
ПРОБЛЕМЫ КОНСТИТУЦИОННОГО И МУНИЦИПАЛЬНОГО ПРАВА PROBLEMS OF CONSTITUTIONAL AND MUNICIPAL LAW

Научная статья
УДК/UDC 342
DOI: 10.21779/2224-0241-2022-43-3-39-45

Информационная безопасность как составная часть национальной безопасности Российской Федерации: конституционно-правовой аспект

З.И. Алиева¹, З.М. Хасбулатова²

^{1,2} Дагестанский государственный университет, г. Махачкала, Российская Федерация

¹ mumina@mail.ru

² hasbulatovazm@mail.ru

Аннотация. В статье изучены современные конституционно-правовые аспекты информационной безопасности в структуре национальной безопасности Российской Федерации. Выявлены основные взаимосвязи, а также дана общая оценка текущей ситуации в информационной безопасности России. Исследованы проблемы и тенденции совершенствования нормативно-правовых актов регулирования информационной безопасности Российской Федерации и наших предприятий с позиции укрепления национальной безопасности в среднесрочной перспективе. Предложены рекомендации по усовершенствованию имеющихся инструментов конституционно-правового аспекта информационной безопасности как составной части национальной безопасности Российской Федерации.

Ключевые слова: киберугроза, информация, информационная безопасность, национальная безопасность, безопасность в сети Интернет

Для цитирования: Алиева З.И., Хасбулатова З.М. Информационная безопасность как составная часть национальной безопасности Российской Федерации: конституционно-правовой аспект // Юридический вестник ДГУ. 2022. Т. 43, № 3. С. 39–45. DOI: 10.21779/2224-0241-2022-43-3-39-45

Original article

Information security as an integral part of the national security of the Russian Federation constitutional and legal aspect

Zulfiya I. Alieva¹, Zarema M. Hasbulatova²

^{1,2} Dagestan State University, Makhachkala, Russian Federation

¹ mumina@mail.ru

² hasbulatovazm@mail.ru

Abstract. The article studies modern constitutional and legal aspects of information security in the structure of the national security of the Russian Federation. The main interrelations are revealed, and a general assessment of the current situation in the information security of Russia is given. The problems and trends in improving the regulatory legal acts regulating the information security of the Russian Federation and our enterprises from the standpoint of strengthening national security in the medium term have been studied. Recommendations are proposed for improving the existing tools of the constitutional and legal aspect of information security as an integral part of the national security of the Russian Federation.

Keywords: cyber threat, information, information security, national security, Internet security

For citation: Alieva Z.I., Hasbulatova Z.M. Information security as an integral part of the national security of the Russian Federation constitutional and legal aspect. *Yuridicheskii vestnik DGU = Law Herald of DSU*, 2022, vol. 43, no. 3, pp. 39–45. DOI: 10.21779/2224-0241-2022-43-3-39-45 (In Russ.).

Современное общество можно с уверенностью назвать информационным, поскольку многие процессы повседневной деятельности личности, общества и всего государства перешло в цифровое пространство. Оно дает возможность существования любого вида информации, а также является универ-

сальным полем деятельности как отдельных людей, их групп или предприятий, так и субъектов государственного управления.

В то же время информационное пространство не имеет конечного, завершенного состояния, оно динамично, и темпы его развития стремительны.

С одной стороны, это положительно влияет на развитие мировой экономики, межгосударственных отношений и т.п. Но, с другой стороны, возникают трудности в осуществлении различных процессов именно из-за специфики информационного пространства. Для обеспечения полноценного, а главное, безопасного осуществления деятельности субъектов в информационном пространстве необходима качественная, своевременная защита информации и информационных процессов. Однако темпы развития информационной безопасности и, в частности, средств защиты информации, существенно ниже темпов появления и развития угроз безопасности информации [10, с. 12].

