Научная статья
УДК 343
doi: 10.35750/2071-8284-2022-3-111-117

Александр Васильевич Пучнин
кандидат юридических наук, доцент
https://orcid.org/0000-0001-8754-9650, lex-puch@yandex.ru

Павел Витальевич Миненко
кандидат юридических наук, доцент
https://orcid.org/0000-0002-2792-8066, pv.minenko@icloud.com

Воронежский институт МВД России
Российская Федерация, 394065, Воронеж, проспект Патриотов, д. 53

Цифровое оружие совершения преступлений XXI века: предмет, средство, орудие

Аннотация: Статья посвящена определению нового предмета преступления – цифрового оружия, анализу степени и характера общественной опасности деяний, совершаемых с его использованием. Исследуется возникший в результате проникновения информационно-телекоммуникационных технологий в повседневную жизнь феномен цифровых средств, орудий, предметов совершения преступлений. Предпринята попытка сформулировать новые категории, определяющие недостоверное поведение в сети интернет и интегрировать их в действующие нормы законодательства. Ставится вопрос о рассмотрении цифрового оружия как угрозы национальной безопасности Российской Федерации. Обосновывается своевременность и социальная обусловленность криминализации оборота цифровых данных, используемых для совершения преступлений, и установления уголовной ответственности за совершение деяний с использованием цифрового оружия, предлагаются основные меры, направленные на противодействие такого рода преступлениям. Исследуется правовая природа и основные принципы функционирования информационных инструментов совершения преступлений. В исследовании в качестве примера цифрового оружия рассматриваются массивы недостоверных учётных записей пользователей информационно-телекоммуникационных сетей, ставится вопрос о необходимости криминализации отдельных цифровых технологий, образующих инструментарий преступников в цифровой среде. С учётом поднятых в статье проблем авторами сформулированы предложения по совершенствованию действующего законодательства в виде новой нормы особенной части Уголовного кодекса Российской Федерации.

Ключевые слова: боты, компьютерная преступность, интернет, информационно-телекоммуникационные технологии, массивы учётных записей, национальная безопасность, недостоверное поведение, фейковые аккаунты, фермы аккаунтов, цифровая преступность

Для цитирования: Пучнин А. В., Миненко П. В. Цифровое оружие совершения преступлений XXI века: предмет, средство, орудие // Вестник Санкт-Петербургского университета МВД России. – 2022.– № 3 (95). – С. 111–117; doi: 10.35750/2071-8284-2022-3-111-117.

Alexander V. Puchnin
Cand. Sci. (Jurid.), Docent
https://orcid.org/0000-0001-8754-9650, lex-puch@yandex.ru

Pavel V. Minenko
Cand. Sci. (Jurid.), Docent
https://orcid.org/0000-0002-2792-8066, pv.minenko@icloud.com

Voronezh Institute of the MIA of Russia
53, Patriotov str., Voronezh, 394065, Russian Federation

Digital crime weapons of the XXI century: object, means, tools

Abstract: The article is devoted to the definition of a new subject of crime - digital weapons, the analysis of the degree and nature of the public danger of acts committed with its use. The phenomenon of digital means, tools, objects of crimes that arose as a result of the penetration of information and telecommunication technologies into everyday life is investigated. An attempt was made to formulate new categories that define inaccurate behavior on the Internet and integrate them into the current legislation. The question is raised about considering digital weapons as a threat to the national security of the Russian Federation. The timeliness and social conditionality of the criminalization of the circulation of digital data used to commit crimes and the establishment of criminal liability for the commission of acts using digital weapons are substantiated, the main measures aimed at counteracting such crimes are proposed. The legal nature and basic principles of the functioning of information tools for committing crimes are investigated. The study considers arrays of inaccurate user accounts of information and telecommunication networks as an example of a digital weapon. The article raises the question of the need to criminalize certain digital technologies that form the tools of criminals in the digital environment. Taking into account the problems raised in the article, the authors formulated proposals for improving the current legislation in the form of a new norm of the special part of the Criminal Code of the Russian Federation.

