

УДК 323

DOI: 10.34670/AR.2020.96.84.016

## **Проблемы защищенности персональных данных в информационной политике Российской Федерации**

**Увижева Алена Владимировна**

Аспирант,

Северо-Осетинский государственный университет им. К.Л. Хетагурова,  
362025, Российская Федерация, Владикавказ, ул. Ватутина, 44-46;  
e-mail: maritab19@yandex.ru

**Койбаев Борис Георгиевич**

Доктор политических наук, кандидат исторических наук, профессор,  
завкафедрой всеобщей истории и исторической политологии,  
Северо-Осетинский государственный университет им. К.Л. Хетагурова,  
362025, Российская Федерация, Владикавказ, ул. Ватутина, 44-46;  
e-mail: koibaevbg@mail.ru

**Пех Артур Александрович**

Старший преподаватель кафедры землеустройства и экологии,  
Горский государственный аграрный университет,  
362040, Российская Федерация, Владикавказ, ул. Кирова, 37;  
e-mail: artur.gejmer@mail.ru

### **Аннотация**

В статье рассмотрены вопросы защищенности персональных данных пользователей в Российской Федерации и странах мира. Раскрыт современный охват проблемы несанкционированного доступа к цифровым банкам и базам данных на уровне государств и в трансграничном пространстве. Выработаны способы обеспечения безопасности пользовательских данных на основе сопоставления правовых национальных и международных регламентов, отдельных соглашений между странами-партнерами, внутренних законодательных актов России. На основе комплексного анализа выявлено, что глобальное информационное пространство не защищено едиными правовыми регламентами и, как следствие, уязвимо к неправомерным действиям со стороны отдельных государств, компаний, осуществляющих бесконтрольный сбор сведений о пользователях, хакерских ячеек. В то же время в российском законодательстве предпринят ряд мер по обеспечению безопасности в цифровом пространстве при заключении двухсторонних конвенций о сотрудничестве между государствами-партнерами. Установлено, что защищенности информационного пространства и пользовательской информации при ее сборе, обработке и хранении можно добиться путем применения комплекса разнонаправленных и разноуровневых мер, приведенных в исследовании. Государственная политика Российской Федерации и иных стран мира, заинтересованных в обеспечении кибербезопасности персональных данных, должна быть нацелена на

достижение максимального эффекта непреступности информационного пространства, что возможно исключительно путем взаимодействия правительств, держателей персональной информации в правовом и цифровом полях.

#### **Для цитирования в научных исследованиях**

Увижева А.В., Койбаев Б.Г., Пех А.А. Проблемы защищенности персональных данных в информационной политике Российской Федерации // Теории и проблемы политических исследований. 2020. Том 9. № 5А. С. 146-154. DOI: 10.34670/AR.2020.96.84.016

#### **Ключевые слова**

Персональные данные, Россия, информационная политика, информационная среда, информационная безопасность, киберпреступность, кибербезопасность.

## **Введение**

В настоящее время общество нашей страны и многих иных государств мира переживает период информатизации и цифровизации, в рамках которого осуществляется развитие нового направления политики государства – информационной политики. Современные информационно-коммуникационные технологии воздействуют и на ряд аспектов политической жизни. Информация, на основе новых технологий, стала проходить через границы существенно быстрее. Доступ к ней качественно изменили глобальные и региональные структуры [Койбаев, 2012, 50].

Востребованность информационных технологий породила переход общественных отношений на цифровой уровень. Государственные механизмы, регулировавшие сбор и систематизацию персональных данных о пользователях, претерпели значительную трансформацию – перешли от бумажных носителей к информационным [Мохов, Преснякова, 2020, 76].

Процессы информатизации с каждым годом охватывают все больше сфер жизни общества, что приводит к совершенствованию стратегического планирования различных видов деятельности, связанной с социальным, экономическим, производственным и иными элементами эффективного и безопасного существования государства, формирования его позитивного образа [Койбаев, 2013, 45].

По мнению многих зарубежных исследователей, процессы глобализации напрямую сказываются на сущности информатизации и скорости цифровизации отдельных сфер жизни и деятельности государства и народов. Первыми претерпевают изменения правовые устои стран: законы и подзаконные акты изменяются и переписываются в «ногу со временем» [Мохов, Преснякова, 2020, 77].

