Северо-Кавказский юридический вестник. 2025. № 3. С. 129–138
North Caucasus Legal Vestnik. 2025;(3):129–138

Научная статья
УДК 342.3+343.7
EDN XEWJEB

Информационные войны и иные киберугрозы личной, общественной и государственной безопасности

Ирина Анатольевна Семенцова[1], Андрей Иванович Фоменко[2]

[1]Московский университет имени С. Ю. Витте, филиал в г. Ростове-на-Дону, Ростов-на-Дону, Россия
[1]Ростовский институт (филиал) Всероссийского государственного университета юстиции (РПА Минюста России), Ростов-на-Дону, Россия
[1, 2]Южный университет (ИУБиП), Ростов-на-Дону, Россия
[1]irina_semen@inbox.ru, https://orcid.org/0000-0003-0888-0877
[2]fomenko300078@mail.ru, https://orcid.org/0000-0002-9946-0634

Аннотация

Введение. Научная статья раскрывает некоторые современные проблемы информационной безопасности российского общества и государства в условиях возникающих рисков, угроз и открытых атак. Рассматриваются преступные проявления и противоборства в различных сферах общественной и политической жизни, реализующиеся в информационном пространстве глобальной сети и с использованием IT-технологий. При этом, согласно актуальной статистике, за последние годы специальные службы задерживали и заключали под стражу десятки шпионов, а также пресекали попытки огромного количества российских граждан, старающихся передать секретную информацию другим государствам, что подрывает государственную безопасность нашей страны.
В статье обозначаются проблемы законодательства и практики его применения при охране цифрового пространства в России и способы их преодоления, виды киберпреступлений и авторское видение по совершенствованию уголовного законодательства в этой области.
Цель. Детальное исследование стратегии, тактики и методов ведения информационных войн для разработки системы активного противодействия.
Материалы и методы. Для достижения обозначенной выше цели исследования были использованы такие методы, как системно-структурный анализ, статистический метод, метод перехода от общего понятия к частному, сравнительно-правовой метод, метод правового моделирования. Также принимались во внимание мнения ученых, выраженные в опубликованных научных трудах по схожей тематике.
Результаты. С точки зрения уголовно-правовых норм рассматриваются формы информационной войны. Делается акцент на высокий диверсионный, экстремистский и террористический потенциал преступлений, совершаемых в сети «Интернет» и посредством информационных баз данных. Проанализированы составы общеуголовных преступлений, в которых в качестве факультативного признака объективной стороны фигурирует способ совершения преступления посредством сети «Интернет».
Выводы. Предлагается дополнить часть норм Уголовного кодекса Российской Федерации уточняющими формулировками квалифицирующего признака его совершения «с использованием информационно-телекоммуникационных сетей, включая сеть «Интернет»», так как использование электронных и информационно-телекоммуникационных сетей при совершении преступления повышает степень его общественной опасности за счет упрощения совершения деяния, анонимности преступников, а также массовости, быстроты и глубины проникновения негативного информационного террористического воздействия на общество.

© Семенцова И. А., Фоменко А. И., 2025

Ключевые слова: цифровизация, информационная война, киберпреступность, угрозы информационной безопасности, уголовно-правовая охрана, искусственный интеллект, сеть «Интернет», цифровые технологии, мошенничество, фишинговые технологии

Для цитирования: Семенцова И. А., Фоменко А. И. Информационные войны и иные киберугрозы личной, общественной и государственной безопасности // Северо-Кавказский юридический вестник. 2025. № 3. С. 129–138. EDN XEWJEB

Problems of Criminal and Procedural Law

Original article

Information wars and other cyber threats to personal, public and state security

Irina A. Sementsova[1], Andrey I. Fomenko[2]

[1]Moscow University named after S.Yu. Witte, branch in Rostov-on-Don, Rostov-on-Don, Russia
[1]Rostov Institute (branch) of the All-Russian State University of Justice (RPA of the Ministry of Justice of Russia), Rostov-on-Don, Russia
[1, 2]Southern University, Rostov-on-Don, Russia
[1]irina_semen@inbox.ru, https://orcid.org/0000-0003-0888-0877
[2]fomenko300078@mail.ru, https://orcid.org/0000-0002-9946-0634

Abstract

Introduction. The scientific article reveals some modern problems of information security of the Russian society and the state in the context of emerging risks, threats and open attacks. Criminal manifestations and confrontations in various spheres of public and political life, realized in the information space of the global network and using IT technologies, are considered. At the same time, according to current statistics, in recent years, special services have arrested dozens of spies, as well as thwarted attempts by a huge number of Russian citizens trying to transfer classified information to other states, which undermines the national security of our country.