Keywords: bots, computer crime, Internet, information and communication technologies, arrays of accounts, national security, inauthentic behavior, fake accounts, account farms, digital crime

For citation: PuchninA.V., Minenko P.V. Digital crime weapons of the XXI century: object, means, tools // Vestnik of St. Petersburg University of the Ministry of Internal Affairs of Russia. – 2022. – № 3 (95). – P. 111–117; doi: 10.35750/2071-8284-2022-3-111-117.

Современный уровень цифровизации коммуникации в обществе ставит вопрос: скоординированное недостоверное поведение – свобода или преступление?

Совершение квалифицированных, профессиональных преступлений сопровождается использованием специфических средств, орудий и оружия. На стадиях приготовления и покушения, в ходе их приискания, они могут выступать в качестве предмета предиктивных преступлений.

Современное состояние регистрируемой преступности указывает на то, что наиболее распространенными, сложными с позиций раскрытия и предупреждения преступлений являются те из них, которые совершаются в сфере информационных и телекоммуникационных технологий, а также с использованием таких технологий для достижения преступной цели. Этот неоспоримый тезис ставит перед законодателем и правоприменителем вопрос о криминализации отдельных цифровых технологий, образующих инструментарий преступников в цифровой среде.

В теории уголовного права существуют различия между орудием и средством совершения преступления. Под орудиями совершения преступления принято понимать предметы материального мира, приспособления, применяемые для усиления физических возможностей лица, совершающего общественно опасное деяние (например, применение лома для вскрытия дверей гаража); средствами же являются предметы, наркотические средства, химические и ядовитые вещества, химические и физические процессы и т. д., при помощи которых совершается преступление, т. е. оказывается преступное воздействие на общественные отношения, охраняемые уголовным законом[1].

В современной литературе, как правило, средства и орудия совершения преступления не разграничиваются, а, говоря о преступлениях в сфере информационно-телекоммуникационных технологий, провести такую демаркацию просто невозможно, что позволяет использовать эти понятия в нашем исследовании как тождественные. Так, например, в парадигме приведенной позиции отнести вредоносное программное обеспечение к одному из названных элементов объективной стороны состава преступления будет затруднительно даже специалистам в области цифровой юриспруденции.

Использование орудий или средств совершения преступления существенно повышает степень его общественной опасности и зачастую используется законодателем в качестве квалифицирующего признака, отягчающего уголовную ответственность. В некоторых случаях общественная опасность последствий их использования высока настолько, что правовыми нормами установлен запрет на их оборот или ограничения путем лицензирования деятельности субъектов, наделённых правом к ним прикасаться.

Вопрос о криминализации плодов использования и эксплуатации цифровых технологий непрост, однако в свете названных обстоятельств настоятельно требует постановки по ряду причин.

[1] Уголовное право Российской Федерации. Общая часть : учебник / Ю. В. Грачёва, Л. Д. Ермакова, Г. А. Есаков [и др.]; под ред. Л. В. Иногамовой-Хегай, А. И. Рарога, А. И. Чучаева. 2-е изд., перераб. и доп. – Москва: Контракт, Инфра-М, 2008. – 560 с.

Необходимо признать, что в настоящий момент виртуальная среда не только заменила традиционные способы коммуникации между людьми, но и сформировала новые, став специфичным и неотъемлемым элементом повседневной жизни. Особенность современных информационных технологий, заключающаяся в их доступности, возможностях мгновенного обмена информацией между участниками и сохранения анонимности, привела к диффузии между традициями, обычаями, языками и т. д., образовав цифровую среду обитания человека, цифровую мультикультуру и цифровые общественные отношения.

В связи с этим возникла целая когорта людей, которые стали использовать цифровые технологии и результаты их эксплуатации в преступных целях и которые образовали своими действиями отдельную специфическую цифровую компьютерную преступность [6].

Несмотря на то, что часть совершаемых ими деяний охватывается имеющимися в Особенной части УК РФ составами преступлений (например, ст. 1593, п. «г» ч. 3 ст. 158) и правоохранительная система адаптируется, вырабатывая методологию противодействия им, приходится констатировать, что «под носом» общества и государства совершаются действия с использованием цифровых технологий, которые, по нашему мнению, создают угрозу государственной, военной, экономической, информационной и экологической безопасности Российской Федерации, обладая такой степенью общественной опасности, что следует осознать их криминальный характер и рассматривать через призму уголовного законодательства.

