УДК 343.213 DOI: 10.14529/law220302

ВЗАИМОДЕЙСТВИЕ СУБЪЕКТОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННО-ЦИФРОВОЙ БЕЗОПАСНОСТИ: СТРАНОВЕДЧЕСКИЙ АНАЛИЗ

Ю. А. Воронин, А. А. Дмитриева, Т. В. Кухтина
Южно-Уральский государственный университет, г. Челябинск

Интенсивный рост информационно-цифровой преступности в современном мире диктует настоятельную необходимость взаимодействия между субъектами, противодействующими ей как на национальном, так и межгосударственном уровнях. В полной мере это относится к России, Великобритании и США, в которых система борьбы с данной категорией преступлений складывается из совместных усилий целого ряда субъектов. При этом все в большей мере указанная система базируется на использовании современных достижений науки, совершенствовании информационно-коммуникационных технологий. Особенно важную роль в каждой из упомянутых стран играют сотрудничество в сфере межведомственного взаимодействия национальных правоохранительных структур, координация этой деятельности с органами власти и управления, институтами гражданского общества. Кроме того, как свидетельствует страноведческий анализ практики борьбы с цифровой преступностью, чрезвычайно актуальным является межгосударственное сотрудничество, в частности обмен оперативной информацией для успешного расследования соответствующей категории уголовных дел. Следует подчеркнуть, что эффективность всех перечисленных элементов взаимодействия субъектов противостояния с информационно-цифровой преступностью достигается лишь при добросовестном выполнении ими взятых на себя обязательств.

Ключевые слова: цифровая преступность, информационно-коммуникационные технологии, правоохранительные структуры, межведомственное взаимодействие, межгосударственное сотрудничество.

1. В соответствии с нормами национального законодательства и международного права каждое государство вправе защищать себя и своих граждан от криминальных посягательств, в том числе от всех возрастающих в масштабах информационно-цифровых деликтов. Как подчеркивается в принятых в 2001 года Генеральной Ассамблеей ООН двух резолюциях № 55/63 и № 56/121 «О борьбе с преступным использованием информационных технологий», интенсивный рост информационно-цифровой преступности диктует настоятельную необходимость взаимодействия государств в противодействии ей не только на национальном, но и на международном уровнях. В равной мере это относится к Российской Федерации, Великобритании и США, в которых система противодействия цифровой преступности, складывающаяся из совместных усилий целого ряда субъектов, все в большей степени основывается на использовании современных достижений науки, совершенствовании информационно-цифровых и компьютерных технологий. Особенно важную роль в каждой из упомянутых стран играет сотрудничество в сфере межведомственного информационного взаимодействия их национальных правоохранительных структур, координация этой деятельности с органами власти и управления, институтами гражданского общества. Несомненное значение имеют также их международные связи в этой области, в частности обмен оперативно значимой информацией с зарубежными коллегами для оптимизации производства по уголовным делам.

2. Как свидетельствует практика борьбы с информационно-цифровой преступностью в России, Великобритании и США, речь идет, прежде всего, о совместных усилиях, ведомственном сотрудничестве правоохранительных органов, их специализированных подразделений и служб безопасности на национальном уровне.

Так, в Российской Федерации в соответствии с п. 5 Положения о координации деятельности правоохранительных органов по борьбе с преступностью, утвержденного Указом Президента РФ от 18 апреля 1996 г. № 567 основным субъектом, стимулирующим

такую «кооперацию», являются Генеральная прокуратура и ее органы на территории всей страны. Именно прокуратуре, в соответствии с законом, принадлежит функция главного координатора в деле взаимодействия правоохранительных структур, других органов власти и управления, а также общественных формирований, противодействующих преступности, в том числе в сфере цифровых коммуникаций. Одновременно, используя инструментарий государственной автоматизированной системы правовой статистики, прокурорские органы всех уровней выполняют информационно-аналитические функции. Речь идет, в частности, об информировании субъектов государственной власти – прежде всего Совета безопасности РФ, Администрации Президента РФ, руководителей правоохранительных ведомств – о выявленных, раскрытых киберпреступлениях и предпринимаемых мерах по стабилизации ситуации. Наряду с этим, чрезвычайно важной является инициируемая прокуратурой (совместно с другими правоохранительными ведомствами) разработка мер в сфере использования цифровых технологий в рамках противодействия преступности, включая информационно-цифровые деликты. В контексте выполнения этих задач большое значение, несомненно, имеет практикуемое прокурорскими органами проведение координационных совещаний и семинаров с соответствующей повесткой обсуждаемых вопросов.

