Информационные потери: понятие, отражение в бухгалтерском учете

Information losses: concept and reflection in accounting

УДК 332.012
Получено: 19.12.2025 Одобрено: 22.01.2026 Опубликовано: 25.02.2026

Голова Е.Е.
Канд. экон. наук, доцент, ФГБОУ ВО «Омский государственный аграрный университет имени П.А. Столыпина», г. Омск
e-mail: ee.golova@omgau.org

Golova E.E.
Candidate of Economic Sciences, Associate Professor, Omsk State Agrarian University named after P.A. Stolypin, Omsk
e-mail: ee.golova@omgau.org

Аннотация
Вопросы информационной безопасности в последние годы приобретают все большую значимость для национальной безопасности страны. Цифровые технологии позволили существенно повысить качество жизни, появилось множество цифровых платформ, расширяющих возможности населения и предпринимателей, укрепляется технологический суверенитет, но возможности несут в себе одновременно угрозы. Современный этап развития характеризуется возрастающей ролью информационной среды, что заставляет задумываться не только о том, как использовать информацию, но и как отражать ее в учете. В мире, где информация становится новой валютой, а ее хищение новой угрозой, необходимо уметь оценивать потери. На основе проведенного анализа предложено определение понятия «информационные потери», что позволило сформировать мнение о необходимости совершенствования нормативно-правового регулирования на всех его уровнях, что могло бы помочь решить возрастающую потребность противодействию хищению информации, а также формированию информационно-правовой культуры и цифровой грамотности. Также в статье проведен анализ незаконного распространения информации в РФ за 2023-2024 гг. Практическая значимость данного исследования заключается в возможности формирования единых требований в информационной среде в части потерь информации и ее защиты. Результаты исследования могут быть использованы предприятиями для формирования понятийного аппарата в области информационной безопасности и порядка ее отражения в бухгалтерском учёте.
Ключевые слова: бухгалтерский учет, экономика, информация, цифровизация, потери, ущерб, нормативное регулирование.

Abstract
Information security issues have become increasingly important for national security in recent years. Digital technologies have significantly improved the quality of life, numerous digital platforms have emerged that empower individuals and businesses, and technological sovereignty is being strengthened. However, these opportunities also carry threats. The current stage of development is characterized by the growing role of the information environment, necessitating consideration not only of how to use information but also how to reflect it in accounting. In a world where information is becoming the new currency, and its theft a new threat, it is essential to be able to assess losses.

Based on the analysis, a definition of "information loss" has been proposed, which has led to a view on the need to improve legal regulation at all levels. This could help address the growing need to combat information theft, as well as foster information and legal culture and digital literacy. The article also analyzes the illegal dissemination of information in the Russian Federation for 2023-2024. The practical significance of this study lies in the possibility of developing uniform requirements in the information environment regarding information loss and its protection. The results of the study can be used by enterprises to develop a conceptual framework in the field of information security and the procedure for its reflection in accounting.
Keywords: accounting, economics, information, digitalization, losses, damage, regulatory framework.

Введение

В 21 веке информация становится самой желанной валютой. От того, кто владеет актуальной и полезной информацией зависит эффективность деятельности. Цифровизация является одним из приоритетных направлений, которое ставит перед собой государство, и это утверждение справедливо не только для России, но и для многих других государств. Цифровые процессы оказывают влияние не только на бизнес, но и на жизнь простых людей, что открывает новые возможности, улучшает качество жизни, повышает эффективность всех бизнес-идей, но одновременно несет в себе и множество рисков, среди которых хищение информации. Кража данных в настоящее время является актуальной проблемой для всего мирового сообщества, а не только для конкретных государств или предприятий. Злоумышленники стремятся получить конфиденциальную информацию, персональные данные, что становится объектом пристального внимания государства. Именно поэтому в Стратегии национальной безопасности Российской Федерации (Указ Президента РФ от 02.07.2021 № 400) приоритетами обозначено развитие безопасного информационного пространства и обеспечение информационной безопасности. В этой связи актуальным вопросом становится тот факт, что предприятия порой несут существенные финансовые потери, возникает необходимость отражать это в бухгалтерском учете, но в настоящий момент не существует сформированного понятийного аппарата, нормативное регулирование находится в стадии развития цифровых принципов общения и возникающих в информационном пространстве угроз, это предопределяет актуальность исследования.

