ПУБЛИЧНО-ПРАВОВЫЕ (ГОСУДАРСТВЕННО-ПРАВОВЫЕ) НАУКИ / PUBLIC LAW (STATE LAW) SCIENCES

DOI: https://doi.org/10.60797/IRJ.2025.153.92

ЗАЩИТА ИНФОРМАЦИИ ПРИ ИСПОЛЬЗОВАНИИ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Обзор

Кузнецова И.О.[1], Нестеренко Г.А.[2,]*, Нестеренко И.С.[3]
[1] ORCID : 0009-0003-9085-7701;
[2] ORCID : 0000-0003-1528-4627;
[3] ORCID : 0000-0003-4749-010X;
[1] Омский институт водного транспорта, филиал Сибирского государственного университета водного транспорта, Омск, Российская Федерация
[1] Сибирский институт бизнеса и информационных технологий, Омск, Российская Федерация
[2, 3] Омский государственный технический университет, Омск, Российская Федерация

* Корреспондирующий автор (nga112001[at]list.ru)

Аннотация

Тема работы посвящена вопросам сохранения персональных данных при использовании компьютерных систем и коммуникаций. В статье проведен обзор уязвимостей при использовании информационно-коммуникационных технологий. Представлены характерные причины потери конфиденциальной информации. Рассмотрены основные категории причин несанкционированного доступа к персональным данным. Приведены описания данных категорий.

Описаны основные правовые аспекты использования информационно-коммуникационных технологий в контексте сохранения персональных данных частных лиц и организаций. Проведенными исследованиями установлены причины утечки данных и конфиденциальной информации. Приведены описания и рекомендации по улучшению безопасного использования информационно-коммуникационных технологий.

Ключевые слова: информационно-коммуникационные технологии, защита, персональные данные, безопасность, конфиденциальность.

PROTECTION OF INFORMATION IN THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGY

Review article

Kuznetsova I.O.[1], Nesterenko G.A.[2,]*, Nesterenko I.S.[3]
[1] ORCID : 0009-0003-9085-7701;
[2] ORCID : 0000-0003-1528-4627;
[3] ORCID : 0000-0003-4749-010X;
[1] Omsk Institute of Water Transport, branch of the Siberian State University of Water Transport, Omsk, Russian Federation
[1] Siberian Institute of Business and Information Technologies, Omsk, Russian Federation
[2, 3] Omsk State Technical University, Omsk, Russian Federation

* Corresponding author (nga112001[at]list.ru)

Abstract

The topic of the work is dedicated to the issues of personal data security when using computer systems and communications. The article provides an overview of vulnerabilities in the use of information and communication technology. Characteristic causes of loss of confidential information are presented. The main categories of causes of unauthorised access to personal data are considered. Descriptions of these categories are given.

The main legal aspects of the use of information and communication technology in the context of preserving personal data of individuals and organisations are described. The conducted research establishes the causes of data leakage and confidential information. Descriptions and recommendations for improving the safe use of information and communication technologies are presented.

Keywords: information and communication technology, protection, personal data, security, privacy.

Введение

Одним из основных и принципов прогрессивной экономики на сегодняшний день является внедрение в данную отрасль информационно-коммуникационных технологий (ИКТ) [1], [2].

Опираясь на международный опыт применения ИКТ в экономической сфере, следует отметить опыт различных стран, констатирующий, что максимальным эффектом при функционировании общества является грамотное их внедрение. Следовательно, масштаб использования информационно-коммуникационных технологий способствует экономической сфере страны выдержать возникающую конкурентоспособность вследствие чего завоевать ведущее место на мировом рынке.

В силу того, что информационно-коммуникационные технологии развиваются стремительным образом и проникают во все сферы деятельности человечества, все процессы в экономике трансформируются в цифровые.

Внедрение информационно-коммуникационных технологий и цифровых процессов в различных сферах требует соблюдения мер безопасности [3].

Факторы информационной безопасности

Сегодня, когда под воздействием научно-технического прогресса информационно-коммуникационные технологии стали неотъемлемой частью любой области деятельности человека, возникла необходимость введения нового понятия – «Информационная или цифровая безопасность».

Термин «Информационная безопасность» произошел от взаимодействия двух английских словосочетаний Information Security, а также InfoSec, что в переводе означает – «практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации» [4]. Приведенную формулировку принято считать универсальной независимо от того, в какой именно форме существует информация.