The article outlines the problems of legislation and the practice of its application in protecting the digital space in Russia and ways to overcome them, types of cybercrimes and the author's vision for improving criminal legislation in this area.

Purpose. A detailed study of the strategy, tactics and methods of information warfare for the development of an active counteraction system.

Materials and methods. To achieve the above-mentioned research goal, such methods as system-structural analysis, statistical method, method of transition from a general concept to a particular one, comparative legal method, method of legal modeling were used. The opinions of scientists expressed in published scientific papers on similar subjects were also taken into account.

Results. From the point of view of criminal law norms, the forms of information warfare are considered. The emphasis is placed on the high subversive, extremist and terrorist potential of crimes committed on the Internet and through information databases. The composition of ordinary crimes is analyzed, in which the method of committing a crime via the Internet appears as an optional feature of the objective side.

Conclusions. It is proposed to supplement part of the norms of the Criminal Code of the Russian Federation with clarifying formulations of the qualifying sign of its commission "using information and telecommunication networks, including the Internet," since the use of electronic and information and telecommunication networks in the commission of a crime increases the degree of its public danger by simplifying the commission of the act, anonymity of criminals as well as the magnitude, speed and depth of the negative informational terrorist impact on society.

Keywords: digitalization, information warfare, cybercrime, information security threats, criminal law enforcement, artificial intelligence, the Internet, digital technologies, fraud, and phishing technologies

For citation: Sementsova I. A., Fomenko A. I. Information wars and other cyber threats to personal, public and state security. *North Caucasus Legal Vestnik.* 2025;(3):129–138. (In Russ.). EDN XEWJEB

Введение

В качестве первостепенных задач система информационной безопасности российского общества ставит соблюдение конституционных прав и свобод граждан при использовании информационных технологий, их научно-техническое развитие, обеспечение бесперебойного функционирования критической инфраструктуры и противодействие угрозам использования информационных технологий в целях нарушения стратегической стабильности. Также система информационной безопасности должна обеспечивать доступность информации и услуг, сохранение конфиденциальности и целостности данных пользователя, минимизацию потенциального негативного воздействия нарушителя, сохранение работоспособности (неотказности) информационных систем.

Проблема законодательного регулирования использования сети «Интернет» и отношений, возникающих в цифровом пространстве, является весьма актуальной для ученых-современников и правоприменителей. С развитием информационного пространства, неизбежно активизируются и криминальные элементы. Способы и формы преступных проявлений трансформируются в ногу с цифровой эволюцией.

Однако на сегодняшний день именно в данной сфере уголовное законодательство не в полной мере регулирует отношения, возникающие в интернет-пространстве, и не готово к стремительному развитию современных информационных технологий, что свидетельствует о необходимости доработки данного вопроса на законодательном уровне.

Цель исследования. По указанным выше причинам детальное исследование стратегии, тактики и методов ведения информационных войн для разработки системы активного противодействия является целью настоящей статьи.

Материалы и методы. Для достижения обозначенной выше цели исследования были использованы такие методы, как системно-структурный анализ, статистический метод, метод перехода от общего понятия к частному, сравнительно-правовой метод, метод правового моделирования. Также принимались во внимание мнения ученых, выраженные в опубликованных научных трудах по схожей тематике.

Результаты и обсуждение

Все чаще в правовых реалиях нашего государства встает понятие «цифровизация», изначально созданное в целях повышения качества жизни населения, быстрого и эффективного удовлетворения запросов общества. Цифровизация с точки зрения профессора Куксина И. Н. представляется эволюционной положительной тенденцией развития общественных отношений, порожденных цифровыми технологиями в различных сферах, позволяющих достичь более высокого качества продукта на основе применения различных систем искусственного интеллекта с наименьшей затратой труда [1, с. 7].