Кроме того, есть основания констатировать, что наличие реально скоординированного взаимодействия прокурорских органов не только с субъектами в политической и правоохранительной областях, но и с профессионалами в сфере высоких технологий, также способно поднять эффективность решения назревших задач. Яркий пример тому – совместный проект Генеральной прокуратуры РФ и Министерства цифрового развития, связи и массовых коммуникаций РФ, в котором упомянутое министерство выступает в качестве технологического эксперта по внедряемым схемам цифровых новелл трансформации органов прокуратуры, включая использование цифровых платформ координации органов правопорядка, а также органов контроля и надзора [5, с. 4, 5]. В целом подобного рода сотрудничество является одной из основных характеристик, отражающих содержание организационного аспекта работы органов прокуратуры по противодействию преступности, в том числе в цифровой сфере.

Не менее велика и роль органов Министерства внутренних дел РФ и Федеральной службы безопасности, являющихся ведущими ведомствами в деле оперативного противодействия правонарушениям, их предотвращения и раскрытия, включая информационно-цифровые преступления. Достаточно сказать, что наиболее значительная часть таких общественно опасных деяний выявляется именно органами МВД. Что же касается специализированных подразделений ФСБ России, то они являются основными субъектами, обладающими полномочиями по координации оперативных разработок и расследованию особенно сложных преступлений, связанных с киберпосягательствами на объекты стратегических инфраструктур Российского государства. В этой связи, оперативное взаимодействие соответствующих служб того и другого ведомства в немалой степени способствует результативности предпринимаемых ими усилий.

Не менее важна также роль Следственного комитета РФ. Упомянутое правоохранительное ведомство, наряду с осуществлением своей специфической профессиональной компетенции, также реализует в своем сегменте важнейшую интеграционную функцию, а именно: быть связующим элементом, сосредоточивающим и концентрирующим усилия различных государственных ведомств, научных учреждений и специалистов для эффективного и слаженного противодействия преступным проявлениям в информационной сфере [3].

Помимо исключительной важности анализируемого сотрудничества правоохранительных структур Российской Федерации, особую значимость сегодня приобретают усилия по активизации государственного и частного партнерства, поскольку ключевое значение для эффективного противодействия информационно-цифровым преступлениям имеют тесные контакты правоохранителей с другими организациями, располагающими оперативно значимой информацией для их расследования и раскрытия. Это банки, операторы связи, интернет-провайдеры, владельцы интернет-сервисов, центры реагирования на компьютерные инциденты [6, с. 5].

В сложившейся ситуации кадровый состав правоохранительных органов, работаю-

щий в данном сегменте борьбы с преступностью, должен динамично приспосабливаться, овладевать современной методикой расследования и профилактики преступлений, совершаемых в информационно-цифровой сфере. Особенно актуальны в этой связи специализация оперативного состава и следователей, их закрепление на расследовании преступлений в сфере информационных технологий с использованием соответствующего опыта и наличия специальных познаний. Речь, в частности, идет о способности данного контингента сотрудников ориентироваться в специфике и многообразии банковской деятельности. Ведь финансово-банковская система любой страны, являясь одним из основных сегментов экономики, призвана обеспечивать финансовые интересы личности, общества и государства [8, с. 4, 5]. Но, к сожалению, как справедливо констатируют многие специалисты, анализ состояния банковской системы последних лет неизменно свидетельствует, что процесс становления рыночных отношений по-прежнему сопровождается обострением криминогенной ситуации в данной сфере [7, с. 3].

Именно поэтому, наряду с мерами правоохранительных органов по совершенствованию способов выявления следов высокотехнологичной цифровой преступности, следует упомянуть прежде всего о существенном вкладе Банка России в объединенные усилия по предупреждению несанкционированных проникновений и компьютерных взломов в кредитно-финансовой сфере. В частности, речь идет о деятельности (входящего в структуру Банка России) Центра мониторинга и профилактики кибератак со стороны криминальных элементов посредством взлома компьютерной сети кредитно-финансовых организаций. Указанные функции данное подразделение осуществляет в тесном взаимодействии с ФСБ России и МВД России, оказывая специалистам этих органов экспертно-консультационную и аналитическую поддержку [1, с. 32]. И это особенно актуально, учитывая довольно низкий уровень раскрываемости следственным аппаратом РФ информационно-цифровых деликтов, который составлял в 2021 году в среднем около 20 %.

