МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ / METHODS AND SYSTEMS OF INFORMATION PROTECTION, INFORMATION SECURITY

DOI: https://doi.org/10.60797/IRJ.2025.151.51

ОСОБЕННОСТИ СОХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИСПОЛЬЗОВАНИИ ЦИФРОВОГО ДОКУМЕНТООБОРОТА

Обзор

Кузнецова И.О.[1], Нестеренко И.С.[2], Нестеренко Г.А.[3,] *

[1] ORCID : 0009-0003-9085-7701;

[2] ORCID : 0000-0003-4749-010X;

[3] ORCID : 0000-0003-1528-4627;

[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

В работе описывается проблема сохранения персональных данных при использовании цифрового документооборота. Приводится определение персональных данных и документов, в которых эти данные могут быть отражены.

Проведен анализ опасностей, возникающих при использовании электронных документов, которые передаются по системам связи. В работе показано, как могут происходить утечки персональных данных клиентов различных учреждений.

В работе описан процесс оценки уязвимостей программных средств и сетевых продуктов и сделана оценка их формирования. По результатам исследований была проведена классификация таких уязвимостей и выделены три основных направления защиты.

В заключительной части статьи описаны некоторые методы защиты информации и предотвращения утечек персональных данных в организациях и у частных лиц. Приведены рекомендации по их защите.

Ключевые слова: защита персональных данных, безопасность информационных процессов, клиентская база, интернет, программные средства.

SPECIFICS OF PERSONAL DATA STORAGE WHEN USING DIGITAL DOCUMENT MANAGEMENT

Review article

Kuznetsova I.O.[1], Nesterenko I.S.[2], Nesterenko G.A.[3,] *

[1] ORCID : 0009-0003-9085-7701;

[2] ORCID : 0000-0003-4749-010X;

[3] ORCID : 0000-0003-1528-4627;

[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 work describes the problem of preserving personal data when using digital document management. The definition of personal data and documents in which this data can be reflected is given.

The dangers occurring in the use of electronic documents that are transmitted via communication systems have been analysed. The paper shows how personal data of clients of various institutions can be leaked.

The article describes the process of assessing vulnerabilities of software and network products and makes an evaluation of their formation. Based on the results of the research, a classification of such vulnerabilities was carried out and three main areas of protection were identified.

The final part of the work describes some methods of information protection and prevention of personal data leaks in organizations and individuals. Recommendations for their protection are given.

Keywords: personal data protection, information process security, customer base, internet, software tools.

Введение

На протяжении всего своего существования человечество сталкивалось со множеством ситуаций, в которых оно подвергалось опасностям различного рода. Постепенно мир трансформировался до индустриального общества, в котором основной проблемой следует считать возможность безопасно существовать. Большое количество опасных ситуаций возникает у людей ежедневно, чаще всего они связаны с решением конкретных задач, стоящих перед людьми.

Современный миропорядок намного отличается от устоев прошлых веков. Опасности, которые подстерегают человечество в наши дни намного разнообразней. Урбанизация всех жизненных процессов приводит людей к

необходимости не только соблюдать и изучать общепринятые принципы безопасности, но и новые – принципы цифровой безопасности.

Понятие «цифровая безопасность», внедрилось в нашу жизнь практически одновременно с информационно-коммуникационными технологиями.

Одной из главенствующих задач на сегодняшний день является защита персональных данных, в условиях повсеместного использования электронного документооборота.

Особенности сохранения и защиты персональных данных при использовании цифрового документооборота опирается на Российскую государственную политику, ориентированную на необходимость предоставление защиты персональных данных, построенную посредством норм права Конституции РФ.

В данной сфере существует достаточное количество научных трудов. В статье Кириленко В. В. «Проблемы защиты информации в системах электронного документооборота» автор поднимает вопрос целостности присутствующей информации, в том числе и персональных данных, в системе электронного документооборота [1].

Мухиддин Ф. С. В своей статье «Сравнительный анализ электронного документооборота в разных странах», констатирует факт того, что цифровой документооборот, в частности процесс сохранение информации, в том числе персональных данных при его использовании является общей, мировой проблемой, причем не только на постсоветском пространстве, но и ведущих западных стран [2].