Однако это новое прогрессивное явление с другой стороны породило новые вызовы и проблемы. Все чаще юристы-ученые и правоприменители упоминают понятие «информационная война», где местом боевых действий выступает информационное пространство и цифровой мир. Она не имеет четких временных рамок (не объявляется и не прекращается) при этом стратегически выстраивается, постепенно определяя выбор действий в зависимости от шага противника. Информационная война, даже имея цель политического превосходства, всегда в основном обращена на население и сознание человека. Очень сложным оказывается оценка последствий такой войны, так как фактических разрушений от нее нет, оценить вред, нанесённый информационной инфраструктуре проблематично, причинно-следственная связь между действием и последствием сложно доказуема. Информационная война многолика и имеет в своем арсенале множество форм и методов.

Полным ходом идет внедрение в массовое сознание ложных тезисов, взглядов и концепций, а также чуждых нашему обществу установок, ценностей и норм. Все это делается для того, чтобы подвергаемые негативному воздействию суверенные государства оказались неспособными проводить независимую политику, противостоять агрессивным замыслам противника.

Все чаще используется в качестве информационного оружия против нашей страны формат исторического дискурса. В ряде случаев фальсифицированная история используется для проведения недружественных акций влияния, предъявления России территориальных, политических, финансово-экономических претензий, ослабления авторитета на международной арене, принижения роли нашей страны в мировой истории [2, с. 1].

В связи с требованиями времени, специальной военной операцией, санкциями и связанными с этими факторами угрозами для Российской Федерации был издан Указ Президента России от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности РФ» (в ред. Указа Президента России от 13 июня 2024 г. № 500). Этот указ кардинально изменил подход к обеспечению кибербезопасности в российских организациях. Внесенными в него изменениями расширены меры обеспечения информационной безопасности в нашем государстве, к примеру, с 1 января 2025 года органам государственной власти, госкомпаниям, стратегическим предприятиям и системообразующим организациям запрещено не только использовать средства защиты информации из недружественных стран, но и пользоваться их сервисами (работами, услугами) по обеспечению информационной безопасности.

Государственная позиция требует формирования выверенного, научно- исторического взгляда, глубокого интереса и уважения к истории своей страны, распространения объективных знаний о её прошлом.

Одной из разновидностей неизвестных ранее угроз, исходящих от повсеместного внедрения цифровых технологий, является киберпреступность и различные схемы цифровых обманов.

Целями мошенников становятся личные данные физических лиц, доступ к их банковским счетам, базы данных государственных органов и коммерческих и иных организаций, автоматизированные системы управления, в сфере внешнеэкономической безопасности, обороны, финансов, промышленности, здравоохранения, науки, транспорта, связи, энергетики, то есть критическая информационная инфраструктура. Совершенствуются способы информационного противостояния: распространение запрещенной информации, создание зеркальных сайтов для хищения электронных средств и продажи наркотических средств и психотропных веществ, онлайн-казино, экстремистских и террористически сообществ, функционирование параллельно теневой сегмент Интернета, введение различных цифровых активов (коины, токены), неконтролируемых банковской системой, для оплаты товаров и услуг с сети [3, с. 1065].

Достаточно часто мошенники применяют фишинговые технологии интернет-мошенничеств с целью получения доступа к конфиденциальным данным – логинам, паролям, доступам к банковским счетам пользователей. Это происходит, например, с помощью сайтов-копий реальных электронных ресурсов финансовых организаций. Повышаются риски стать жертвами преступных схем при возникновении опосредованных технических отношений или с использованием сервисов искусственного интеллекта, в частности, при оказании дистанционных образовательных или медицинских услуг, оказании правовой помощи, продажи авиа-, ж/д-билетов, билетов на развлекательные мероприятия и пр.

В научной юридической литературе отмечается, что с появлением новых общественных отношений в сфере информационного пространства, цифровой безопасности формируется новая подотрасль права, которая призвана урегулировать новые процессы. Появляются новые термины – «цифровые права», «цифровые обязанности», «цифровая ответственность». В этой связи предлагается принцип разделенной ответственности, когда за ошибки робота или даже ущерб, причиненный им, ответственность несет разработчик программы и оператор, обеспечивающий его использование и эксплуатацию [4, с. 8]. Исследователь Иткина Я.Я. считает необходимым наделить искусственный интеллект правосубъектностью, признать и официально закрепить в гражданско-правовом поле появления «электронного лица» как нового субъекта правоотношений. При этом в отличие от действий юридического лица,

за интересами которого стоят конкретные индивиды, в данном случае ответственность предлагается возложить на компанию-разработчика [5, с. 41].

