
ОПЕРАТИВНО-РОЗЫСКНАЯ ДЕЯТЕЛЬНОСТЬ INVESTIGATION ACTIVITIES

Научная статья
УДК 343.98:351.74
EDN SCCIIJ

DOI 10.17150/2411-6122.2023.2.87-93



Особенности осуществления оперативно-розыскной деятельности и основные угрозы безопасности киберпространства в условиях цифровизации общества и виртуализации реальности

К.П. Малянова

Ростовский юридический институт МВД России, г. Ростов-на-Дону, Российская Федерация,
kari_rostov@mail.ru

Аннотация. В статье описывается влияние двух основных процессов, характеризующих современное общество — цифровизации и виртуализации окружающей действительности, на осуществление оперативно-розыскной деятельности правоохранительными органами. В первую очередь, речь идет о виртуализации информационного пространства современного общества, где особое значение имеет информационное поле, в котором содержится оперативно значимая информация. Рассмотрено негативное влияние информационных технологий на достоверность такой информации, в связи с этим выделены ключевые факторы, которые должны учитываться субъектами оперативно-розыскной деятельности при выполнении своих полномочий. Кроме того, в статье названы и раскрыты основные криминальные угрозы безопасности киберпространства, к числу которых относятся: использование возможностей киберпространства в преступных целях, увеличение масштабов наносимого ущерба, формирование опасных криминогенных зон, таких как DarkNet, увеличение методов противодействия правоохранительным органам, повышенный интерес криминальных группировок к технологиям Искусственного интеллекта. В статье предлагается обратить внимание на совершенствование форм и методов получения цифровой оперативно значимой информации.

Ключевые слова: цифровизация общества, виртуализация реальности, киберпространство, осуществление оперативно-розыскной деятельности, оперативно значимая информация.

Для цитирования: Малянова К.П. Особенности осуществления оперативно-розыскной деятельности и основные угрозы безопасности киберпространства в условиях цифровизации общества и виртуализации реальности / К.П. Малянова. — DOI 10.17150/2411-6122.2023.2.87-93. — EDN SCCIIJ // Сибирские уголовно-процессуальные и криминалистические чтения. — 2023. — № 2. — С. 87–93.

Original article

Specifics of Operative Search Activities and Key Threats to the Security of Cyberspace in the Conditions of the Digitization of Society and the Virtualization of Reality

K.P. Malyanova

Rostov Law Institute of the Russian Ministry of Internal Affairs, Rostov-on-Don, the Russian Federation, kari_rostov@mail.ru

Abstract. The article describes the influence of two key processes typical of modern society — the digitization and virtualization of the world around us — on operative search activities carried out by the law enforcement bodies. It primarily concerns the virtualization of the information space of the modern society with an emphasis on the information field that contains operatively valuable information. The author examines the negative impact of information technologies on the reliability of such information and, in connection with this, singles out key factors that should be taken into account by officers involved in operative search activities. Besides, key criminal threats to cyberspace security are enumerated and described, including: the use of cyberspace for criminal purposes, widening the scale of the inflicted damage, formation of dangerous criminogenic zones, such as DarkNet, new methods of counteracting the work of law enforcement bodies, heightened interest of criminal groups to the technologies of artificial intelligence. The author suggests paying special attention to the improvement of the forms and methods of obtaining operatively valuable information.

Keywords: digitalization of the society, virtualization of reality, cyberspace, operative search activities, operatively relevant information.

For citation: Malyanova K.P. Specifics of Operative Search Activities and Key Threats to the Security of Cyberspace in the Conditions of the Digitization of Society and the Virtualization of Reality. *Sibirskie Uголовно-Processual'nye i Kriminalisticheskie Chteniya = Siberian Criminal Procedure and Criminalistic Readings*, 2023, no 2, pp. 87–93. (In Russian). EDN: SCCIJ. DOI: 10.17150/2411-6122.2023.2.87-93.