Проблема информационной безопасности зародилась в период создания первых электронно-вычислительных машин.

В 1975г. двумя крупными учеными в области компьютерных информационных систем из Массачусетского технологического института Дж. Зальцера и М. Шрёдера был опубликован материал «Защита информации в компьютерных системах» в данной публикации были приведены рекомендации о разделении всех существующих, на тот момент, нарушений безопасности. Таким образом, были выделены три основные категории, нарушений они представлены на рис. 1.

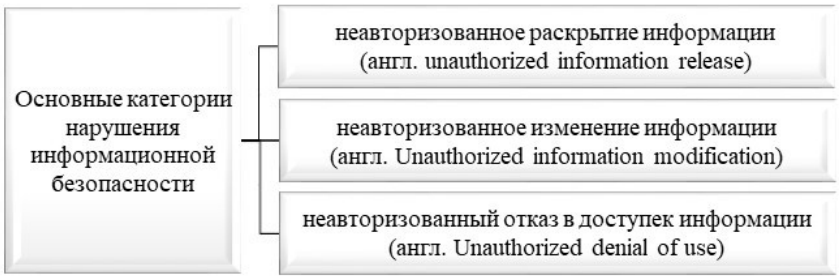

Рисунок 1 - Основные категории нарушения информационной безопасности, сформулированные Дж. Зальцера и М. Шрёдера

DOI: https://doi.org/10.60797/IRJ.2025.153.92.1

В дальнейшем этим категориям были присвоены более конкретные и точные формулировки, кроме того, они были сертифицированы (рис. 2).

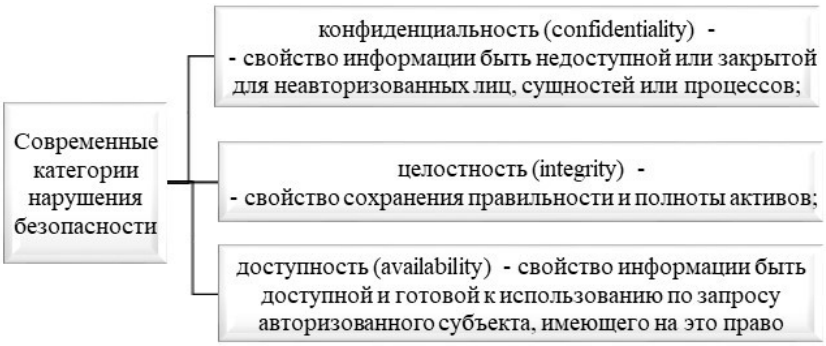

Рисунок 2 - Современные категории нарушения информационной безопасности

DOI: https://doi.org/10.60797/IRJ.2025.153.92.2

Несоблюдение конфиденциальности считается преступлением, которое направлено на разрушение неприкосновенности личной жизни, а это кража персонализации индивидуума.

Первостепенной мерой для обеспечения неприкосновенности персональных данных выступает классификация информации, это обеспечивается дифференциацией её на публичную, четко конфиденциальную, или информацию для внутреннего использования. Самым ярким примером обеспечения конфиденциальности является шифрование [5].

К шифрованию данных следует отнести метод конверсии данных, когда из легко распознаваемого текста, который можно назвать «открытым текстом», происходит трансформация в зашифрованный вид. Такие данные возможно распознать только после их преобразования – дешифровки, применяя для этого специальный ключ, так называемый код, при помощи которого возможно расшифровать существующий текст и трансформировать его в понимаемый и доступный формат.

Владение ключом предоставляется очень ограниченному кругу участников данного процесса, а именно непосредственному отправителю данных и структурному ответственному за получение этих данных сотруднику. Засекреченная путем шифрования информация способствует невозможности доступа к конфиденциальным данным.

Данную категорию информационной безопасности следует считать неотъемлемым элементом структуры информационной безопасности [5].

Следующая категория – это целостность, которая также регламентируется ГОСТом [6].

Не владея достоверными данными, невозможно принимать какие-либо решения или реализовывать необходимые мероприятия с целью защиты информации от изменения посредством случайности или намеренности при хранении, передаче или ее обработке. Более того, целостность информации могут нарушить многие различные действия, такие как изготовление логических бомб, совершение при программировании ошибок, целенаправленная, приносящая вред, модернизация программного кода, замена данных, доступ без авторизации и прочие подобные вредоносные явления [7], [8].

