Научная статья
УДК 330.354
DOI 10.24888/2949-2793-2024-6-81-89

ОРГАНИЗАЦИЯ ЗАЩИТЫ ЦИФРОВЫХ ДАННЫХ НА ПРЕДПРИЯТИИ

С.В. Воробьев, Е.Э. Эфендиева

Елецкий государственный университет им. И.А. Бунина
(Елец, Россия)

Аннотация. *В статье рассмотрены основные аспекты организации защиты цифровых данных на предприятии. Были определены основные понятия и термины, связанные с безопасностью данных, рассмотрена законодательная база в этой области. Показано, как политика и стратегия защиты цифровых данных на предприятии влияет на общую безопасность бизнеса. Определены возможные роли и обязанности сотрудников предприятия в обеспечении безопасности данных, которые существенным образом оказывают положительное влияние на организацию защиты цифровых данных. В рамках статьи описаны организационные мероприятия и технические средства защиты цифровых данных, которые позволяют обеспечить их конфиденциальность, целостность и доступность на предприятиях любой сферы деятельности*.

Ключевые слова: *защита цифровых данных, конфиденциальность информации, угрозы безопасности цифровых данных, политика безопасности, стратегия защиты данных на предприятии*.

ORGANIZATION OF DIGITAL DATA PROTECTION IN THE ENTERPRISE

S.V. Vorobyev, E.E. Efendieva

Bunin Yelets State University
(Yelets, Russia)

Abstract. *The article discusses the main aspects of the organization of digital data protection in the enterprise. The basic concepts and terms related to data security were defined, and the legislative framework in this area was reviewed. It is shown how the policy and strategy of protecting digital data in an enterprise affects the overall security of a business. The possible roles and responsibilities of the company's employees in ensuring data security have been identified, which significantly have a positive impact on the organization of digital data protection. The article describes organizational measures and technical means of protecting digital data, which make it possible to ensure their confidentiality, integrity and accessibility in enterprises of any field of activity.*

Keywords: *protection of digital data, confidentiality of information, threats to the security of digital data, security policy, data protection strategy in the enterprise*.

В современном высокотехнологичном мире цифровые данные стали одним из самых ценных активов для предприятий. Они содержат информацию о клиентах, финансовых операциях, конфиденциальных сделках и прочих внутренних процессах компаний. Это может включать в себя всё, начиная от персональных данных клиентов и заканчивая деталями о продуктах или услугах компании. Защита этих данных от несанкционированного доступа, модификации или уничтожения является критически

важной задачей для обеспечения стабильности и успешного развития бизнеса. Для этого необходимо внедрение эффективных мер безопасности, включающих в себя использование современных технологий шифрования, систем контроля доступа и регулярного аудита.

Существует несколько факторов, которые объясняют важность защиты цифровых данных. Во-первых, утечка конфиденциальной информации может негативно сказаться на репутации компании и привести к потере доверия клиентов. Это может привести к снижению продаж, увеличению затрат на устранение последствий утечки данных и даже к юридическим последствиям. Во-вторых, потеря или повреждение данных может прервать бизнес-процессы, что влечет за собой финансовые потери и упущенные возможности. Это может затруднить выполнение повседневных операций, привести к сбоям в обслуживании клиентов и даже к полной остановке бизнеса. В-третьих, многие страны ужесточили законодательство в области защиты данных, и несоблюдение требований может повлечь за собой штрафы и другие санкции. Это может нанести серьёзный ущерб компании, привести к большим финансовым потерям и даже к уголовной ответственности.

Однако, обеспечение безопасности цифровых данных связано с рядом проблем и рисков. Покажем некоторые них. Во-первых, это растущая сложность и распространенность кибератак. Злоумышленники постоянно совершенствуют методы и инструменты взлома, что затрудняет защиту от них. Это требует от компаний постоянного обновления своих систем безопасности и проведения регулярного мониторинга для обнаружения и предотвращения кибератак. Во-вторых, это человеческий фактор. Недостаточная осведомленность сотрудников или их халатность могут привести к утечке или потере данных. Это требует проведения регулярного обучения персонала и создания культуры безопасности в организации. В-третьих, это развитие новых технологий. С появлением таких новых технологий, как облачные вычисления и искусственный интеллект, увеличиваются риски утечки информации, появляются новые угрозы и вызовы в области защиты данных. Это требует от компаний постоянного мониторинга новых технологий и адаптации своих систем безопасности для обеспечения защиты данных. В связи с этим организация эффективной защиты цифровых данных на предприятии является актуальной и сложной задачей, решение которой нуждается в постоянном совершенствовании и комплексном подходе.

