the second part of the work is devoted more to the prevention of digital crime. The analysis of such a concept as a crime committed using information (digital) technologies shows that in the scientific literature there are different points of view regarding the content of this concept, however, each of the definitions is more or less based on the norms of current legislation in the field of information. The key purpose of this scientific research and the tasks arising from this goal are formulated as the disclosure of the definition of digital crime, the description of its types and the presentation of common positions on the issue of digital crime prevention. The research methodology is based on the use of general scientific and private scientific methods of cognition, in particular, the method of induction, deduction, generalization, analysis, research of official information sources, the method of expert assessments, etc. The resolution of the issue of the prevention of such crimes is of the greatest practical importance. The largest amount of authority in the fight against digital crimes is vested in specialized subjects of the prevention of digital crimes. However, only all actors together can ensure the systematic implementation of all prevention measures. In the fight against digital crimes, the subjects of prevention must act together and build an effective mechanism for interaction and exchange of necessary information. Countering the crimes in question includes a full range of operational and technical, search, operational and investigative measures, including explanatory and preventive means of general and individual prevention of offenses, which are provided for by current legislation.

Keywords: digital crimes, cybercrime, information technology, digitalization, prevention of digital crimes.

Ранее проводимых нами научных исследованиях мы уделяли внимание понятию цифровой преступности [8, с. 70]. Обращение к данной проблематике обусловлено тем, что современные общественные отношения трудно представить без участия в них цифровых и других современных информационных технологий [4, с. 38], и данным трендом не устают пользоваться и представители криминального сообщества.

Как известно, все составы преступлений предусмотрены в Уголовном кодексе РФ (далее – УК РФ)[1]. Иных нормативных правовых актов, обеспечивающих уголовно-правовую охрану общественных отношений, нет. Романо-германская правовая система, на которой строится современная российская правовая база, позволяет сформировать уголовный закон, группируя все составы преступлений в зависимости от охраняемого блага (объекта). Соответственно, Особенная часть УК РФ состоит из разделов, глав и статей. Однако, несмотря на то что преступления, совершаемые с использованием информационных (цифровых) технологий, занимают значительное место в структуре современной преступности, самостоятельных раздела или главы, посвященных данным видам преступлений, в действующем уголовном законе нет. Исключение составляет только гл. 28 «Преступления в сфере компьютерной информации», однако преступления данной главы составляют только небольшую часть всей цифровой преступности.

Нам представляется, что целесообразно на теоретическом уровне определить, какие именно виды преступлений следует относить к преступлениям, совершаемым с использованием информационных (цифровых) технологий. Для этого необходимо обратиться к дефиниции данного термина.

Цель и задачи исследования

Цель настоящей работы заключается в анализе такого понятия, как «преступление, совершенное с использованием информационных (цифровых) технологий». Иными словами, речь идет о понятии цифрового преступления. Авторы ставят перед собой следующие научно-исследовательские задачи: дать определение указанному термину, представить виды цифровых преступлений, осветить современное криминологическое состояние цифровой преступности в России в целом, а также затронуть вопрос о предупреждении данного вида преступности.

Работа строится на использовании общенаучных и частнонаучных методов познания, в частности, авторы опираются на методы индукции, дедукции, обобщения, анализа, исследования официальных информационных источников, метод экспертных оценок и др.

Особенности характеристики цифровых преступлений

В научной литературе можно встретить различные термины, характеризующие цифровые преступления:

– преступления, совершаемые с использованием информационных технологий;

– компьютерная преступность;

– преступность в сфере информационно-коммуникационных технологий;

– преступность в социальных сетях;

– киберпреступления;

– посягательства на цифровую информацию;

– информационные преступления;

– преступления в сфере высоких технологий;

– цифровая преступность и др. [10, с. 32; 2, с. 87].

При разнообразии терминов, обозначающих цифровую (информационную) преступность, можно опираться на любой из указанных терминов, поскольку легального закрепления какого-либо из них в настоящее время нет. В частности, при определении обозначенного феномена можно использовать термин «информационная преступность», предлагая, таким образом, рассмотрение цифровых преступлений (или киберпреступлений) только в контексте информационной сферы, элементом которой она является.

