КРИМИНАЛИСТИКА

УДК 343.6

И.П. Родивилин,
В.В. Коломинов,
Д.Э. Брыжак

ИНТЕЛЕКТУАЛЬНЫЙ РАЗВРАТ НЕСОВЕРШЕННОЛЕТНИХ В СЕТИ ИНТЕРНЕТ

В МВД отмечают увеличение количества случаев развратных действий в сети Интернет, где жертвами становятся несовершеннолетние и даже малолетние. Современные цифровые технологии расширяют доступ детей к полезной и нужной информации, но вместе с тем делают их особенно уязвимыми к негативному воздействию. Авторами не делается различия между виртуальными и реальными развратными действиями, в связи с тем, что вред психическому здоровью несовершеннолетних наносится одинаковый. Анализируется практика расследования уголовных дел в Восточно-Сибирском регионе России по преступлениям, квалифицируемым по ст. 135, 242^1 УК РФ, совершенным с использованием сети «Интернет», в период с 2008 г. по 2018 г., а также деятельность правоохранительных органов в сфере профилактики совершения развратных действий среди несовершеннолетних. Делается вывод о латентности виртуальных педофилов и пути решения данной проблемы.

Ключевые слова: преступления против половой неприкосновенности и половой свободы личности, насильственные действия сексуального характера, иные действия сексуального характера, квалификация, сеть Интернет.

I.P. Rodivilin,
V.V. Kolominov,
D.A. Bryzhak

INTELLECTUAL DEBAUCHMENT OF MINORS ONLINE

The Ministry of the Interior states that there is a growing number of online indecent assaults against juveniles or even children. Modern digital technologies give minors a wider access to necessary and useful information but, at the same time, make them especially vulnerable to negative impacts. The authors do not differentiate between virtual and real-life indecent assaults because they inflict equal damage on the psychological health of minors. They analyze the practice of investigating criminal cases under Art. 135, 242^1 of the Criminal Procedure Code of the Russian Federation in the East-Siberian Region of Russia, study crimes committed using the Internet in the time period between 2008 and 2018, and the work of the law

enforcement bodies on preventing indecent assaults against minors. The authors conclude that the crimes of virtual pedophiles are characterized by a high latency and describe ways of solving this problem.

Keywords: crimes against sexual integrity and sexual freedom, violent acts of sexual nature, other actions of sexual nature, qualification, the Internet.

На расширенных заседаниях коллегии Министерства внутренних дел последние несколько лет[1] глава государства отмечает положительную тенденцию снижения числа регистрируемых тяжких и особо тяжких преступлений. Однако при этом нераскрытыми остаются практически каждое второе из преступлений против личности[2].

Государство всегда уделяло внимание охране прав несовершеннолетних, как категории граждан наименее защищенной. Особенное внимание уделяется их психическому и физическому здоровью. Уголовный закон охраняет половую неприкосновенность и половую свободу несовершеннолетних. Однако, с развитием информационных технологий социальные взаимоотношения все больше перемещаются в сеть Интернет, где защитить указанные права становится сложнее ввиду специфики Интернета. Таким образом в современном обществе появилась повышенная виктимность в интернет-пространстве, создающая условия, в которых с высокой долей вероятности несовершеннолетние могут стать жертвами психологического, эмоционального и даже сексуального насилия. Под воздействием компьютеризации изменилось общество и цифровая реальность – наше настоящее [1, с. 38–39].

В России усиливается интенсификация процессов информатизации различных сфер деятельности в связи с тем, что информационные ресурсы, и информационная инфраструктура в совокупности образуют глобальную информационную среду нашего общества. Вопросы безопасности информации представляют собой важную часть процесса внедрения новых информационных технологий во все сферы жизни общества [2, с. 5]. Как верно отмечает А.В. Шободоева, защита информационного пространства в условиях возрастающей роли информационной сферы является одной из базовых задач общества и государства. Информационная безопасность приобретает все большую зна-

---

[1] Расширенное заседание коллегии МВД 04.03.2015. URL: http://kremlin.ru/events/president/news/47776 (дата обращения: 20.12.2018); Расширенное заседание коллегии МВД 15.03.2016. URL: http://kremlin.ru/events/president/news/51515/ (дата обращения: 20.12.2018); Расширенное заседание коллегии МВД 09.03.2017. URL: http://kremlin.ru/events/president/news/54014 (дата обращения: 20.12.2018); Расширенное заседание коллегии МВД 28.02.2018. URL: http://kremlin.ru/events/president/news/54014 (дата обращения: 20.12.2018).