Введение

На сегодняшний день уровень информационного развития общества достиг невообразимого уровня. Сотни компаний работают над разработкой новых видов гаджетов и технологических устройств, упрощающих жизнедеятельность человека. Уровень проникновения технологий в бытовую сферу также является колоссальным.

Поскольку мировой тенденцией XXI в. является глобализация, множество направлений в разработке технических устройств направлено на обеспечение бесперебойной и постоянной связи, как в бытовой, так и в экономической

сфере. Среди процессов, которые в наибольшей степени оказывают влияние на социальные изменения, особенно выделяются два связанных между собой тренда — цифровизация и виртуализация окружающей действительности.

Основная часть

Цифровизация представляет собой процесс масштабного внедрения цифровых технологий в большинство сфер общественной жизни (экономику, науку, здравоохранение, обеспечение общественной безопасности и др.). Она зиждется на интенсивном развитии информационных технологий и поддержки-

вается государством в целях перехода к информационному обществу в ускоренном темпе. В Российской Федерации на данный момент действует ряд разработанных программных документов, которые направлены на создание условий для осуществления цифровизации. С 2019 г. реализуется Государственная программа «Научно-техническое развитие Российской Федерации»¹ и «Национальная стратегия развития искусственного интеллекта до 2030 года»². Данные программы содержат ряд целей (например, нейротехнологии, компоненты робототехники), из числа которых особенно выделяют технологии искусственного интеллекта, позволяющие решать сложные задачи, которые требуют интеллектуальных усилий. Это «самобытное образование со своей онтологией, в которой тождество и различие, реальность и виртуальность, упорядоченность и хаос, контролируемость и непредсказуемость образуют объект, новый даже для его создателей» [1].

Виртуализация, в отличие от цифровизации, является менее очевидным процессом, однако это не умаляет ее существенного влияния на протекание множества общественных процессов, которые также сказываются и на изменении условий осуществления оперативно-разыскной деятельности.

Виртуализация реальности возникла в тот момент, когда при помощи

компьютерной техники стали создаваться гиперреалистичные объекты, поэтому справедливым будет замечание относительно того, что она не является порождением нашего времени. Однако развитие информационных технологий активизировало процессы виртуализации. Исследователями отмечается тот факт, что «информационное пространство сегодняшнего общества значительно отличается от того, что окружало человека в 70–80-х гг. XX в., главным образом тем, что широкое распространение получили технологии виртуальной реальности... Глубина проникновения виртуальности в социальную и индивидуальную жизнь позволяет говорить о «виртуализации» общества» [2]. Виртуализация достаточно объективно характеризует новые экономические, политические новшества социальной реальности, иначе говоря, социальная и культурная жизнь приобретает символический характер ввиду их перехода в поле виртуальных коммуникаций [3]. В подобных условиях происходит размытие реальности с ее последующей подменой различными копиями, что приводит к оторванности человека от реального мира, поскольку он воспринимает искусственную подмену как истинную действительность.

С точки зрения ОРД интерес представляет виртуализация информационного пространства современного общества. В нем может быть выделено информационное поле, в котором содержится оперативно значимая информация [4]. Следует помнить, что из-за расширения и усложнения информационного пространства появляется большое количество противоречивых сведений, к которым практически нет доверия ввиду отсутствия ответственности авторов, за достоверность размещаемой им информации. Кроме того,

¹ Об утверждении государственной программы Российской Федерации «Научно-технологическое развитие Российской Федерации»: Постановление Правительства РФ от 29 марта 2019 г. № 377 // СПС КонсультантПлюс (дата обращения: 20.01.2023 г.).

² О развитии искусственного интеллекта в Российской Федерации (вместе с Национальной стратегией развития искусственного интеллекта на период до 2030 года): Указ Президента РФ от 10 окт. 2019 г. № 490 // СПС КонсультантПлюс (дата обращения: 20.01.2023 г.).

совершенствование технологий дезинформации является свидетельством того, что любая информация может быть искажена. При помощи информационных технологий осуществляется управление обществом и формирование его сознания. Все вышеперечисленные факторы должны быть учтены субъектами ОРД при добывании оперативно значимой информации.