Цифровые данные представляют собой информацию, обычно закодированную в двоичном виде, хранящуюся на цифровых носителях или в облачных сервисах. Это может включать в себя всё, начиная от текстовых документов и электронных таблиц и заканчивая мультимедийными файлами и базами данных. В зависимости от степени важности и конфиденциальности, цифровые данные могут быть классифицированы на следующие категории: открытые данные – информация, доступная для всех и не требующая специальных мер защиты; внутренние данные – информация, предназначенная для использования внутри предприятия и не подлежащая распространению за его пределами; конфиденциальные данные – информация, доступ к которой должен быть строго ограничен и контролируем, например, это могут быть персональные данные клиентов, коммерческая тайна, финансовая и иная конфиденциальная информация. Каждая из этих категорий данных требует своего подхода к защите и управлению.

Основные аспекты безопасности цифровой информации включают в себя три пункта: конфиденциальность, целостность и доступность. Конфиденциальность означает защиту информации от несанкционированного доступа. Это требование достигается при помощи криптографических инструментов, систем управления доступом и других технических и организационных мер. Часто для обеспечения конфиденциальности применяются передовые криптографические алгоритмы, такие как AES или RSA, а также используются системы идентификации и аутентификации пользователей, включая пароли, биометрические данные или цифровые сертификаты. Не менее важным требованием является целостность – обеспечение защиты информации от несанкционированного

изменения или уничтожения. Это требование достигается с помощью инструментов контроля версий, аудита и других технических и организационных мер. Также может включать использование систем контроля версий, например Git, для отслеживания изменения данных и хранения предыдущих версий, а также использование систем резервного копирования и восстановления данных для обеспечения их восстановления в случае потери или повреждения. Доступность, которая обеспечивает возможность доступа к данным авторизованными пользователями в нужное время и в нужном объеме, также является одним из ключевых параметров безопасности информации. Достигается с помощью систем резервного копирования, отказоустойчивых хранилищ данных и других технических и организационных мер. Как и целостность данных может включать использование систем резервного копирования, также отказоустойчивых хранилищ данных, например, объектных, как S3 от компании AWS. Кроме того, могут быть использованы системы резервного копирования и восстановления данных, такие как RAID или облачные сервисы, для обеспечения доступности данных в случае их потери или повреждения, а также системы мониторинга и управления производительностью для обеспечения быстрого доступа к данным.

Угроза безопасности цифровых данных включает в себя любое событие или действие, которое может привести к нарушению основных аспектов безопасности данных. Угрозы бывают двух типов: внешние – кибератаки, физическое взаимодействие, стихийные бедствия; внутренние – халатность сотрудников или намеренные действия по уничтожению или изменению данных. За внешними угрозами обычно стоят злоумышленники или компании конкурентов, которые пытаются получить или повредить данные. Это может включать в себя различные виды кибератак, такие как вирусы, трояны, атаки по типу «отказ в обслуживании» и другие. Ко внутренним же обычно относятся действия сотрудников компании, которые приводят к утечке данных, изменению или уничтожению. Подобные ситуации происходят прежде всего из-за недостаточной осведомленности работников, халатности или саботажа.

При разработке системы защиты цифровых данных на предприятии необходимо учесть концепцию уязвимости информационной системы. Уязвимость – это недостаток в системе защиты данных, который может быть эксплуатирован злоумышленником для проведения атаки. Подобные недостатки появляются, как из-за технической характеристики системы (недостаточная защита паролей, устаревшие программные продукты), а также могут быть связаны с человеческим фактором (недостаточная осведомленность сотрудников, халатность). Понимание угроз и уязвимостей в области безопасности цифровых данных является ключевым для разработки эффективной стратегии их защиты на предприятии.

