УДК 659

ПОНЯТИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИИ: ОСНОВНЫЕ ПОДХОДЫ И ПРАКТИЧЕСКИЕ АСПЕКТЫ

Е.В. Романовская, Н.С. Андряшина, А.В. Пенягин
Нижегородский государственный педагогический университет имени Козьмы Минина, Нижний Новгород, email: alenarom@list.ru

Аннотация. *Настоящая статья посвящена теоретическому осмыслению понятия информационной безопасности применительно к деятельности современного предприятия. Авторы исходят из того, что в условиях цифровой трансформации экономики и стремительного роста числа киберугроз обеспечение сохранности, целостности и доступности информационных активов становится не просто технической задачей, а стратегическим приоритетом любой организации. В работе анализируются нормативно-правовые основы определения информационной безопасности, закреплённые в российском законодательстве и международных стандартах. Рассматриваются ключевые свойства защищаемой информации – конфиденциальность, целостность и доступность, а также специфика их реализации в корпоративной среде. Отдельное внимание уделяется современным угрозам, среди которых особое место занимают внутренние инсайдерские риски, на долю которых, по данным исследований, приходится значительная часть инцидентов. На основе анализа статистических данных о масштабах утечек конфиденциальной информации в российской экономике в 2024–2025 годах делается вывод о том, что информационная безопасность предприятия представляет собой комплексную систему, объединяющую организационные, правовые, технические и кадровые компоненты, и требует постоянного совершенствования в ответ на изменяющийся ландшафт угроз.*

Ключевые слова: *информационная безопасность, предприятие, угрозы, утечки данных, конфиденциальность, система защиты информации.*

THE CONCEPT OF INFORMATION SECURITY IN AN ENTERPRISE: BASIC APPROACHES AND PRACTICAL ASPECTS

E.V. Romanovskaya, N.S. Andryashina, A.V. Penyagin
Minin Nizhny Novgorod State Pedagogical University, Nizhny Novgorod, email: alenarom@list.ru

Abstract. *This article is devoted to the theoretical understanding of the concept of information security in relation to the activities of a modern enterprise. The authors proceed from the fact that in the context of the digital transformation of the economy and the rapid growth of the number of cyber threats, ensuring the safety, integrity, and accessibility of information assets has become not just a technical task, but a strategic priority for any organization. The article analyzes the legal and regulatory framework for defining information security, which is established in Russian legislation and international standards. It examines the key properties of protected information, such as confidentiality, integrity, and accessibility, as well as the specifics of their implementation in a corporate environment. Special attention is paid to modern threats, among which internal insider risks occupy a special place, accounting for a significant portion of incidents, according to research. Based on the analysis of statistical data on the scale of confidential information leaks in the Russian economy in 2024-2025, it is concluded that enterprise information security is a complex system that combines organizational, legal, technical, and personnel components and requires continuous improvement in response to the changing threat landscape.*

Keywords: *information security, enterprise, threats, data leaks, confidentiality, information protection system.*

Дата поступления статьи в редакцию: 04.04.2026
Дата принятия статьи в печать: 18.05.2026

Введение

Современное предприятие невозможно представить без информации. Каждый день накапливаются тысячи файлов - это договоры с клиентами, счета, накладные, базы данных, переписка. Вся эта информация имеет ценность. Для одних компаний важнее всего клиентская база. Для других – технологические разработки. Для третьих – финансовая отчётность. Если эта

информация попадёт к конкурентам или злоумышленникам, компания может понести серьёзные убытки. В некоторых случаях утечка информации приводит к закрытию бизнеса. Поэтому защита информации стала одной из главных задач современного менеджмента.

Цифровая эпоха принесла с собой не только удобства, но и новые риски. Раньше важные бумаги хранились в сейфах под замком. Доступ к ним имел узкий круг людей. Сегодня информация разлетается за секунды. Она копируется на флешки, пересылается по электронной почте, загружается в облачные сервисы. Это сильно ускоряет работу. Но это же делает информацию уязвимой. Украсть или испортить электронные данные можно незаметно. Иногда даже не выходя из дома. Злоумышленники могут находиться за тысячи километров. И при этом нанести огромный ущерб.