[2] Состояние преступности в 2015 г. URL: https://мвд.рф/reports/item/7087734/ (дата обращения: 05.01.2019); Состояние преступности в 2016 г. URL: https://мвд.рф/upload/sitel/document_news/009/338/947/sb_1612.pdf (дата обращения: 05.01.2019); Состояние преступности в Российской Федерации за январь - декабрь 2017 года. URL: https://xn--b1aew.xn--p1ai/reports/item/12167987/(дата обращения: 09.01.2019); Состояние преступности в Российской Федерации за январь - декабрь 2018 года. URL: https://мвд.рф/reports/item/7087734/(дата обращения: 09.01.2019).

чимость в общей системе обеспечения национальной безопасности страны в целом [3, с. 74].

В соответствии с ч. 2 ст. 5 Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию» к информации, являющейся запрещенной для распространения среди детей, относится информация, способная вызвать у детей желание заниматься проституцией, пропагандирующая нетрадиционные сексуальные отношения, содержащая информацию порнографического характера. Кроме того в соответствии с п. 3 ч. 3 этой же статьи к информации, распространение которой среди детей определенных возрастных категорий ограничено, относится информация, представляемая в виде изображения или описания половых отношений между мужчиной и женщиной[3].

Не стоит делать различия между виртуальными и реальными развратными действиями, так как вред психическому здоровью несовершеннолетних наносится одинаковый. Соответствующая норма присутствует и в постановлении Пленума Верховного Суда РФ от 4 декабря 2014 г. № 16 «О судебной практике по делам о преступлениях против половой неприкосновенности и половой свободы личности»[4], в котором указанно, что развратными признаются действия, «при которых непосредственный физический контакт с телом потерпевшего лица отсутствовал, включая действия, совершенные с использованием сети Интернет, иных информационно-телекоммуникационных сетей».

Лица, страдающие педофилией в последнее время зачастую для удовлетворения своих сексуальных потребностей, уходят в виртуальное пространство. Каждый третий несовершеннолетний в возрасте от 11 до 16 лет когда-либо получал электронные сообщения сексуального характера, каждому шестому приходят подобные письма как минимум раз в месяц [4]. Действительно, в современном мире все сферы жизнедеятельности находятся в прямой зависимости от работы вычислительных и информационных сетей. Вместе с тем «широкое использование для обработки информации средств вычислительной техники с программным обеспечением, позволяющим сравнительно легко модифицировать, копировать и разрушать информацию» [5] повышает уязвимость информационного пространства.

Сложно переоценить значимость информационно-телекоммуникационного пространства, включая социальные сети. Так, Д.А. Степаненко и А.А. Рудых называют его «ценным, а порой единственным источником криминалистической информации» [6, с. 17].

В ходе изучения архивных материалов уголовных дел в Восточно-Сибирском регионе России по преступлениям, квалифицируемым по п. б, ч. 4 ст. 132, ст. 135, ст. 242[1] УК РФ, совершенным с использованием сети «Интернет», в период с 2008 г. по 2018 г., установлено, что в 95 % процентов случаев

[3] О защите детей от информации, причиняющей вред их здоровью и развитию : Федеральный закон РФ от 29 дек. 2010 г. № 436-ФЗ : (ред. от 1 мая. 2019 г.) // Собрание законодательства РФ. – 2011.– № 1.– Ст. 48.

[4] Российская газета. – 2015. – № 284.

преступник ищет свою жертву в социальных сетях «Одноклассники» и «В Контакте». Остальные знакомства происходят на менее популярных Интернет-ресурсах, таких как «Мой мир», «Фотострана» и т.п.

Склонность ребенка к общению на сексуальные темы или сексуальную расторможенность будущей жертвы виртуальные педофилы определяют абсолютно не задумываясь, наугад, высылая файлы с предложениями и фотоснимками эротического содержания, видеоматериалы порнографического характера, ведут циничные разговоры на сексуальные темы. Однако иногда, жертва подыскивается из числа пользователей, состоящих в определенных сообществах эротического характера. То есть у этих детей уже имеются склонности к девиантному сексуальному поведению, что облегчает злоумышленнику процесс совершения в отношении несовершеннолетнего развратных действий.