Проблема осознания общественной опасности таких действий и инструментов кроется в непонимании субъектами законотворчества и правоприменения природы этих явлений, тенденций и направлений развития цифровой криминальной среды, возможностей применения существующих цифровых инструментов и технологий в общественных отношениях. Из этого вытекает задача научного анализа и разработки категориального аппарата, позволяющего обосновать опасность и криминальность таких действий, явлений, технологий, которые, безо всякой экзажерации, можно назвать современным цифровым оружием.

Авторы специально используют термин «оружие» понимая, что в юридической терминологии ему семантически соответствует главным образом понятие, приведенное в ФЗ «Об оружии», которое трактует его как устройства и предметы, конструктивно предназначенные для поражения живой или иной цели, подачи сигналов[2]. Однако толковый словарь С. И. Ожегова позволяет рассматривать данный термин в контексте проводимого исследования шире, а именно как «всякое средство, технически пригодное для нападения или защиты, а также совокупность таких средств»[3].

Примером цифрового оружия является администрирование массивов недостоверных учётных записей пользователей (ферм аккаунтов) в глобальной сети интернет, под которыми авторы предлагают понимать совокупность учетных записей пользователей, в том числе объединённых взаимными связями в одну группу, созданную с помощью специальных алгоритмов и автоматизированного программного обеспечения, действующего на основе возможностей нейронных сетей и позволяющего осуществлять одновременное управление ими.

Данное явление распространяется стремительно, активно используется в масс-медиа, а также видными публичными личностями, в том числе политическими деятелями.

По данным компании-разработчика программного обеспечения SparkToro, объём фейковых учётных записей, подписанных на официальный аккаунт президента США Джо Байдена в Twitter, составляет 49,3 % от общего числа (22,2 млн пользователей), что позволяет владельцам данной совокупности фейковых учётных записей путём скоординированного недостоверного поведения воздействовать на вторую половину подписчиков (реальных пользователей), влиять на их гражданскую позицию и пр.

Стремление пользователей информационных ресурсов к расширению охвата аудитории в глобальной сети обусловлено частью возможностей, предоставляемых интернетом, обеспечивающих повседневное общение между людьми, которое всё чаще реализуется посредством социальных сетей и форумов. С их помощью возможен обмен информацией, организованный различными способами по времени и типу сообщений между широким кругом лиц, в том числе незнакомых. В данном случае традиционные средства массовой информации уступают создаваемым в социальных сетях «пабликам» и сообществам, имеющим значительное количество участников и подписчиков. На начальных этапах их возникновения и развития интерес к ним в основном проявляло молодое поколение (лица в возрасте от 14 до 28 лет). В настоящее время в социальных сетях зарегистрированы люди разных возрастов и социальных групп. Результаты анализа этих лиц скорее введут в заблуждение, нежели позволят систематизировать полученную информацию, поэтому подробный портрет действительного пользователя интернет-пространства нами не исследовался.

Для организации общения и обеспечения возможности идентификации пользователей сети интернет в социальных сетях, форумах,

[2] Об оружии : Федеральный закон от 13 декабря 1996 г. № 150-ФЗ [Электронный ресурс]// СПС «КонсультантПлюс» (дата обращения: 15.04.2022).

[3] Толковый словарь Ожегова [Электронный ресурс] // Сайт «Словарь Ожегова». – Режим доступа: https://slovarozhegova.ru/word.php?wordid=18744 (дата обращения: 15.04.2022).

мессенджерах и иных ресурсах необходима регистрация учётной записи (аккаунта)[4]. Это правило возникло практически одновременно с появлением социальных сетей. Отсутствие необходимости подтверждения личных данных приводит к тому, что пользователи создают учётные записи под вымышленными именами или используют данные других лиц, получая возможность действовать анонимно.

В процессе развития информационно-коммуникационной среды были созданы неформальные сообщества с уникальным набором инструментов общения, передачи и получения информации, выражения своего мнения, оценки чего-либо, в том числе анонимно или под псевдонимом, имеющие своей целью воздействие на массовое мнение при восприятии информации.