В качестве особого объекта, на который должно быть обращено внимание, выступает киберпространство — виртуальная среда, где происходят коммуникации и наполнение, использование информационных ресурсов в результате взаимодействий пользователей сети Интернет. В нем и происходит образование цифровых следов любой активности пользователей, что может стать полезным источником добывания необходимой правоохранительным органам информации [5; 6].

В киберпространстве происходят процессы, далекие от реальной жизни, ведь там человек может полностью принять возникающие в его воображении образы, в результате чего стираются границы между правдой и вымыслом, идет подмена ценностей, которые позже вступают в противоречие с отдельными социальными нормами. Это отражает распространение в социальных сетях таких явлений, как склонение к суициду и потреблению наркотических веществ, вовлечение в экстремистскую деятельность и террористические организации.

Приведенные явления и процессы не могут оставаться без внимания со стороны органов правопорядка. Именно поэтому важно с позиций ОРД выработать системное представление о складывающейся цифровой реальности, чтобы решать задачи, стоящие перед оперативными подразделениями сообразно ей.

Для того чтобы сформулировать особенности осуществления ОРД в новой среде, необходимо произвести анализ и выявить криминальные угрозы безопасности киберпространства.

Во-первых, следует отметить стремление преступности освоить киберпространство и использовать его особые характеристики в своих целях (средства анонимизации, наднациональный экстерриториальный характер, а также возможность применения дистанционных способов совершения преступлений). Также необходимо обратить внимание на то, что постоянно нарастают масштабы наносимого ущерба и количества пострадавших от данных преступлений и расширяется состав участвующих лиц [7]. Эти изменения связаны с изменением принципов функционирования преступных сообществ: когда на смену хакерам-одиночкам, которые совершают определенные действия из интереса, приходят организованные группы (к примеру, MoneyTaker, Cobalt, Lazarus), действующие на постоянной основе и совершающие масштабные акции преступного характера.

Во-вторых, криминализация киберпространства отражается не только на интересах отдельной личности и общества, но также и государства, так как проблема обеспечения национальной безопасности приобретает наднациональный характер и требует привлечения к решению данной проблемы сил правоохранительных органов различных государств на основе реализации процедур взаимной правовой помощи.

В-третьих, отмечается формирование криминогенных зон киберпространства, которые требуют особого внимания оперативных служб, к которым можно отнести в первую очередь DarkNet («теневой Интернет»). Даркнет — это отдельные сети, состоящие из некоторого количества серверов в

сети интернет, к которым можно подключиться только с помощью специальных инструментов — например, специально разработанных браузеров. К наиболее популярным сетям можно отнести Tor (Onion Router). Причины существования даркнета связывают с возможностью свободного доступа к любой закрытой информации. Кроме того, он привлекает пользователей фактором анонимности: информация в этих сетях шифруется, так что невозможно определить содержимое или конечный адрес получателя информации. Таким образом, в таких сетях невозможна систематическая слежка за пользователями. Вместе с тем, даркнет является площадкой для осуществления преступной деятельности: через него распространяется все, что ограничено в использовании и распространении на федеральном уровне (оружие, наркотические и психотропные вещества, информация экстремистского и террористического характера, детская порнография). Согласно оценке зарубежных исследователей, почти 57 % сайтов в сети Tor вовлечены в преступную деятельность [8].

В-четвертых, ввиду того, что в киберпространстве появляется все больше цифровых следов, которые могут представлять интерес и выступать в качестве доказательств, важно этот объем аккумулировать и вовлечь в процесс раскрытия и расследования преступлений. Чтобы достичь цели концентрации больших объемов оперативно значимой информации, оперативно-розыскной наукой разрабатываются специфические формы и методы доступа к ней. Для этого сотрудники, работающие по обозначенным направлениям, должны обладать рядом необходимых компетенций, в связи, с чем создаются подразделения, специализирующиеся на противодействии киберпреступности [9].