Несмотря на попытки государств обеспечить безопасность и комфортное функционирование информационных систем на национальном и глобальном уровнях, при взаимодействии между странами-партнерами возникает множество проблем: обеспечения информационной безопасности в коммуникационных сетях, принятия эффективных регламентов межнационального уровня; обеспечения прав и свобод пользователей в накоплении, хранении и распространении информации любыми доступными ими способами. Среди перечисленных проблем одной из главных является проблема обеспечения информационной безопасности в компьютерных и коммуникационных системах.

Природа проблемы информационной безопасности в цифровых сетях заключается в том,

что компьютерные и коммуникационные системы имеют широкое применение и повсеместное распространение. Персональные данные пользователей хранятся в электронно-вычислительных машинах и компьютерных системах в офисах крупных и малых компаний, государственных и частных фирм, в домах населения. Повсеместное распространение компьютерных технологий делает уязвимой информацию пользователей к хакерским атакам, связанным с хищением десятков гигабайт личной информации [Горбенко, 2016, 16].

### **Основная часть**

Информационной основой для хранения и систематизации персональных данных о пользователях служит современная геоинформационная среда, формируемая на национальном и глобальном уровнях. Безопасность информации проявляется и в степени ее защищенности от раскрытия, определения факта передачи и изменения, уничтожения или искажения, и в отсутствии в программных средствах, обеспечивающих такую безопасность, уязвимостей (вирусов, троянских коней, закладок, а также иных вредоносных программ, встраиваемых с целью хищения, уничтожения или искажения пользовательской информации).

Не будет ошибочным утверждать, что информационная составляющая является неотделимой частью «информационной» жизни современного, прогрессивного общества. В эру глобализации, набирающей все большие темпы, противостояние стран в информационном пространстве вышло на новый уровень, отбросив на задний план военное и экономическое противоборство. Информационное поле на сегодняшний день позволяет эффективно влиять на мировые события, внедрять культурные и духовные ценности в том или ином регионе, формировать положительное или отрицательное отношение к стране или группам стран, отдельным народностям, событиям, личностям [Басманов, 2018, 35]. В связи с этим доступ к пользовательской информации (персональным данным) людей становится объектом информационных атак, киберпреступлений, краж, происходят «сливания» сведений о миллионах пользователей в сети общего доступа.

Одним из государств, осуществляющих проведение активной работы по обеспечению безопасности в цифровом пространстве, является Российская Федерация. Меры, предпринимаемые нашей страной в сфере защиты информационного пространства от кибератак извне, строятся на нормативно-правовой основе – государственных и международных правовых актах, регламентирующих «поведение» при возникновении информационных конфликтов и войн, противостоянии агрессии в цифровом поле.

Периодическое внесение изменений в нормативную и правовую базы в части информационной безопасности персональных данных является следствием стремительно меняющихся реалий времени. Новая сфера деятельности для Российской Федерации основана на построении адекватных технологий. Принятие Постановления Правительства РФ от 01 ноября 2012 г. № 1119 (далее – Постановление № 1119) привело к тому, что проблема защиты персональных данных существенно актуализировалась.

Многие требования утратившего силу Постановления № 781, на смену которому пришло Постановление № 1119, были упрощены и исключены из правового поля, что сделало пользовательскую (персональную) информацию в некоторой степени уязвимой ввиду ликвидации мероприятий, направленных на предотвращение несанкционированного доступа к таким данным, передачи их лицам, не имеющим права доступа к ней, и некоторые другие [Астахова, Рублев, 2013, 32].

В глобальном же пространстве иначе воспринимается понятие «государственный суверенитет», поскольку многие государства Запада позиционируют себя как социально

ответственные перед гражданами, проживающими на территории Европейского союза. Повсеместно вводимая ими система электронного учета личных данных пользователей отвечает требованиям не только безопасности, но и их неприкосновенности, охраны достоинства человека. Предотвращение преступного доступа к пользовательской информации стоит во главе принципов осуществления информационной безопасности западных государств. Российская Федерация уже в 2020 г. стоит на пороге принятия решений, аналогичных западным, и не намерена пускать «на самотек» проблему разработки рациональных способов надзора за защитой прав человека в своих федеральных границах [Голуб, Кудлай, 2015, 80].

Проблема уязвимостей в сфере прав и свобод человека и несостоятельности многих государств мира в качестве гаранта безопасности персональных данных граждан по-прежнему сводится к нормативно-правовой плоскости.