Между тем компьютерная информация является специфичным видом информации, а кроме того, формально представляет собой объект самостоятельной уголовно-правовой охраны, что не дает возможности ее рассмотрения в контексте информационной сферы, так же как и компьютерные преступления не могут быть рассмотрены как информационные.

Можно использовать понятие «компьютерная преступность», предполагая рассмотрение исследуемого феномена в качестве преступности, совершаемой с помощью ЭВМ, высоких технологий.

Вместе с тем мы придерживаемся той позиции авторов, согласно которой использование компьютера аналогично использованию любого инструмента или средства, применение которых

[1] Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ // Собр. законодательства РФ. 1996. № 25. Ст. 2954.

возможно для того, чтобы совершенствовать то или иное преступление, а компьютерная сеть является средой или обстановкой совершения уголовно наказуемого деяния [3, с. 56].

В связи с вышесказанным считаем возможным в настоящей работе использовать указанные термины как равнозначные, несмотря на то, что определенные отличия между ними все же есть [5, с. 38].

Ключевым термином, на котором основывается раскрываемое нами понятие, является понятие «информационные технологии». Согласно Федеральному закону от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» информационные технологии – это процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов[1].

На наш взгляд, преступление, совершаемое с использованием информационных (цифровых) технологий (или цифровое преступление, или киберпреступление), – это преступление, связанное с незаконным вторжением или доступом в компьютерные программы или данные. В обществе, которое все больше полагается на компьютеры (гаджеты), опасность цифровых преступлений постоянно возрастает. Киберпреступления являются преступной деятельностью, которая предполагает использование информационных технологий для незаконного или несанкционированного доступа к компьютерной системе (в широком понимании слова «компьютер») с намерением повреждения, удаления или изменения имеющейся там информации. Кроме того, к цифровым преступлениям можно относить и те преступления, которые совершаются посредством использования современных компьютерных технологий и средств связи.

Опираясь на официальные статистические отчеты МВД России и Генеральной прокуратуры России, можно заключить, что в настоящее время правоприменитель к цифровым преступлениям относит следующие уголовно наказуемые деяния:

1) кражу (ст. 158 УК РФ);

2) мошенничество (ст. 159 УК РФ);

3) мошенничество с использованием электронных средств платежа (ст. 159.3 УК РФ);

4) мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ);

5) незаконные организацию и проведение азартных игр (ст. 171.2 УК РФ);

6) публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганду терроризма (ст. 205.2 УК РФ);

7) незаконные производство, сбыт или пересылку наркотических средств, психотропных веществ, а также незаконные сбыт или пересылку растений, содержащих наркотические средства или психотропные вещества (ст. 228.1 УК РФ);

8) изготовление порнографических материалов (ст. 242, 242.1, 242.2 УК РФ);

9) публичные призывы к осуществлению экстремистской деятельности (ст. 280 УК РФ);

10) неправомерный доступ к компьютерной информации (ст. 272 УК РФ);

11) создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ).

Подчеркнем, что, на наш взгляд, на этом перечне цифровые преступления не заканчиваются. Можно, в частности, обратить внимание на преступления, совершаемые в сфере оборота цифровых активов (криптовалюты) (на примере ст. 205.1 УК РФ «Содействие террористической деятельности» и ст. 290 УК РФ «Получение взятки»).

В настоящее время все чаще правоприменительная практика сталкивается с такими случаями террористической деятельности, как ее финансирование. При этом, как отмечают представители Росфинмониторинга, с развитием цифровых технологий террористическое финансирование все чаще осуществляется посредством использования информационно-телекоммуникационного пространства[2]. В этой связи обращение к уголовно-правовой характеристике такого состава преступления, как финансирование терроризма, в рамках исследования, посвященного изучению преступлений, совершаемых с использованием информационных (цифровых) технологий, является обоснованным и актуальным.