Кроме того, изменился сам характер угроз. Раньше основными нарушителями считались хакеры-одиночки или конкуренты. Сегодня спектр угроз гораздо шире. Это и организованные преступные группы, которые специализируются на краже данных. Это и недобросовестные партнёры. Это и собственные сотрудники, которые могут ошибиться или действовать умышленно. Причём, как показывает статистика, внутренние угрозы встречаются не реже внешних. А иногда даже чаще. Об этом часто забывают руководители, вкладывая все средства в защиту от внешних атак.

Ещё одна проблема заключается в том, что информационная безопасность часто воспринимается как что-то второстепенное. Многие считают, что это дело IT-отдела. Или что это нужно только крупным корпорациям с секретными разработками. Это не так. Утечка данных может ударить по любому бизнесу. Будь то небольшой магазин, частная клиника или строительная фирма. Персональные данные клиентов, коммерческие предложения, внутренняя переписка – всё это может быть использовано во вред. Поэтому понимание основ информационной безопасности необходимо руководителям всех уровней [1].

Однако, многие руководители недостаточно хорошо понимают, что такое информационная безопасность. Они думают, что достаточно купить хороший антивирус и поставить сложный пароль. Это заблуждение. Информационная безопасность – это гораздо более широкое понятие. Она включает в себя не только технические средства, но и организационные меры, и работу с людьми. Без комплексного подхода любые вложения в безопасность будут малоэффективны. Именно поэтому вопрос о том, что же представляет собой понятие информационной безопасности на предприятии, требует детального теоретического разбора.

В данной статье мы постараемся рассмотреть суть этого понятия. Мы рассмотрим, из каких элементов складывается система защиты. Обсудим, какие угрозы сегодня наиболее опасны. И дадим практические советы, с чего начать выстраивание безопасности тем, у кого нет больших бюджетов.

Без комплексного подхода любые вложения в безопасность будут малоэффективны. Именно поэтому вопрос о том, что же представляет собой понятие информационной безопасности на предприятии, требует детального теоретического разбора.

Цель исследования

Цель исследования состоит в систематическом анализе понятия информационной безопасности предприятия. Для достижения этой цели решаются следующие задачи. Во-первых, уточняется содержание термина «информационная безопасность» применительно к предприятию. Во-вторых, детально раскрываются три базовых свойства защищаемой информации. В-третьих, анализируются современные угрозы с выделением внутренних и внешних источников. В-четвёртых, на основе статистических данных оцениваются масштабы проблемы в России. В-пятых, формулируются практические рекомендации по построению системы информационной безопасности для предприятий с ограниченными ресурсами.

Материалы и методы исследования

Для проведения данного исследования авторы обратились к нескольким типам источников. Прежде всего, это нормативные документы. Среди них можно назвать государственный стандарт Российской Федерации, в котором зафиксированы основные термины, используемые в области защиты информации. Помимо этого, был привлечён международный стандарт, регламентирующий требования к системам, которые управляют информационной безопасностью на предприятиях.

Вторую группу источников составила учебная и научная литература. В ходе работы изучались труды известных отечественных учёных, которые на протяжении долгого времени занимаются исследованием проблем, связанных с защитой информации. Их работы позволили сформировать теоретическую базу для анализа.

Третья группа источников представлена отчётами компаний, которые профессионально расследуют инциденты в сфере информационной безопасности. Речь идёт, прежде всего, о ежегодных глобальных исследованиях, посвящённых утечкам информации. Дополнительно использовались публикации в деловых средствах массовой информации. В них содержатся актуальные статистические данные за 2024 и 2025 годы, что позволило подкрепить теоретические рассуждения реальными цифрами.

Что касается методов исследования, то здесь применялись логический анализ, сравнительный метод, структурно-функциональный анализ, а также метод обобщения. С помощью логического анализа удалось выделить наиболее существенные признаки, характеризующие информационную безопасность. Сравнительный метод дал возможность сопоставить различные подходы к определению ключевых понятий, которые используются в этой области. Структурно-функциональный анализ помог выявить, как именно связаны между собой отдельные элементы системы защиты информации. Метод обобщения был использован на заключительном этапе, для формулирования выводов и практических рекомендаций на основе всего изученного материала.

Результаты исследования

Обратимся к определению информационной безопасности. Согласно государственному стандарту, под информационной безопасностью понимается состояние защищённости информации. При этом должны обеспечиваться три свойства. Это конфиденциальность, целостность и доступность. Каждое из этих свойств требует отдельного рассмотрения.