Поэтому, как справедливо подчеркивают российские специалисты, пока еще предстоит более основательно проработать механизмы и порядок такого сотрудничества. В том числе это касается и совместной законопроектной деятельности упомянутых субъектов противодействия цифровой преступности. Характерным примером успешного продвижения в этом отношении является положительный опыт совместных усилий МВД России, Роскомнадзора, Банка России и Генеральной прокуратуры Российской Федерации, в частности по разработке оптимальных санкций за мошенничество под видом предоставления государственных выплат [4, с. 158].

Помимо уже упомянутых форм взаимодействия, особое значение для России сегодня приобретает межгосударственное сотрудничество отечественных и зарубежных правоохранительных служб в области укрепления безопасности информационно-коммуникационных систем, защиты их от криминальных деликтов. Российская Федерация постоянно стремится к налаживанию взаимодействия с иностранными коллегами в этой сфере. В частности российские органы предварительного следствия, осуществляя мероприятия, направленные на своевременное раскрытие и расследование указанных преступлений, нередко направляют соответствующие запросы в правоохранительные организации иностранных государств в соответствии с существующими международными договорами. И это вполне объяснимо и целесообразно. Но упомянутая ключевая составляющая международного сотрудничества – обмен информацией – может по-настоящему эффективно реализовываться лишь с принятием единого документа, который содержал бы общее понимание таких преступлений и их видов. Именно поэтому необходимо наладить механизм «международного слежения» за добросовестностью соблюдения государствами взятых на себя договорных обязательств в противостоянии с цифровой преступностью. И именно в этом направлении следует двигаться, так как сегодня это важнейшее условие обеспечения ощутимых результатов. Не случайно Российская Федерация играет активную роль в разработке международной стратегии совместного участия государств мирового сообщества в противодействии информационно-цифровой преступности, включая унификацию уголовно-правовых норм, регулирующих ответственность за неправомерный доступ к компьютерной информации и использование вредоносных компьютерных программ. В этих целях она использует потенциал таких международных организаций, как ООН, ШОС, БРИКС,

для активизации международных правовых механизмов укрепления сотрудничества государств – членов этих организаций.

К сожалению, усилия России по разработке и принятию единой нормативно-правовой базы сотрудничающих государств для противодействия все возрастающему использованию в преступных целях информационно-цифровой среды не всегда встречают понимание и поддержку. Пример тому – судьба инициированного Российской Федерацией и внесенного на рассмотрение в Третий комитет Генеральной Ассамблеи ООН еще в 2019 году пакета предложений и проекта резолюции «Противодействие использованию информационно-коммуникационных технологий в преступных целях». Запланированное согласование и окончательное принятие поддержанных большинством голосов документов, намеченные на 2020 год, до сих пор остаются не реализованными, вопреки их очевидной актуальности и настойчивым усилиям России по активизации этого процесса.

3. Несмотря на возникающие трудности, упомянутые выше элементы и формы взаимодействия субъектов борьбы с информационно-цифровой преступностью в той или иной степени характерны сегодня не только для России, но и для других стран мирового сообщества, особенно для Великобритании и США.

Так, провозгласив своей важнейшей задачей реализацию принятой еще в 2011 году «Стратегии кибербезопасности Соединенного Королевства», а затем Национальной стратегии кибербезопасности Великобритании на период 2016–2021 гг., правительство данного государства в течение десятилетия последовательно профинансировало на общую сумму более 1,5 миллиардов фунтов стерлингов осуществление мер по снижению уровня киберпреступности. В комплексе этих мер было создание Национального подразделения по вопросам киберпреступности (NCCU), ответственного за координацию совместных действий в отношении данной категории общественно опасных деяний. Речь прежде всего шла о финансовом, экспертном, информационном содействии различным национальным и региональным ведомствам и агентствам, а также международным правоохранительным структурам в целях обеспечения эффективного реагирования на наиболее серьезные киберугрозы. Можно констатировать, что именно в русле анализируемой тенденции шло дальнейшее развитие событий. Особенно примечательным для Великобритании в этом плане стал ноябрь 2020 года, который ознаменовался созданием новой, еще более консолидированной структуры – Национальных кибернетических сил страны. Задекларированной задачей нового ведомства (NCF) явилось обеспечение теснейшей координации и взаимодействия профильных сотрудников различных британских спецслужб, а именно: отдела по киберпреступности при Агентстве по борьбе с организованной преступностью (SOCA), Центрального отдела по борьбе с киберпреступностью столичной полиции и других учреждений.