Проблематика информационной безопасности выходит на первый план в современном обществе. Стремительно проходящие процессы социальной трансформации, в основе которых информационно-коммуникационные, технико-технологические изменения, закономерно приводят к возникновению рисков дисфункциональных и дезорганизационных состояний социальной системы, ее отдельных институтов, подсистем. Глобализация и информатизация охватывают с большей или меньшей интенсивностью все страны, в том числе и Россию. В настоящее время суверенитет национального государства значительно ограничен в информационной, интеллектуальной сфере. Именно поэтому в условиях современной России возрастают угрозы и риски, связанные с информационной сферой, являющейся неотъемлемой частью всей национальной безопасности [16, с. 1].

Национальная безопасность представляет собой состояние защищенности жизненно важных интересов личности, общества и государства в различных сферах жизнедеятельности от внутренних и внешних угроз политического, правового, экономического, социального, военного, техногенного, экологического, информационного и иного характера, обеспечивающая устойчивое развитие страны.

Как видно из определения, национальная безопасность включает в себя несколько основополагающих направлений, одним из которых является обеспечение защищенности в сфере информацион-

ного характера. Только комплекс мероприятий, системное взаимодействие направлений в различных областях, направленных на защиту интересов как на микроуровне личности, так и на макроуровне всего государства, способен обеспечить устойчивое развитие страны.

В настоящий момент состояние российской сети «Интернет» специалисты называют одним из самых устойчивых. Это зависит от многих факторов. Например, важную роль играет небольшое количество операторов, которые предоставляют услуги Интернета. В условиях конкуренции на рынке предоставления услуг связи наблюдается большая устойчивость, в отличие от монополии. В том случае, когда на рынке представлен единственный провайдер, создаются условия для реализации рисков недоступности сетевых ресурсов у большинства пользователей как на уровне региона, так и на уровне всего государства.

Кроме того, постоянно создается и совершенствуется законодательная база в области защиты информации, а также национальной безопасности в целом. К сожалению, нормативно-правовая база обновляется не с той скоростью и эффективностью, какой хотелось бы специалистам в области информационной безопасности. К тому же некоторые проекты нормативно-правовых актов (НПА) ставятся под сомнения.

В настоящее время тенденции развития российского законодательства, связанного с информационными технологиями, направлены на укрепление правового регулирования общественных отношений, а именно приведение их в соответствие с актуальным положением в государстве и мире. Это обуславливается тем, что темпы развития общественных отношений в сфере информационных технологий значительно превышают реакцию законодателя на эти изменения, ввиду чего данные нормы часто имеют явные пробелы в механизме нормативного регулирования.

Стоит отметить, что информационная безопасность занимает одну из ключевых ролей в национальной безопасности Российской Федерации (РФ):

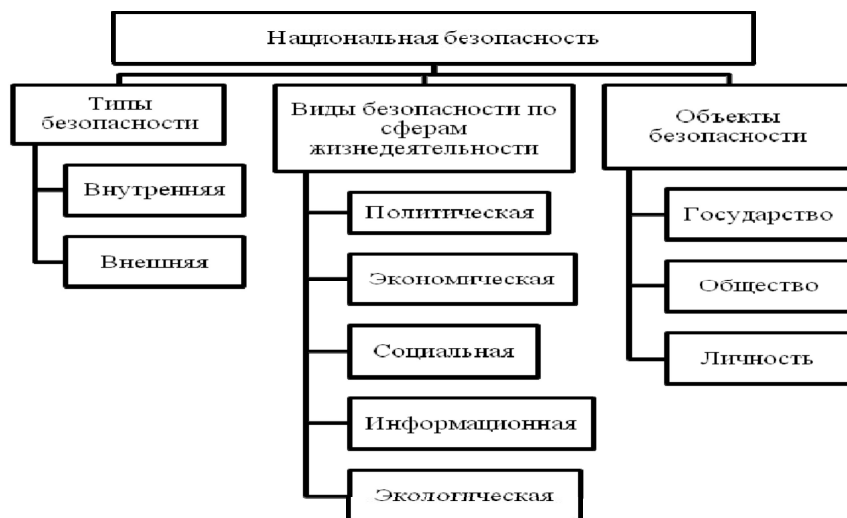


Рис. 1

Как видно из предложенной схемы, информационная безопасность занимает ведущее положение в структурно-национальной безопасности России. Это обусловлено тем фактом, что современный мир – это сплошь информационные технологии, поэтому обеспечение безопасного проникновения информационных технологий в жизнь общества может быть осуществлено лишь при комплексном обеспечении национальной безопасности страны в целом [11, с. 65].