Защита цифровых данных регулируется на уровне национального и международного законодательства, а также отраслевыми стандартами и рекомендациями. Соблюдение требований законодательства и стандартов является обязательным условием для обеспечения эффективной защиты данных и избегания юридических и финансовых рисков. Это может включать в себя соблюдение требований законов о защите персональных данных, стандартов безопасности информации, таких как ISO 27001 или PCI DSS, а также требований специфических для отрасли стандартов и регуляторов.

В области защиты цифровых данных действуют следующие наиболее значимые нормативные акты и стандарты. Основным нормативным актом, регулирующим отношения в области обработки персональных данных в Российской Федерации, выступает закон «О персональных данных». Согласно этому закону, обработка персональных данных должна осуществляться на законных и честных основаниях, с соблюдением прав и законных интересов субъектов персональных данных. Следующим важным элементом нормативной базы является ГОСТ Р 51945-2021 «Информационная технология. Требования к системам защиты информации», представляющий собой стандарт, который устанавливает

требования к системам защиты информации и используется для обеспечения безопасности цифровых данных. Наряду с ним можно отметить международный стандарт ISO/IEC 27001:2013 «Информационные технологии. Техники безопасности. Системы управления безопасностью информации. Требования», устанавливающий требования к системам управления безопасностью информации на предприятии. Также часто применяется стандарт безопасности данных платежной карточной индустрии PCI DSS (Payment Card Industry Data Security Standard), устанавливающий требования к безопасности обработки данных платежных карт. Для обеспечения комплексной защиты цифровых данных важно учитывать как национальные, так и международные стандарты, их требования. В области защиты цифровых данных действуют следующие требования.

Международные требования к защите данных устанавливают международные организации: Европейский союз, Совет Европы, Организация Объединенных Наций и другие. Подобные требования включают в себя предписания к обработке персональных данных, к трансграничной передаче данных, к защите прав субъектов персональных данных. Сюда относятся соблюдение требований Общего регламента по защите данных (GDPR) Европейского союза, Конвенции Совета Европы о защите лиц в связи с автоматизированной обработкой персональных данных и других международных нормативных актов.

Национальные требования к защите данных устанавливаются законодательством конкретной страны. В нашей стране основными нормативными актами в этой области являются Закон «О персональных данных» и ГОСТ Р 51945-2021. Данные акты включают в себя соблюдение требований этих законов, а также требований других национальных законов и нормативных актов, регулирующих обработку и защиту цифровых данных.

Обеспечение эффективной защиты цифровых данных на предприятии невозможно без разработки и реализации политики безопасности и стратегии защиты данных. Данные документы должны определять цели, принципы и методы защиты данных, а также роли и обязанности всех участников процесса. Они должны быть разработаны с учетом специфики деятельности предприятия, его информационных систем и ресурсов, а также угроз и уязвимостей, с которыми оно сталкивается.

Политика безопасности – документ, который служит основой для обеспечения безопасности цифровых данных на предприятии. В нем описаны основные принципы и требования, которым необходимо следовать для защиты данных от потенциальных угроз, пример которых показан на рисунке 1.

Рис. 1. Разделы политики безопасности

Для обеспечения безопасности данных необходимо четко структурировать политику безопасности, включив в нее все ключевые аспекты. В ее составе должны быть такие разделы, как управление доступом, защита от вредоносного программного обеспечения, защита сетевой инфраструктуры, реагирование на инциденты безопасности и другие важные направления. Каждый раздел обязан содержать детализированные требования и процедуры для обеспечения надежной защиты данных. Политика безопасности должна быть одобрена руководством компании и полностью поддерживаться на высшем уровне, чтобы все принимаемые решения по защите данных соответствовали данной политике. Также, соблюдение политики безопасности обязательно для всех сотрудников. Это подразумевает, что каждый работник должен быть ознакомлен с положениями политики и соблюдать их. В эту деятельность входит регулярное обучение персонала и мониторинг исполнения установленных норм безопасности. Политика безопасности имеет важнейшее значение для защиты цифровых данных в организации. Она формирует основу всех мероприятий по защите данных и способствует созданию культуры безопасности внутри компании. Поэтому крайне важно, чтобы политика безопасности была тщательно проработана, регулярно пересматривалась и строго соблюдалась всеми сотрудниками.