На содержание данной структуры в рамках министерства обороны страны, привлекшей к сотрудничеству несколько тысяч экспертов в информационно-технологической и финансовой сферах, было ассигновано пять миллиардов фунтов стерлингов. Следует подчеркнуть, что значительные ресурсы из упомянутых ассигнований были выделены именно для обеспечения государственно-частного партнерства, а не только деятельности правоохранительных структур в области противодействия информационно-цифровой преступности. Одной из самых эффективных форм такого взаимодействия между правоохранительными ведомствами и бизнес-структурами явилось информационно-аналитическое сотрудничество между ними, обмен информацией о киберугрозах в целях противодействия криминальным деликтам. Классическим примером такого взаимодействия служит вклад Британской торговой ассоциации «TechUK» – крупнейшего игрока в сферах высоких технологий, включая обеспечение безопасности национальных инфраструктур от террористических посягательств и борьбу с организованной преступностью в информационно-цифровой сфере. Вполне логично, что важнейшими партнерами в таком сотрудничестве являются не только спецслужбы и оборонное ведомство, но и крупнейшие банки страны. Кроме того, большой вклад в это взаимодействие вносят Совет Великобритании по электронному бизнесу, Британское компьютерное общество (BCS) и ряд других коммерческих и некоммерческих организаций, в том числе на международном уровне. Все это – преимущественно в рамках выполнения давних между

народных договоренностей в духе Конвенции Совета Европы о борьбе с преступностью в сфере компьютерной информации.

4. Не менее динамичной в этом отношении является деятельность США. Так, в 2021 году конгломерат спецслужб (с привлечением к сотрудничеству профессионалов высокой квалификации) был сформирован под общим руководством главного оборонного ведомства страны – Пентагона. Подчеркнем, однако, что это не упразднило интенсивное развитие и кооперацию национальной сети других, уже существовавших и демонстрировавших достаточно высокую активность, многочисленных субъектов противодействия преступности, включая цифровую. В том числе, речь идет об одном из аспектов деятельности Национального контртеррористического центра, Агентства Национальной Безопасности (АНБ), Агентства по кибербезопасности, соответствующего отдела в структуре ФБР, Государственного департамента криминальных расследований Службы внутренних доходов США (IRS), Государственного казначейства США, а также целого ряда других федеральных учреждений, сотрудничающих в рамках так называемых «Совместных антитеррористических сил» (Joint Terrorism Forces) на всей территории страны. В самом же широком контексте ответственность за координацию (с учетом интересов заинтересованных ведомств) и финансирование соответствующих разделов национальных программ противодействия преступности, включая киберпреступность, по-прежнему возложена на АСПД – Администрацию содействия правоприменительной деятельности при Минюсте США.

Очевидно, однако, что успех этой деятельности не может быть достигнут лишь силами перечисленных специализированных структур и ведомств. Как свидетельствует складывающаяся в США ситуация, другим важнейшим элементом комплекса взаимодействия субъектов противостояния с высокотехнологичной цифровой преступностью является их сотрудничество с финансовыми институтами и бизнес-организациями. С учетом проникновения цифровых технологий в каждую «клеточку» экономического организма американского социума и государства, принципиально важным является использование самих финансовых институтов в противостоянии с киберпреступлениями. Правовой базой организационных шагов в этом направлении послужил принятый Конгрессом США в 2015 году Акт о кибербезопасности (CSA). В свою очередь его финансовую основу обеспечило включение этого законодательного акта в Акт о консолидированных ассигнованиях 2016 года (Consolidated Appropriations Act). Оба они легитимизируют процесс обмена информацией о кибератаках между бизнес-организациями (главным образом, кредитно-финансовыми структурами), и правительственными учреждениями. Так, в рамках самого мощного национального Центра по обмену и анализу информации о финансовых услугах функционирует специальное подразделение по борьбе с киберпреступлениями, посягающими на финансовые институты, – Центр по финансовому системному анализу и устойчивости. Одной из важнейших его функций является координация антихакерской деятельности американских банков в тесном взаимодействии с правительственными организациями, прежде всего с ФБР. При этом упомянутый Центр демонстрирует высокую результативность благодаря финансовой и кадровой поддержке со стороны восьми крупнейших банковских структур страны. Среди них – «Бэнк оф Америка», «Голден Закс», «Морган Стэнли» и ряд других мощных финансово-кредитных организаций. Правда, оценивая сложившуюся ситуацию в целом, есть основания констатировать следующее. Хотя борьба с киберпреступниками в США идет давно и с определенным успехом, однако на каждый новый изощренный метод защиты финансово-кредитных структур хакеры отвечают созданием новых вирусных программ, новых технологий взлома [1, с. 12–18; 1, с. 30, 32, 33].