Существенными факторами, делающими борьбу с современными информационными угрозами неэффективной, являются недостаточное нормативное регулирование функционирования социальных сетей, слабые средства противостояния кибер-атакам (уязвимость, неустойчивая антивирусная защита), отсутствие механизмов защиты частной жизни и персональных данных пользователей, неадекватные ответные меры против массового распространения клеветы и иной заведомо недостоверной информации, отсутствие законодательно закрепленной специальной терминологии и отставание в развитии уголовного законодательства, не успевающего эволюцией преступных способов [6, с.41].

Преступления в сфере компьютерной информации отдельно выделены в главу 28 Уголовного кодекса Российской Федерации. Считаем, что в целом законодатель предусмотрел достаточный перечень оснований для уголовной ответственности за совершение деяний, причиняющих вред или создающих угрозу его применения отношениям в сфере производства, хранения, использования и распространения компьютерной информации. Изучение этих составов не входит в предмет данного исследования. При этом хотелось бы остановиться на особенностях квалификации некоторых составов общеуголовных преступлений против личности, собственности, общественной безопасности, совершаемых с использованием информационных технологий в сети.

СМИ, в том числе и «Интернет», указаны как возможный способ совершения преступлений, связанных с доведением до самоубийства, содействием и склонением к самоубийству (ст. 110–110.2 УК РФ). И действительно, посредством угроз, травли, советов в социальных сетях достаточно часто происходят различного рода понуждение покончить жизнь. Законодатель предусмотрел квалифицирующий признак публичности и «использование информационно-телекоммуникационной сети «Интернет» при распространении клеветнической информации, которая нередко доводится и становится известной через соцсети, форумы, мессенджеры. Также как и угрозы расправы, за которые предусмотрена ответственность в соответствии во ст. 119 УК РФ, хотя, в последней норме уголовного закона не указан данный признак, что значительно усложняет уголовно-правовую квалификацию при совершении преступления, например, публично и/или в Интернете. Считаем это нормативной недоработкой.

Аналогично следует поступить законодателю при вовлечении несовершеннолетнего в преступные или антиобщественные деяния, включив в ст. 150 и 151 УК РФ признак, когда субъект действует через сеть «Интернет».

При тайном хищении чужого имущества законодатель п. «г» ч.3 ст. 158 посвятил краже электронных денежных средств. Речь идет об использовании чужой или поддельной платежной карты либо числе, получив к ней доступ (пин-код, контрольную информацию). В случае же если с чужой банковской карты происходят безналичные расчеты по оплате товаров в Интернете, или с помощью зеркальных сайтов (без обмана или злоупотребления доверием) считаем необходимым применить квалифицированный состав с признаком «использования информационно-телекоммуникационных сетей, включая сеть "Интернет"».

Обманные способы при совершении простого мошенничества (ст. 159 УК РФ), в сфере кредитования (ст. 159.1 УК РФ), получения выплат (ст. 159.2 УК РФ), страхования (ст. 159.5 УК РФ) с использованием цифровых технологий, также недостаточно урегулированы уголовным законом. Пора внести соответствующие изменения в нормы о заведомо ложном сообщении о теракте (ст. 207 УК РФ), вовлечение в участие в экстремистском сообществе (организации) (ст. 282.1 и 282.2 УК РФ). Очевидно, что данные виновные деяния могут быть совершены с использованием Интернет-ресурсов. Данный факт набирает все большую актуальность ввиду того, что только за 2023 год Роскомнадзором и прокуратурами было заблокировано более 558 тыс. интернет-страниц с материалами пронаркотического, суицидального,

экстремистского и террористического содержания[1]. Львиная доля пользователей таких каналов молодые люди в возрасте от 15 лет [7, с. 11].

Опорой и преемственностью населения выступает молодежь. Именно эта социальная группа больше всех остальных подвержена воздействию преступности, как традиционной, так и цифровой. Преступники пользуются уязвимостью подростков, их неокрепший разум становится еще одним средством на пути к победе в информационной войне. Никуда не уходит из России и мода на молодежные субкультуры. Молодые люди на протяжении всей истории развития общества стремились к обособлению в группы по различным признакам, интересам, устремлениям. Зачастую идеи таких общностей близки к экстремистским. Участников подобных групп призывают к антиобщественной деятельности, массовым дракам, унижению инакомыслящий и инаковыглядящих.