Поведение и реакция групп людей на ту или иную информацию сильно влияют на мнение остальных. Данное явление в современной психологии получило название «психология толпы». Науке известно, что человек, действующий не самостоятельно, а в рамках группы других людей, чувствует иной уровень свободы действий. Такое состояние, присущее отдельным личностям в группе, приводит к тому, что вместе они становятся единой силой, которая способна производить социальные изменения, обходя привычные механизмы поведения.

Такое поведение свойственно и современному человеку, активному пользователю сети. Это наглядно демонстрирует анализ новостей, связанных с актуальными для общества вопросами, в первую очередь политическими. При этом новости, как правило, сопровождаются потоком негативных комментариев. В результате человек, который анализирует общественное мнение, становится жертвой и попадает под влияние откликов. Зачастую он включается в этот процесс и тоже становится активным участником обсуждения, которое может привести к негативным последствиям – от ошибочности оценки события до вовлечения в преступную деятельность.

В отечественном сегменте интернета наиболее популярной является социальная сеть «ВКонтакте», при этом в ней используются алгоритмы защиты от учётных записей, за которыми скрываются программы-роботы (боты[5]), имеющие своей целью распространение спама[6] и массовых бот-аккаунтов, позволяющих манипулировать мнением иных пользователей, осуществляя информационные вбросы на страницах ресурса. Именно это явление среди пользователей и администраций интернет-ресурсов образует массивы недостоверных учётных записей пользователей (фермы аккаунтов) в глобальной сети.

Создание массивов недостоверных учетных записей пользователей (ферм аккаунтов) не криминализировано действующим законодательством Российской Федерации, если при этом не используются персональные данные конкретного лица[7] и сведения о его частной жизни, составляющие личную или семейную тайну, и в соответствии с действующим законодательством может рассматриваться лишь как этап подготовки к противоправным действиям.

Задача администратора массивов недостоверных учётных записей пользователей[8] – создать, правильно их развивать, придавать им вид используемых реальными людьми определённой, при необходимости конкретной социально-демографической группы, максимально продлевать период существования и обеспечивать попадание в категорию имеющих уровень высокого доверия (трастовости)[9].

На ресурсах интернета регулярно появляются новые алгоритмы выявления недостоверных учётных записей.

Для этого администратором постоянно должны осуществляться следующие действия:

– подбор и наполнение учётной записи информационным материалом вместе с графическими изображениями;

– удаление ежедневно нежелательных записей (спама);

– удаление нецензурных и оскорбительных комментариев;

– инициализация переходов на сайты;

– ведение общения и ответы на вопросы реальных пользователей;

– поддержание дружеской атмосферы среди друзей, подписчиков и в группах;

– стимулирование общения (инициализация комментариев).

В связи с этим администратору приходится использовать специальные программы, которых на ресурсах сети интернет немало.

Учётная запись, в том числе недостоверная, в цифровом пространстве может быть использована для решения локальных задач конкретного пользователя: распространение информации, идей, влияние на других пользователей и пр.

Для достижения желаемого результата администраторы создают сеть таких недосто-

[4] Учётная запись (от англ. account) — хранимая в компьютерной системе совокупность данных о пользователе, необходимая для его опознавания (аутентификации) и предоставления доступа к его личным данным и настройкам. В качестве синонима используются также «аккаунт».

[5] Робот, или бот, а также интернет-бот, бот-аккаунт и пр. (англ. bot, сокращение от чеш. robot) – специальная программа, выполняющая автоматически и (или) по заданному расписанию какие-либо действия через интерфейсы, предназначенные для людей.

[6] Спам (англ, spam) – массовая рассылка корреспонденции рекламного характера лицам, не выражавшим желания её получить, а также рассылка массовых сообщений.

[7] Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ. ст. 13.11 «Нарушение законодательства Российской Федерации в области персональных данных», ст. 137 «Нарушение неприкосновенности частной жизни») [Электронный ресурс] // СПС «КонсультантПлюс» (дата обращения: 15.04.2022).

[8] Создающие, распространяющие и использующие такие учётные записи лица (администраторы) именуются в сети Интернет «фармерами».

[9] Трастовость (от англ. trast rate — уровень доверия).

верных учётных записей, которые путём взаимодействия между собой имитируют общение и вовлекают реальных пользователей. В результате ресурсы глобальной сети используются не только в целях рекламы и распространения товаров и услуг, но и для продвижения экстремистских и прочих деструктивных идей и взглядов.