Что же касается взаимодействия США с зарубежными субъектами в рамках реализации международных конвенций по противодействию информационно-цифровой преступности, есть основания утверждать, что оно по-прежнему активно развивается. В частности в 2007 году Соединенные Штаты, наряду с целым рядом других государств, также ратифицировали Конвенцию о преступности в сфере компьютерной информации (ETS № 185), принятую Советом Европы 23 ноября 2001 г. (Будапештскую Конвенцию).

В связи с этим налаживание более тесных контактов с зарубежными партнерами в плане противодействия информационно-цифровой преступности, а также постоянная координация различных инициатив в этой области яв-

ляются типичными формами участия в международном сотрудничестве со стороны Госдепартамента, Министерства юстиции и Министерства внутренней безопасности США. Но во многом это относится и к деятельности киберподразделений ФБР, оперирующих на постоянной или временной основе вне пределов Соединенных Штатов в кооперации с правоохранительными органами других государств. Вместе с тем, не умаляя вклада США в различные формы международного сотрудничества, приходится констатировать их определенную непоследовательность. Так, именно Соединенные Штаты без убедительных аргументов продемонстрировали негативную позицию в отношении упомянутого нами выше пакета документов, внесенного Российской Федерацией 15 ноября 2019 г. на рассмотрение Генеральной Ассамблеи ООН, блокируя тем самым его принятие.

5. Подводя итог изложенному, есть основания констатировать, что в современных условиях именно повседневное взаимодействие и эффективное сотрудничество субъектов системы противодействия преступности в цифровой среде во многом являются залогом достижения успеха в решении поставленных задач. Понимание подобной необходимости, правда, с учетом национальной специфики, находит отражение в государственных решениях, определяющих стратегию защиты национальной кибербезопасности не только в России, Великобритании, США, но и в других странах мирового сообщества. Особенно очевидно это на примере сотрудничества правоохранительных органов с экспертно-консультационными специалистами и аналитиками в сфере цифровых технологий. Вместе с тем реальная практика свидетельствует, что, к сожалению, информационно-цифровая преступность нередко опережает сотрудников правоохранительных структур, имеющих менее фундаментальное образование в сфере высоких технологий, по сравнению с самими субъектами данной категории преступлений. Поэтому взаимодействие различных ведомств и организаций в борьбе с цифровой преступностью – как важнейший элемент этой борьбы – должно обладать принципиально важным качеством, а именно: быть высоко технологичным и опережающим по уровню профессионализма степень технической подготовленности и «квалифицированности» действий преступников. Только тогда объединение усилий и профессиональной квалификации правоохранителей и специалистов в сфере высоких технологий положительно скажется на качестве выявления, расследования и раскрываемости преступлений в информационно-цифровой среде.

В этой связи, по мнению экспертов в данной области, целесообразно было бы создание единой электронной сети участников информационно-цифрового пространства – государственных служб, банковских структур, интернет-провайдеров, средств массовой информации – для регулярного анализа и обмена информацией в рамках противодействия информационно-цифровой преступности. Что касается Российской Федерации, то эту функцию было бы целесообразно возложить на централизованный координирующий орган с соответствующей компетенцией. На наш взгляд, в соответствии с п. 5 Положения о координации деятельности правоохранительных органов по борьбе с преступностью, утвержденного Указом Президента РФ от 18 апреля 1996 г. № 567; и Приказом Генерального прокурора РФ от 16 января 2012 г. № 7 «Об организации работы органов прокуратуры Российской Федерации по противодействию преступности» подобная функция по существу (и вполне логично) вписывается в компетенцию именно прокурорских органов.