В ранее проводимом нами научном исследовании мы отмечали, что самостоятельная (отдельная) норма в области финансирования террористической деятельности в уголовном за-

[1] Об информации, информационных технологиях и о защите информации : федер. закон от 27 июля 2006 г. № 149-ФЗ // Собр. законодательства РФ. 2006. № 31 (ч. 1). Ст. 3448.

[2] Росфинмониторинг фиксирует факты финансирования терроризма с использованием криптовалют // Российское государственное федеральное информационное агентство «ТАСС». URL: https://tass.ru/ekonomika/10978989?ysclid=lmab3xthbe784153136 (дата обращения: 24.10.2023).

конодательстве отсутствует. Однако о финансировании терроризма можно говорить в рамках ст. 205.1 УК РФ («Содействие террористической деятельности») [9, с. 29]. Правоприменительная практика свидетельствует о том, что финансирование терроризма может быть реализовано посредством передачи заинтересованным лицам, помимо наличных денежных средств, безналичных ценностей, цифровых прав, цифровой валюты и т. п.

В свою очередь, криптовалюта может также присутствовать при совершении такого преступления, как получение взятки (ст. 290 УК РФ). В литературе неоднократно подчеркивалось, что в настоящее время судебная практика[1] и научное сообщество склоняются к тому, чтобы признавать криптовалюту в качестве иного имущества как предмета взяточничества («имущество в электронной форме») [1, с. 377]. Однако до конца данный вопрос еще не решен, поскольку в настоящее время не в полном объеме определена правовая природа криптовалюты.

Если мы рассматриваем современные цифровые технологии в качестве предмета обозначенных составов преступлений, то подчеркнем, что в этом случае можно вести речь:

– о безналичных денежных средствах;

– цифровых правах;

– цифровой валюте.

Прежде чем использовать криптовалюту в своих преступных целях, террористы и представители киберкриминала всегда оценивают свои риски. И если 6–8 лет назад представители террористических организаций и организованной преступности скептически относились к возможностям использования криптовалюты, то в настоящее время цифровая валюта используется преступниками повсеместно. Прежняя позиция была основана на следующих тезисах, которые озвучивали эксперты Европарламента:

– террористы и другие преступники с подозрением относятся к криптовалютам, поскольку считают, что биткоин специально создан ФБР для возможности их выявления и раскрытия их преступной деятельности;

– многие представители террористических организаций, в первую очередь их руководители, – это люди старшего возраста (40–50 лет), которые не всегда понимают сути криптовалюты и, соответственно, испытывают к ней недоверие;

– представители организованной преступности и террористы видят особо пристальный интерес международных и национальных финансовых организаций и правоохранительных структур к сфере криптовалют, вследствие чего не хотят оказаться в поле зрения их интересов[2].

Сейчас ситуация изменилась. Террористы и представители организованной преступности видят, как развивается сфера цифровых технологий, и в особенности сфера финансов. Ни для кого не секрет, с каким количеством технических, юридических, организационных, материальных, кадровых трудностей сталкиваются представители правоохранительных органов для того, чтобы выявить проводимые транзакции криптовалюты. В этой связи в настоящее время для террористов и представителей организованной преступности использование криптовалюты остается по-прежнему привлекательным и актуальным. Однако общественные отношения не стоят на месте, они развиваются. Развивается и государственная политика в области противодействия цифровым преступлениям, в том числе финансированию террористической деятельности посредством криптовалюты. Как подчеркивают специалисты, актуальные, отвечающие современным реалиям и требованиям безопасности правовые предписания, касающиеся работы криптобирж, заставят последних более внимательно относиться к проводимым транзакциям, поскольку в противном случае возможно будет привлечь к ответственности не только самих преступников, использующих криптовалюту в преступных целях, но и представителей криптобирж за то, что последние допустили использование криптовалюты в криминальных целях [6, с. 198].