Бухгалтерский учет информационных потерь лишь формируется, многие термины нуждаются в четких трактовках, а система бухгалтерского учета оценки конфиденциальной информации еще не сформирована. В этой связи становится очевидным, что в условиях информационного общества и повсеместной цифровизации требуется решение правовых вопросов, связанных с порядком отражения в бухгалтерском учете потерь от хищения конфиденциальной информации, что обуславливает необходимость научного осмысления этого вопроса [1].

Вопросами изучения понятия конфиденциальности в бухгалтерском учете, ее безопасности и особенностей отражения в учете занимались такие ученные как: Глухов Н.И., Наседкин П.Н., Милько Д.С. [2], Винтайкина Д.А., Астанаева Ю.Р. [3], Сотникова В.А., Ивченко М.А. [4], Москаленко Е.А., Ветрова А.Д. [5], Бондарь А.С., Дайнеко Д.Ф. [6], Бабаева З.Ш., Гаджимагомедова А.Г. [7], Сунгатуллина З.А. [8], Кизилов А.Н., Кюсева М.С. [9], Гранкова А.Н., Кузьмина И.А. [10], Кузьмина И.А. [11], Токмакова Е.Г., Юхтанова Ю.А., Скипин Д.Л. [12], Мишучкова Ю.Г., Коське М.С., Воюцкая И.В. [13], Секирина Н.В. [14], Башкатов В.В., Литун В.Е., Вендина О.Д. [15] и мн. др.

Несмотря на широкий спектр научных публикаций по изучаемому вопросу, понятийный аппарат относительно информационных потерь еще находится в стадии формирования и нуждается в точных трактовках.

Цель статьи – разработка теоретических подходов к определению информационных потерь в бухгалтерском учете и практических рекомендаций по вопросам ее отражения на счетах бухгалтерского учета.

В качестве основных **методов исследования** использовались: метод сравнения, метод графического и табличного представления данных, логический метод, методы статистического анализа, сопоставление и обобщение.

Объектом исследования выступает учетно-аналитическое обеспечение бухгалтерского учета организаций всех форм собственности, осуществляющих свою деятельность в условиях цифровизации.

Научная новизна статьи состоит **в** совершенствовании понятийного аппарата в отношении информационных потерь и особенностей отражения данного понятия на счетах бухгалтерского учета.

Основные результаты исследования

Говоря о хищениях информации важно рассмотреть аналитические данные, подтверждающие значимость и распространённость этой проблемы в нашей стране. По данным экспертно-аналитического центра InfoWatch, которое специализируется на сборе и анализе данных в сфере информационной безопасности за 2024 г. было зафиксировано 778 случаев утечки информации в российских предприятиях (оцениваются персональные данные и платежная информация) (рис. 1).