К повреждению целостности могут привести следующие действия: нечаянное уничтожение файлов, ошибочное введение значений, диверсификация настроек, осуществление неточных команд, и эти действия могут совершаться не только самими пользователями, но и системными администраторами [9].

Проводились исследования в различных организациях с целью определения роли личности в проблеме нарушения прав граждан на защиту персональных данных. Оказалось, что чаще всего допускают ошибки операторы, не имеющие высшего образования. Была выявлена закономерность увеличения ошибок по понедельникам, скорее всего это связано со снижением внимания операторов после выходного дня и пятницам в связи с нарастанием усталости к концу трудовой недели.

С целью защиты информации от повреждения и несоблюдения целостности рекомендуется использовать совокупность действий, связанных с контролированием и регулированием возможности вносить изменения не только в саму информацию, но и в системы, занимающиеся ее трансформацией.

К самым распространенным подобным мерам предосторожности относится строгое ограничение доступа определенных лиц наделенных возможностью изменения информации согласно непосредственно должностной инструкции. Необходимо применять цифровые системы, направленные на проверку наличия прав доступа, контролирование порядка идентификации и аутентификации пользователей, и обеспечение информационной безопасности. Параллельно требуется придерживаться принципа разделения полномочий.

Сущностью данного принципа является то, что изменяет данные или саму информационную систему один человек, другой же подтверждает это действие или не подтверждает. Наряду с этим, все вносимые модификации в жизненный цикл в обязательном порядке подлежат согласованию, а также проведению тестирования с целью определения информационной целостности. Кроме того, необходимо следить, чтобы в систему вносилась только корректно сформулированные транзакции.

Программное обеспечение следует обновлять, руководствуясь конкретными мерами безопасности. Каждое действие, вследствие которого происходит изменение, требуется тщательно и последовательно заносить в специальный протокол.

Далее рассмотрим доступность, соблюдение данной категории нарушения информационной безопасности обосновано ГОСТом РИСО/МЭК 27000-2012 [6].

Данный принцип заключается в том, что при необходимости авторизованные лица в обязательном порядке должны получить доступ к информации [10], [11].

Главными отрицательным показателем, воздействующим на информационные системы и препятствующие доступности, считаются DoS-атаки. Или Denial of Service, это английское словосочетание, перевод которого означает «отказ в обслуживании», сущность данной программы это вредоносная атака, которая саботирует доступ.

Но это не единственная угроза категории нарушения информационной безопасности – доступности, параллельно данному явлению следует считать человеческий фактор, а именно – ошибки, которые присущи человеку. Они могут быть не преднамеренные, а случайные вследствие некачественной профессиональной подготовки, из-за рассеянности и невнимательности или физической усталости и плохого самочувствия.

Отсутствие достаточных мер информационной безопасности способствуют ликвидации данных, увеличению риска воздействия вредоносных программ, например, таких как DoS-атак, на целостность информации и способствуют отсутствия возможности доступа к информационным системам рядовым пользователям [12].

В совокупности эти три ключевых принципа информационной безопасности именуются триадой CIA (Confidentiality – «конфиденциальность», Integrity – «целостность», Availability – «доступность»), они представляют собой стандартную общепринятую модель информационной безопасности [13].

Последствия утечки данных

Проведенными исследованиями установлено, что утечка персональных данных не вызывает у нас опасений, мы миримся с происходящим, не задумываясь о том, что в любой момент информация о нас, может оказаться в открытом доступе. Угрозы и риски, которые могут принести утечка сведений о гражданине, представлены на рис. 3. [14].