В результате анализа изученных уголовных дел, выявлено, что в большинстве случаев, педофил подыскивает жертву, находящуюся в другом регионе Российской Федерации. Из чего можно сделать вывод о том, что реально встречаться с детьми он не желает, а предпочитает виртуальный разврат. В тех случаях, когда жертва выбрана педофилом в территориальной близости, нередко имеется умысел на совершение иных половых преступлений в отношении несовершеннолетней жертвы в дальнейшем, после того когда он уговорит ее встретиться лично.

В электронных сообщениях «виртуального педофила» присутствуют высказывания, тематически относящиеся к сексуальной сфере. Сексуальная тематика вводится посредством употребления злоумышленником диалогов с большим количеством разнообразных лексических единиц, обозначающих фрагменты языковой действительности, непосредственно связанные с половой жизнью, с проявлением и удовлетворением полового влечения. Как правило, общение на сексуальные темы сопровождается демонстрацией своих и (или) загруженных из сети Интернет, половых органов.

Также, встречаются случаи, когда виртуальный педофил представляется врачом (урологом или гинекологом, в зависимости от того какого пола жертва). В процессе взросления и социализации дети пытаются найти ответы на интересующие их интимные темы в сети Интернет у незнакомых им людей, которые представляются профессионалами, а не у родителей или родственником, чем и пользуются преступники.

Для виртуального мира еще не в полной мере разработаны меры профилактики и предупреждения совершения преступлений в отношении несовершеннолетних, поэтому необходимо уделить этой ситуации особое внимание.

Представляется необходимым с целью эффективного противодействия рассматриваемым и иным преступлениям против несовершеннолетних подключить различные государственные органы и общественные организации, также этого требует и ювенальное уголовное судопроизводство, на что указывает ряд ученых [7, с. 336; 8, с. 771–772], кроме того следует наладить взаимодействие с правоохранительными органами, занимающимися обеспечением кибербезопасности, а также Национальным контактным пунктом, Интерполом, Европолом, Евроюстом [9]. Также в рамках международного сотрудничества

необходимо создание нормативных актов и выработка общих рекомендаций, внедрение эффективных моделей организационного взаимодействия между государствами, как в рамках взаимопомощи, так и ответов на запросы [10, с. 291].

Кроме того, правоохранительные органы обязаны выявлять несовершеннолетних и семьи, которые находятся в социально опасном положении, и безотлагательно принимать меры при выявлении фактов жесткого обращения с несовершеннолетними со стороны родителей, законных представителей и иных лиц, вовлекающих их в совершение преступления, других противоправных и (или) антиобщественных действий, а также несовершеннолетних, совершивших правонарушение или антиобщественные действия.

Кроме того, правоохранительные органы должны проводить индивидуальную профилактическую работу в отношении родителей или иных законных представителей несовершеннолетних, если они не исполняют своих обязанностей по их воспитанию, обучению и (или) содержанию и (или) оказывают отрицательное влияние на несовершеннолетнего, что отражается на его поведении, либо жестоко обращаются с ними.

В качестве профилактических мер необходимо организовать разъяснительные беседы с родителями детей предпубертатного и пубертатного возраста о правилах общения в сети Интернет. Разъяснять родителем и детям о том, что если незнакомый человек желает пообщаться на «непристойные» темы, то необходимо сразу обращаться в правоохранительные органы с целью найти и изолировать виртуального педофила. Подобную работу необходимо вести как в условиях учебного заведения, так и демонстрируя специальную социальную рекламу на телевидении и на популярных Интернет-ресурсах.

Деятельность правоохранительных органов в сфере профилактики совершения развратных действий среди несовершеннолетних проводится, как правило, по следующим направлениям:

1) мониторинг сети Интернет на предмет выявления деструктивных групп;

2) информационно-просветительская деятельность;

3) взаимодействие с психолого-медико-педагогическими комиссиями;

4) взаимодействие с молодежными организациями, волонтерами и общественными организациями правоохранительной направленности.

Сотрудниками оперативных служб территориальных органов МВД России совместно с БСТМ и ГУУР МВД России проводятся оперативно-розыскные мероприятия, направленные на выявление, пресечение и раскрытие преступлений, связанных с деятельностью лиц, склоняющих несовершеннолетних к разврату посредством оказания негативного психологического воздействия через Интернет и социальные сети.