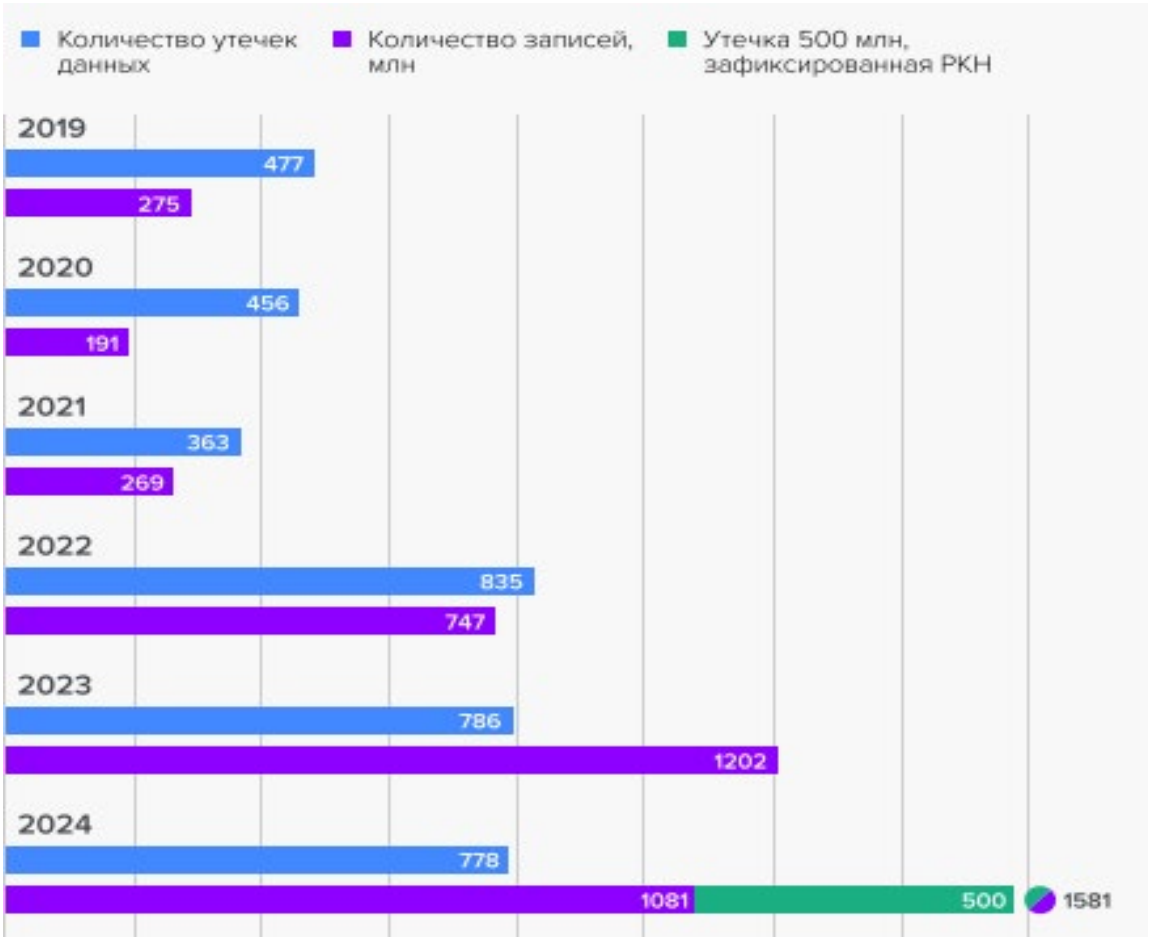

Рис. 1. Динамика утечки информации за 2019-2024 гг. в РФ
Источник: составлено по данным [17]

Как видно из рис. 1, с 2019 г. рост утечки информации растет, но, начиная с 2023 г. утечка данных практически не изменилась, а количество похищенных записей стало даже меньше на 121 случай. Важной деталью является анализ структуры похищенной информации (рис. 2).

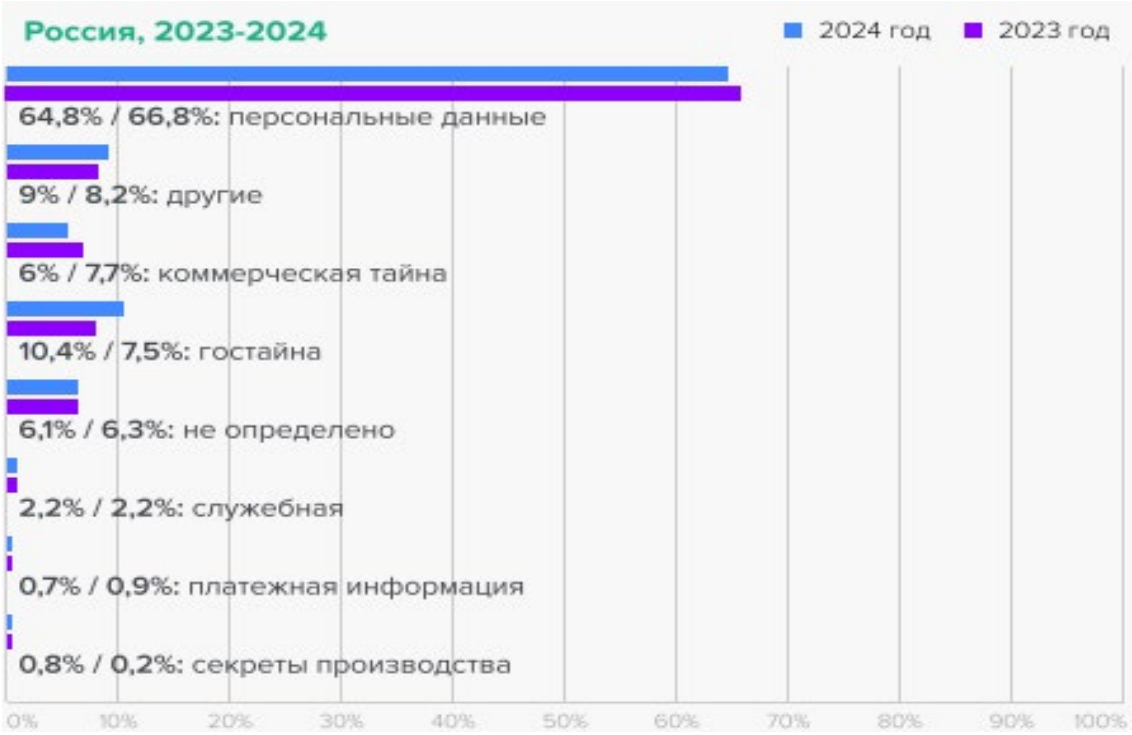

Рис. 2. Распределение утечек информации по типам скомпрометированных данных в России, 2023-2024 гг.
Источник: составлено по данным [17]