Проблема сохранения пользовательской информации имеет глобальный масштаб. Только в одной Южной Корее была обнаружена самая большая утечка личных данных в истории страны: персональные данные о более 3,3 млн пользователей, украденные злоумышленниками, попали в сеть. В 2014 г. произошла громкая кража персональных данных нескольких тысяч пользователей банка Barclays, данных десятков тысяч пользователей социальных сетей «Facebook» и «Twitter». В Российской Федерации самая крупная утечка персональных данных была зафиксирована в октябре 2019 г., когда персональные данные более 60 млн пользователей кредитных карт попала на черный рынок.

Западные страны в содружестве ЕС еще в 2013 г. приняли Директиву о повторном использовании государственной информации (2013/34/EU), согласно которой третьи лица, граждане ЕС, могли использовать любую государственную информацию, за исключением составляющей персональную, коммерческую или государственную тайну. Задумка европейских законодателей претворяет в жизнь открытость (публичность) данных государственных организаций – предоставление их как в заявительном порядке бесплатно, так и за установленную плату (аналог госпошлины в России). Открытость данных, согласно задумке законодателей ЕС, позволит избежать утечки данных о пользователях, поскольку в краже информации, находящейся в открытом доступе или в доступе за определенную плату, не будет необходимости.

В Российской Федерации способы сбора, систематизации и предоставления персональной информации были закреплены в Федеральном законе от 27 июля 2006 г. № 152-ФЗ. Однако спустя три года, 16 декабря 2009 г., из данного закона были исключены положения о защите персональных данных.

Искоренение некоторых положений настоящего закона о защите персональных данных, содержание которых обязывало компании и фирмы использовать специальные средства, функционирующие на криптографических и шифровальных системах при сборе и хранении персональных данных пользователей, должно снизить уровень криминальных манипуляций с таковыми. По мнению законодателей нашей страны, данные правовые меры будут эффективным способом воздействия на проблему информационной безопасности.

В 2018 г. в Государственную Думу был внесен законопроект № 5711247 «О внесении изменений в Федеральный закон “Об информации, информационных технологиях и защите информации”». Данный законопроект предусматривал запреты для операторов обработки больших пользовательских данных для целей использования третьими лицами. Запреты также касались обработки данных для идентификации конкретного частного лица, за исключением случаев запроса розыскных органов [Жарова, Елин, 2018; Камалова, 2019, 48]. Таким образом, законопроект № 5711247 внес изменения в федеральное законодательство о защите информации и ограничил возможность получения третьими лицами персональных данных

физических лиц, что, на наш взгляд, предопределяет возможность появления цензуры, ограничения права свободно собирать и распространять информацию. Данный законопроект, несмотря на наши опасения и опасения многих исследователей данной проблемы, затрагивает деятельность исключительно крупных операторов, накапливающих и предоставляющих персональные данные о пользователях-гражданах.

Анализируя политику стран Запада и сравнивая ее с политикой Российской Федерации, регламентирующей процессы использования и защиты персональных данных, можно провести ряд аналогий:

- 8) и Европейский Союз, и Российская Федерация стремятся обезопасить информационное пространство вокруг своей территории и за ее пределами в рамках своей компетенции;
- 9) и Европейский Союз, и Российская Федерация стараются привести в регламенты и Правила осуществления информационной безопасности при ООН, исходя из своих глобальных и национальных интересов и преследуя одинаковые цели;
- 10) страны Запада и Российская Федерация одинаково заинтересованы в сохранении конфиденциальности персональных данных, однако в отличных друг от друга правовых плоскостях.

Следует отметить, что инициатива в области создания единой правовой базы в части регламентирования использования пользовательской информации с 1998 г. исходила от Российской Федерации, тогда как многие страны-партнеры пришли к тем же положениям, о чем утверждали российские дипломаты в рамках ООН, спустя десятилетие.

Немаловажно в раскрытии вопросов информационной безопасности и то, что Российская Федерация за четыре года до стран Запада приняла ослабляющие меры в части защиты персональной информации пользователей и предоставления таковой по запросу (в заявительном порядке) бесплатно или в рамках оплаты государственной пошлины, что повсеместно активно используется при взаимодействии заявителей и органов государственной власти во всех сферах жизни и деятельности народов России.

В области обеспечения информационной безопасности персональных данных Российская Федерация выступает в качестве законодателя и партнера, заинтересованного в создании цифрового пространства. В рамках такого партнерства возможно эффективное взаимодействие между развивающимися и развитыми государствами. Заключаются соглашения между правительствами таких стран, как США, Куба, Беларусь, Индия, Китай и др. Соглашения основаны на доктринах ООН от 1948 г., резолюциях от 2014 г. и инициативах в рамках ШОС и ЕАЭС от 2013 г.