Ушаков Н.О. в работе «Информационная безопасность в системах электронного документооборота» выделяет различные угрозы для систем электронного документооборота, в том числе нарушение конфиденциальности, а именно доступность персональных [3].

В последнее время утечка персональных данных приводит к достаточно серьезным мошенническим действиям, возникают угрозы для рядовых граждан страны, такие как значительные финансовые потери, компрометация добропорядочных граждан с унижением человеческого достоинства, кража интеллектуальной собственности. В связи с этим перед государственной властью возникла задача создание обеспечение сохранности и неприкосновенности персональных данных при использовании цифрового документооборота.

Целью данной работы является выявление возможных каналов компрометации персональных данных и предложение мер воздействия, направленных на снижение или устранение риска их утечки.

Определение персональных данных

С момента внедрения цифровых технологий, появились новые требования для обеспечения безопасности жизни человека. Несмотря на то, что еще в 2006 г. был издан Федеральный закон «О персональных данных» [4], безопасность этих данных оставалась под угрозой.

Сущность самого определения персональных данных – это дилемма в определенном разделе законодательства: от того, как мы ответим на этот вопрос, зависит, станет ли применяться данная норма этого законодательства к действиям, происходящих непосредственно с используемой информацией.

Опираясь на пункт 1 ст. 3 закона «О персональных данных» [4] персональные данные – «это любая информация, относящаяся к прямо или косвенно определённому, или определяемому физическому лицу (субъекту персональных данных)». В реальных условиях достаточно часто возникают сложности с определением, представленным выше, из-за его объёмного восприятия и трактовки. Это связано с введением электронного документооборота во многие сферы деятельности как производственные, так социальные, но в первую очередь в структуры государственных учреждений, что обусловлено Указом Президента Российской Федерации в состав, которого включена «Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы» [5], [6].

В практической жизни возникают ситуации, когда, опираясь на определение персональных данных, трудно понять следует ли считать персональными данными ту или иную информацию [7].

Ученными России были выделены два подхода к толкованию персональных данных – узкий и широкий. Опираясь на узкий подход, следует признавать только те данные, при использовании которых возможно определить непосредственно физическую личность человека, а это паспортные данные, номер водительских права, ИНН, СНИЛС, удостоверение личности [4].

Следует понимать, что в основе функционирования любого учреждения лежит электронный документооборот, и соответственно необходимо предъявлять определенные требования к его степени защиты.

Персональные данные, которыми обладает компания, разделяются на данные, которые принадлежат сотрудникам и клиентам. Кроме того, в зависимости от содержащей информации их следует разделить еще на четыре (рис. 1).

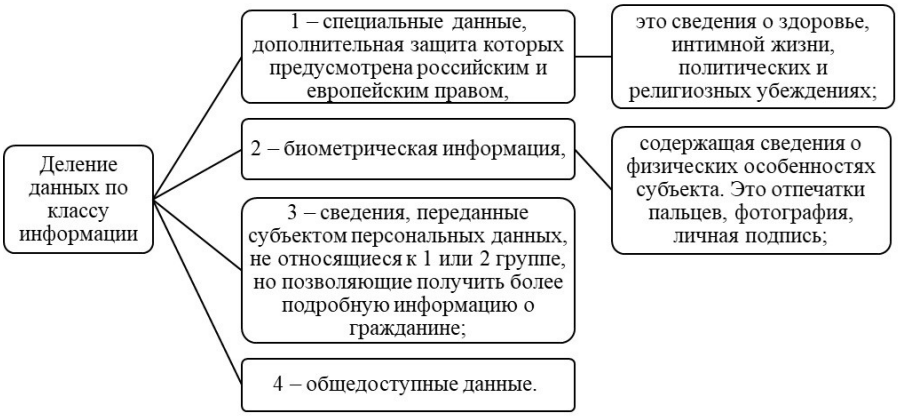

Рисунок 1 - Деление данных на группы по классу информации
DOI: https://doi.org/10.60797/IRJ.2025.151.51.1

Определившись, к какой группе защищенности, следует отнести данные, системы электронного документооборота, следует построить актуальную модель угроз. В ее основу лягут угрозы трех типов (рис. 2).