В рамках указанных акций и учебной программы с детьми и подростками проводятся профилактические беседы, интерактивные викторины, интеллектуальные игры, круглые столы, семинары, диспуты, уроки-практикумы и иные мероприятия, направленные на формирование у несовершеннолетних навыков безопасного использования Интернет-пространства, на которых до сведения

детей также доводится необходимая информация. Освещаются проблемы интернет-зависимости, способы защиты от противоправных посягательств, организуются тестирования на знание правил поведения на Интернет-ресурсах.

Например, в ГУ МВД России по Ростовской области проводятся профилактические мероприятия с целью обучения родителей распознаванию признаков и факторов риска вовлечения детей в интеллектуальный разврат, адекватному реагированию на эти угрозы. При взаимодействии с педагогами-психологами при проведении профилактических мероприятий используются интерактивные формы и методы обучения (групповые дискуссии, ролевые и образовательные игры, тренинги и др.)[5]. Проводимые мероприятия сопровождаются распространением наглядных материалов правовой направленности (плакатов, памяток, листовок, информационных буклетов).

В УМВД России по Тюменской области проводятся мероприятия, направленные на недопущение и пресечение преступлений и правонарушений в среде несовершеннолетних; в региональные средства массовой информации рассылаются материалы, пропагандирующие законопослушный образ жизни и разъясняющие ответственность за совершение преступлений и правонарушений. Также ежегодно сотрудники УМВД России по Тюменской области принимают участие в проведении Единого урока по безопасности в сети Интернет в общеобразовательных учреждениях.

УМВД России по Оренбургской области проводятся рабочие встречи с руководством учебных заведений, на которых доводится порядок информирования о фактах участия несовершеннолетних в деструктивных группах. В 2017 г. проведено 1 860 лекций профилактического характера, в ходе которых разъяснена ответственность за распространение деструктивных взглядов.

В соответствии с приказом Минобрнауки России от 20 сентября 2013 г. № 1082 «Об утверждении Положения о психолого-медико-педагогической комиссии» в субъектах Российской Федерации созданы психолого-медико-педагогические комиссии (далее – Комиссия), основными направлениями деятельности которых являются:

– своевременное выявление детей с особенностями в физическом и (или) психическом развитии и (или) отклонениями в поведении;

– проведение комплексного психолого-медико-педагогического обследования детей в возрасте до 18 лет;

– подготовка по результатам обследования рекомендаций по оказанию детям психолого-медико-педагогической помощи и организации их обучения и воспитания, а также подтверждения, уточнения или изменения ранее данных рекомендаций.

[5] Мероприятие, направленное на повышение педагогической культуры, просвещение родителей. В рамках родительского всеобуча могут быть использованы традиционные формы работы: родительские собрания, направленные на обсуждение с родителями общих и наиболее актуальных вопросов воспитания детей в семье и образовательном учреждении; родительские конференции, посвященные обмену опытом семейного воспитания.

Комиссия имеет право запрашивать у органов исполнительной власти, правоохранительных органов, организаций и граждан сведения, необходимые для осуществления своей деятельности[6]. Взаимодействие с молодежными организациями, волонтерамии общественными организациями правоохранительной направленности вносит неоценимый вклад в работу по выявлению в сети Интернет запрещенной информации.

В рамках взаимодействия МВД России с Всероссийской общественной организацией «Молодая гвардия Единой России» (далее – МГЕР)[7] осуществляется анализ страниц подростков социальных сетей в сети Интернет.

В постоянном режиме сотрудниками БСТМ ГУ МВД России по г. Москве осуществляется мониторинг сети Интернет на предмет выявления деструктивных и суицидальных групп. В рамках указанной работы осуществляется обмен информацией между региональными подразделениями органов внутренних дел, а также с АНО «Интернациональный центр спасения детей от киберпреступлений»[8].

В Тюменской области в целях решения проблем информационной безопасности несовершеннолетних сотрудниками ОВД налажено взаимодействие с волонтерами областного проекта «Киберпатруль Тюменской области», который реализуется в регионе с 2014 г.

Необходимо отметить, что правонарушители, использовавшие сеть Интернет для ведения деструктивной деятельности, регистрировались в социальных сетях с помощью мобильных средств связи посредством неперсонифицированных SIM-карт[9] или оформленных на третьих лиц (корпоративных, физических лиц, установочные данные которых не соответствуют действительности).