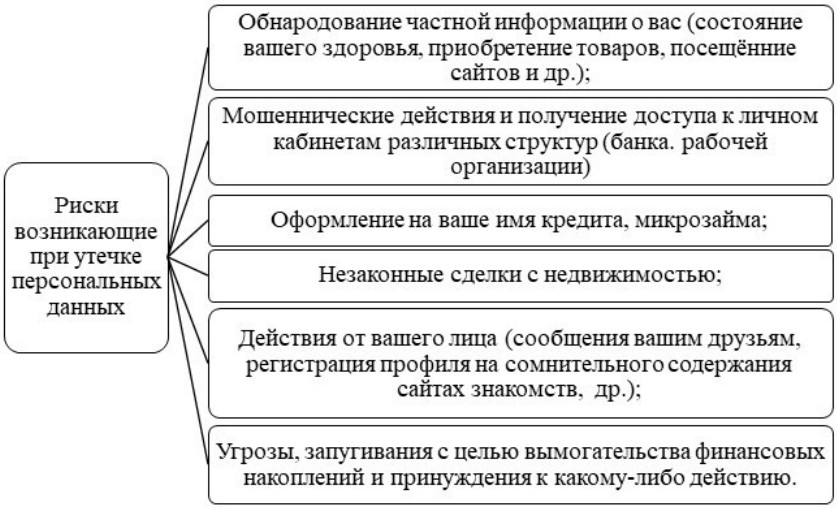

Рисунок 3 - Угрозы и риски, которые могут принести утечка сведений о гражданине
DOI: https://doi.org/10.60797/IRJ.2025.153.92.3

Одним из методов обеспечения безопасности в киберпространстве является использование современных технологий защиты данных и криптографии. Это предполагает использование сильных паролей, двухфакторную аутентификацию, шифрование данных в хранилищах и передачу информации. Организациям и пользователям необходимо принимать регулярные меры по обновлению ПО для устранения уязвимостей и обеспечения безопасности своих систем и данных.

Государство и различные организации, будь это структуры власти или промышленные, и торговые предприятия играют очень важную роль в защите информационной безопасности, и прежде всего в защите персональной информации. Необходимо строгое регулирование обработки данных и хранения. Важно также, чтобы работодатели и социальные службы вкладывали средства в защиту информации и обучение персонала и граждан по информационной безопасности [15].

Заключение

На сегодняшний день обеспечение информационной безопасности является залогом правового существования. Соблюдение мер защиты информации, таких как безукоризненное соблюдение законодательных и нормативно-правовых актов РФ, тщательный подбор персонала связанного с контролем идентификации и аутентификации пользователей, организация обучения данного персонала, разработка руководств действия при возникновении критических ситуаций, связанных с возможным хищением данных или взломом аккаунтов, составление должностных инструкций, использование специальных компьютерных разработок и технологий, при помощи которых возможно скрывать важную персональную информацию, все это позволит эффективно использовать цифровые ресурсы без риска утечки и неправомерного использования данных.

Конфликт интересов

Не указан.

Рецензия

Сообщество рецензентов Международного научно-исследовательского журнала
DOI: https://doi.org/10.60797/IRJ.2025.153.92.4

Conflict of Interest

None declared.

Review

International Research Journal Reviewers Community
DOI: https://doi.org/10.60797/IRJ.2025.153.92.4

Список литературы / References

1. Оразбердиева Я.А. Роль информационно-коммуникационных технологий в экономическом развитии / Я.А. Оразбердиева, Г.Ч. Аманмырадова // Молодой ученый. — 2022. — № 47 (442). — С. 118–120.

2. Нестеренко Г.А. Перспективы внедрения электронного документооборота при использовании корпоративных информационных систем / Г.А. Нестеренко, И.О. Щука, И.С. Нестеренко // Международный научно-исследовательский журнал. — 2022. — № 11 (125). — DOI 10.23670/IRJ.2022.125.15. — EDN: EJGZPY.

3. Корнев Л.В. Обеспечение информационной безопасности в условиях цифровизации / Л.В. Корнев // Молодой ученый. — 2022. — № 12 (407). — С. 7–11.

4. Ищейнов В.Я. Информационная безопасность и защита информации: словарь терминов и понятий: словарь / В.Я. Ищейнов. — Москва: Русайнс, 2024. — 226 с.

5. Карачаев А.Р. Методы защиты и технология шифрования данных / А.Р. Карачаев, З.А. Шогенов, Т.К. Курбанов [и др.] // Образование и право. — 2022. — № 9.

6. ГОСТ Р ИСО/МЭК 27000-2012: Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология / Росстандарт.

7. Пушкарев А.В. Анализ подходов обеспечения целостности информации / А.В. Пушкарев, С.Н. Новиков // Интерэкспо Гео-Сибирь. — 2019. — № 1. — URL: https://cyberleninka.ru/article/n/analiz-podhodov-obespecheniya-tselostnosti-informatsii (дата обращения: 16.10.2024).

8. Щука И.О. Перспективы, достоинства и недостатки электронной подписи / И.О. Щука, И.С. Нестеренко, Г.А. Нестеренко // Международный научно-исследовательский журнал. — 2023. — № 2 (128). — DOI: 10.23670/IRJ.2023.128.7. — EDN: WSRDIN.