Если провести анализ текущего состояния информационной безопасности Российской Федерации в доктрине национальной безопасности, можно отметить особую динамику в период с 2020 по 2022 годы. Большая часть населения перешла на удаленный формат работы, в силу чего вопрос об информационной безопасности встает очень остро. То есть за последние два года этот вопрос вошел в обычную повестку национальной безопасности нашей страны.

Стоит также отметить, что существует актуальная проблема международного терроризма, ко-

торый, пользуясь современными технологиями в области компьютерной информации и связи, угрожает национальной безопасности Российской Федерации. Речь идет не только о коммуникации между членами террористических группировок, но и об их деятельности в рамках информационного поля и сети «Интернет», направленной на подрыв государственных систем безопасности, дестабилизацию функционирования систем, напрямую связанных с технологиями, за счёт которых они работают. Именно этими факторами обусловлена актуальность выбранной темы и необходимость в формировании практических предложений по нормативному регулированию данной сферы общественных отношений.

Правовое регулирование имеет принципиально важное значение в сфере безопасности федеральной и государственной службы, включающей гражданскую, военную и правоохранительную сферы [12, с. 66].



Рис. 2

Как видно из представленного выше рисунка, к основным конституционно-правовым актам можно отнести на текущем этапе Конституцию РФ, Гражданский кодекс РФ, Уголовный кодекс РФ, Доктрину информационной безопасности России, Указ Президента РФ «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей (ИТКС) международного информационного обмена» и ряд федеральных законов (ФЗ), в числе которых:

- ФЗ «Об информации, информационных технологиях и о защите информации» [2];
- ФЗ «О государственной тайне», регулирующий отношения, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации [3, ст. 1];
- ФЗ «О коммерческой тайне», в ведении которого находятся отношения, связанные с установ-

лением, изменением и прекращением режима коммерческой тайны в отношении информации, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам [4, ст. 1];

- ФЗ «О персональных данных», в котором сферой деятельности являются отношения, связанные с обработкой персональных данных, осуществляемой органами власти, юридическими и физическими лицами с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств [5, ст. 1];

Следует отметить, что персональные данные пользователей нарушаются в связи с использованием социальных сетей. Прежде всего, нарушается право на неприкосновенность частной жизни, личные и семейные тайны, защиту чести и доброго имени, когда пользователь размещает свои фотографии в сети, а мошенник использует эти фотографии в своих целях. Во-вторых, если произошел взлом

страницы пользователя, то нарушается его право на тайну переписки, телефонных разговоров. Не следует в социальной сети хранить, использовать и распространять информацию о личной жизни пользователя без его согласия [13, с. 1];

- ФЗ «О связи», в частности, главы 7, 7.1, 9 и 10, в которых затронут вопрос обеспечения безопасных способов установления связи на территории Российского государства [6, ст. 1];

- ФЗ «О безопасности», определяющий основные принципы и содержание деятельности по обеспечению всех видов безопасности государства, предусмотренных законодательством Российской Федерации, включая информационную и национальную [7, ст. 1] и др.

Дополнительными нормативными правовыми актами, регулирующими информационные технологии и безопасность, являются:

- Положение Федеральной службы охраны РФ «О сегменте информационно-телекоммуникационной сети Интернет», устанавливающее функционирование органов государственной власти на всех уровнях в ИТКС «Интернет» [8];

- международные нормативные правовые акты и нормы в сфере регулирования информационной безопасности;

- внутренние распоряжения ведомств;
- документы малого, среднего и крупного бизнеса и др.