Яркая демонстрация тому – появившаяся в 2023 г. молодежная организация любителей аниме «Рёдан», создание и руководство которой осуществлялось через Интернет-сообщества. Члены этой группы по своим идейным соображениям не раз становились участниками массовых беспорядков и хулиганских действий в крупных городах России. Очевидно, что для подобных правонарушителей сегодня стирается грань между стремлением законно реализовать конституционные права на самовыражение и экстремистскими проявлениями.

В преступлениях террористической направленности обращения о готовящихся взрывах, поджогах и иных устрашающий действиях, угрожающих безопасности, все чаще направляются с помощью Интернет ресурсов. В 2022 г. произошёл всплеск поступивших сообщений о грядущих терактах. Письма такого содержания поступали на официальные адреса электронной почты государственных органов и коммерческих и иных организаций (правоохранительных органов, школ, вузов, организаций системы здравоохранения, торговых центров и т.д.), что неизбежно привело к сбоям учебного процесса и работы административного персонала. Сообщения поступали массово и регулярно. Настолько, что пользователи просто переставали реагировать на них, удаляя из электронного ящика. Это еще раз говорит о несовершенстве уголовно-правовой охраны, в частности, проблемах квалификации заведомо ложного сообщения об акте терроризма [8, с. 84], а также о неготовности госорганов к информационному противостоянию.

В российских нормативных источниках нет дефиниции не категории «информационная война», не «война» в общем её понимании. Очевидно, что «информационная война» сложная, комплексная, но не неопределяемая в рамках российского федерального законодательства категория. А раз так, то существует возможность и нормативного ее закрепления как это сделано в некоторых международно-правовых актах, а именно в приложении № 1 к Соглашению между Правительством Российской Федерации и Правительством Республики Беларусь о сотрудничестве в области обеспечения международной информационной безопасности, подписанного 25 декабря 2013 г. Кроме этого, данное определение также предложено в статье 2 концепции Конвенции об обеспечении международной информационной безопасности (проект), внесенной в ООН на рассмотрение 15 мая 2023 г. ее разработчиками Россией, Белоруссией, КНДР, Никарагуа и Сирией.

Информационная война – открытые или скрытые целенаправленные информационные воздействия систем друг на друга с целью получения определенного выигрыша в материальной, военной, политической или идеологической сферах [9, с. 194].

В узком смысле слова информационная война – это вооруженный конфликт, в котором столкновение сторон происходит в форме информационных операций с применением информационного оружия.

Полагаем, что именно такое определение и следовало бы закрепить на законодательном уровне, так как оно не содержит в себе оценочных понятий, а также качественных и количественных характеристик.

[1] Роскомнадзор в 2023 году заблокировал более 558 000 сайтов и интернет-страниц. - URL: https://https://www.vedomosti.ru/technology/articles/2024/01/26/1016847-roskomnadzor-zablokiroval-bolee-558-000-saitov. (дата обращения: 06.07.2025).- Текст: электронный

Иными словами, можно сказать, что информационная война включает в себя интегрированное использование возможностей, среди которых выделяются психологические и компьютерные сетевые операции в качестве электронного оружия. В условиях военного политического конфликта информационные технологии способны обеспечивать операции с военной дезинформацией и дезорганизацией [10, с. 34].

Понятие «информационная война» весьма широкое и может быть рассмотрено в двух аспектах: социальном и политическом. О социальных аспектах говорилось нами выше, и речь шла о явлении, в котором информация и информационное пространство выступает средством достижения преступных целей нарушения прав и свобод человека, подрыва традиционных ценностей, корыстной наживы, дестабилизации общества. Итог такой информационной войны как социального явления – рост общеуголовной преступности.

Войны в информационном пространстве ведутся при помощи информационного оружия, в этом понятии исследователи объединяют самый широкий спектр средств уничтожения, искажения, хищения информации, получения или ограничения доступа к информационным системам, нарушения функционирования информационной техники и сетей. Так, в кибератаках применяются компьютерные вирусы, логические бомбы, программы-оборотни и убийцы информации, средства несанкционированного доступа к информационным ресурсам и подавления информационных систем и т.д.