В связи с этим существенным препятствием для привлечения лиц к ответственности за противоправную деятельность в сети Интернет является их «обезличенность», когда не удается установить личность абонента с привязкой к конкретному идентификационному модулю. Причиной указанной проблемы является бесконтрольное распространение неперсонифицированных SIM-карт, которое приводит к их использованию в противоправных целях, охватывая различные сферы уголовно наказуемых деяний от преступлений против личности

---

[6] Об утверждении Положения о психолого-медико-педагогической комиссии : Приказ Минобрнауки России от 20 сент. 2013 г. № 1082, п. 12 : зарег. в Минюсте России 23 окт. 2013 г. № 30242 // СПС КонсультантПлюс.

[7] Молодая гвардия Единой России – молодежная организация, региональные отделы которой действуют в большинстве субъектов Российской Федерации. В состав организации входят более 170 тыс. человек. URL: http://molgvardia.ru/history-organization (дата обращения: 02.07.2019).

[8] Интернациональный центр спасения детей от киберпреступлений. URL: http://62ru.ru/index.html (дата обращения: 10.07.2019).

[9] SIM-карта или идентификационный модуль – электронный носитель информации, установленный в абонентской станции (абонентском устройстве), с помощью которого осуществляется идентификация абонента оператором связи, доступ абонентской станции (абонентского устройства) к сети подвижной связи, а также обеспечивается защита от несанкционированного использования абонентского номера

до преступлений против общественной безопасности, включая террористическую и экстремистскую деятельности.

Как правило, при совершении противоправного деяния, злоумышленники пытаются обезопасить себя и используют разные способы для того, чтобы остаться анонимными в виртуальном пространстве. Однако, даже не задумываясь о сокрытии своей личности виртуальный педофил может остаться анонимным ввиду того, что не все операторы связи хранят сведения об Интернет-активности своих абонентов, хотя формально на операторов связи возложена обязанность по хранению информации о фактах приема, передачи, доставки и (или) обработки голосовой информации, текстовых сообщений, изображений, звуков, видео- или иных сообщений пользователей услугами связи – в течение трех лет с момента окончания осуществления таких действий. При регистрации IP-адреса владельцы в основном указывают номер телефона, почтовый адрес, адрес места жительства и изредка паспортные данные (хотя, по нашему мнению, это должно быть обязательным требованием при регистрации) [11, с. 29–30]. И действительно, некоторые операторы связи хранят в установленном порядке эти сведения и предоставляют их по запросу компетентных органов.

В соответствии со ст. 10.1 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[10], организаторы распространения информации в сети Интернет – лица, осуществляющие деятельность по обеспечению функционирования информационных систем и (или) программ для ЭВМ, которые предназначены и (или) используются для приема, передачи, доставки и (или) обработки электронных сообщений пользователей сети Интернет, обязаны хранить на территории России и предоставлять в установленном порядке для целей уголовного судопроизводства данные о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков, видео- или иных электронных сообщений пользователей и информацию о них. Развернутый перечень этих сведений, правила их хранения и предоставления уполномоченным государственным органам, осуществляющим оперативно-разыскную деятельность или обеспечение безопасности России были утверждены постановлением Правительства Российской Федерации от 31 июня 2014 № 759.

Аналогичные требования предъявляются и к операторам связи – юридическим лицам или индивидуальным предпринимателям, оказывающим услуги связи на основании соответствующей лицензии, которые во исполнение частей 1 и 2 ст. 64 Федерального закона от 07 июля 2003 г. № 126-ФЗ «О связи»[11] обязаны хранить на территории Российской Федерации и предоставлять в порядке, предусмотренном действующим законодательством, сведения, определенные Правилами взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации.

[10] Собрание законодательства РФ. – 2006. – № 31. – Ст. 3448.
[11] Собрание законодательства РФ. – 2003. – № 28. – Ст. 2895.