Анализируя распределение утечки информации по видам, можно отметить преобладание хищение персональных данных, в 2024 г. - 64,8%. Вторым по объему утечки информации стала государственная тайна (10,4%), что обусловлено попытками со стороны враждебно настроенных государств похитить информацию посредством вербовки российских граждан. Третье место в 2024 г. заняла прочая информация (9%). При этом, более 98% всех случившихся инцидентов по-прежнему носят умышленный характер (рис. 3).

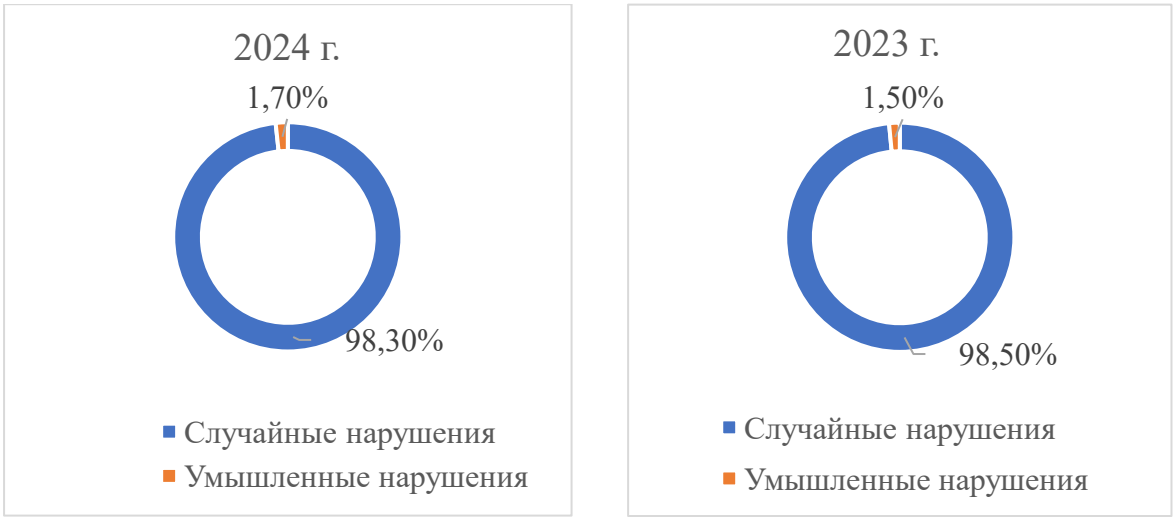

Рис. 3. Распределение утечек информации по умыслу в Россия в 2023-2024 гг.
Источник: составлено по данным [17]

Говоря об утечке информации, важно отметить, что злоумышленников интересует конфиденциальная информация, а не те данные, что можно найти в открытом доступе, например, выложенная в открытых источниках отчетность.

Понятие конфиденциальности дается в Федеральном законе Российской Федерации от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите

информации», которое трактует ее как обязательное требование, которое должно выполнять лицо, получившее доступ к определённой информации, суть которого заключается в том, чтобы не передавать эту информацию третьим лицам без получения согласия обладателя этой информации [18].

Федеральным законом от 29.07.2004 г. № 98-ФЗ «О коммерческой тайне» дается определение коммерческой тайны, что тоже формирует понятийный аппарат ограниченного доступа к информации. Коммерческая тайна, согласно данному закону, рассматривается как конфиденциальный режим по отношению к информации, что может дать возможность обладателю получить доходы, избежать расходов, укрепиться на рынке товаров или иную выгоду. Отдельно дается определение информации, составляющей коммерческую тайну, которая определена как любые сведения, имеющие ценность, поскольку неизвестны другим лицам, а у последних нет к ней доступа в силу закона, так как к ним применимо понятие коммерческой тайны [19]. В настоящее время около тридцати законов регулируют вопросы секретности (конфиденциальности) информации.