9. Пушкарев А.В. Исследование методов обеспечения целостности информации в информационных системах с оптическими каналами связи / А.В. Пушкарев, С.Н. Новиков // Интерэкспо Гео-Сибирь. — 2020. — № 2. — С. 66–71.

10. Назарова К.Е. Анализ угроз доступности информационной системы / К.Е. Назарова, Л.Е. Мартынова, Е.В. Ананьин [и др.] // Молодой ученый. — 2017. — № 1 (135). — С. 74–76.

11. Кузнецова И.О. Особенности сохранения персональных данных при использовании цифрового документооборота / И.О. Кузнецова, И.С. Нестеренко, Г.А. Нестеренко // Международный научно-исследовательский журнал. — 2025. — № 1 (151). — DOI: 10.60797/IRJ.2025.151.51. — EDN: YTZMYA.

12. Богомолова Л.В. Классификация DDOS-атак и их реализация / Л.В. Богомолова // Современные инновации. — 2022. — № 1 (41). — URL: https://cyberleninka.ru/article/n/klassifikatsiya-ddos-atak-i-ih-realizatsiya (дата обращения: 26.01.2025).

13. Дубень А.К. Опыт международного сотрудничества в сфере информационной безопасности: проблемы и перспективы / А.К. Дубень // Международное право и международные организации. — 2023. — № 3. — URL: https://cyberleninka.ru/article/n/opyt-mezhdunarodnogo-sotrudnichestva-v-sfere-informatsionnoy-bezopasnosti-problemy-i-perspektivy (дата обращения: 26.01.2025).

14. Иванова А.П. Утечка персональных данных: большая проблема в цифровую эпоху / А.П. Иванова // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. 4, Государство и право: Реферативный журнал. — 2020. — № 4.

15. «Конвенция о защите физических лиц при автоматизированной обработке персональных данных» (Заключена в г. Страсбурге 28.01.1981; (вместе с Поправками к Конвенции о защите физических лиц при автоматизированной обработке персональных данных (СДСЕ N 108), позволяющими присоединение европейских сообществ, принятыми Комитетом Министров в Страсбурге 15.06.1999)) // Собрание законодательства РФ. — 03.02.2014. — N 5. — ст. 419.

Список литературы на английском языке / References in English

1. Orazberdieva Ya.A. Rol' informacionno-kommunikacionnyh tehnologij v jekonomicheskom razvitii [The role of information and communication technologies in economic development] / Ya.A. Orazberdieva, G.Ch. Amanmyradova // Molodoj uchenyj [Young Scientist]. — 2022. — № 47 (442). — P. 118–120. [in Russian]

2. Nesterenko G.A. Perspektivy vnedrenija jelektronnogo dokumentooborota pri ispol'zovanii korporativnyh informacionnyh sistem [Prospects for the introduction of electronic document management in the use of corporate information systems] / G.A. Nesterenko, I.O. Shchuka, I.S. Nesterenko // Mezhdunarodnyj nauchno-issledovatel'skij zhurnal [International Scientific Research Journal]. — 2022. — № 11(125). — DOI: 10.23670/IRJ.2022.125.15. — EDN: EJGZPY. [in Russain]

3. Kornev L.V. Obespechenie informacionnoj bezopasnosti v uslovijah cifrovizacii [Ensuring information security in the context of digitalization] / L.V. Kornev // Molodoj uchenyj [Young Scientist]. — 2022. — № 12 (407). — P. 7–11. [in Russian]

4. Ishcheinov V.Ya. Informacionnaja bezopasnost' i zashhita informacii: slovar' terminov i ponjatij: slovar' [Information security and information protection: dictionary of terms and concepts] / V.Ya. Ishcheinov. — Moscow: Rusains, 2024. — 226 p. [in Russian]

5. Karachaev A.R. Metody zashhity i tehnologija shifrovanija dannyh [Data protection methods and encryption technology] / A.R. Karachaev, Z.A. Shogenov, T.K. Kurbanov [et al.] // Obrazovanie i pravo [Education and Law]. — 2022. — № 9. [in Russian]

6. GOST R ISO/MJeK 27000-2012: Informacionnaja tehnologija (IT). Metody i sredstva obespechenija bezopasnosti. Sistemy menedzhmenta informacionnoj bezopasnosti. Obshhij obzor i terminologija [GOST R ISO/IEC 27000-2012: Information technology (IT). Methods and means of ensuring security. Information security management systems. General overview and terminology] / Rosstandart. [in Russian]