Рисунок 2 - Деление цифровых угроз на типы
DOI: https://doi.org/10.60797/IRJ.2025.151.51.2

В существующих нормативных актах не указывается, каким образом и по каким критериям определяется тип угроз, руководство компании это определяет самостоятельно, либо поручает разработчику программного обеспечения спроектировать модель угроз.

Следует помнить об актуальности подобающей защите персональных данных хранящихся в системе электронного документооборота.

Еще одним параметром персональных данных следует считать электронную подпись. Глобальное использование возможностей цифровых технологии, а именно внедрение электронной подписи в работу государственных и частных социальных, юридических и производственных структур, позволяет сэкономить трудовые, временные, и финансовые ресурсы. Оформление любого правового акта в независимости от территориального присутствия, возможно произвести без особых затрат благодаря электронной подписи [8].

С появлением электронной подписи появились возможности облегчения процесса оформления документов, однако, возникли и значительные проблемы. Эти недостатки как раз и заключаются в формировании новой формации информационной безопасности.

И так, кроме стандартных принципов безопасности жизнедеятельности вместе с цифровизацией, которая внедрилась практически во все области нашего существования, появились и цифровые принципы, основные из них представлены на рис. 3.

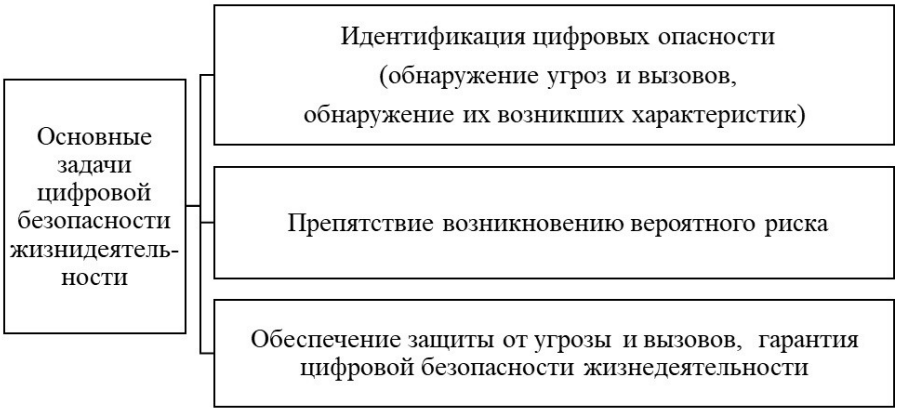

Рисунок 3 - Основные задачи безопасности цифровой жизнедеятельности
DOI: https://doi.org/10.60797/IRJ.2025.151.51.3

Определение идентификации цифровых опасностей идентично определению стандартных опасностей – «… процесс осознания того, что опасность существует…» [9], отличие только в сущности самой опасности. В нашем случае рассматриваются опасности, связанные с работой информационно-коммуникационными технологиями, конкретней – с утечкой персональных данных, вторжением в частную жизнь [10], угрозами завладением интеллектуальной собственности [11], и т.п.

Определение идентификации цифровых опасностей идентично определению стандартных опасностей, отличие только в сущности самой опасности. В нашем случае рассматриваются опасности, связанные с работой информационно-коммуникационных технологий, конкретней – с утечкой персональных данных, вторжением в частную жизнь [12], угрозами завладением интеллектуальной собственности, и т.п.

Обеспечение защиты от угрозы и вызовов, гарантия цифровой безопасности жизнедеятельности в основном связана с мерами, которые направлены на защиту информации [13], [14].

Уязвимости в работе с цифровыми продуктами

Если рассматривать проблему защиты персональных данных по отношению к какому-либо предприятию, то очевидно, что с этой целью необходимо создать алгоритмы процесса защиты информации. Такой алгоритм представлен на рис. 4.

Рисунок 4 - Алгоритм процесса защиты информации
DOI: https://doi.org/10.60797/IRJ.2025.151.51.4

Основной проблемой в информационной безопасности являются уязвимости в программном обеспечении [12], [13]. Сам термин «уязвимость» произошел от английского слова – vulnerability, это не литературное слово, а сленг, и в

дословном переводе звучит как «дыра». Данное выражение применяется для описания изъяна в системе, который может разрушить структуру данного комплекса и спровоцировать отклонение от правильности функционирования.