Особенности уголовной политики в области противодействия цифровой преступности

Продолжая наше исследование, обратимся к анализу современной уголовной политики в сфере обеспечения цифровой безопасности, а именно коснемся вопроса о предупреждении и профилактике данного вида преступлений. В научной литературе обоснованно подчеркивается, что эффективная криминологическая профилактика осуществляется за счет различных средств и методов, в том числе посредством построения грамотных криминологических про-

[1] Суд впервые признал криптовалюту имуществом // Российский медиахолдинг «РБК». URL: https://www.rbc.ru/finances/07/05/2018/5af0280d9a7947165a6e8c22?ysclid=lmaeguk8vq139837849 (дата обращения: 24.10.2023).

[2] Криптовалюта, блокчейн и преступность // Livejournal. URL: https://sell-off.livejournal.com/27856173.html?ysclid=lmaanwxby896569801 (дата обращения: 24.10.2023).

гнозов [7, с. 157], посредством выявления особенностей того или иного вида преступности и т. д. Данный постулат характерен и в отношении профилактики цифровой (информационной) преступности.

Информация – одна из важнейших составляющих в жизни, оказывающая влияние практически на все сферы жизнедеятельности человека. На сегодняшний день киберпреступность представляет большую угрозу современному миру, стремительно растет киберпреступность и в Российской Федерации.

В этой связи обращение к вопросам профилактики и противодействия цифровой преступности является крайне актуальным и социально обусловленным.

Противодействие киберпреступности, а также различным преступным проявлениям, направленным на получение особо важной информации и преимущественно на хищение денег граждан и организаций, совершаемым при помощи информационных технологий и телекоммуникаций (ИТТ), относятся к глобальным задачам, стоящим перед государством. Всплеск преступлений, совершаемых при помощи ИТТ, вызывает обеспокоенность среди правоохранительных органов (причем не только органов внутренних дел, но и органов прокуратуры и ФСБ России), а также в целом затрагивает национальные интересы Российской Федерации.

Поэтому предупреждение и раскрытие цифровых преступлений является неотъемлемой частью правоохранительной деятельности соответствующих субъектов профилактики. В частности, предупреждение, выявление, пресечение и раскрытие оперативными подразделениями органов внутренних дел преступлений в сфере компьютерной информации являются первоочередными задачами, решаемыми оперативно-разыскными органами полиции.

Основными направлениями предупреждения цифровых преступлений являются правовые, организационные, материально-технические, методические, кадровые и т. п.

Подчеркнем, что названные направления предупреждения цифровой преступности должны применяться вместе, в совокупности. При этом, несомненно, их реализация должна основываться на нормах действующего законодательства. В этой связи отметим, что правовое регулирование предупреждения цифровых преступлений имеет первостепенное значение. Источниками правовых мер предупреждения цифровых преступлений традиционно являются уголовно-правовые нормы законодательства, устанавливающие ответственность за их совершение, а также нормы иных отраслей права, так или иначе затрагивающие вопросы предупреждения цифровых преступлений.

Однако, на наш взгляд, недостаточно только формально закрепить запрет на совершение того или иного цифрового преступления. Требуется выработать эффективный механизм реализации данных норм, что обеспечивается при помощи фактической реализации закрепленных превентивных мер борьбы с цифровой преступностью. Именно поэтому мы можем с уверенностью говорить о том, что нужен комплексный подход к реализации различных направлений предупреждения цифровой преступности.

На наш взгляд, помимо правовых мер превенции, большим профилактическим потенциалом обладают организационные меры борьбы с цифровыми преступлениями. К организационным мерам предупреждения цифровых преступлений можно отнести совокупность мероприятий, схематично изложенную ниже (рис.).