Таким образом, интегрированные в сообщества реальных пользователей недостоверные учётные записи могут использоваться как в законных целях (сбор информации о востребованности товаров, услуг и их групп, сбор статистических сведений с целью изучения социально значимых вопросов и др.), так и в противоправных. При этом возникает угроза не только интересам отдельных физических, юридических лиц, но и информационной, государственной безопасности.

Массивы учётных записей пользователей сети интернет могут использоваться злоумышленниками в целях:

– обмана физических лиц и представителей юридических лиц при предоставлении некачественных услуг маркетинга в социальных сетях[10], в том числе в части качества товаров и услуг посредством введения в заблуждение;

– недобросовестной конкуренции путём распространения ложной информации;

– обмана в ранжировании значимости новостного события;

– романтизации преступного образа жизни и распространения его идеалов;

– дискредитации органов государственной власти;

– подготовки населения к «цветным революциям»;

– поиска физических лиц, которые могут выступить в качестве активистов и официальных представителей «цветных революций»;

– провокации и управления массовыми беспорядками;

– разжигания религиозной, расовой, социальной нетерпимости в определённой группе людей или государстве.

Отметим, что невозможно определить исчерпывающий перечень неправомерных направлений и целей использования объединённых недостоверных учётных записей в глобальной сети.

В результате гарантируется попадание в ленту важных новостей охваченных пользователей информации, размещаемой администратором за счёт возможностей управления страницами «фермы аккаунтов» и создания искусственного обсуждения, в том числе видимости одобрения продвигаемых им сведений.

Действия с фиктивными учётными записями в социальных сетях осуществляются по следующим направлениям:

1) скоординированное «недостоверное поведение» в интересах внутренних негосударственных субъектов;

2) скоординированное «недостоверное поведение» в интересах внешних негосударственных субъектов;

3) скоординированное «недостоверное поведение» в интересах иностранного государственного субъекта.

С помощью такого цифрового оружия, как массивы недостоверных учётных записей сети интернет, в настоящее время совершается значительное количество преступлений с различными объектами посягательств и способами их совершения, например, доведение до самоубийства (ст. 110 УК РФ), склонение к совершению самоубийства или содействие совершению самоубийства (ст. 110^1 УК РФ), клевета (ст. 128^1 УК РФ), нарушение неприкосновенности частной жизни (ст. 137 УК РФ), воспрепятствование осуществлению избирательных прав или работе избирательных комиссий (ст. 141 УК РФ), нарушение права на свободу совести и вероисповедания (ст. 148 УК РФ), вовлечение несовершеннолетнего в совершение преступления (ст. 150 УК РФ), мошенничество (ст. 159 УК РФ), оказание противоправного влияния на результат официального спортивного соревнования или зрелищного коммерческого конкурса (ст. 184 УК РФ), публичные призывы к осуществлению террористической деятельности, публичное оправдание или пропаганда терроризма (ст. 205^2 УК РФ), публичные действия, направленные на дискредитацию использования Вооруженных Сил Российской Федерации в целях защиты интересов Российской Федерации и её граждан, поддержания международного мира и безопасности или исполнения государственными органами Российской Федерации своих полномочий в указанных целях (ст. 280^3 УК РФ). Данный список можно дополнить иными составами.

Злоумышленникам для реализации объективной стороны названных составов преступлений необязательно самостоятельно создавать и развивать недостоверные учётные записи пользователей интернета (в том числе и их массивы), так как существует рынок предоставления доступа к ним, на котором можно приобрести готовые учётные записи или заказать их создание с заданными параметрами.

Изложенное позволяет сделать вывод, что в настоящее время налажен и широко используется оборот исследуемого феномена, который является неотъемлемой частью механизма совершения преступлений и в связи с этим обладает самостоятельной общественной опасностью, аналогично традиционным предметам и орудиям, таким как огнестрельное и холодное оружие, наркотические средства и психотропные вещества, специальные технические средства для негласного получения информации и т. п.

Производство, изготовление, переработка, хранение, учёт, отпуск, реализация, продажа, распределение, перевозка, пересылка, приобретение, использование, ввоз, вывоз, уничтожение

[10] Задача маркетинга в социальных сетях (от анг. Social Media Marketing) – привлечение внимания аудитории к своему товару с целью его продажи.