В Интернете терроризм развивается стремительно, поскольку сеть - это идеальная среда для его развития и распространения. Отсутствие цензуры приводит к распространению информации, изображений, угроз или сообщений независимо от их законности или потенциального воздействия на человеческое сознание. Кибертеррористы использует открытость Интернета для своих целей: дискредитации правительств и государств, размещения сайтов террористической направленности, порчи и разрушения ключевых систем (путем внесения в них фальсифицированных данных или постоянного вывода этих систем из строя). Это в свою очередь порождает страх или тревогу среди населения, и является дополнением к традиционному виду терроризма. Данные преступные деяния предусмотрены ст. 205, 205.1, 205.2 Уголовного кодекса РФ.

К сожалению, многие средства массовой информации употребляют термин «кибертерроризм» весьма некорректно, создавая путаницу в понятиях, ставя знак равенства между понятием «хакер» и «кибертеррорист». Вряд ли это можно счесть правильным. Безусловно, терроризм – это преступление, но не каждое преступление есть терроризм, точно так же как кибертеррориста, как правило, можно назвать хакером, но не всякий хакер совершает терракты в киберпространстве или с помощью компьютера.

Итак, на наш взгляд, кибертерроризм можно отнести к так называемым технологическим видам терроризма. В отличие от традиционного, этот вид терроризма использует в террористических акциях новейшие достижения науки и техники в области компьютерных и информационных технологий, радиоэлектроники, генной инженерии, иммунологии.

В политическом смысле информационная война ведется за власть и представляет собой противоборство двух или более сторон путем воздействия, оказываемого на государственный аппарат, вооруженные силы и политические структуры. Примером может служить массовое распространение ложной информации (фейков) о действиях Вооружённых сил, о ходе специальной военной операции, о стратегических объектах и политических курсах, атака на критическую информационную инфраструктуру. Такое воздействие может осуществляться как внутри страны, так и с внешней стороны государствами-противниками.

С целью подрыва власти, зарождения недоверия общества государству, возникновения паники совершаются крупные хакерские атаки как формы неправомерного доступа к компьютерной информации. Последствиями могут быть полное или частичное уничтожение, блокирование, модификация, копирование информационных баз. Противодействие подобным атакам сегодня осуществляют субъекты защиты критической информационной

инфраструктуры, к которым относят государственные органы, прежде всего, ФСБ России, отвечающую, в том числе, за создание национального координационного центра по компьютерным инцидентам; ФСТЭК России, осуществляющую государственный контроль в области обеспечения безопасности значимых объектов критической информационной инфраструктуры; их должностные лица, а также подразделения и должностные лица самих субъектов такой инфраструктуры.

Ярким примером успешного отражения серьезной кибератаки на ведомственные сервера может служить восстановление работоспособности электронных систем ФТС России после массированной DDoS-атаки на операторов связи весной 2023 года. В мае-июне 2024 г. произведена масштабная хакерская атака на известную логистическую компанию, которая парализовала ее работу на несколько дней. Не функционировал сайт и другие сервисы организации, не работами пункты выдачи отправлений. Кибератакам были подвержены также сервис «Госуслуги», сайты кредитных организаций и СМИ, судов, сайты вузов накануне приемных кампаний.

В связи с событиями 2022 г. против России ведется ожесточенная информационная внешнеполитическая война, которая в рамках данного исследования понимается как конфликт между государствами либо негосударственными формированиями, основывающийся на комплексе средств воздействия, усложняющих сбор, обработку, хранение, передачу и использование информации противником (вооруженными силами, госорганами, мирным населением), оказывающих влияние на военный и государственный аппарат с целью подрыва независимости страны, искажении достоверных сведений одного государства, и (или) использование их же против другой стороны [11, с. 109].

В подобной формулировке в России необходимо узаконить данное понятие, потому как это послужит основой защиты государственных информационных систем и процессов в условиях военно-политического противостояния.

Выводы

Для исключения указанных ранее пробелов необходимо восполнить в федеральных актах терминологию, характерную для преступлений, связанных с информационными технологиями («аккаунт», «сообщество», «хакерская атака», «фейк», «инфо-поле» и т.д.) либо отказаться от их использования в такой формулировке в официальных изданиях.