Основная проблема развития правового обеспечения информационной безопасности в РФ связана с реализацией государственной политики в этой области. Система информационного обеспечения государственной политики в сфере информационной безопасности представляет собой совокупность государственных органов и других уполномоченных субъектов, которые участвуют в осуществлении информационного сопровождения обеспечения государственной политики, а также установленных нормативными правовыми актами общественные отношения. Государственная политика в области информации должна основываться на научных и методологических разработках, объединённых в единую концепцию, такую концепцию следует формировать как совокупность целей, что отражают национальные интересы в информационной сфере, а также стратегии и тактики управленческих решений и методов их реализации [14, с. 2].

На представленном ниже рисунке продемонстрированы основные показатели влияния факторов на формирование бюджета по защите данных на государственном уровне. Так, по данным отчета «Исследование российского рынка информационной безопасности» в 2021 году наиболее значимыми факторами, которые влияли на формирование бюджета на информационную безопасность, стала защита персональных данных (54%), критической информационной структуры (45%) и государственных информационных систем (40%):



Рис. 3

В числе ключевых факторов также отмечались проблемы конфиденциальности данных (38%), предписание к устранению нарушений требований регуляторов (35%), требования сотрудников, отвечающих за безопасность (32%). Наименее приоритетными факторами стали положение Банка России ГОСТ 57580.1-2017 (5%) и переход на облачные технологии для оптимизации затрат (6%).

Посредством телекоммуникационной сети «Интернет», с которой связана большая часть

функционирующего оборудования служб и организаций по всему миру, может осуществляться, так называемая, сетевая разведка, направленная на сканирование наличия информации, степени ее защищенности, и непосредственно извлечение этой информации для дальнейшего использования. Это касается не только информации государственного и коммерческого уровня, но и конституционного права граждан на неприкосновенность частной жизни, а также запрета на использование и распро-

странение информации о частной жизни лица без его согласия [1, ст. 23].

Последний фактор, обуславливающий тенденции развития законодательства в сфере обеспечения информационной безопасности России, состоит в положении дел на международной арене и осложнёнными отношениями Российской Федерации с отдельными государствами. Таким образом, решение данной проблемы связано с обеспечением государственного суверенитета. Согласно первой части Конституции Российской Федерации, суверенитет Российской Федерации распространяется на всю ее территорию [1, ст. 4], однако здесь необходимо говорить не только о составляющих правовой категории «территория Российской Федерации», которая закреплена в национальном законодательстве в части 1 Конституции РФ [1, ст. 67], но и об информационном пространстве как части территории нашего государства.

Также достаточно обсуждаемыми в этом году являются упомянутые выше Федеральный закон «О внесении изменений в ФЗ "О связи"» и Федеральный закон «Об информации, информационных технологиях и о защите информации». Данные нормативно-правовые акты затрагивают такие вопросы государственного интереса как оборона и безопасность.

Основной задачей последнего закона является обеспечение безопасного и устойчивого функционирования сети «Интернет» на территории Российской Федерации с целью обеспечения безопасности личности, общества и государства в целом. По смыслу закона преследуется цель технологического обеспечения получения доступа в Интернет не через устройства, предоставляемые иными государствами, а посредством создания единой системы коммуникации, принадлежащей нашему государству. Это обуславливается тем, что в рамках информационного пространства имеется условное деление, объясняемое принадлежностью определенных участков сети (так называемого Российского интернета) к российской территории. Данная принадлежность выражается в следующих юридически значимых факторах:

- нормативно-правовое регулирование общественных отношений, осуществляемых посредством сетевой инфраструктуры, в пределах Российской Федерации;
- доменная принадлежность части сетевых ресурсов по месту их регистрации. Речь идёт о таких сертифицированных доменах, как «.rf», «.ru»;
- юридическая регистрация субъектов информационных отношений, а именно операторов связи, владельцы сайтов и т.д.

Проблема обеспечения государственного суверенитета и его соотношения в рамках реализации отдельных прав граждан в информационном поле часто поднимается как дискуссионная в научных кругах. Так, российский ученый А.К. Дубень

говорит о «важности отражения суверенитета личности и неприкосновенности его конституционных прав в рамках информационных ресурсов» [10, с. 41].