Все соглашения, заключаемые Российской Федерацией со странами-партнерами, строятся на учете резолюции Генеральной Ассамблеи ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» и содержат такие направления сотрудничества, как создание систем мониторинга потенциальных угроз в области информационной безопасности, выработка совместных мер по развитию норм международного права в данной области, противодействие информационной преступности и др. (См., например, Соглашение между Правительством Российской Федерации и Правительством Республики Беларусь о сотрудничестве в области обеспечения международной информационной безопасности.)

Сотрудничество в сфере информационной безопасности строится на равных правах каждой из сторон на защиту информационных ресурсов своего государства от несанкционированного вмешательства и неправомерного использования, информационных атак на них.

На наш взгляд, среди наиболее перспективных путей развития защищенности персональных данных и обеспечения информационной безопасности на национальном и глобальном уровнях

можно выделить два направления:

- 1) тесное взаимодействие стран на глобальной арене в решении проблем информационной безопасности и защиты персональных данных на основе создания единой правовой основы, способной регламентировать порядок сбора, систематизации, хранения пользовательских данных;
- 2) приверженность государств нормам и правам в области защиты персональных данных и информационной безопасности на национальном уровне, уважительное отношение к свободе слова, свободе сбора информации любыми доступными гражданам и сообществам способами, международным регламентам, принятым и утвержденным в рамках Генеральной Ассамблеи ООН.

Защита информации в цифровом пространстве может строиться исключительно на базе законодательного закрепления требований о недопустимости произвольной обработки пользовательской информации при функционировании системы искусственного интеллекта и защите программных обеспечений, осуществляющих автоматический сбор и обработку личной информации пользователей, от несанкционированного доступа.

Проанализировав зарубежные и отечественные источники, среди которых можно выделить труды В.В. Архипова, А.К. Жаровой, Г.Г. Камаловой, В.Б. Наумова и других исследователей данной проблемы, можно сформировать упорядоченную систему, способную «закрыть» уязвимости персональных данных в нормативной и цифровой среде. Обобщенно методы ликвидации проблемы защищенности информации пользователей можно представить следующим образом:

- при разработке единого правового документа для регулирования оборота и использования информации на глобальном уровне необходимо учитывать интересы всех государств, заинтересованных в обеспечении безопасности в цифровом пространстве;
- при разработке программных средств и автоматизированных комплексов по сбору, систематизации и хранении данных необходимо опираться на единые правовые основы и внутренние регламенты государств в области обеспечения безопасности информационного пространства;
- государства, политический строй или религиозные убеждения которых не позволяют в полной степени осуществить слияние национальных нормативных и правовых регламентов с единым правовым документом (или построение на основе единого правового документа), необходимо исключить из общего поля взаимодействия стран-партнеров как субъекты, не способные гарантировать безопасность пользовательских данных на своей территории и в своем цифровом пространстве.

Существует множество рычагов воздействия на информационную уязвимость цифрового пространства и пользовательских данных. Говорить о них можно бесконечно долго, однако без должного сотрудничества стран, без разработки комплексного и единого документа, способного регулировать оборот и защищенность потока информации в сфере информационных технологий, невозможно ни правовое, ни технологическое совершенствование современных цифровых отношений между государствами.

## **Заключение**

Защищенности информационного пространства и пользовательской информации при ее сборе, обработке и хранении можно достичь путем применения комплекса разнонаправленных и разноуровневых мер, приведенных в исследовании. Государственная политика Российской Федерации и иных стран мира, заинтересованных в обеспечении кибербезопасности

персональных данных, должна быть нацелена на достижение максимального эффекта защищенности информационного пространства, что возможно исключительно путем взаимодействия правительств, держателей персональной информации в правовом и цифровом полях.