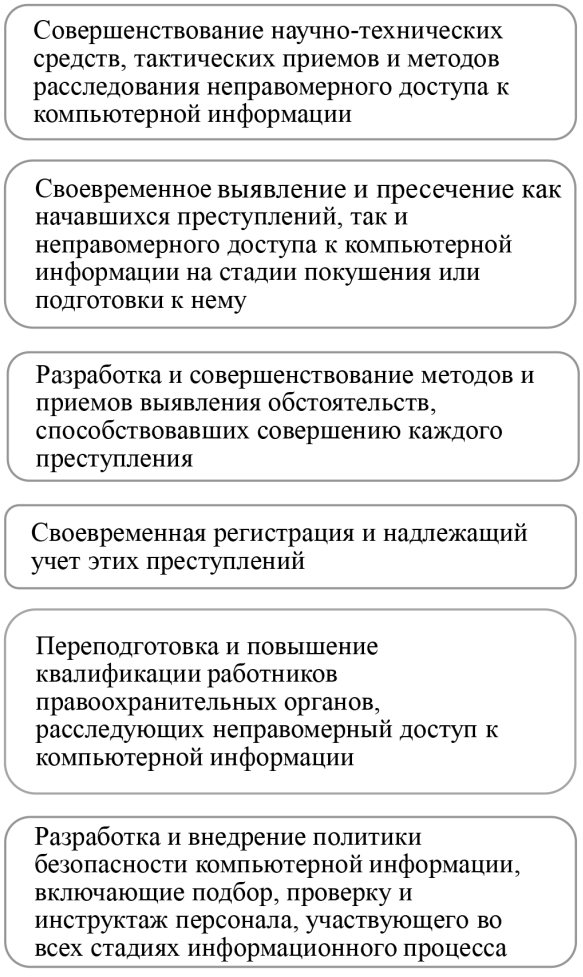

Рис. Организационные меры борьбы с цифровой преступностью

На наш взгляд, организационные меры борьбы с цифровой преступностью являются фундаментом, на котором строится вся система защиты компьютерной информации от неправомерного доступа.

Подчеркнем, что различные меры предупреждения цифровых преступлений всегда реализуются теми или иными субъектами, отдельными лицами. В зависимости от предназначения субъектов предупреждения и от того, для чего данные субъекты были созданы и функционируют, они подразделяются на специализированные и неспециализированные:

1. Специализированные органы, основной целью которых является обеспечение цифровой безопасности в государстве. К данной категории субъектов следует отнести:

– ФСБ РФ;

– Службу внешней разведки РФ;

– Министерство обороны РФ;

– Росгвардию;

– МВД РФ;

– ФСО РФ.

2. Неспециализированные государственные и общественные органы, организации и объединения, занимающиеся превентивной работой наравне с иной деятельностью (предупреждение цифровой преступности не является основным видом деятельности):

– органы государственной власти Российской Федерации и органы местного самоуправления, осуществляющие управление в различных сферах жизнедеятельности общества;

– образовательные организации;

– институт семьи, родители, близкие родственники;

– средства массовой информации;

– отдельные граждане и в целом общество, поскольку в той или иной мере каждый гражданин задействован в предупреждении цифровой преступности.

Поскольку цифровые технологии стали широко применяться в повседневной жизни, очень важно осуществлять комплексное взаимодействие различных субъектов профилактики (как специализированных, так и неспециализированных) между собой.

В профилактике киберпреступности большая роль отводится частным (негосударственным) структурам. Например, на базе ИТ-компании «Лаборатория Касперского», а также в компаниях, занимающихся цифровой безопасностью, большое внимание уделяется вопросам обучения сотрудников навыкам обеспечения цифровой безопасности. Подобная деятельность осуществляется и в государственном секторе, например на базе международного учебно-методического центра финансового мониторинга (МУМЦФМ).

Особое место в системе субъектов, осуществляющих деятельность по предупреждению цифровых преступлений, занимают органы внутренних дел, в особенности Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий.

В настоящей работе авторы обратились к анализу понятия цифрового преступления (преступления, совершаемого с использованием цифровых, информационных, технологий). Сделано заключение, что в настоящее время отсутствует легальное определение данного термина, что в теории вызывает определенные споры и дискуссии относительно содержания данного понятия. Вместе с тем наибольшим практическим значением обладает разрешение вопроса о профилактике подобных преступлений. Авторы обоснованно подчеркивают, что наибольшим объемом полномочий в вопросах борьбы с цифровыми преступлениями наделены специализированные субъекты профилактики цифровых преступлений. Однако обеспечить системную реализацию всех мер превенции могут только все субъекты вместе. В вопросах борьбы с цифровыми преступлениями субъекты профилактики должны действовать сообща и выстраивать эффективный механизм взаимодействия и обмена необходимой информацией.