В-пятых, отмечается увеличение методов противодействия правоохранительным органам со стороны криминалитета, базирующегося в киберпространстве. Он демонстрирует повышенный уровень операционной безопасности и ясно дает понять, что сокрытие личности и преступной деятельности осуществляется целенаправленно. Кроме того, преступность в киберпространстве все больше опирается на применение технологий шифрования и криптографических алгоритмов, что затрудняет доступ к скрываемой компьютерной информации. В том числе использование криптовалют значительно усложняет процесс отслеживания платежей, которые связаны с преступной деятельностью.

В-шестых, особенно настораживающим оказывается повышенный интерес криминальных группировок к технологиям искусственного интеллекта, применение которых может полностью вывести их из поля зрения правоохранительных органов. Использование преступниками таких технологий направлено на поиск оптимальных способов осуществления противоправной деятельности, повышение ее прибыльности и снижение вероятности обнаружения и уличения их компетентными органами.

Выводы и заключение

Совершенно очевидно, что внедрение новых технологий позволит разрешить ряд сложных задач, однако в то же время важно обратить внимание на то, что при применении такого рода технологий необходимо соблюдать осторожность, особенно, когда их использование приводит к ограничению прав граждан. Результативность их применения должна определяться полнотой и достоверностью исходных данных и качественными характеристиками закладываемых разработчиками правил их обработки.

Список использованной литературы

1. Игнатов А.Н. Противодействие преступности: симулякры и симуляции / А.Н. Игнатов. — EDN AKKZNE // Ученые записки Крымского федерального университета им. В.И. Вернадского. Юридические науки. — 2020. — Т. 6, № 1. — С. 215–226.
2. Емелин В.А. Симулякры и технологии виртуализации в информационном обществе / В.А. Емелин. — DOI 10.11621/npj.2016.0312. — EDN YLPEPF // Национальный психологический журнал. — 2016. — № 3. — С. 86–97.
3. Радевич Е.В. Глобальное информационное пространство современности: естественное vs виртуальное / Е.В. Радевич. — EDN IIGXWV // Проблема соотношения естественного и социального в обществе и человеке. — 2020. — № 11. — С. 89–95.
4. Ожерельева Т.А. Об отношении понятий информационное пространство, информационное поле, информационная среда и семантическое окружение / Т.А. Ожерельева. — EDN SNYDID // Международный журнал прикладных и фундаментальных исследований. — 2014. — № 10-2. — С. 21–24.
5. Фойгель Е.И. Некоторые возможности использования поведенческой биометрии в расследовании преступлений / Е.И. Фойгель. — EDN YOFAMS // Развитие российского общества: вызовы современности : материалы Всерос. науч.-практ. конф., Иркутск, 15 окт. 2020 г. — Иркутск, 2021. — С. 417–420.
6. Протасевич А.А. О возможностях криминалистической габитоскопии при реализации мер противодействия современной киберпреступности / А.А. Протасевич, Е.И. Фойгель. — DOI 10.17150/2500-4255.2020.14(3).471-480. — EDN VSWSNK // Всероссийский криминологический журнал. — 2020. — Т. 14, № 3. — С. 471–480.
7. Дремлюга Р.И. Преступления в виртуальной реальности: миф или реальность? / Р.И. Дремлюга, А.В. Крипакова. — DOI 10.17803/1994-1471.2019.100.3.161-169. — EDN ZEUUHB // Актуальные проблемы российского права. — 2019. — № 3. — С. 161–169.
8. Дерендяева Т.М. Противодействие киберпреступности в аспекте обеспечения безопасности информационного общества / Т.М. Дерендяева, Г.А. Мухина. — EDN WIBBZL // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. — 2022. — № 1. — С. 85–89.
9. Антонян Е.А. Киберпреступность на современном этапе: тенденции и направления противодействия / Е.А. Антонян, Е.Н. Клещина. — DOI 10.24412/2414-3995-2022-5-11-15. — EDN SXPUMZ // Вестник экономической безопасности. — 2022. — № 5. — С. 11–15.