Стоит упомянуть, что вышеназванный ФЗ «Об информации, информационных технологиях и о защите информации» вызвал большой общественный резонанс: по мнению российских граждан, он непосредственно нарушает их конституционное право на получение и использование информации, а также свободу мысли. В социальных сетях его уже называют «Законом об изоляции Интернета». Вероятнее всего, данное негативное восприятие основано на неверном толковании текста законов. По смыслу данного закона основной задачей правового регулирования данного вида общественных отношений является не ограничение доступа к всемирной сети «Интернет», а создание необходимых условий для обеспечения национальной безопасности государства в случаях чрезвычайных ситуаций, наличия угрозы извне либо прекращения предоставления доступа со стороны внешних источников и иных негативных факторов.

Притом, несмотря на наделение федеральных органов исполнительной власти широкими полномочиями в сфере контроля за деятельностью операторов связи, данная деятельность никоим образом не касается граждан, а также их конституционных прав на тайну переписки и иных сообщений.

Как уже отмечалось ранее, в приоритете находится именно реализация прав и свобод граждан, которые могут быть ограничены только в установленном законом порядке и только в той мере, которая необходима для защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства [1, ст. 2, 18, 55]. Более того, опыт такого нормативного регулирования в области ограничения личных прав граждан уже давно существует в нашем государстве и урегулирован уголовным и административным законодательством.

Обществу ещё только предстоит выработать порядок и нормы безопасного информационного взаимодействия, безопасного, как для индивида, так и для общества в целом. Российское общество особенно уязвимо в связи с его переходным состоянием, сменой социально-политического и экономического устройства, с глубоким разрывом в уровне социально-экономического развития регионов и различных социальных групп [15, с. 2].

Исходя из вышеизложенного, можно сделать вывод о том, что законодательные инициативы, в первую очередь, должны преследовать цель обеспечения суверенитета государства, а также прав и свобод собственных граждан, создавая условия для устойчивого функционирования достаточно важного аспекта нашей современной жизни как информационная безопасность, учитывая его тесную связь с отраслью национальной безопасности страны.

Список источников

1. Конституция Российской Федерации: принята всенародным голосованием 12 дек. 1993 г., в ред. от 1 июля 2020 г. Доступ из справ.-правовой системы «КонсультантПлюс».
2. Об информации, информационных технологиях и о защите информации: федер. закон от 27 июля 2006 г. № 149-ФЗ: в ред. от 1 октяб. 2021 г. Доступ из справ.-правовой системы «КонсультантПлюс».
3. О государственной тайне: федер. закон от 21 июля 1993 № 5485-1: в ред. от 11 июня 2021 г. Доступ из справ.-правовой системы «КонсультантПлюс».
4. О коммерческой тайне: федер. закон от 29 июня 2004 г. № 98-ФЗ: в ред. от 9 марта 2021 г. Доступ из справ.-правовой системы «КонсультантПлюс».
5. О персональных данных: федер. закон от 27 июля 2006 г. № 152-ФЗ: в ред. от 2 июля 2021 г. Доступ из справ.-правовой системы «КонсультантПлюс».
6. О связи: федер. закон от 07 июля 2003 г. № 126-ФЗ: в ред. от 30 дек. 2021 г. Доступ из справ.-правовой системы «КонсультантПлюс».
7. О безопасности: федер. закон от 28 дек. 2010 г.: в ред. от 09 нояб. 2020 г. Доступ из справ.-правовой системы «КонсультантПлюс».
8. Об утверждении Положения о российском государственном сегменте информационно-телекоммуникационной сети «Интернет»: приказ Федеральной службы охраны РФ от 7 сент. 2016 г. № 443. Доступ из справ.-правовой системы «КонсультантПлюс».
9. *Пешкова (Белогорцева) Х. В.* Правовые основы информационной безопасности // Воронежский институт ФСИН России: Практикум. Воронеж, 2021. С. 74–76.
10. *Дубень А. К.* Информационная безопасность как составная часть национальной безопасности Российской Федерации // *The Scientific Heritage*. 2021. № 74-4(74). С. 41–45.
11. *Попов Р.С., Криволапов И.П., Чечевицын И.Д., Щербаков С.Ю.* Нормативно-правовая основа обеспечения информационной безопасности // *Наука и Образование*. 2021. Т. 4, № 2. С. 3–4.
12. *Федоричев Е. А.* Правовые основы обеспечения информационной безопасности российского государства // *Передовые технологии современного гуманитарного знания: перспективы развития и модернизации: материалы всероссийской научно-практической конференции*, 2021. С. 65–70.
13. *Буянов Д.С.* Информационная безопасность в социальных сетях // *Молодой ученый*. 2020. № 47. С. 14–15.
14. *Николаев И.А.* Правовое обеспечение информационной безопасности РФ // *Молодой ученый*. 2019. № 39. С. 344–346.
15. *Гаврилова Н.С., Есмуржаева Ж.Б.* К вопросу о проблемах информационной безопасности в РФ // *Актуальные проблемы информационной безопасности: материалы международной научной конференции*. 2020. С. 34–36.
16. *Жуйков А.А.* Современные проблемы информационной безопасности // *Вестник Краснодарского университета МВД России*. 2020. С. 111–114.
17. Исследование российского рынка информационной безопасности: аналитическое исследование за октябрь 2021 г. // «Код безопасности». Российский разработчик программных и аппаратных средств защиты информации. 2021. С. 10–11.