Литература

1. Воронин, Ю. А. Преступления в сфере обращения цифровой информации: сравнительные аспекты / Ю. А. Воронин. – Челябинск: Издательский центр ЮУрГУ, 2021. – 40 с.

2. Воронин, Ю. А. Стратегические направления противодействия преступности в цифровой сфере: страноведческий анализ / Ю. А. Воронин, И. М. Беляева, Т. В. Кухтина // Вестник Южно-Уральского государственного университета. Серия «Право». – 2020. – Т. 20. – № 2. – С. 12–18.

3. Интервью А. И. Бастрыкина от 10 июля 2020 г. URL: https://www.interfax.ru/russia.

4. Маныч, Е. Г. Кража финансовых данных или данных банковских карт – один из видов киберпреступлений / Е. Г. Маныч // Цифровые технологии в борьбе с преступностью: проблемы, состояние, тенденции: материалы Всерос. науч.-практ. конф. – М.: Университет прокуратуры РФ, 2021. – С. 158–162.

5. Реализация Концепции цифровой трансформации органов и организаций прокуратуры в современных условиях: сб. материалов круглого стола / под общ. ред. Е. Ю. Лихачевой. – М., 2019. – 76 с.

6. Разинкин, А. В. Вступительное слово / А. В. Разинкин // Цифровые технологии в борьбе с преступностью: проблемы, состояние, тенденции (Долговские чтения): сб. материалов I Всерос. науч.-практ. конф. – М., 2021. – 460 с.

7. Саркисян, М. С. Противодействие преступлениям, совершаемым в сфере банковской деятельности: дис. ... канд. юрид. наук / М. С. Саркисян. – М., 2009. – 167 с.

8. Хисамова, З. И. Уголовно-правовые меры противодействия преступлениям, совершаемым в финансовой сфере с использованием информационно-телекоммуникационных технологий: дис. ... канд. юрид. наук / З. И. Хисамова. – Краснодар, 2016. – 222 с.

Воронин Юрий Александрович – доктор юридических наук, профессор кафедры уголовного и уголовно-исполнительного права, криминологии, Южно-Уральский государственный университет, г. Челябинск. E-mail: voroninya@yandex.ru.

Дмитриева Анна Александровна – доктор юридических наук, заведующий кафедрой уголовного и уголовно-исполнительного права, криминологии, Южно-Уральский государственный университет, г. Челябинск. E-mail: dmitrievaaa@susu.ru.

Кухтина Татьяна Владимировна – старший преподаватель кафедры уголовного и уголовно-исполнительного права, криминологии, Южно-Уральский государственный университет, г. Челябинск, Российская Федерация. E-mail: kukhtinatv@susu.ru.

Статья поступила в редакцию 21 апреля 2022 г.

DOI: 10.14529/law220302

INTERACTION OF SUBJECTS OF INFORMATION AND DIGITAL SECURITY: COUNTRY-SPECIFIC ANALYSIS

Yu. A. Voronin, A. A. Dmitrieva, T. V. Kukhtina
South Ural State University, Chelyabinsk, Russian Federation

The intensive growth of information and digital crime in the modern world dictates the urgent need for interaction between entities that counteract it both at the national and interstate levels. This fully applies to Russia, the United Kingdom and the United States, where the system of combating this category of crimes consists of the joint efforts of a number of subjects. At the same time, to an increasing extent, this system is based on the use of modern scientific achievements, the improvement of information and communication technologies. A particularly important role in each of the above-mentioned countries is played by cooperation in the field of interdepartmental interaction of national law enforcement agencies, coordination of this activity with authorities and management bodies, civil society institutions. In addition, as evidenced by the country-specific analysis of the practice of combating digital crime, interstate cooperation is extremely relevant, in particular, the exchange of operational information for the successful investigation of the relevant category of criminal cases. It should be emphasized that the effectiveness of all these elements of interaction between the subjects of confrontation with information and digital crime is achieved only if they faithfully fulfill their obligations.

Keywords: digital crime, informational technologies, law enforcement agencies, interdepartmental cooperation, interstate cooperation.

References

1. Voronin Û. A. *Prestupleniâ v sfere obraŝeniâ cifrovoj informacii: sravnitel'nye aspekty* [Crimes in the sphere of digital information circulation: comparative aspects]. Chelyabinsk, 2021, 40 p.