Стратегия защиты данных, не просто документ, а комплексный подход, который охватывает все аспекты обеспечения безопасности цифровых данных на предприятии, которые изображены на рисунке 2. Помимо использования технологий защиты данных, данный подход учитывает также много различных деталей, включая особенности предприятия, требования законодательства и стандартов безопасности, а также уровень риска и уязвимостей в безопасности данных.

Рис. 2. Элементы стратегии защиты данных

Характеристики предприятия существенно влияют на формирование стратегии защиты данных. Уникальные особенности, такие как размер, отрасль, структура и корпоративная культура, определяют типы обрабатываемых данных и методы их защиты. Например, финансовые учреждения часто предъявляют более строгие требования к защите данных по сравнению с небольшими торговыми компаниями. Важную роль играют также законодательные требования и стандарты безопасности. Законы и нормативы, такие как Общий регламент по защите данных (GDPR) в Европейском союзе или стандарт безопасности данных индустрии платежных карт (PCI DSS), устанавливают определенные требования, которые предприятия должны соблюдать при разработке своей стратегии защиты данных.

При формировании стратегии защиты данных необходимо учитывать уровень риска и уязвимости. Это включает оценку потенциальных угроз: кибератаки или внутренние угрозы, а также выявление слабых мест в системах и процессах предприятия, которые могут быть использованы для несанкционированного доступа к данным. Стратегия защиты данных должна предусматривать меры по управлению этими рисками и устранению уязвимостей.

Эффективная стратегия защиты данных должна быть гибкой и адаптируемой, чтобы оперативно реагировать на изменения в сфере безопасности данных. Это может включать регулярное обновление стратегии в ответ на появление новых угроз или изменений в законодательстве, а также обучение персонала новым методам защиты данных. Такая стратегия будет оставаться актуальной и эффективной в долгосрочной перспективе.

Кроме того, успешная защита цифровых данных невозможна без участия всех сотрудников предприятия. Важно четко определить роли и обязанности каждого сотрудника в области безопасности данных. Организационные мероприятия являются ключевым элементом системы защиты данных, направленным на обеспечение безопасности через внедрение соответствующих процедур, правил и норм поведения для сотрудников.

Управление доступом и аутентификацией пользователей является одним из основных организационных мероприятий по защите цифровых данных. Оно предусматривает следующие меры, показанные на рисунке 3.

Управление правами доступа и контроль изменений являются ключевыми элементами обеспечения целостности и конфиденциальности цифровых данных. Эти механизмы составляют основу информационной безопасности в цифровой среде. Определение прав доступа в зависимости от должностных обязанностей сотрудников помогает минимизировать риск несанкционированного доступа и утечки информации, предоставляя доступ к данным только тем сотрудникам, которым он необходим для выполнения их задач.

Контроль изменений в цифровых данных также играет важную роль в поддержании их целостности. Использование журналов регистрации и аудита позволяет отслеживать все внесенные изменения, что способствует быстрому обнаружению и исправлению несанкционированных или ошибочных модификаций.

Периодическое обновление прав доступа в соответствии с изменениями должностных обязанностей сотрудников обеспечивает актуальность системы доступа. Это гарантирует, что права доступа всегда соответствуют текущим обязанностям, что дополнительно укрепляет безопасность данных.

Отчетность о действиях сотрудников с цифровыми данными повышает прозрачность и контроль. Управляющие могут отслеживать действия сотрудников, обеспечивая их ответственность за любые изменения данных. Внедрение организационных мероприятий, таких как разработка и реализация политик безопасности, обучение персонала и использование технических средств защиты, способствует повышению уровня безопасности данных на предприятии.