References

1. Konstitutsiya Rossiiskoi Federatsii: prinyata vsenarodnym golosovaniem 12 dek. 1993 g., v red. ot 1 iyulya 2020 g. [The Constitution of the Russian Federation: adopted by popular vote on 12 Dec. 1993, ed. from July 1, 2020]. Access from help-legal system "ConsultantPlus". (In Russ.).
2. Ob informacii, informacionnyh tehnologijah i o zashhite informacii [About information, information technologies and information protection]: RF Federal Law No. 149-FZ of July 27, 2006: as amended from October 1, 2021. Access from help-legal system "ConsultantPlus". (In Russ.).
3. O gosudarstvennoj tajne [On state secrets]: RF Federal Law No. 5485-1 of July 21, 1993: as amended dated June 11, 2021. Access from help-legal system "ConsultantPlus". (In Russ.).
4. O kommercheskoj tajne [About trade secrets]: RF Federal Law No. 98-FZ of June 29, 2004: as amended from March 9, 2021. Access from help-legal system "ConsultantPlus". (In Russ.).
5. O personal'nyh dannyh [About personal data]: RF Federal Law No. 152-FZ of July 27, 2006: as amended dated July 2, 2021. Access from help-legal system "ConsultantPlus". (In Russ.).
6. O svyazi [About communication]: RF Federal Law No. 126-FZ of July 07, 2003: as amended from December 30, 2021. Access from help-legal system "ConsultantPlus". (In Russ.).
7. O bezopasnosti [About security]: RF Federal Law of December 28, 2010: as amended from November 09, 2020. Access from help-legal system "ConsultantPlus". (In Russ.).
8. Ob utverzhenii Polozhenija o rossijskom gosudarstvennom segmente informacionno-telekommunikacionnoj seti «Internet» [On approval of the Regulations on the Russian State Segment of the Internet Information and Telecommunications network]: Order of the Federal Security Service of the Russian Federation No. 443 dated September 7, 2016. Dostup iz sprav.-pravovoj sistemy "Konsul'tantPljus". (In Russ.).