Начнём с конфиденциальности. Конфиденциальность означает, что информация доступна только тем лицам, которые имеют на это право. Все остальные не должны знать содержание информации. Нарушение конфиденциальности происходит, когда информация попадает к посторонним. Например, в банке хранятся сведения о счетах клиентов. Эти сведения имеют право видеть только сам клиент и сотрудники банка, которые ведут его счёт. Если хакер взломает базу данных и скачает сведения о счетах, конфиденциальность будет нарушена. Если сотрудник банка продаст базу данных мошенникам, это тоже нарушение конфиденциальности. Для многих предприятий конфиденциальность является самым важным свойством. Особенно это касается тех компаний, которые работают с персональными данными.

Целостность означает, что информация остаётся правильной и неизменной. Любые изменения должны вноситься только авторизованными лицами. И эти изменения должны быть задокументированы. Никто не должен иметь возможности незаметно подправить информацию. Нарушение целостности происходит, когда данные изменяются без разрешения. Например, в учётной системе предприятия хранятся суммы на счетах. Если злоумышленник проникнет в систему и увеличит сумму на своём счету, это нарушение целостности. Если вирус зашифрует файлы и изменит их содержимое, это тоже нарушение целостности. Для производственных предприятий целостность особенно важна. Если в технологической карте изменить дозировку компонента, продукция может стать опасной.

Наконец, доступность. Доступность означает, что информация может быть получена законными пользователями в нужное время. Если информация есть, но до неё нельзя добраться, она бесполезна. Нарушение доступности происходит, когда сервер выходит из строя, сеть подвергается атаке или файлы оказываются заблокированными. Пример. Интернет-магазин работает круглосуточно. Если сайт перестаёт открываться из-за хакерской атаки, клиенты не могут сделать заказ. Магазин теряет выручку. Это нарушение доступности. Для многих компаний доступность критически важна. Особенно для тех, кто работает в сфере электронной коммерции, банковских услуг, связи.

Три указанных свойства образуют классическую триаду информационной безопасности. Все три свойства равнозначны. Нельзя пренебрегать ни одним из них. В разных условиях на первый план выходят разные свойства. Для адвокатской конторы важнее всего конфиденциальность. Для завода, управляющего опасным производством, – целостность. Для интернет-магазина – доступность. Но идеальная система защиты должна обеспечивать все три свойства одновременно.

В последние годы специалисты добавляют к триаде дополнительные свойства. Одно из них – аутентичность. Аутентичность означает, что информация действительно исходит от того источника, от которого она якобы исходит. Это важно для борьбы с подделками и мошенничеством. Другое свойство – неотказуемость. Неотказуемость означает, что сторона, совершившая действие с информацией, не может впоследствии отказаться от этого действия. Это важно для электронного документооборота и судебных разбирательств. Третье дополнительное свойство — подотчётность. Подотчётность означает, что все действия с информацией могут быть отслежены. Известно, кто, когда и что сделал. Эти дополнительные свойства становятся всё более актуальными по мере цифровизации экономики.

Угрозы информационной безопасности можно разделить на две большие группы. Первая группа – внешние угрозы. Они исходят от лиц, не работающих на предприятии. Это хакеры, конкуренты, мошенники. Вторая группа – внутренние угрозы. Они исходят от сотрудников предприятия. Долгое время основное внимание уделялось внешним угрозам. Считалось, что главный враг – это хакер. Однако накопленная статистика показывает, что внутренние угрозы не менее опасны. А в некоторых отраслях даже более опасны.

Почему внутренние угрозы так опасны? Потому что сотрудник уже имеет доступ к информации. Ему не нужно взламывать систему. Он знает пароли, он знает, где что лежит. Он может действовать быстро и незаметно. Кроме того, сотрудник может навредить даже без злого умысла. Простая неосторожность может привести к утечке. Например, сотрудник переслал файл на личную почту, чтобы поработать дома. Его личная почта была взломана. Файл попал к злоумышленникам. Сотрудник не хотел навредить, но навредил.

По данным отчётов за 2024 год, в России произошло несколько сотен крупных утечек конфиденциальной информации. В большинстве случаев источником были сотрудники. Действующие сотрудники стали причиной примерно половины утечек. Уволенные сотрудники, которые сохранили доступ к системам, — ещё около трети. И только пятая часть утечек была вызвана действиями посторонних злоумышленников. Эти цифры убедительно показывают, что пренебрегать внутренними угрозами нельзя [2].