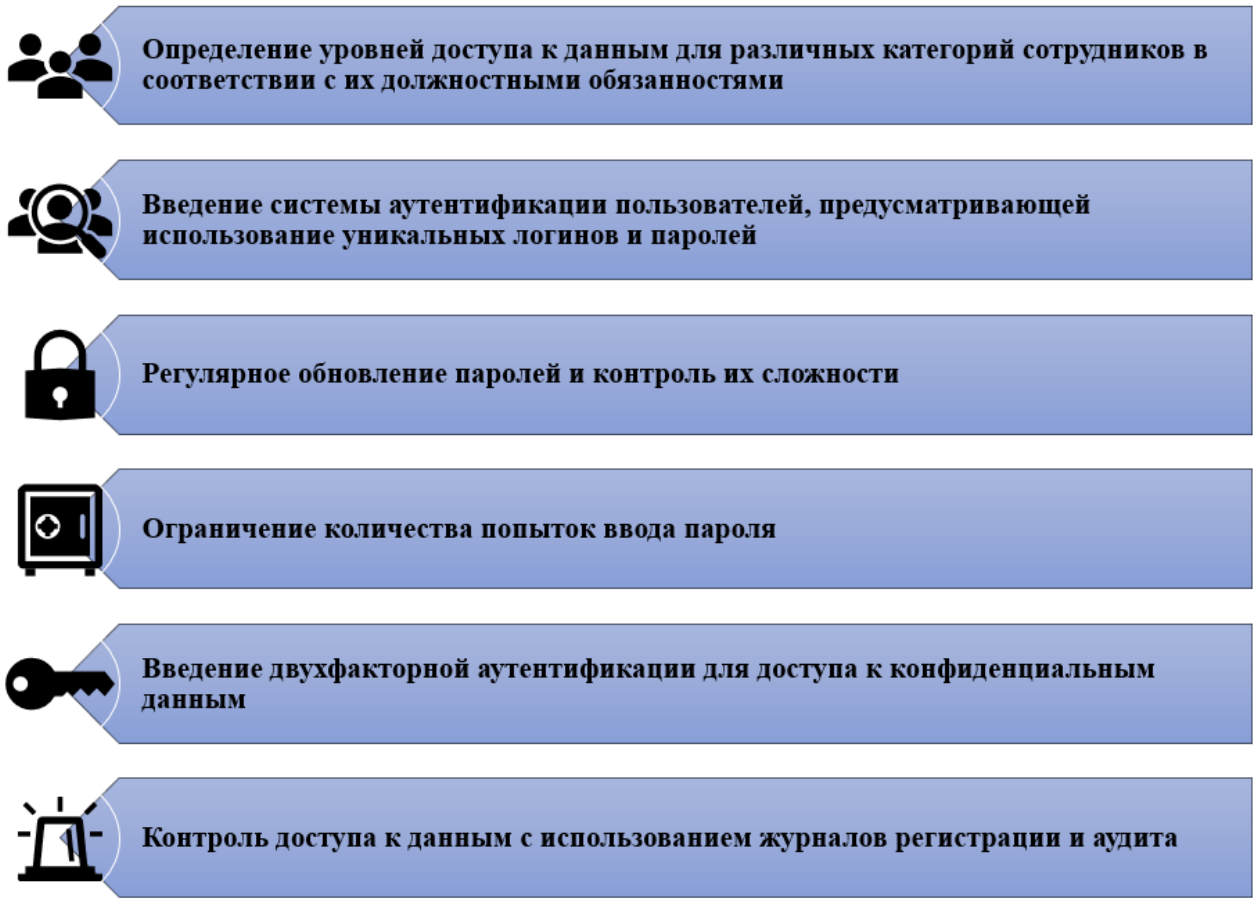

Рис. 3. Варианты организационных мероприятий по защите цифровых данных

Перспективы развития защиты цифровых данных связаны с внедрением новых технологий и адаптацией к новым угрозам. Это требует постоянного совершенствования системы защиты данных, внедрения современных технических и организационных мер, а также повышения квалификации сотрудников в области информационной безопасности. Гибкость и адаптивность системы защиты данных позволяют эффективно реагировать на изменяющиеся угрозы.

Защита цифровых данных на предприятии представляет собой многослойный процесс, который невозможно осуществить без всестороннего подхода и коллективной ответственности всех работников. Для достижения надежной безопасности требуется сочетание организационных мер и современных технических средств. Совместное применение этих инструментов позволяет гарантировать конфиденциальность, целостность и доступность данных, снижая вероятность утечек и несанкционированного доступа. Необходимо постоянно обучать сотрудников и повышать их квалификацию в области информационной безопасности, чтобы они могли эффективно реагировать на новые угрозы и следовать установленным протоколам. Только комплексный подход, включающий регулярное обновление знаний и внедрение передовых технологий, способен обеспечить надежную защиту данных. Таким образом, поддержание безопасности данных – это неотъемлемая часть успешной деятельности любой организации, требующая постоянного внимания и усилий со стороны всех членов коллектива.