СПИСОК ЛИТЕРАТУРЫ

1. Асатрян Х. А., Христюк А. А. Проблемы определения предмета взяточничества и особенности его выявления в современных реалиях // Всероссийский криминологический журнал. 2022. Т. 16, № 3. С. 374–383.

2. Евдокимов К. Н. Структура и состояние компьютерной преступности в Российской Федерации // Юридическая наука и правоохранительная практика. 2016. № 1 (35). С. 86–94.

3. Жмыхов А. А. Компьютерная преступность за рубежом и ее предупреждение : дис. … канд. юрид. наук : 12.00.08. М. : Всерос. науч.-исслед. ин-т МВД РФ, 2003. 178 с.

4. Зеер В. А., Родикова Л. Н. Цифровые технологии в определении интегрального показателя качества проектируемой техники в условиях недостатка информации // Социально-экономический и гуманитарный журнал. 2021. № 4 (22). С. 38–49.

5. Машевская О. В. Цифровые технологии как основа цифровой трансформации современного общества // Вестник Полесского государственного университета. Серия общественных и гуманитарных наук. 2020. № 1. С. 37–44.

6. Мурадян С. В. Перспективы использования криптовалют для целей финансирования терроризма и меры по предупреждению указанной тенденции // Закон и право. 2022. № 5. С. 196–201.

7. Сидорова Е. З. Примерный прогноз развития криминальной ситуации на объектах транспортной инфраструктуры

Восточно-Сибирской железной дороги // Социально-экономический и гуманитарный журнал. 2022. № 3 (25). С. 155–173.

8. Сидорова Е. З. Современные криминологические характеристики цифровой преступности (цифровой преступник и его жертва) // Сибирский юридический вестник. 2023. № 3(102). С. 70–78.

9. Сидорова Е. З. Уголовно-правовое противодействие финансированию экстремистской деятельности и терроризма : монография. Иркутск : Вост.-Сиб. ин-т МВД России, 2023. 96 с.

10. Ульянов М. В. Преступления, совершаемые с использованием информационных технологий: динамика и тенденции // Общество и право. 2020. № 2 (72). С. 32–36.

REFERENCES

1. Asatryan H.A., Hristyuk A.A. Problemy opredeleniya predmeta vzyatochnichestva i osobennosti ego vyyavleniya v sovremennyh realiyah [Problems of determining the subject of bribery and features of its detection in modern realities]. *Vserossijskij kriminologicheskij zhurnal* [All-Russian Criminological Journal], 2022, vol. 16, no. 3, pp. 374-383. (in Russian)

2. Evdokimov K.N. Struktura i sostoyanie komp'yuternoj prestupnosti v Rossijskoj Federacii [Structure and state of computer crime in the Russian Federation].*Yuridicheskaya nauka i pravoohranitelnaya praktika* [Legal science and law enforcement practice], 2016, no. 1 (35), pp. 86-94. (in Russian)

3. Zhmyhov A.A. *Kompyuternaya prestupnost za rubezhom i ee preduprezhdenie* [Computer crime abroad and its prevention]. Moscow, All-Russian scientific Research Institute of the Ministry of Internal Affairs of the Russian Federation Publ., 2003, 178 p. (in Russian)

4. Zeer V.A., Rodikova L.N. Cifrovye tekhnologii v opredelenii integral'nogo pokazatelya kachestva proektiruemoj tekhniki v usloviyah nedostatka informacii [Digital technologies in determining the integral indicator of the quality of the designed equipment in conditions of lack of information]. *Socialno-ekonomicheskij i gumanitarnyj zhurnal* [Socio-economic and Humanitarian Journal], 2021, no. 4 (22), pp. 38-49. (in Russian)

5. Mashevskaya O.V. Cifrovye tekhnologii kak osnova cifrovoj transformacii sovremennogo obshchestva [Digital technologies as the basis of digital transformation of modern society]. *Vestnik Polesskogo gosudarstvennogo universiteta. Seriya obshchestvennyh i gumanitarnyh nauk* [Bulletin of the Polessky State University. A series of social sciences and humanities], 2020, no. 1, pp. 37-44. (in Russian)