Рассмотрим, как распределяются утечки по отраслям. На первом месте находится розничная торговля. Почти 30% всех утечек приходится на магазины и торговые сети. В торговле обрабатываются огромные массивы персональных данных клиентов. Имена, адреса, номера телефонов, данные банковских карт. Эта информация очень ценится на чёрном рынке. Кроме того, в торговле высокая текучесть персонала. Сотрудники приходят и уходят. Не всегда успевают вовремя отключить учётные записи. Этим пользуются злоумышленники [4].

На втором месте находится здравоохранение. Больницы, поликлиники, частные медицинские центры. Здесь хранятся истории болезней, результаты анализов, сведения о здоровье. Это тоже очень чувствительная информация. Её утечка может нанести серьёзный вред пациентам. Кроме того, медицинские данные могут использоваться для шантажа или дискредитации.

Замыкает тройку лидеров по числу утечек финансовый сектор. Сюда входят банки, страховые организации и инвестиционные фонды. В этих учреждениях хранится огромное количество сведений о счетах клиентов, об их доходах и расходах. Если такая информация попадёт в чужие руки, последствия могут быть самыми прямыми — люди потеряют деньги, компании понесут убытки. Именно поэтому финансовые организации обычно тратят на информационную безопасность больше средств, чем представители многих других отраслей. Однако, как показывают статистические данные, даже крупные вложения не дают стопроцентной гарантии. Полностью защитить себя от утечек не удаётся никому [2].

Если говорить о том, как меняется ситуация с утечками в России, то здесь данные расходятся. Официальная статистика, которую публикует Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации, свидетельствует о снижении. В 2025 году было зарегистрировано 118 утечек персональных данных. Это на тринадцать процентов меньше, чем годом ранее. При этом объём утёкших персональных данных сократился ещё сильнее — на девяносто три процента, составив 52 миллиона строк. Тем не менее, проблема остаётся весьма острой [3].

Введение крупных штрафов за утечку персональных данных, безусловно, заставило бизнес относиться к вопросам защиты серьёзнее. Но, как показывают результаты опросов, многие компании до сих пор не обзавелись самыми базовыми инструментами безопасности. Речь идёт

о таких вещах, как чёткая политика в отношении паролей, прописанная процедура отключения доступа для уволенных сотрудников или заранее подготовленный план действий на случай инцидента. Отсутствие этих элементарных вещей говорит о том, что формальные требования закона далеко не всегда превращаются в реальные изменения внутри организаций.

Особенно сложная ситуация в малом бизнесе. У крупных компаний есть ресурсы: они могут нанять специалистов по безопасности, купить дорогое программное обеспечение, проводить регулярное обучение персонала. У малого бизнеса таких ресурсов нет. Владелец небольшой фирмы часто сам отвечает и за продажи, и за бухгалтерию, и за безопасность. У него нет времени разбираться в тонкостях защиты информации. Между тем, малый бизнес не менее уязвим, а иногда и более уязвим. Потому что у крупных компаний защита выстроена хотя бы на минимальном уровне. У малых её часто нет вообще [5].

Что может сделать малый бизнес? Специалисты рекомендуют начинать с простых и недорогих мер. Первая мера – инвентаризация информационных активов. Нужно составить список всей ценной информации. Где она хранится? Кто имеет к ней доступ? Насколько она важна для бизнеса? Без ответа на эти вопросы любые меры защиты будут случайными. Вторая мера – внедрение политики паролей. Пароли должны быть сложными. Их нельзя записывать на стикерах и клеить на монитор. Их нужно менять раз в несколько месяцев. Третья мера – ограничение доступа. Сотрудники должны иметь доступ только к той информации, которая нужна им для работы. Всё лишнее должно быть закрыто. Четвёртая мера – отключение учётных записей уволенных сотрудников. Это нужно делать в день увольнения. Пятая мера – регулярное резервное копирование. Если данные будут испорчены или зашифрованы вирусом, их можно восстановить из резервной копии. Всё это не требует больших затрат. Но эти меры закрывают большинство типовых уязвимостей.