Проведенный нами анализ работы оперативных сотрудников и следователей свидетельствует о том, что успех их деятельности по раскрытию и расследованию преступлений, связанных с сетью Интернет, наряду с другими факторами, в определенной мере зависит от своевременного предоставления операторами связи информации об абоненте, которому выделялись IP-адреса в интересующее время. В этой связи, хочется обратить внимание на проблему, так называемых, «серых» IP-адресов, то есть публичные сетевые адреса, преобразованные по технологии NAT (Network Address Translation). Благодаря этой технологии один IP-адрес может быть одновременно предоставлен нескольким абонентам или устройствам, количество которых может доходить до нескольких тысяч. Так как большинство преступлений в сфере компьютерной информации возможно раскрыть лишь благодаря получению сведений от оператора связи о владельце IP-адреса, с использованием которого было совершено преступление, то сетевые адреса, преобразование по технологии NAT, затрудняют работу правоохранительных органов по выявлению и раскрытию преступлений. Технология NAT позволяет преступникам безнаказанно совершать все новые и новые преступления, в виду сложности их изобличения. Также преступниками используется динамический IP-адрес, предоставляющийся анонимными прокси-серверами, а также последовательностью анонимных прокси-серверов. Такие злоумышленники применяют «АнтиАОН» и другие программные средства, маскирующие реальный IP-адрес [5, с. 79].

Операторы связи в своей работе применяют Internet Protocol (IP) версии IPv4, который использует 32-битные адреса, ограничивающие адресное пространство 4 294 967 296 уникальными адресами и этих адресов уже на всех абонентов и устройств не хватает. По причине постоянного увеличения пользователей и ограниченности сетевой адресов, операторы связи прибегают к технологии NAT, которая внедряется достаточно просто. Протоколу Ipv4 имеется альтернатива интернет протокол IPv6, который предусматривает наличие 340,000,000,000,000,000,000,000,000,000,000,000,000 уникальных адресов [12]. Внедрение нового протокола может способствовать борьбе с преступлениями в сети Интернет, в силу более точного выявления абонента, оставляющего цифровые следы. Таким образом, предлагаем на законодательном уровне обязать операторов связи использовать интернет протокол Ipv6 по предоставлению телекоммуникационных услуг на территории Российской Федерации и полностью отказаться от технологии NAT.

В ходе расследования уголовных дел положительных результатов можно добиться путем изучения служебных файлов cookies, содержащих служебную информацию об IP-адресе устройства пользователя. [13, с. 56]. К.С. Сидорова рекомендует в ходе оперативно-розыскных и следственных действий «подробно устанавливать факты, связанные со временем использования какого-либо интернет-ресурса в целях корректного сопоставления времени интернет-сессии и используемого технического устройства, а в дальнейшем физического лица» [14, с. 86].

Подводя итог вышеизложенному, можно сделать следующие выводы о том, что отсутствие должного государственно регулирования за социальными

сетями и операторами связи позволяют виртуальным педофилам скрывать свою личность в сети Интернет, что затрудняет выявление и раскрытие рассмотренных в данном исследовании преступлений. Зная, что их личность будет легко установлена, многие из виртуальных педофилов не станут совершать преступления. Так же необходимо отметить, что привлечение общественных организаций и волонтеров может исключить некоторые причины и условия совершения развратных действий в отношении несовершеннолетних в сети Интернет.

Список использованной литературы

1. Степаненко Д.А. Цифровая реальность и криминалистика / Д.А. Степаненко, В.В. Коломинов // Глагол правосудия. – 2018. – № 3 (17). – С. 38–43.

2. Сачков Д.И. Обеспечение информационной безопасности в органах власти : учеб. пособие / Д.И. Сачков, И.Г. Смирнова. – Иркутск : Изд-во БГУЭП, 2015. – 122 с.

3. Шободоева А.В. Развитие понятия «информационная безопасность» в научно-правовом поле России / А.В. Шободоева. – DOI 10.17150/2500-2759.2017.27(1).73-78 // Известия Байкальского государственного университета. – 2017. – Т. 27, № 1. – С. 73–78.

4. Солдатова Г. Рассказова Е., Зотова Е., Лебешева М., Роггендорф П. Дети России онлайн. Результаты международного проекта EU Kids Online II в России / Г. Солдатова, Е. Рассказова, Е. Зотова [и др.]. Москва, 2012. – URL: http://docplayer.ru/27337424-Deti-rossii-onlayn-rezultaty-mezhdunarodnogo-proekta-eu-kids-online-ii-v-rossii-g-soldatova-e-rasskazova-e-zotova-m-lebesheva-p-roggendorf.html.