Список источников

1. Амандурдыевна, О. А. Защита информации и кибербезопасность на предприятии / О. А. Амандурдыевна, О. Ш. Хыдырова, Э. Р. Мырадова // In Situ. – 2023. – № 2. – С. 36-38.
2. Головина, Е. Ю. Бизнес-процесс защита конфиденциальной информации на предприятии / Е. Ю. Головина, А. А. Расаева // Наука. Технология. Производство – 2023 : Материалы Всероссийской научно-технической конференции, посвященной 75-летию ООО «Газпром нефтехим Салават», Салават, 24–28 апреля 2023 года. Том Часть 1. – Салават: Уфимский государственный нефтяной технический университет, 2023. – С. 7-9.
3. Грицько, В. В. Цифровизация производственных процессов на предприятии АПК / В. В. Грицько // Актуальные вопросы современной экономики. – 2023. – № 12. – С. 82-86.
4. Есина, Е. П. Информационная безопасность и киберпреступность финансового рынка РФ / Е. П. Есина, И. Р. Зимникова, Ю. В. Марышева // Управление инновационным развитием агропродовольственных систем на национальном и региональном уровнях : Материалы международной научно-практической конференции, Воронеж, 11–12 октября 2023 года. – Воронеж: Воронежский государственный аграрный университет им. Императора Петра I, 2023. – С. 388-394.
5. Информационная безопасность в цифровой экономике / Т. Г. Хетагурова, И. Ю. Хетагурова, З. В. Соскиева, М. Г. Багиева // Экономика и управление: проблемы, решения. – 2023. – Т. 5, № 1(133). – С. 128-132. – DOI 10.36871/ek.up.p.r.2023.01.05.016.
6. Карепова, С. Г. Информационная безопасность: специфика феномена, методы и способы ее обеспечения / С. Г. Карепова, С. В. Некрасов, А. Н. Пинчук // Вестник Московского университета. Серия 18. Социология и политология. – 2023. – Т. 29, № 4. – С. 200-220. – DOI 10.24290/1029-3736-2023-29-4-200-220.
7. Лобанова, В. А. Информационная безопасность в обработке персональных данных / В. А. Лобанова // Современные парадигмы устойчивого развития региональных социально-экономических систем в условиях роста неопределенности внешней среды : Материалы Международной научно-практической конференции, Гатчина, 21 апреля 2023 года. – Гатчина: Государственный институт экономики, финансов, права и технологий, 2023. – С. 425-429.
8. Маняхина, З. А. цифровизация системы складирования на предприятии / З. А. Маняхина, Д. В. Черемухов, Н. В. Кривоносова // Наука, образование, транспорт: актуальные вопросы, приоритеты, векторы взаимодействия : Материалы II Международной научно-методической конференции. В 3-х частях, Оренбург, 08–09 ноября 2023 года. – Оренбург: Самарский государственный университет путей сообщения, 2023. – С. 66-70.
9. Мугаева, Е. В. Цифровизация управленческих процессов на предприятии / Е. В. Мугаева // Дневник науки. – 2023. – № 8(80). – DOI 10.51691/2541-8327_2023_8_3.
10. Назаров, Д. М. Анализ семантики понятий экономическая безопасность и информационная безопасность в цифровой экономике / Д. М. Назаров, А. Д. Назаров // Международный журнал прикладных наук и технологий Integral. – 2023. – № 4.
11. Погорелова, С. Р. Информационная безопасность: ключевые угрозы и средства защиты / С. Р. Погорелова, С. М. Петросян, В. И. Найденков // Проблемы и перспективы развития России: Молодежный взгляд в будущее : Сборник научных статей 6-й Всероссийской научной конференции. В 3-х томах, Курск, 19–20 октября 2023 года / Редколлегия: А.А. Горохов (отв. редактор). Том 2. – Курск: Закрытое акционерное общество "Университетская книга", 2023. – С. 471-475.
12. Яриков, В. Г. Информационная безопасность и защита информации на предприятии / В. Г. Яриков, М. В. Пашков // НБИ технологии. – 2023. – Т. 17, № 4. – С. 47-51. – DOI 10.15688/NBIT.jvolsu.2023.4.6.