Отдельного внимания заслуживает обучение персонала. Многие компании экономят на обучении. Считают, что это лишние траты. Это ошибка. Как показывают исследования, большинство успешных атак начинаются с ошибки сотрудника. Сотрудник перешёл по фишинговой ссылке. Сотрудник сообщил пароль по телефону. Сотрудник оставил компьютер без присмотра. Всех этих проблем можно избежать, если регулярно обучать людей. Обучение не должно быть скучным и формальным. Лучше всего работают короткие практические занятия. Раз в месяц можно рассылать памятки. Можно проводить тренировки: отправлять тестовые фишинговые письма и смотреть, кто на них клюнул. Тем, кто постоянно ошибается, назначать дополнительное обучение. Такая система стоит недорого, но даёт отличные результаты [6].

Есть и психологический аспект. Меры безопасности не должны восприниматься как шпионаж. Если сотрудники чувствуют, что за ними следят, они будут сопротивляться. Они будут находить способы обойти правила. Поэтому важно объяснять, зачем нужна безопасность. Нужно говорить сотрудникам, что защита информации защищает и их самих. Их личные данные тоже не попадут в чужие руки. Их зарплата не будет украдена. Компания не обанкротится, и они не потеряют работу. Когда люди понимают смысл правил, они начинают их соблюдать добровольно.

Хорошим ориентиром для построения системы информационной безопасности является международный стандарт. Он не предписывает конкретные технические решения. Вместо этого он описывает процесс. Процесс состоит из нескольких шагов. Шаг первый: определить, какая информация нуждается в защите. Шаг второй: оценить риски. Шаг третий: выбрать меры защиты. Шаг четвёртый: внедрить меры. Шаг пятый: регулярно проверять, как работает система. Шаг шестой: постоянно улучшать систему. Следуя этой логике, любое предприятие, даже с небольшим бюджетом, может выстроить эффективную защиту. Не нужно пытаться охватить всё сразу. Начните с самого ценного. Затем постепенно расширяйте систему.

Ущерб от нарушений информационной безопасности может быть огромным. При этом защита могла быть обеспечена простыми и недорогими средствами. Не нужно было покупать сложные системы за миллионы. Достаточно было соблюдать базовые правила.

Заключение

Проведённое исследование позволяет сделать несколько выводов.

Информационная безопасность предприятия – это комплексное понятие. Оно не сводится к установке антивируса или другого технического средства. Информационная безопасность включает в себя организационные меры, технические средства и работу с персоналом. Только при

сочетании всех трёх составляющих можно добиться надёжной защиты. Нельзя перекладывать ответственность на один отдел или на одну программу. Безопасность – это общая задача. Она требует участия и руководства, и рядовых сотрудников.

Основа информационной безопасности – три свойства информации - это конфиденциальность, целостность и доступность. Любая система защиты должна обеспечивать все три свойства. Пренебрежение любым из них ведёт к уязвимостям. Руководителю важно понимать, какое из свойств для его бизнеса наиболее критично. От этого зависит выбор приоритетных мер. Но забывать о двух других нельзя.

Основным источником угроз для большинства предприятий являются собственные сотрудники. Доля внутренних инцидентов составляет от шестидесяти до восьмидесяти процентов от общего числа утечек. При этом примерно две трети инцидентов носят непреднамеренный характер. Это означает, что эффективное обучение персонала может предотвратить большинство утечек. Ошибки людей неизбежны. Но их можно свести к минимуму. Для этого нужны регулярные тренировки, понятные инструкции и доброжелательная атмосфера. Сотрудник, который боится наказания, будет скрывать свои ошибки. А это только усугубит ситуацию.

Ситуация с утечками данных остаётся напряжённой. Ежегодно происходит несколько сотен крупных утечек. Наиболее уязвимыми секторами являются розничная торговля, здравоохранение и финансовые услуги. Это не значит, что другим отраслям можно расслабиться. Угрозы есть везде. Просто в перечисленных сферах информация особенно ценна и доступна. Кроме того, малый бизнес часто остаётся вне поля зрения аналитиков.

Даже при ограниченном бюджете можно выстроить эффективную систему защиты. Для этого необходимо начать с инвентаризации информационных активов. Затем внедрить базовые организационные меры: политику паролей, ограничение доступа, отключение учётных записей уволенных, резервное копирование. Параллельно организовать регулярное обучение персонала. Эти меры не требуют больших затрат, но закрывают большинство типовых уязвимостей. Не нужно гнаться за дорогими решениями. Часто простые вещи работают лучше.