### Библиография

1. Астахова Л.В., Рублев Е.Л. Проблемы защиты персональных данных в период смены нормативной базы и пути их решения // Вестник УрФО. Безопасность в информационной сфере. 2013. № 1. С. 32-41.
2. Басманов А.Е. Правовое обеспечение информационной безопасности Российской Федерации // Актуальные проблемы истории, политики и права. Пенза, 2018. С. 35-38.
3. Голуб Н.Н., Кудлай А.А. Информационная безопасность и социальная ответственность российского государства // Вестник Международного юридического института. 2015. № 2. С. 79-88.
4. Горбенко А.О. Основы информационной безопасности (введение в профессию). СПб.: Интермедия, 2016. 336 с.
5. Жарова А.К., Елин В.М. Обеспечение безопасности персональных данных в эпоху больших данных // Динамика институтов информационной безопасности: правовые проблемы. М., 2018. С. 174-181.
6. Камалова Г.Г. Проблемы и приоритетные направления организационно-правового обеспечения конфиденциальности информации при использовании цифровых технологий // Вестник Университета им. О.Е. Кутафина (МГЮА). 2019. № 12. С. 45-52.
7. Койбаев Б.Г. Политический имидж государства в современном глобальном информационном пространстве // Вестник Северо-Осетинского государственного университета им. К.Л. Хетагурова. 2013. № 1. С. 45-48.
8. Койбаев Б.Г. Формирование новой системы международных отношений в условиях становления глобального информационного общества // Вестник Северо-Осетинского государственного университета им. К.Л. Хетагурова. 2012. № 1. С. 50-54.
9. Мохов А.Ю., Преснякова А.А. Информационная безопасность и информационный суверенитет Российской Федерации: правовые основы // Право и государство: теория и практика. 2020. № 4. С. 76-78.
10. О персональных данных: федер. закон Рос. Федерации от 27.07.2006 № 152-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 08.07.2006: одобр. Советом Федерации Федер. Собр. Рос. Федерации 14.07.2006. URL: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_61801/](http://www.consultant.ru/document/cons_doc_LAW_61801/)
11. Об утверждении требований к защите персональных данных при их обработке в информационной системе персональных данных: постановление Правительства РФ от 01.11.2012 № 1119. URL: <http://www.rg.ru/2012/11/07/pers-dannye-dok.html>
12. Соглашение между Правительством Российской Федерации и Правительством Республики Беларусь о сотрудничестве в области обеспечения международной информационной безопасности. URL: <http://docs.cntd.ru/document/499074140>

### The problems of personal data protection in the information policy of the Russian Federation

**Alena V. Uvizheva**

Postgraduate,  
Khetagurov North Ossetian State University,  
362025, 44-46 Vatutina st., Vladikavkaz, Russian Federation;  
e-mail: [maritab19@yandex.ru](mailto:maritab19@yandex.ru)

**Boris G. Koibaev**

Doctor of Political Science, PhD in History, Professor,  
Head of the Department of universal history and historical political science,  
Khetagurov North Ossetian State University,  
362025, 44-46 Vatutina st., Vladikavkaz, Russian Federation;  
e-mail: koibaevbg@mail.ru

**Artur A. Pekh**

Senior Lecturer at the Department of land management and ecology,  
Gorsky State Agrarian University,  
362040, 37 Kirova st., Vladikavkaz, Russian Federation;  
e-mail: artur.gejmer@mail.ru

**Abstract**

The article aims to study the protection of users' personal data in the Russian Federation and other countries of the world. It deals with the modern coverage of the problem of unauthorised access to digital banks and databases at the state level and in the cross-border space and identifies the methods that have been developed to ensure the security of users' data on the basis of the comparison of national and international legal regulations, agreements between countries, and Russia's national legislative acts. The comprehensive analysis reveals that the global information space is not protected by uniform legal regulations, as a result, it is vulnerable to illegal actions carried out by states, companies that uncontrollably collect information about users, hackers. At the same time, Russia takes a number of measures to ensure security in the digital space when concluding bilateral conventions on cooperation between the participating states. The protection of information during its collection, processing and storage can be ensured by taking a complex of multidirectional and multi-level measures described in the study. The state policy of the Russian Federation and other countries of the world that are interested in cybersecurity, should be aimed at achieving the maximum effect of the inaccessibility of the information space.

**For citation**

Uvizheva A.V., Koibaev B.G., Pekh A.A. (2020) Problemy zashchishchennosti personal'nykh dannykh v informatsionnoi politike Rossiiskoi Federatsii [The problems of personal data protection in the information policy of the Russian Federation]. *Teorii i problemy politicheskikh issledovaniy* [Theories and Problems of Political Studies], 9 (5A), pp. 146-154. DOI: 10.34670/AR.2020.96.84.016

**Keywords**

Personal data, Russia, information policy, information environment, information security, cybercrime, cybersecurity.