5. Кувычков С.И. К вопросу об использовании электронной информации в уголовно-процессуальном доказывании: теоретико-прикладной аспект / С.И. Кувычков // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2015. – № 2 (30). – С. 76–81.

6. Степаненко Д.А. Использование открытых информационных технологий для расследования преступлений в отношении несовершеннолетних / Д.А. Степаненко, А.А. Рудых // Российский следователь. – 2019. – № 4. – С. 16–19.

7. Марковичева Е.В. Борьба с преступностью и назначение уголовного судопроизводства: критерии разработки оптимальной уголовно-процессуальной стратегии в отношении несовершеннолетних / Е.В. Марковичева, И.Г. Смирнова. – DOI 10.17150/1996-7756.2016.10(2).331–338 // Всероссийский криминологический журнал. – 2016. – Т. 10, № 2. – С. 339–348.

8. Михайлов М.А. Единообразие в определении круга преступлений террористической и экстремистской направленности – необходимая предпосылка эффективности методики их расследования / М.А. Михайлов, В.С. Кряжев. – DOI 10.17150/2500-4255.2016.10(4).770–778 // Всероссийский криминологический журнал. – 2016. – Т. 10, № 4. – С. 770–778.

9. Якимова Е.М. Международное сотрудничество в борьбе с киберпреступностью / Е.М. Якимова, С.В. Нарутто // Всероссийский криминологический журнал. – 2016. – Т. 10, № 2. – С. 369–378.

10. Международное сотрудничество в борьбе с экологическими преступлениями / Е.М. Якимова, В.В. Чуксина, Г.Н. Комкова. – DOI 10.17150/2500-4255.2018.12(2).288-298 // Всероссийский криминологический журнал. – 2018. – Т. 12, № 2. – С. 288–298.

11. Егерева О.А. Некоторые вопросы методики расследования киберпреступлений / О.А. Егерева, В.В. Коломинов, М.С. Сизова // Сибирские уголовно-процессуальные и криминалистические чтения. – 2018. – № 4 (22). – С. 24–32.

12. Хазов В. Все, что вам надо знать о разнице между IPv4 и IPv6 / В. Хазов // Vas Experts. – URL: http://blog.vasexperts.ru/?p=815 (дата обращения: 20.04.2019).

13. Вехов В.Б. К вопросу криминалистического исследования анонимайзеров / В.Б. Вехов, М.А. Ульянова // Актуальные научные исследования в современном мире. – 2018. – № 7-3 (39). – С. 54–57.

14. Сидорова К.С. IP-адрес как один из идентификаторов личности в расследовании преступлений / К.С. Сидорова // Психопедагогика в правоохранительных органах. – 2018. – № 3 (74). – С. 84–87.

References

1. Stepanenko D.A., Kolominov V.V. Digital Reality and Criminalistics. *Glagol pravosudiya = The Verb of Justice*, 2018, no. 3 (17), pp. 38–43. (In Russian).

2. Sachkov D.I., Smirnova I. G. *Obespechenie informatsionnoi bezopasnosti v organakh vlasti* [Ensuring Information Security in the Bodies of Power]. Irkutsk, Baikal State University of Economics and Law Publ., 2015. 122 p.

3. Shobodoyeva A.V. The Development of the Notion of «Information Security» in the Russian Legal and Research Framework. *Izvestiya Baykal'skogo gosudarstvennogo universiteta = Bulletin of Baikal State University*, 2017, vol. 27, no. 1, pp. 73–78. DOI: 10.17150/2500-2759.2017.27(1).73-78. (In Russian).

4. Soldatova G., Rasskazova E., Zotova E., Lebesheva M., Roggendorf P. *Deti Rossii onlain. Rezul'taty mezhdunarodnogo proekta EU Kids Online II v Rossii* [Дети России онлайн. Результаты международного проекта EU Kids Online II в России]. Moscow, 2012. Available at: http://docplayer.ru/27337424-Deti-rossii-onlayn-rezultaty-mezhdunarodnogo-proekta-eu-kids-online-ii-v-rossii-g-soldatova-e-rasskazova-e-zotova-m-lebesheva-p-roggendorf.html. (In Russian).

5. Kuvychkov S.I. On the Use of Electronic Information in Criminal Procedure Proving: Theoretical and Applied Aspects. *Yuridicheskaya nauka i praktika: Vestnik Nizhegorodskoi akademii MVD Rossii = Legal Science and Practice: Journal of Nizhniy Novgorod Academy of the Ministry of the Interior of the Russian Federation*, 2015, no. 2 (30), pp. 76–81. (In Russian).