Ошибка программиста в написании кода программы, неправильные расчеты в создании системы, вирусы, проникшие в программное обеспечение, слабые пароли – все это, порождает уязвимости. Основные виды уязвимостей представлены на рис. 5.

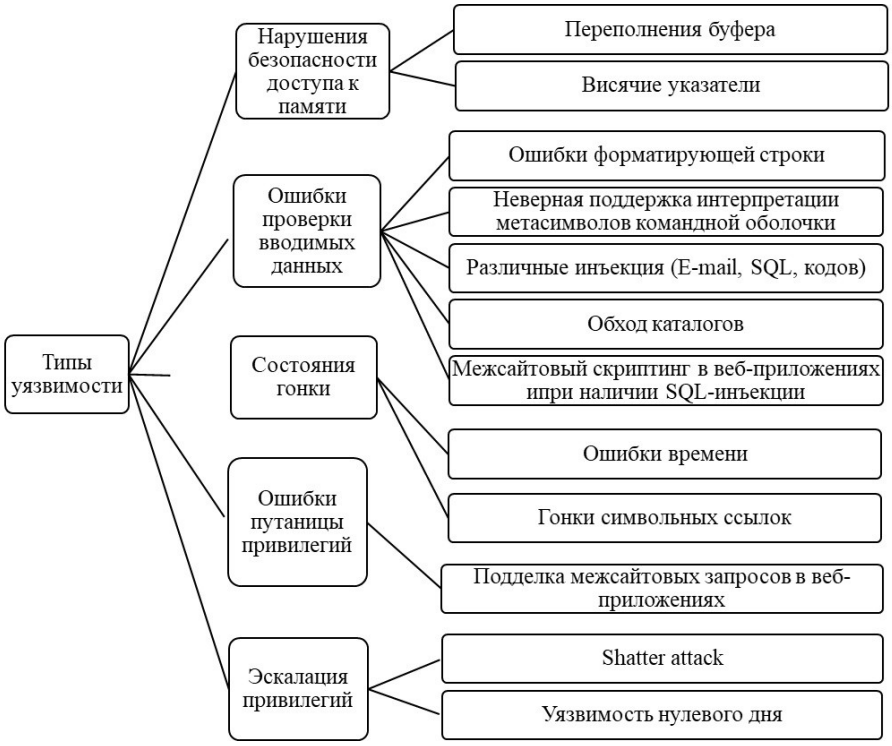

Рисунок 5 - Основные виды уязвимостей
DOI: https://doi.org/10.60797/IRJ.2025.151.51.5

Примечание: по ист. [15]

Зная, какие уязвимости могут возникнуть при работе с программными средствами, можно найти подходящее решение по защите персональных данных.

Направления защиты цифровых данных

В начале мая 2024 г. «Лаборатории Касперского» были опубликованы статистические данные (рис. 6), связанные с обнаружением уязвимостей в программном обеспечении [16].

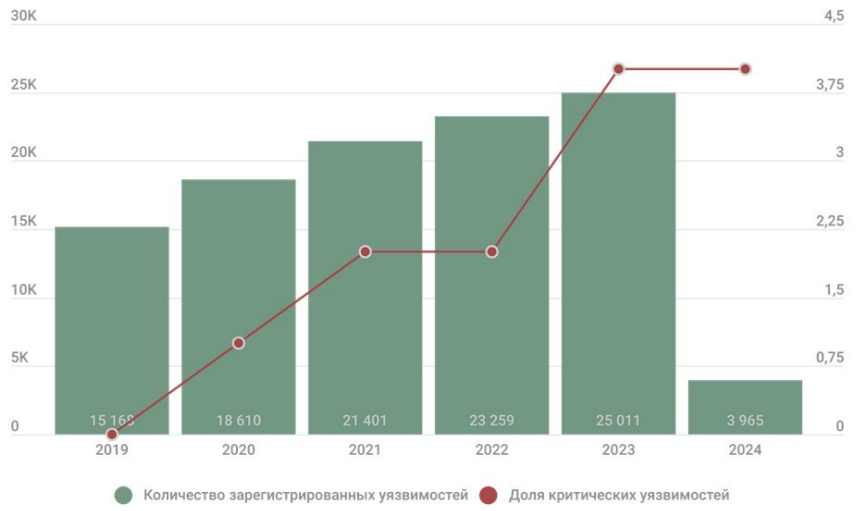

Рисунок 6 - Статистические данные уязвимостей в программном обеспечении за последние 5 лет и первый квартал 2024 г