6. Muradyan S.V. Perspektivy ispolzovaniya kriptovalyut dlya celej finansirovaniya terrorizma i mery po preduprezhdeniyu ukazannoj tendencii [Prospects of using cryptocurrencies for the purposes of financing terrorism and measures to prevent this trend]. *Zakon i pravo* [Law and Law], 2022, no. 5, pp. 196-201. (in Russian)

7. Sidorova E.Z. Primernyj prognoz razvitiya kriminalnoj situacii na ob"ektah transportnoj infrastruktury Vostochno-Sibirskoj zheleznoj dorogi [Approximate forecast of the development of the criminal situation at the transport infrastructure facilities of the East Siberian Railway]. *Socialno-ekonomicheskij i gumanitarnyj zhurnal* [Socio-economic and Humanitarian Journal], 2022, no. 3 (25), pp. 155-173. (in Russian)

8. Sidorova E.Z. Sovremennye kriminologicheskie harakteristiki cifrovoj prestupnosti (cifrovoj prestupnik i ego zhertva) [Modern criminological characteristics of digital crime (digital criminal and his victim)]. *Sibirskij yuridicheskij vestnik* [Siberian Legal Bulletin], 2023, no. 3(102), pp. 70-78. (in Russian)

9. Sidorova E.Z. *Ugolovno-pravovoe protivodejstvie finansirovaniyu ekstremistskoj deyatelnosti i terrorizma* [Criminal legal counteraction to the financing of extremist activity and terrorism]. Irkutsk, East Siberian Institute of the Ministry of Internal Affairs of Russia Publ., 2023, 96 p. (in Russian)

10. Ul'yanov M.V. Prestupleniya, sovershaemye s ispolzovaniem informacionnyh tekhnologij: dinamika i tendencii [Crimes committed using information technologies: dynamics and trends]. *Obshchestvo i pravo* [Society and law], 2020, no. 2 (72), pp. 32-36. (in Russian)

Статья поступила в редакцию 10.10.2023; одобрена после рецензирования 15.01.2024; принята к публикации 04.09.2024

Received on 10.10.2023; approved on 15.01.2024; accepted for publication on 04.09.2024

Сидорова Екатерина Закариевна – кандидат юридических наук, доцент, заместитель начальника кафедры уголовного права и криминологии, Восточно-Сибирский институт МВД России (Россия, 664071, г. Иркутск, ул. Лермонтова, 110), ORCID: 0000-0002-3477-3816, РИНЦ AuthorID: 828571, e-mail: ketrik6@mail.ru

Sidorova Ekaterina Zakarievna – Candidate of Juridical Sciences, Associate Professor, Deputy Head of the Department of Criminal Law and Criminology, East Siberian Institute of the Ministry of Internal Affairs of Russia (110, Lermontov st., Irkutsk, 664071, Russian Federation), ORCID: 0000-0002-3477-3816, RSCI AuthorID: 828571, e-mail: ketrik6@mail.ru

Усов Евгений Геннадьевич – кандидат юридических наук, доцент Байкальского института БРИКС, Иркутский национальный исследовательский технический университет (Россия, 664074, г. Иркутск, ул. Лермонтова, 83), ORCID: 0000-0002-5373-8346, РИНЦ AuthorID: 919465, e-mail: usov.evgeniy@list.ru

Usov Evgeny Gennadievich – Candidate of Juridical Sciences, Associate Professor of the Baikal Institute of BRICS, Irkutsk National Research Technical University (83, Lermontov st., Irkutsk, 664074, Russian Federation), ORCID: 0000-0002-5373-8346, RSCI AuthorID: 919465, e-mail: usov.evgeniy@list.ru

Вклад авторов

Сидорова Екатерина Закариевна – концепция исследования (формирование идеи, формулировка ключевых целей и задач), написание текста, утверждение окончательного варианта статьи.

Усов Евгений Геннадьевич – сбор и обработка материала, работа с нормативными актами и методическими материалами, редактирование статьи (внесение замечаний).