References

1. Ignatov A.N. Counteraction Crime: Simulacra and Simulation. *Uchenye zapiski Krymskogo federal'nogo universiteta im. V.I. Vernadskogo. Sotsiologiya. Yuridicheskie nauki = Scientific Notes of V. I. Vernadsky Crimean Federal University. Juridical Science*, 2020, vol. 6, no. 1, pp. 215–226. (In Russian). EDN: AKKZNE.
2. Emelin V.A. Simulacra and Virtualization Technologies in Information Society. *Natsional'nyi psikhologicheskii zhurnal = National Psychological Journal*, 2016, no. 3, pp. 86–97. (In Russian). EDN: YLPEPFD. DOI: 10.11621/npj.2016.0312.
3. Radevich E.V. The Global Information Space of the Modern Time: Natural vs Virtual. *Problema sootnosheniya estestvennogo i sotsial'nogo v obshchestve i cheloveke = Problems of the Correlation of Natural and Social in Society and Man*, 2020, no. 11, pp. 89–95. (In Russian). EDN: IIGXWV.
4. Ozherelyeva T.A. Regard to the Concept of Information Space, Information Field, Information Environment and Semantic Environment. *Mezhdunarodnyi zhurnal prikladnykh i fundamental'nykh issledovaniy = International Journal on Practical and Fundamental Research*, 2014, no. 10-2, pp. 21–24. (In Russian). EDN: SNYDID.
5. Foigel E.I. Some Possibilities of Using Behavioral Biometrics in Crime Investigation. *Development of Russian Society: Modern Challenges. Materials of All-Russian Research Conference, Irkutsk, October 15, 2020*. Irkutsk, 2021, pp. 417–420. (In Russian). EDN: YOFAMS.

6. Protasevich A.A., Foigel E.I. On the Scope of Criminalistic Habitoscropy in the Implementation of Measures against Modern Cyber Crime. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2020, vol. 14, no. 3, pp. 471–480. (In Russian). EDN: VSWSNK. DOI: 10.17150/2500-4255.2020.14(3).471-480.

7. Dremlyuga R.I., Kripakova A.V. Crimes in Virtual Reality: Myth or Reality? *Aktual'nye problemy rossiiskogo prava = Topical Problems of Russian Law*, 2019, no. 3, pp. 161–169. (In Russian). EDN: ZEUUHB. DOI: 10.17803/1994-1471.2019.100.3.161-169.

8. Derendyaeva T.M., Mukhina G.A. Countering Cybercrime in the Aspect of Ensuring the Security of the Information Society. *Vestnik Kaliningradskogo filiala Sankt-Peterburgskogo universiteta MVD Rossii = Bulletin of the Kaliningrad branch of the St. Petersburg University of the Ministry of Interior Affairs of Russia*, 2022, no. 1, pp. 85–89. (In Russian). EDN: WIBBZL.

9. Antonyan E.A., Kleshchina E.N. Cybercrime at the Present Stage: Trends and Directions of Counteraction. *Vestnik ekonomicheskoi bezopasnosti = Bulletin of Economic Security*, 2022, no. 5, pp. 11–15. (In Russian). EDN: SXPUMZ. DOI: 10.24412/2414-3995-2022-5-11-15.

Информация об авторе

Малянова Карина Петровна — кандидат юридических наук, заместитель начальника кафедры криминалистики и ОРД, подполковник полиции, Ростовский юридический институт МВД России г. Ростов-на-Дону, Российская Федерация.

Author Information

Malyanova, Karina P. — Ph.D. in Law, Deputy Head, Chair of Criminalistics and Operative Search Activities, Police Lieutenant Colonel, Rostov Law Institute of the Russian Ministry of Internal Affairs, Rostov-on-Don, the Russian Federation.

Поступила в редакцию / Received 10.11.2022

Одобрена после рецензирования / Approved after reviewing 21.12.2022

Принята к публикации / Accepted 06.06.2023

Дата онлайн-размещения / Available online 13.06.2023