DOI: https://doi.org/10.60797/IRJ.2025.151.51.6

Из представленного графика следует, что за время проводимых исследований угрозы безопасности программному обеспечению возросли, но и обнаружение уязвимостей, также увеличилось, а это свидетельствует о том, что меры для создания безопасного использования информационно-коммуникационных технологий, использования преимуществ цифровизации возрастают с каждым днем.

Одним из ярких примеров информационной безопасности является борьба с выявлением уязвимости и информационными преступлениями. В качестве примера можно привести работу сотрудников правоохранительных органов, отвечающих за информационную безопасность. Ими были разоблачены два менеджера АО «Россельхозбанк», занимающихся преступными деяниями по отношению к клиентам банка. В отношении данных работников были возбуждены уголовные дела. В дальнейшем эти сотрудники были осуждены по ч. 4 ст. 274.1 и ч. 3 ст. 159 УК РФ, и получили по четыре года лишения свободы условно с назначением испытательного срока два года.

Кроме этого, благодаря выявлениям угроз программному обеспечению операторам сотовой связи удалось обнаружить несколько сотрудников сотовой связи, продававших персональные данные клиентов с целью хищения их финансовых средств. Данные граждане также были осуждены по ч. 4 ст. 274.1 УК РФ и получили в виде наказания лишение свободы условно на срок три года с лишением права заниматься деятельностью по оформлению подключения абонентов к операторам сотовой связи на два года.

Некий гражданин сделал попытку внедриться в информационную систему органов исполнительной власти. Данную уязвимость обнаружили на ранней стадии, ему объявили предостережение [17].

По результатам исследований была проведена классификация уязвимостей программных средств и сетевых продуктов и выделены три основных направления защиты.

К первому направлению было отнесено исключение ошибок при составлении программного кода, который не содержит встроенных средств защиты программного продукта.

Вторым направлением является исключение внедрения вирусных вредоносных программных продуктов, полученных из сторонних источников и через интернет-приложения.

Третьим направлением является повышение ответственности и добросовестности сотрудников учреждений, которые имеют доступ к персональным данным своих клиентов и партнеров.

Заключение

Современная жизнь не существенно отличается от уклада жизни тридцатилетней давности. Однако, с внедрением в производственные процессы автоматизированного документооборота, следует помнить о необходимости обеспечения сохранности персональных данных. Для безопасного функционирования электронного документооборота следует использовать проверенный и безопасный способ хранения и использования персональных данных.

На сегодняшний день, чтобы обезопасить свою жизнь, недостаточно соблюдать привычные правила безопасности. Необходимо усвоить и следовать дополнительным законам информационной безопасности, которые можно назвать цифровыми.

Основные рекомендации по безопасному использованию систем автоматизированного документооборота:

1. Необходимо тщательно следить за тем, на каких информационных ресурсах пользователь оставляет свои персональные данные.

2. В процессе работы с программными средствами следует помнить, что цифровое поле — это новая сфера деятельности для мошенников и есть риск попасться на их уловки.

3. Необходимо пользоваться лицензионным программным обеспечением, а в силу международной ситуации следует отдавать предпочтение отечественному программному обеспечению.

4. Следует применять и своевременно обновлять антивирусные программы.

5. Не заходить на сомнительные сайты, это позволит избежать внедрения вредоносных программных продуктов в используемые компьютерные средства и мобильные телефоны [18], [19].

6. Обеспечить многоступенчатую систему аутентификации.

Конфликт интересов

Не указан.

Рецензия

Артамонов В.А., Международная академия информационных технологий (МНОО "МАИТ), Минск, Беларусь
DOI: https://doi.org/10.60797/IRJ.2025.151.51.7

Conflict of Interest

None declared.

Review

Артамонов V.A., International Academy of information technologies, Minsk, Belarus
DOI: https://doi.org/10.60797/IRJ.2025.151.51.7

Список литературы / References

1. Кириленко В.В. Проблемы защиты информации в системах электронного документооборота / В.В. Кириленко // Научная палитра. — 2021. — № 4 (34) — С. 24–29.