Требуется дальнейшее внесение изменений в уголовный закон в части указания квалифицирующего признака «совершение преступления с использованием информационно-телекоммуникационной сети «Интернет» в составах, для которых данный способ характерен (ст. 119, 150, 151, 158, 159 – 159.2 , 159.5, 207, 282.1, 282.2УК РФ).

Перечисленные предложения помогут эффективнее использовать нормы Уголовного закона для решения проблемы информационных преступлений, формирования новой базы уголовно-правовой характеристики данных деяний и разработки методик расследования указанных правонарушений, а также окажут влияние на формирование правовой базы для охраны цифрового пространства России.

Информационные войны со своими кибератаками анонимны, стремительны, не требуют вооружения или дорогостоящей техники. Распространением одной вредоносной программы можно причинить вред, сопоставимый с военной операцией, а ущерб дистанционных хищений в разы превышает нетехнологические способы. Защита персональных данных, борьба с дистанционными видами мошенничества, защита банковских транзакций, блокировка запрещенных Интернет-ресурсов – эта лишь начальная, но обязательная стадия и доля мер, направленных на упреждение информационных угроз личной безопасности. Следующим этапом противостояния являются информационные войны с угрозами общественной и государственной безопасности в различных формах, в том числе, кибертерроризм, кибершпионаж. Важно, чтобы борьба с информационными атаками перешла со стадии «своевременное реагирование» на ступень выше «законодательное регулирование» и «пресечение».

Список источников

1. Куксин И.Н. Цифровизация – новая реальность в праве // Вестник Московского университета им. С.Ю. Витте. Серия 2: Юридические науки. 2020. № 1 (23). С. 6-12. DOI 10.21777/2587-9472-2020-1-6-12.

2. Копичев О.А., Николаев А.Е. Современные войны: анализ тенденций развития межгосударственного противоборства, классификация форм и способов борьбы, формирование признаков и критериев военного конфликта // Системы управления, связи и безопасности. 2021. №1. С.1-34. DOI: 10.24411/2410-9916-2021-10101.

3. Дубень А. К. Аспекты и угрозы информационной безопасности в эпоху современных информационных войн // Вестник Удмуртского университета. Серия «Экономика и право». 2022. № 6. С.1064-1068. DOI: 10.35634/2412-9593-2022-32-6-1064-1068.

4. Романова И.Н., Видова Т.А. Проблемы правового регулирования искусственного интеллекта в сфере юриспруденции // Вестник Московского университета им. С.Ю. Витте. Серия 2: Юридические науки. 2023. № 3 (39). С. 5-10. DOI 10.21777/2587-9472-2023-3-5-10.

5. Иткина Я.Я. Правовые аспекты искусственного интеллекта // Вестник Московского университета им. С.Ю. Витте. Серия 2: Юридические науки. 2022. № 2.1 (33). С. 39-43. DOI 10.21777/2587-9472-2022-2.1-39-43.

6. Игнатьева И.В., Зедгенизова И.И., Власова Е.Л. Влияние информационных войн на снижение уровня национальной безопасности государств и формирование правосознания общества // Проблемы экономики и юридической практики. 2021. Т. 17. № 6. С. 38-42.

7. Кобец П.Н. Информационное воздействие как один из современных методов терроризма и меры борьбы с ним // Вестник Краснодарского университета МВД России. 2022. № 1. С. 10–14.

8. Просочкин А.М., Петрашева Н.В. Усиление уголовной ответственности за заведомо ложное сообщение об акте терроризма: проблема конструирования уголовно-правовых санкций // Юристъ-Правоведъ. 2019. №1 (88). С. 84–89.

9. Основы информационной безопасности : учебное пособие для студентов вузов / Е.В. Вострецова. Екатеринбург : Изд-во Урал. ун-та, 2019. 204 с.

10. Муратова Ю.Д. Сущность информационной войны в региональном политическом конфликте и основные формы ее проявления // Коммуникология. 2018. №1. С. 34–45.

11. Крылова И.А. Информационно-психологические войны как фактор дезинтеграционных процессов в современном мире // Большая Евразия: развитие, безопасность, сотрудничество. 2021. № 4-1. С. 106–110.