2. Voronin Û. A., Belâeva I. M., Kuhtina T. V. [Strategic directions of combating crime in the digital sphere: a country-specific analysis]. *Vestnik Ûžno-Ural'skogo gosudarstvennogo universiteta. Seriâ «Pravo» [Bulletin of the South Ural State University. Series "Law"]*, 2020, Vol. 20, no. 2, pp. 12–18. (in Russ.)

3. *Interv'û A. I. Bastrykina ot 10 iûlâ 2020 g.* [Interview by A. I. Bastrykin from July 10, 2020]. Available at: www.interfax.ru/russia.

4. Manyč E. G. *Kraža finansovyh dannyh ili dannyh bankovskih kart – odin iz vidov kiberprestuplenij. Cifrovye tehnologii v bor'be s prestupnost'û: problemy, sostoânie, tendencii* [Theft of financial data or bank card data is a type of cybercrime. In the collection: Digital technologies in the fight against crime: problems, state, trends]. *Materialy Vserossijskoj naučno-praktičeskoj konferencii [Materials of the All-Russian Scientific and Practical Conference]*. Moscow, 2021, pp. 158–162.

5. Lihačeva E. Û. *Realizaciâ Koncepcii cifrovoj transformacii organov i organizacij prokuratury v sovremennyh usloviâh: sb. materialov kruglogo stola* [Implementation of the Concept of digital transformation of bodies and organizations of the Prosecutor's office in modern conditions: collection of materials of the round table]. Moscow, 2019, 76 p.

6. Razinkin A. V. *Vstupitel'noe slovo* [Introductory speech]. *Cifrovye tehnologii v bor'be s prestupnost'û: problemy, sostoânie, tendencii (Dolgovskie čteniâ): sb. materialov I Vseros. nauč.-prakt. Konf. [Digital technologies in the fight against crime: problems, state, trends (Dolgov readings): collection of materials I All-Russian scientific-practical. Conf.]*. Moscow, 2021, 460 p.

7. Sarkisân M. S. *Protivodejstvie prestupleniâm, soveršaemym v sfere bankovskoj deâtel'nosti: dis. ... kand. ûrid. nauk* [Countering crimes committed in the field of banking. Diss. Kand. (Law)]. Moscow, 2009, 167 p.

8. Hisamova Z. I. *Ugolovno-pravovye mery protivodejstviâ prestupleniâm, soveršaemym v finansovoj sfere s ispol'zovaniem informacionno-telekommunikacionnyh tehnologij: dis. ... kand. ûrid. nauk* [Criminal legal measures to counteract crimes committed in the financial sphere using information and telecommunication technologies. Diss. Kand. (Law)]. Krasnodar, 2016, 222 p.

Yuri Alexandrovich Voronin – Doctor of Sciences (Law), Professor of the Department of Criminal and Criminal-Executive Law, Criminology, South Ural State University, Chelyabinsk, Russian Federation. E-mail: voroninya@yandex.ru.

Anna Alexandrovna Dmitrieva – Doctor of Sciences (Law), Head of the Department of Criminal and Criminal-Executive Law, Criminology, South Ural State University, Chelyabinsk, Russian Federation. E-mail: dmitrievaaa@susu.ru.

Tatyana Vladimirovna Kukhtina – Research assistant of the Department of Criminal and Criminal-Executive Law, Criminology, South Ural State University, Chelyabinsk, Russian Federation. E-mail: kukhtinatv@susu.ru.

References 21 April 2022.

ОБРАЗЕЦ ЦИТИРОВАНИЯ

Воронин, Ю. А. Взаимодействие субъектов обеспечения информационно-цифровой безопасности: страноведческий анализ / Ю. А. Воронин, А. А. Дмитриева, Т. В. Кухтина // Вестник ЮУрГУ. Серия «Право». – 2022. – Т. 22, № 3. – С. 13–20. DOI: 10.14529/law220302.

FOR CITATION

Voronin Yu. A., Dmitrieva A. A., Kukhtina T. V. Interaction of subjects of information and digital security: country-specific analysis. *Bulletin of the South Ural State University. Ser. Law*, 2022, vol. 22, no. 3, pp. 13–20. (in Russ.) DOI: 10.14529/law220302.