2. Мухиддин Ф.С. Сравнительный анализ электронного документооборота в разных странах / Ф.С. Мухиддин // Международный журнал гуманитарных и естественных наук. — 2022. — № 1-3 (64) — С. 87–89.

3. Ушаков Н.О. Информационная безопасность в системах электронного документооборота / Н.О. Ушаков, И.В. Сибикина, И.М. Космачева // Техническая эксплуатация водного транспорта: проблемы и пути развития. — 2021. — № 1. — URL: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-v-sistemah-elektronnogo-dokumentooborota (дата обращения: 11.12.2024).

4. Российская Федерация. Законы. О персональных данных : федер. закон : [No 152-ФЗ: 2006-07-27: одобр. Советом Федерации 2024-09-04]. — URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 11.12.2024).

5. 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.

6. О Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы: Указ Президента Российской Федерации от 09 мая 2017 г. № 203. Москва, Кремль.

7. Воронков Н.А. Определение персональных данных / Н.А. Воронков // Молодой ученый. — 2022. — № 27 (422). — С. 78–80. — EDN: OMYIRB.

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. Об утверждении Рекомендаций по классификации, обнаружению, распознаванию и описанию опасностей: Приказ Минтруда России от 31.01.2022 N 36. — URL: https://www.consultant.ru/document/cons_doc_LAW_408713/ (дата обращения: 11.12.2024).

10. Российская Федерация. Законы. О внесении изменений в подраздел 3 раздела I части первой Гражданского кодекса Российской Федерации : федер. закон : [No 142-ФЗ: принят Государственной Думой 2024-09-04 :одобр. Советом Федерации2024-09-04]. — URL: https://www.consultant.ru/document/cons_doc_LAW_148454/ (дата обращения: 11.12.2024).

11. Российская Федерация. Законы. Гражданский кодекс Российской Федерации : федер. закон : [30 ноября 1994 года N 51-ФЗ]. — Ч. 4. — Ст. 1225. Охраняемые результаты интеллектуальной деятельности и средства индивидуализации.

12. Горлов А.П. Сущность комплексного подхода к разработке системы защиты информации / А.П. Горлов, М.Л. Гулак, Е.В. Лексиков [и др.] // Информационная безопасность и защита персональных данных. Проблемы и пути их решения : Сборник материалов и докладов XV межрегиональной научно-практической конференции, Брянск, 28 апреля 2023 года / Под общ. ред. О.М. Голембиовской. — Брянск: Брянский государственный технический университет, 2023. — С. 83–87. — EDN: BLMGRJ.

13. Liang W. Information Security Monitoring and Management Method Based on Big Data in the Internet of Things Environment / W. Liang, W. Li, L. Feng // IEEE Access. — 2021. — Vol. 9. — P. 39798–39812. — DOI: 10.1109/ACCESS.2021.3064350. — EDN: IGITDE.

14. Дудкина И.А. Технологии и методы обеспечения комплексной защиты информации / И.А. Дудкина // Молодой ученый. — 2016. — № 16(120). — С. 37–39. — EDN: WINLOV.

15. Кузнецова И.О. Необходимость внедрения информационно-коммуникационных технологий в работу государственных служб / И.О. Кузнецова // Евразийская интеграция: современные тренды и перспективные направления : Материалы Международной научно-практической конференции, Омск, 14 марта 2023 года / Под общ. ред. М.Г. Родионова. — Омск: Омский государственный технический университет, 2023. — С. 105–110. — DOI: 10.24412/cl-37031-2023-2-105-110. — EDN: MDRIFF.

16. Щука И.О. Цифровые технологии в управлении и экономике / И.О. Щука // Социально-экономические и правовые системы стран евразийской экономической интеграции, Омск, 03 марта 2021 года / Сибирский институт бизнеса и информационных технологий. — Омск: Омский государственный технический университет, 2021. — С. 319–322. — EDN: KTWWZE.

17. Iskanderov Y. Comprehensive Intelligent Information Security Management System (CIISMS) for Supply Networks: The Actor-Network Perspective / Y. Iskanderov, M. Pautov // Advances in Intelligent Systems and Computing. — 2020. — Vol. 1294. — P. 130–142. — DOI: 10.1007/978-3-030-63322-6_10. — EDN: BCKIVY.