последних жёстко контролируется правоохранительными органами, регулируется путем лицензирования и в случае нарушения карается в соответствии с действующим законодательством, в том числе уголовным.

Авторы полагают, что настало время подобные правила распространить и на цифровое оружие, признав его предметом преступления, когда речь идёт о его обороте или оно является орудием преступления, когда речь идёт о его использовании для совершения иных преступлений, установив ответственность, в том числе уголовную, за скоординированное недостоверное поведение в информационно-телекоммуникационном пространстве.

В связи с этим считаем необходимым наряду с разработкой механизма контроля и лицензирования цифрового оружия:

1. Дополнить главу 28 УК РФ составом преступления следующего содержания:

«***Статья 273[1]. Оборот и администрирование недостоверных учётных записей пользователей в информационно-телекоммуникационных сетях.***

1. Создание и администрирование недостоверных учётных записей пользователей в информационно-телекоммуникационных сетях, предназначенных для публичного манипулирования мнением людей посредством ресурсов информационно-телекоммуникационных сетей, путём распространения дезинформации, создающее угрозу государственной, военной, экономической, информационной или экологической безопасности Российской Федерации и её граждан.

2. Сбыт, приобретение в целях сбыта или использования для публичного манипулирования мнением людей посредством ресурсов информационно-телекоммуникационных сетей путём распространения дезинформации, создающие угрозу государственной, военной, экономической, информационной или экологической безопасности Российской Федерации и её граждан.

Примечание 1. Под учётной записью пользователя понимается уникальный набор компьютерной информации, используемый для идентификации пользователя услуг связи при доступе к сети передачи данных и телематическим услугам связи.

Примечание 2. Под недостоверной учётной записью пользователя понимается уникальный набор компьютерной информации, используемый для идентификации пользователя услуг связи при доступе к сети передачи данных и телематическим услугам связи, анонимности или введения в заблуждение относительно личности создающего или эксплуатирующего его лица».

2. Предусмотреть в качестве квалифицирующего признака составов преступлений, связанных с распространением недостоверной информации, способ, связанный с использованием для этого недостоверных учётных записей пользователей информационно-телекоммуникационных сетей.

Предложенные авторами тезисы, безусловно, носят дискуссионный характер, их цель – привлечь внимание к появлению новых феноменов, которые характеризуются общественной опасностью, поскольку они стали частью механизма совершения значительного количества преступлений.

В связи со сложностью рассматриваемого феномена цифрового оружия в статье исследован лишь один его вид – недостоверные учётные записи пользователей информационно-телекоммуникационных сетей, что предполагает необходимость широкого обсуждения поднятой в исследовании темы.

Список литературы

1. *Поликарпов В. С., Палеев А. В., Поликарпова Е. В., Шибанов В. Е.* Интернет как киберфизическое оружие: монография / Южный федеральный университет. – Ростов-на-Дону; Таганрог: Южный федеральный университет, 2020. – 107 с.

2. *Щекотихин В. М. [и др.].* Информационная война. Информационное противоборство: теория и практика : монография / под общ. ред. В. М. Щекотихина; Акад. Федеральной службы охраны Российской Федерации, Центр анализа террористических угроз. – Москва: Акад. ФСО России, 2011. – 999 с. – ISBN 978-5-7295-0297-4.

3. *Корсаков Г. Б.* Роль информационного оружия в военно-политической стратегии США // США и Канада: экономика, политика, культура. – 2012. – № 1 (505). – С. 39–60.

4. *Маруев А. Ю.* Проблемы обеспечения информационной безопасности России и ведения информационного противоборства // Стратегическая стабильность. – 2007. – № 3 (40). – С. 56–64.

5. *Мелешенко В. А.* Информационная война и современные аспекты информационного противоборства // Научный резерв. – 2021. – № 1 (13). – С. 73–79.

6. *Осипенко А. Л.* Сетевая компьютерная преступность. Теория и практика борьбы : монография. – Омск, Омская академия МВД России, 2009. – 480 с.

7. *Попова А. К.* Информационные войны как новая угроза цифрового общества / Возможности и угрозы цифрового общества : сборник научных статей / под общ. ред. А. В. Соколова, А. А. Власовой. – Ярославль: Цифровая типография, 2019. – С. 116–119.