Человеческий фактор остаётся самым слабым звеном в системе информационной безопасности. Но при правильной организации обучения и мотивации он может стать самым сильным. Сотрудники, которые понимают важность безопасности и обучены правильным действиям, способны предотвратить атаки, с которыми не справляются никакие технические средства. Поэтому инвестиции в обучение персонала – это, возможно, самые выгодные инвестиции в безопасность. Они окупаются многократно.

В заключение стоит добавить несколько общих замечаний. Информационная безопасность – это не разовое мероприятие. Нельзя один раз настроить всё и забыть. Угрозы постоянно меняются. Появляются новые виды вирусов, новые схемы обмана, новые уязвимости. То, что работало год назад, сегодня может быть бесполезно. Поэтому систему защиты нужно регулярно пересматривать и обновлять. Проводить аудиты, тестировать сотрудников, обновлять программы. Только так можно оставаться в безопасности.

Также важно понимать, что безопасность не должна быть самоцелью. Нельзя заблокировать всё и вся в ущерб работе. Слишком жёсткие ограничения приведут к тому, что сотрудники начнут их обходить. Нужно искать разумный баланс. Защита должна быть достаточной, но не избыточной. И она не должна мешать людям выполнять свою работу.

Руководитель играет ключевую роль в построении системы безопасности. Если он сам игнорирует правила, то и сотрудники будут их игнорировать. Если он относится к безопасности формально, то и вся система будет формальной. Личный пример и постоянное внимание к теме – вот что действительно меняет ситуацию. Когда сотрудники видят, что руководитель серьёзно относится к защите информации, они начинают относиться серьёзнее и сами.

Наконец, нельзя полагаться только на свои силы. Полезно обмениваться опытом с коллегами из других компаний. Участвовать в отраслевых мероприятиях. Читать отчёты аналитических центров. Подписываться на рассылки по информационной безопасности. Информация о новых угрозах распространяется быстро. И тот, кто узнаёт о них первым, получает преимущество.

Таким образом, информационная безопасность предприятия – это не статичное состояние, а непрерывный процесс. Процесс, в который вовлечены все – от директора до рядового сотрудника. И только при таком подходе можно быть уверенным, что информация компании находится под надёжной защитой.

Литература

1. Быльева Д.С. Цифровые моральные системы в симулированной и социальной реальности // Вестник Мининского университета. 2025. Т. 13, № 2(51). DOI: 10.26795/2307-1281-2025-13-2-15 EDN: VGAYUK.

2. Грачев В.И., Гарин А.П. Предпосылки к научно-техническому развитию промышленного предприятия: реализация процессного подхода и моделей системы менеджмента качества // Промышленное развитие России: проблемы, перспективы: Сборник статей по материалам XXII Международной научно-практической конференции преподавателей вузов, ученых, специалистов, аспирантов, студентов, Нижний Новгород, 07 ноября 2024 года. Нижний Новгород: Нижегородский государственный педагогический университет им. К. Минина, 2024. С. 21-23. EDN BKMAXM.

3. Полянская В.А., Романова Ю.В., Пермовский А.А. Национальный проект "Экономика данных и цифровая трансформация государства": перспектива для промышленных предприятий // Modern Economy Success. 2025. № 5. С. 392-398. EDN: YKYPOQ.

4. Полянская В.А., Кузнецов В.П. Цифровая экономика: ключевые тренды для промышленных предприятий: монография. Нижний Новгород: Нижегородский государственный педагогический университет им. К. Минина, 2025. 108 с. ISBN: 978-5-85219-992-8 EDN: YDWBDU.

5. Гарин А.П., Ясынова С.Ф., Назарова Е.Н., Шеленина О.В. Современная дефиниция понятия "конкурентоспособность компаний" и факторы, её определяющие // Экономика и предпринимательство. 2025. № 2(175). С. 888-891. DOI: 10.34925/EIP.2025.175.2.160 EDN: INENBD.

6. Шустова К.В., Назарова Е.Н. Цифровой рубль и трансформация платежных систем: влияние на финансовую отчетность организаций // Экономическое развитие России: тенденции, перспективы: Сборник статей по материалам XI Международной научно-практической конференции преподавателей вузов, ученых, специалистов, аспирантов, студентов. В 2-х томах, Нижний Новгород, 24 апреля 2025 года. Нижний Новгород: Мининский университет, 2025. С. 170-174.