18. Хромова А.Р. Анализ уязвимостей в системах безопасности данных / А.Р. Хромова, Л.Э. Петросян // Инженерный вестник Дона. — 2023. — № 6 (102). — С. 67–76. — EDN: XBDQNP.

19. Кузнецова И.О. Предпосылки появления искусственного интеллекта / И.О. Кузнецова, Г.А. Нестеренко, И.С. Нестеренко // Международный научно-исследовательский журнал. — 2024. — № 8 (146). — URL: https://research-journal.org/archive/8-146-2024-august/10.60797/IRJ.2024.146.36 (дата обращения: 17.08.2024). — DOI: 10.60797/IRJ.2024.146.36

Список литературы на английском языке / References in English

1. Kirilenko V.V. Problemy zashhity informacii v sistemah jelektronnogo dokumentooborota [Problems of information security in electronic document management systems] / V.V. Kirilenko // Nauchnaja palitra [Scientific Palette]. — 2021. — № 4 (34). — P. 24–29. [in Russian]

2. Mukhiddin F.S. Sravnitel'nyj analiz jelektronnogo dokumentooborota v raznyh stranah [Comparative analysis of electronic document management in different countries] / F.S. Muhiddin // Mezhdunarodnyj zhurnal gumanitarnyh i estestvennyh nauk [International Journal of Humanities and Natural Sciences]. — 2022. — № 1-3 (64). — P. 87–89. [in Russian]

3. Ushakov N.O. Informacionnaja bezopasnost' v sistemah jelektronnogo dokumentooborota [Information security in electronic document management systems] / N.O. Ushakov, I.V. Sibikina, I.M. Kosmacheva // Tehnicheskaja jekspluatacija vodnogo transporta: problemy i puti razvitija [Technical Operation of Water Transport: Problems and Development Paths]. — 2021. — № 1. — URL: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-v-sistemah-elektronnogo-dokumentooborota (accessed: 11.12.2024). [in Russian]

4. Rossijskaja Federacija. Zakony. O personal'nyh dannyh [Russian Federation. Laws. About personal data] : Federal Law : [No 152-ФЗ: 2006-07-27: approved by the Federation Council 2024-09-04]. — URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (accessed: 11.12.2024). [in Russian]

5. Nesterenko G.A. Perspektivy vnedrenija jelektronnogo dokumentooborota pri ispol'zovanii korporativnyh informacionnyh sistem [Prospects for the introduction of electronic document management when using 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 Russian]

6. O Strategija razvitija informacionnogo obshhestva v Rossijskoj Federacii na 2017–2030 gody [On the Strategy for the Development of the Information Society in the Russian Federation for 2017-2030]: Decree of the President of the Russian Federation dated May 09, 2017 No. 203. Moscow, Kremlin. [in Russian]

7. Voronkov N.A. Opredelenie personal'nyh dannyh [Determination of personal data] / N.A. Voronkov // Molodoj uchenyj [Young Scientist]. — 2022. — № 27 (422). — P. 78–80. — EDN: OMYIRB. [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. Ob utverzhdenii Rekomendacij po klassifikacii, obnaruzheniju, raspoznavaniju i opisaniju opasnostej [On approval of Recommendations on classification, detection, recognition and description of hazards]: Order of the Ministry of Labor of the Russian Federation dated 01/31/2022 No. 36. — URL: https://www.consultant.ru/document/cons_doc_LAW_408713/ (accessed: 11.12.2024). [in Russian]

10. Rossijskaja Federacija. Zakony. O vnesenii izmenenij v podrazdel 3 razdela I chasti pervoj Grazhdanskogo kodeksa Rossijskoj Federacii [Russian Federation. Laws. On Amendments to Subsection 3 of Section I of Part One of the Civil Code of the Russian Federation] : Federal Law : [No 142-ФЗ: accepted by the State Duma 2024-09-04 :approved by the Federation Council 2024-09-04]. — URL: https://www.consultant.ru/document/cons_doc_LAW_148454/ (accessed: 11.12.2024). [in Russian]