6. Stepanenko D.A., Rudykh A.A. The Use of Open Information Technology for the Investigation of Crimes Committed against Minors. *Rossiiskii sledovatel' = Russian Investigator*, 2019, no. 4, pp. 16–19. (In Russian).

7. Markovicheva E.V., Smirnova I.G. Crime Counteraction and the Purpose of Criminal Court Proceedings: Criteria of Developing the Optimal Criminal Procedure Strategy for Juveniles. *Criminology Journal of Baikal National University of Economics and Law*, 2016, vol. 10, no. 2, pp. 331–338. DOI: 10.17150/1996-7756.2016.10(2).331-338. (In Russian).

8. Mikhailov M.A., Kryazhev V.S. The Uniformity of Defining the Crimes of Terrorism and Extremism as a Prerequisite for the Effective Methodology of their Investigation. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2016, vol. 10, no. 4, pp. 770–778. DOI: 10.17150/2500-4255.2016.10(4).770-778. (In Russian).

9. Yakimova E.M., Narutto S.V. International Cooperation in Cybercrime Counteraction. *Criminology Journal of Baikal National University of Economics and Law*, 2016, vol. 10, no. 2, pp. 369–378. DOI: 10.17150/1996-7756.2016.10(2).369-378. (In Russian).

10. Yakimova E.M., Chuksina V.V., Komkova G.N., Nesmeyanova S.E. International Cooperation in Counteracting Environmental Crimes. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2018, vol. 12, no. 2, pp. 288–298. DOI: 10.17150/2500-4255.2018.12(2).288-298. (In Russian).

11. Egereva O.A., Kolominov V.V., Sizova M.S. Some Questions of the Technique of the Investigation of Cyber Crimes. *Sibirskie ugolovno-protsessual'nye i kriminalisticheskie chteniya = Siberian criminal procedure and criminalistic readings*, 2018, no. 4 (22), pp. 24–32. (In Russian).

12. Khazov V. Everything you Need to Know About the Difference Between IPv4 and IPv6. *Vas Experts*. Available at: http://blog.vasexperts.ru/?p=815. (In Russian).

13. Vekhov V.B., Ulyanova M.A. To the Question of the Criminalistic Study of Anonimayzers. *Aktual'nye nauchnye issledovaniya v sovremennom mire = Current Scientific Research in the Modern World*, 2018, no. 7-3 (39), pp. 54–57. (In Russian).

14. Sidorova K.S. IP address as one of Personal Identities in Criminal Investigation. *Psikhopedagogika v pravookhranitel'nykh organakh = Psychopedagogics in Law Enforcement Agencies*, 2018, no. 3 (74). pp. 84–87. (In Russian).

Информация об авторах

Родивилин Иван Петрович – старший оперуполномоченный по особо важным делам, отдел «К» ГУ МВД России по Иркутской области, г. Иркутск, Депутатская, 32; e-mail: 377a@bk.ru.

Коломинов Вячеслав Валентинович – кандидат юридических наук, доцент кафедры криминалистики, судебных экспертиз и юридической психологии, Институт государства и права, Байкальский государственный университет, г. Иркутск, ул. Ленина, 11; e-mail: KolominovVV88@gmail.com.

Брыжак Диана Эдуардовна – помощник директора Института государства и права, Байкальский государственный университет, г. Иркутск, ул. Ленина, 11; e-mail: OffRoad88@mail.ru.

Information about the authors

Rodivilin, Ivan P. – Senior Operative for Specially Important Cases, Department "K" of Russian Ministry of the Interior for Irkutsk Region, 32 Deputatskaya st., Irkutsk, Russian Federation; e-mail: 377a@bk.ru.

Kolominov, Vyacheslav V. – Ph.D. in Law, Ass. Professor, Chair of Criminalistics, Judicial Examinations and Legal Psychology, Institute of State and Law, Baikal State University, 11 Lenin st., Irkutsk, Russian Federation; e-mail: KolominovVV88@gmail.com.

Bryzhak, Diana E. – Assistant to the Director, Institute of State and Law, Baikal State University, 11 Lenin st., Irkutsk, Russian Federation; e-mail: OffRoad88@mail.ru.