**References**

1. Astakhova L.V., Rublev E.L. (2013) Problemy zashchity personal'nykh dannykh v period smeny normativnoi bazy i puti ikh resheniya [The problems of personal data protection during the change in the regulatory framework and the ways to

- solve them]. *Vestnik UrFO. Bezopasnost' v informatsionnoi sfere* [Journal of the Ural Federal District. Information security], 1, pp. 32-41.
2. Basmanov A.E. (2018) Pravovoe obespechenie informatsionnoi bezopasnosti Rossiiskoi Federatsii [Legal support for the information security of the Russian Federation]. In: *Aktual'nye problemy istorii, politiki i prava* [Topical problems of history, politics and law]. Penza, pp. 35-38.
  3. Golub N.N., Kudlai A.A. (2015) Informatsionnaya bezopasnost' i sotsial'naya otvetstvennost' rossiiskogo gosudarstva [The information security and social responsibility of the Russian state]. *Vestnik Mezhdunarodnogo yuridicheskogo instituta* [Bulletin of the International Law Institute], 2, pp. 79-88.
  4. Gorbenko A.O. (2016) *Osnovy informatsionnoi bezopasnosti (vvedenie v professiyu)* [The fundamentals of information security (an introduction to the profession)]. St. Petersburg: Intermediya Publ.
  5. Kamalova G.G. (2019) Problemy i prioritetye napravleniya organizatsionno-pravovogo obespecheniya konfidentsial'nosti informatsii pri ispol'zovanii tsifrovyykh tekhnologii [The problems of and the priority directions in the organisational legal ensuring of information confidentiality in the use of digital technologies]. *Vestnik Universiteta im. O.E. Kutafina (MGYuA)* [Bulletin of Kutafin Moscow State Law University], 12, pp. 45-52.
  6. Koibaev B.G. (2012) Formirovanie novoi sistemy mezhdunarodnykh otnoshenii v usloviyakh stanovleniya global'nogo informatsionnogo obshchestva [Building a new system of international relations in the context of the formation of a global information society]. *Vestnik Severo-Osetinskogo gosudarstvennogo universiteta im. K.L. Khetagurova* [Bulletin of the Khetagurov North Ossetian State University], 1, pp. 50-54.
  7. Koibaev B.G. (2013) Politicheskiy imidzh gosudarstva v sovremennom global'nom informatsionnom prostranstve [The political image of a state in the modern global information space]. *Vestnik Severo-Osetinskogo gosudarstvennogo universiteta im. K.L. Khetagurova* [Bulletin of the Khetagurov North Ossetian State University], 1, pp. 45-48.
  8. Mokhov A.Yu., Presnyakova A.A. (2020) Informatsionnaya bezopasnost' i informatsionnyi suverenitet Rossiiskoi Federatsii: pravovye osnovy [The information security and information sovereignty of the Russian Federation: legal foundations]. *Pravo i gosudarstvo: teoriya i praktika* [Law and state: theory and practice], 4, pp. 76-78.
  9. *O personal'nykh dannykh: feder. zakon Ros. Federatsii ot 27.07.2006 № 152-FZ: prinyat Gos. Dumoi Feder. Sobr. Ros. Federatsii 08.07.2006: odobr. Sovetom Federatsii Feder. Sobr. Ros. Federatsii 14.07.2006* [On personal data: Federal Law of the Russian Federation No. 152-FZ of July 27, 2006]. Available at: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_61801/](http://www.consultant.ru/document/cons_doc_LAW_61801/) [Accessed 14/08/20].
  10. *Ob utverzhdenii trebovaniy k zashchite personal'nykh dannykh pri ikh obrabotke v informatsionnoi sisteme personal'nykh dannykh: postanovlenie Pravitel'stva RF ot 01.11.2012 № 1119* [On approving the requirements for the protection of personal data during their processing in the personal data information system: Decree of the Russian Government No. 1119 of November 1, 2012]. Available at: <http://www.rg.ru/2012/11/07/pers-dannye-dok.html> [Accessed 14/08/20].
  11. *Soglasenie mezhdru Pravitel'stvom Rossiiskoi Federatsii i Pravitel'stvom Respubliki Belarus' o sotrudnichestve v oblasti obespecheniya mezhdunarodnoi informatsionnoi bezopasnosti* [The agreement between the Russian Government and the Government of the Republic of Belarus on cooperation in the field of ensuring international information security]. Available at: <http://docs.cntd.ru/document/499074140> [Accessed 14/08/20].
  12. Zharova A.K., Elin V.M. (2018) Obespechenie bezopasnosti personal'nykh dannykh v epokhu bol'shikh dannykh [Ensuring the security of personal data in the era of big data]. In: *Dinamika institutov informatsionnoi bezopasnosti: pravovye problemy* [The dynamics of information security institutions: legal problems]. Moscow, pp. 174-181.