References

1. Kuksin I.N. Digitalization is a New Reality in Law. *Bulletin of Moscow Witte University. Series 2: Legal science*. 2020;1 (23):6-12. DOI 10.21777/2587-9472-2020-1-6-12 (In Russ.)

2. Kopichev O.A., Nikolaev A.E. Modern Wars: Analysis of Trends in Interstate Conflict, Classification of Forms and Methods of Warfare, and Formation of Signs and Criteria of Military Conflict. *Systems of Control, Communication and Security*. 2021;(1):1-34. DOI: 10.24411/2410-9916-2021-10101. (In Russ.)

3. Duben' A.K. Aspects and Threats of Information Security in the Era of Modern Information Wars. *Bulletin of Udmurt University. Series Economics and Law.* 2022;(6):1064-1068. DOI: 10.35634/2412-9593-2022-32-6-1064-1068. (In Russ.)

4. Romanova I.N., Vidova T.A. Legal Issues in the Regulation of Artificial Intelligence in the Legal Field. *Bulletin of Moscow Witte University. Series 2: Legal science*. 2023;3(39):5-10. DOI: 10.21777/2587-9472-2023-3-5-10. (In Russ.)

5. Itkina Ya.Ya. Legal aspects of artificial intelligence. *Bulletin of Moscow Witte University. Series 2: Legal science*. 2022;2.1 (33):39-43. DOI 10.21777/2587-9472-2022-2.1-39-43. (In Russ.)

6. Ignat'eva I.V., Zedgenizova I.I., Vlasova E.L. The impact of information wars on reducing the national security of states and shaping public consciousness. *Economic Problems and Legal Practice.* 2021;17(6):38–42. (In Russ.)

7. Kobec P.N. Informational influence as one of the modern methods of terrorism and measures to combat it. *Bulletin of Krasnodar University of Russian MIA.* 2022;(1):10–14. (In Russ.)

8. Prosochkin A.M., Petrasheva N.V. Strengthening Criminal Liability for False Reports of Terrorist Acts: The Problem of Constructing Criminal Sanctions. *Jurist-Pravoved.* 2019;1(88):84–89. (In Russ.)

9. Vostretsova E. V. *Fundamentals of Information Security:* A Textbook for University Students. Yekaterinburg: Ural University Press; 2019. 204 p. (In Russ.)

10. Muratova Yu. D. The Essence of Information Warfare in a Regional Political Conflict and Its Main Forms. *Communicology.* 2018;(1):34–45. (In Russ.)

11. Krylova I.A. Information and psychological warfare as a factor in the disintegration of the modern world. *Greater Eurasia: development, security, cooperation.* 2021;(4-1):106–110. (In Russ.)

Информация об авторах

И. А. Семенцова – кандидат юридических наук, доцент, доцент кафедры уголовного права и процесса, Московский университет имени С. Ю. Витте, филиал в г. Ростове-на-Дону; доцент кафедры уголовного права и криминологии, Ростовский институт (филиал) Всероссийского государственного университета юстиции (РПА Минюста России); доцент кафедры «Уголовно-правовые дисциплины», Южный университет (ИУБиП).

А. И. Фоменко – кандидат юридических наук, доцент, заведующий кафедрой «Уголовно-правовые дисциплины», проректор по воспитательной работе и молодежной политике, Южный университет (ИУБиП).

Information about the authors

I. A. Sementsova – Cand. Sci. (Law), Associate Professor of the Department of Criminal Law and Procedure, Moscow University named after S.Yu. Witte, branch in Rostov-on-Don; Associate Professor of the Department of Criminal Law and Criminology, Rostov Institute (branch) of the All-Russian State University of Justice (RPA of the Ministry of Justice of Russia); Associate Professor of the Department "Criminal Law Disciplines", Southern University.

A. I. Fomenko – Cand. Sci. (Law), Associate Professor, Head of the Department "Criminal Law Disciplines", Vice-Rector for Educational Work and Youth Policy, Southern University.

Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации. Авторы заявляют об отсутствии конфликта интересов.
Contribution of the authors: the authors contributed equally to this article. The authors declare no conflicts of interests.

Статья поступила в редакцию 07.07.2025; одобрена после рецензирования 03.09.2025; принята к публикации 04.09.2025.
The article was submitted 07.07.2025; approved after reviewing 03.09.2025; accepted for publication 04.09.2025.