7. Pushkarev A.V. Analiz podhodov obespechenija celostnosti informacii [Analysis of information integrity approaches] / A.V. Pushkarev, S.N. Novikov // Interjekspo Geo-Sibir' [Interexpo Geo-Siberia]. — 2019. — № 1. — URL: https://cyberleninka.ru/article/n/analiz-podhodov-obespecheniya-tselostnosti-informatsii (accessed: 16.10.2024). [in Russian]

8. Shchuka I.O. Perspektivy, dostoinstva i nedostatki jelektronnoj podpisi [Prospects, advantages and disadvantages of an electronic signature] / I.O. Shchuka, I.S. Nesterenko, G.A. Nesterenko // Mezhdunarodnyj nauchno-issledovatel'skij zhurnal [International Scientific Research Journal]. — 2023. — № 2 (128). — DOI: 10.23670/IRJ.2023.128.7. — EDN: WSRDIN. [in Russian]

9. Pushkarev A.V. Issledovanie metodov obespechenija celostnosti informacii v informacionnyh sistemah s opticheskimi kanalami svjazi [Research of information integrity assurance methods in information systems with optical communication channels] / A.V. Pushkarev, S.N. Novikov // Interjekspo Geo-Sibir' [Interexpo Geo-Siberia]. — 2020. — № 2. — P. 66–71. [in Russian]

10. Nazarova K.E. Analiz ugroz dostupnosti informacionnoj sistemy [Analysis of information system accessibility threats] / K.E. Nazarova, L.E. Martynova, E.V. Ananyin [et al.] // Molodoj uchenyj [Young Scientist]. — 2017. — № 1 (135). — P. 74–76. [in Russian]

11. Kuznetsova I.O. Osobennosti sohranenija personal'nyh dannyh pri ispol'zovanii cifrovogo dokumentooborota [Features of personal data preservation when using digital document management] / I.O. Kuznetsova, I.S. Nesterenko, G.A.

Nesterenko // Mezhdunarodnyj nauchno-issledovatel'skij zhurnal [International Research Journal]. — 2025. — № 1 (151). — DOI: 10.60797/IRJ.2025.151.51. — EDN: YTZMYA. [in Russian]

12. Bogomolova L.V. Klassifikacija DDOS-atak i ih realizacija [Classification of DDOS attacks and their implementation] / L.V. Bogomolova // Sovremennye innovacii [Modern Innovations]. — 2022. — № 1 (41). — URL: https://cyberleninka.ru/article/n/klassifikatsiya-ddos-atak-i-ih-realizatsiya (accessed: 26.01.2025). [in Russian]

13. Duben A.K. Opyt mezhdunarodnogo sotrudnichestva v sfere informacionnoj bezopasnosti: problemy i perspektivy [Experience of international cooperation in the field of information security: problems and prospects] / A.K. Duben' // Mezhdunarodnoe pravo i mezhdunarodnye organizacii [International Law and International Organizations]. — 2023. — № 3. — URL: https://cyberleninka.ru/article/n/opyt-mezhdunarodnogo-sotrudnichestva-v-sfere-informatsionnoy-bezopasnosti-problemy-i-perspektivy (accessed: 26.01.2025). [in Russian]

14. Ivanova A.P. Utechka personal'nyh dannyh: bol'shaja problema v cifrovuju jepohu [Leakage of personal data: a big problem in the digital age] / A.P. Ivanova // Social'nye i gumanitarnye nauki. Otechestvennaja i zarubezhnaja literatura. Ser. 4, Gosudarstvo i pravo: Referativnyj zhurnal [Social Sciences and Humanities. Domestic and foreign literature. Series 4, State and Law: An abstract journal]. — 2020. — № 4. [in Russian]

15. «Konvencija o zashhite fizicheskih lic pri avtomatizirovannoj obrabotke personal'nyh dannyh» ["Convention for the Protection of Natural Persons with Automated Processing of Personal Data"] (Concluded in Strasbourg on 28.01.1981; (together with Amendments to the Convention for the Protection of Natural Persons with Automated Processing of Personal Data (CTS No. 108), allowing the accession of the European Communities, adopted by the Committee of Ministers in Strasbourg on 15.06.1999)) // Sobranie zakonodatel'stva RF [Collection of Legislation of the Russian Federation]. — 02/03/2014. — N 5. — art. 419. [in Russian]