9. Peshkova (Belogorceva) H. V. Pravovye osnovy informacionnoj bezopasnosti [Legal basis for information security], *Voronezhskij institut FSIN Rossii: Praktikum [Voronezh Institute of the Federal Penitentiary Service of Russia: Workshop]*, Voronezh, 2021, pp. 74–76. (In Russ.).
10. Duben' A. K. Informacionnaja bezopasnost' kak sostavnaja chast' nacional'noj bezopasnosti Rossijskoj Federacii [Information security as an integral part of the national security of the Russian Federation], *The Scientific Heritage*, 2021, no. 74-4 (74), pp. 41–45. (In Russ.).
11. Popov R.S., Krivolapov I.P., Chechevicyn I.D., Shherbakov S.Ju. Normativno-pravovaja osnova obespechenija informacionnoj bezopasnosti [Regulatory framework for ensuring information security], *Nauka i Obrazovanie [Science and education]*, 2021, vol. 4, no. 2, pp. 3–4. (In Russ.).
12. Fedorichev E. A. Pravovye osnovy obespechenija informacionnoj bezopasnosti rossijskogo gosudarstva [Legal basis for ensuring information security of the Russian state], *Peredovye tehnologii sovremennogo gumanitarnogo znanija: perspektivy razvitiya i modernizacii: Materialy vserossijskoj nauchno-prakticheskoj konferencii [Advanced technologies of modern humanitarian knowledge: prospects for development and modernization: Proceedings of the All-Russian scientific and practical conference]*, 2021, pp. 65–70. (In Russ.).
13. Bujanov D.S. Informacionnaja bezopasnost' v social'nyh setjah [Information security in social networks], *Molodoj uchenyj [Young scientist]*, 2020, no. 47, pp. 14–15. (In Russ.).
14. Nikolaev I.A. Pravovoe obespechenie informacionnoj bezopasnosti RF [Legal support of information security of the Russian Federation], *Molodoj uchenyj [Young scientist]*, 2019, no. 39, pp. 344–346. (In Russ.).
15. Gavrilova N.S., Esmurzhaeva Zh.B. K voprosu o problemah informacionnoj bezopasnosti v RF [On the issue of information security problems in the Russian Federation], *Aktual'nye problemy informacionnoj bezopasnosti: Materialy mezhdunarodnoj nauchnoj konferencii [Actual problems of information security: Proceedings of the international scientific conference]*, 2020, pp. 34–36. (In Russ.).
16. Zhujkov A.A. Sovremennye problemy informacionnoj bezopasnosti [Modern problems of information security], *Vestnik Krasnodarskogo universiteta MVD Rossii [Bulletin of the Krasnodar University of the Ministry of Internal Affairs of Russia]*, 2020, pp. 111–114. (In Russ.).
17. Issledovanie rossijskogo rynka informacionnoj bezopasnosti: analiticheskoe issledovanie za oktjabr' 2021 g. [A study of the Russian information security market: an analytical study for October 2021], «Kod bezopasnosti». Rossijskij razrabotchik programmyh i apparatnyh sredstv zashhity in-formacii [Security Code. Russian developer of software and hardware information security], 2021, pp. 10–11. (In Russ.).

ИНФОРМАЦИЯ ОБ АВТОРАХ

Алиева Зульфия Ибрагимовна, доцент кафедры конституционного и муниципального права юридического института Дагестанского государственного университета, кандидат юридических наук, г. Махачкала, Российская Федерация. E-mail: mumina@mail.ru

Хасбулатова Зарема Магомедалимовна, магистрант кафедры конституционного и международного права юридического института Дагестанского государственного университета, г. Махачкала, Российская Федерация. E-mail: hasbulatovazm@mail.ru

Поступила в редакцию 15.04.2022 г.; одобрена после рецензирования 03.09.2022 г.; принята к публикации 10.09.2022 г.

INFORMATION ABOUT THE AUTHORS

Aliyeva Zulfya Ibragimovna, Associate Professor of the Department of Constitutional and Municipal Law of the Law Institute of Dagestan State University, Candidate of Law, Makhachkala, Russian Federation. E-mail: mumina@mail.ru

Khasbulatova Zarema Magomedkamilovna, Master's student of the Department of Constitutional and International Law of the Law Institute of Dagestan State University, Makhachkala, Russian Federation. E-mail: hasbulatovazm@mail.ru

Received 15.04.2022; approved after reviewing 03.09.2022; accepted for publication 10.09.2022.

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.