8. *Стадник А. Н., Лозовский В. В.* Информационное противоборство разработка рекомендаций по подготовке военных специалистов по защите от информационных воздействий в киберпространстве // Вестник военного образования. – 2021. – № 2 (29). – С. 33–39.

9. *Хачидогов Р. А.* Кибертерроризм в глобальном информационном пространстве: новые вызовы и меры противодействия // Образование и право. – 2021. – № 6. – С. 362–366.

10. *Чучаев А. И., Грачева Ю. В., Маликов С. В.* Цифровизация и её уголовно-правовые риски // Правосудие. – 2019. – Т. 1. – № 2. – С. 133–155. – DOI 10.17238/issn2686-9241.2019.2.133-155.

References

1. *Polikarpov V. S., Paleyev A. V., Polikarpova Ye. V., Shibanov V. Ye.* Internet kak kiberfizicheskoye oruzhiye: monografiya / Yuzhnyy federal'nyy universitet. – Rostov-na-Donu; Taganrog: Yuzhnyy federal'nyy universitet, 2020. – 107 s.

2. *Shchekotikhin V. M. [i dr.].* Informatsionnaya voyna. Informatsionnoye protivoborstvo: teoriya i praktika : monografiya / pod obshch. red. V. M. Shchekotikhina; Akad. Federal'noy sluzhby okhrany Rossiyskoy Federatsii, Tsentr analiza terroristicheskikh ugroz. – Moskva: Akad. FSO Rossii, 2011. – 999 s. – ISBN 978-5-7295-0297-4.

3. *Korsakov G. B.* Rol' informatsionnogo oruzhiya v voyenno-politicheskoy strategii SShA // SShA i Kanada: ekonomika, politika, kul'tura. – 2012. – № 1 (505). – S. 39–60.

4. *Maruyev A. Yu.* Problemy obespecheniya informatsionnoy bezopasnosti Rossii i vedeniya informatsionnogo protivoborstva // Strategicheskaya stabil'nost'. – 2007. – № 3 (40). – S. 56–64.

5. *Meleshenko V. A.* Informatsionnaya voyna i sovremennyye aspekty informatsionnogo protivoborstva // Nauchnyy rezerv. – 2021. – № 1 (13). – S. 73–79.

6. *Osipenko A. L.* Setevaya komp'yuternaya prestupnost'. Teoriya i praktika bor'by : monografiya. – Omsk, Omskaya akademiya MVD Rossii, 2009. – 480 s.

7. *Popova A. K.* Informatsionnyye voyny kak novaya ugroza tsifrovogo obshchestva / Vozmozhnosti i ugrozy tsifrovogo obshchestva : sbornik nauchnykh statey / pod obshch. red. A. V. Sokolova, A. A. Vlasovoy. – Yaroslavl': Tsifrovaya tipografiya, 2019. – S. 116–119.

8. *Stadnik A. N., Lozovskiy V. V.* Informatsionnoye protivoborstvo razrabotka rekomendatsiy po podgotovke voyennykh spetsialistov po zashchite ot informatsionnykh vozdeystviy v kiberprostranstve // Vestnik voyennogo obrazovaniya. – 2021. – № 2 (29). – S. 33–39.

9. *Khachidogov R. A.* Kiberterrorizm v global'nom informatsionnom prostranstve: novyye vyzovy i mery protivodeystviya // Obrazovaniye i pravo. – 2021. – № 6. – S. 362–366.

10. *Chuchayev A. I., Gracheva Yu. V., Malikov S. V.* Tsifrovizatsiya i yeyo ugolovno-pravovyye riski // Pravosudiye. – 2019. – T. 1. – № 2. – S. 133–155. – DOI 10.17238/issn2686-9241.2019.2.133-155.

Статья поступила в редакцию 23.06.2022; одобрена после рецензирования 06.09.2022; принята к публикации 13.09.2022.

The article was submitted June 23, 2022; approved after reviewing September 6, 2022; accepted for publication September 13, 2022.

Авторы заявляют об отсутствии конфликта интересов.
The authors declare no conflicts of interests.

Авторами внесён равный вклад в написание статьи.
The authors have made an equal contribution to the writing of the article.