References

1. Amandurdyevna, O. A. Information protection and cybersecurity at the enterprise / O. A. Amandurdyevna, O. S. Khydyrova, E. R. Myradova // In Situ. – 2023. – No. 2. – pp. 36-38.

2. Golovina, E. Y. Business process protection of confidential information at the enterprise / E. Y. Golovina, A. A. Rasaeva // Science. Technology. Production – 2023 : Materials of the All-Russian Scientific and Technical Conference dedicated to the 75th anniversary of Gazprom Neftekhim Salavat LLC, Salavat, April 24-28, 2023. Volume Part 1. – Salavat: Ufa State Petroleum Technical University, 2023. – pp. 7-9.

3. Gritsko, V. V. Digitalization of production processes at the agro-industrial complex enterprise / V. V. Gritsko // Current issues of the modern economy. - 2023. – No. 12. – pp. 82-86.

4. Yesina, E. P. Information security and cybercrime of the financial market of the Russian Federation / E. P. Yesina, I. R. Zimnikova, Yu. V. Marysheva // Management of innovative development of agro-food systems at the national and regional levels : Materials of the international scientific and practical conference, Voronezh, October 11-12, 2023. – Voronezh: Voronezh State Agrarian University named after Emperor Peter I, 2023. – pp. 388-394.

5. Information security in the digital economy / T. G. Khetagurova, I. Y. Khetagurova, Z. V. Soskieva, M. G. Bagieva // Economics and management: problems, solutions. - 2023. – Vol. 5, No. 1(133). – pp. 128-132. – DOI 10.36871/ek.up.p.r.2023.01.05.016.

6. Karepova, S. G. Information security: the specifics of the phenomenon, methods and methods of its provision / S. G. Karepova, S. V. Nekrasov, A. N. Pinchuk // Bulletin of the Moscow University. Series 18. Sociology and Political Science. – 2023. – Vol. 29, No. 4. – pp. 200-220. – DOI 10.24290/1029-3736-2023-29-4-200-220.

7. Lobanova, V. A. Information security in the processing of personal data / V. A. Lobanova // Modern paradigms of sustainable development of regional socio-economic systems in conditions of increasing uncertainty of the external environment : Proceedings of the International Scientific and Practical Conference, Gatchina, April 21, 2023. – Gatchina: State Institute of Economics, Finance, Law and Technology, 2023. – pp. 425-429.

8. Manyakhina, Z. A. digitalization of the warehousing system at the enterprise / Z. A. Manyakhina, D. V. Cheremukhov, N. V. Krivonosova // Science, education, transport: topical issues, priorities, vectors of interaction : Materials of the II International Scientific and Methodological Conference. In 3 parts, Orenburg, November 08-09, 2023. Orenburg: Samara State University of Railway Engineering, 2023. – pp. 66-70.

9. Mugaeva, E. V. Digitalization of management processes at the enterprise / E. V. Mugaeva // The diary of Science. – 2023. – № 8(80). – DOI 10.51691/2541-8327_2023_8_3.

10. Nazarov, D. M. Analysis of the semantics of the concepts of economic security and information security in the digital economy / D. M. Nazarov, A.D. Nazarov // International Journal of Applied Sciences and Technologies Integral. – 2023. – No. 4.

11. Pogorelova, S. R. Information security: key threats and means of protection / S. R. Pogorelova, S. M. Petrosyan, V. I. Naidenkov // Problems and prospects of development of Russia: Youth perspective on the future : A collection of scientific articles of the 6th All-Russian Scientific Conference. In 3 volumes, Kursk, October 19-20, 2023 / Editorial Board: A.A. Gorokhov (editor-in-chief). Volume 2. – Kursk: Closed Joint Stock Company "University Book", 2023. – pp. 471-475.

12. Yarikov, V. G. Information security and information protection at the enterprise / V. G. Yarikov, M. V. Pashkov // NBI technologies. - 2023. – Vol. 17, No. 4. – pp. 47-51. – DOI 10.15688/NBIT.jvolsu.2023.4.6.