11. Rossijskaja Federacija. Zakony. Grazhdanskij kodeks Rossijskoj Federacii [Russian Federation. Laws. The Civil Code of the Russian Federation] : Federal Law : [November 30, 1994, No. 51-FZ]. — Pt. 4. — Article 1225. Protected results of intellectual activity and means of individualization. [in Russian]

12. Gorlov A.P. Sushhnost' kompleksnogo podhoda k razrabotke sistemy zashhity informacii [The essence of an integrated approach to the development of an information security system] / A.P. Gorlov, M.L. Gulak, E.V. Leksikov [et al.] // Informacionnaja bezopasnost' i zashhita personal'nyh dannyh. Problemy i puti ih reshenija [Information security and protection of personal data. Problems and ways to solve them] : Collection of materials and reports of the XV Interregional Scientific and Practical Conference, Bryansk, April 28, 2023 / Gen. ed. by O.M. Golembiovskaya. — Bryansk: Bryansk State Technical University, 2023. — P. 83–87. — EDN: BLMGRJ. [in Russian]

13. Liang W. Information Security Monitoring and Management Method Based on Big Data in the Internet of Things Environment / W. Liang, W. Li, L. Feng // IEEE Access. — 2021. — Vol. 9. — P. 39798–39812. — DOI: 10.1109/ACCESS.2021.3064350. — EDN: IGITDE.

14. Dudkina I.A. Tehnologii i metody obespechenija kompleksnoj zashhity informacii [Technologies and methods of ensuring complex information protection] / I.A. Dudkina // Molodoj uchenyj [Young Scientist]. — 2016. — № 16(120). — P. 37–39. — EDN: WINLOV. [in Russian]

15. Kuznetsova I.O. Neobhodimost' vnedrenija informacionno-kommunikacionnyh tehnologij v rabotu gosudarstvennyh sluzhb [The need to introduce information and communication technologies into the work of public services] / I.O. Kuznetsova

// Evrazijskaja integracija: sovremennye trendy i perspektivnye napravlenija [Eurasian integration: current trends and promising directions] : Materials of the International Scientific and Practical Conference, Omsk, March 14, 2023 / Gen. ed. by M.G. Rodionov. — Omsk: Omsk State Technical University, 2023. — P. 105–110. — DOI: 10.24412/cl-37031-2023-2-105-110. — EDN: MDRIFF. [in Russian]

16. Shchuka I.O. Cifrovye tehnologii v upravlenii i jekonomike [Digital technologies in Management and Economics] / I.O. Shchuka // Social'no-jekonomicheskie i pravovye sistemy stran evrazijskoj jekonomicheskoj integracii, Omsk, 03 marta 2021 goda [Socio-economic and legal systems of the countries of the Eurasian Economic integration, Omsk, March 03, 2021] / Siberian Institute of Business and Information Technologies. — Omsk: Omsk State Technical University, 2021. — P. 319–322. — EDN: KTWWZE. [in Russian]

17. Iskanderov Y. Comprehensive Intelligent Information Security Management System (CIISMS) for Supply Networks: The Actor-Network Perspective / Y. Iskanderov, M. Pautov // Advances in Intelligent Systems and Computing. — 2020. — Vol. 1294. — P. 130–142. — DOI: 10.1007/978-3-030-63322-6_10. — EDN: BCKIVY.

18. Khromova A.R. Analiz ujazvimostej v sistemah bezopasnosti dannyh [Vulnerability analysis in data security systems] / A.R. Khromova, L.E. Petrosyan // Inzhenernyj vestnik Dona [Engineering Bulletin of the Don]. — 2023. — № 6 (102). — P. 67–76. — EDN: XBDQNP. [in Russian]

19. Kuznetsova I.O. Predposylki pojavlenija iskusstvennogo intellekta [Prerequisites for the emergence of artificial intelligence] / I.O. Kuznetsova, G.A. Nesterenko, I.S. Nesterenko // Mezhdunarodnyj nauchno-issledovatel'skij zhurnal [International Scientific Research Journal]. — 2024. — № 8 (146). — URL: https://research-journal.org/archive/8-146-2024-august/10.60797/IRJ.2024.146.36 (accessed: 17.08.2024). — DOI: 10.60797/IRJ.2024.146.36 [in Russian]