Важно определиться, что же относится к коммерческой тайне, так ч. 11 ст. 13 Федерального закона № 402-ФЗ «О бухгалтерском учете» говорит, что отчетность не является более коммерческой тайной.

Специалисты сайта БУХ 1С отмечают, что информацию, не подлежащую разглашению, можно поделить на несколько групп. Первая группа определяется, по сути, трактовкой из Закона «О коммерческой тайне». Здесь оговаривается, что при принятии на работу бухгалтера с ним надо подписать документ о неразглашении информации, где будет оговорен перечень и предупредить о мерах ответственности. Вторая группа секретной информации – это персональные данные физических лиц, что оговорено в Федеральном законе от 27.07.2006 №152-ФЗ «О персональных данных», аналогично первой группе бухгалтер должен быть ознакомлен под роспись о неразглашении этой информации. Третья группа сведений относится к государственной тайне, что регулируется Законом РФ «О государственной тайне» от 21.07.1993 № 5485-1. При работе с такой категорией информации работодатель должен сначала взять анкету от претендента на работу с такими данными, оформить согласие на работу с гостайной, кроме того, надо пройти медкомиссию, которая должна исключить психические отклонения. Эти документы должны быть направлены в ФСБ РФ и только после выдачи согласия бухгалтер может работать с такой категорией информации.

Согласно Закону о коммерческой тайне, бухгалтер не имеет право распространять информацию о секретах производства и производственных процессах, различные расчеты и показатели, техдокументацию, данные о зарплате, интеллектуальной деятельности, контрагентах предприятия, порядке ценообразования и ценовой политике и т.д. [20].

Именно конфиденциальность является целью злоумышленников, поэтому важным моментом является понятийная точность такого термина, как информационные потери, что, по сути, означает хищение информации, но и тут важным уточнением является осознанно это сделано или нет. В законах предпринята попытка определить информационные потери, но используются для этого разные термины, которые означают утрату информации.

Важным уточнением является разделение понятий данных и информации. Специалисты Getguru определяют данные как сырье, необработанные факты, например, таблица с цифрами является данными, а вот информация – это уже обработанная и структурированная подача данных, то, что придаёт смысл данным и делает их пригодными для принятия решений, описания тенденций, понимания сложных ситуаций, создания новых знаний [21].

В Федеральном законе № 149-ФЗ «Об информации, информационных технологиях и о защите информации» даётся понятие информации, а также ее конфиденциальности, предоставление информации (передача информации другим лицам), распространение информации (тоже самое что и предоставление, но круг лиц не определён), но понятие информационные потери не указано в списке терминов [22].

В Национальном стандарте РФ ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» много внимания уделено трактовке защиты информации, она делится на техническую, правовую, физическую. Сами термины разделены на группу по видам защиты информации, но понятие информационные потери не определены [23].

Банком России в Рекомендациях в сфере стандартизации Банка РФ «Обеспечение информационной безопасности организаций банковской системы РФ» определены такие понятия, как защита информации от утечки, распространение информации (действия, направленные на получение информации неопределенными лицами), предоставление информации (действия, направленные на получение информации определённым лицам), информация конфиденциального характера, доступ к ней, но информационные потери не рассмотрены [24].

Существуют авторские трактовки понятия информационные потери. Так, на сайте Рувики дано два определения информационных потерь:

1. повреждение/потеря данных в результате умышленных/случайных действий;
2. ошибка в информационной системе, когда информация уничтожается в результате сбоя, неосторожности [25].

Специалисты сайта anti-malware дают определение потери данных как повреждение информации / утрата в результате преднамеренных или непреднамеренных действий [26].

Специалисты компании Solar используют термин утечки данных и делят ее на преднамеренную и непреднамеренную, в связи с чем рассматривают умышленное создание условий для утечки или прямое хищение данных [27].

Потери в плане счетов отражают на счете 28 «Брак в производстве», но информационные потери не являются браком, что делает данный счет непригодным для отражения на нем потерь информации и данных. Счет 94 «Недостачи и потери от порчи ценностей» своим названием предполагает отражение потерь от порчи ценностей, а не информационных. НК РФ не содержит трактовки информационных потерь.

Токмакова Е.Г., Юхтанова Ю.А., Скипин Д.Л. считают, что надо открыть отдельный счет 93 «Потери», который будет отражать потери как уменьшение экономических выгод. Счет будет бессальдовым, записи будут формироваться по аналогии с счетом 94 «Недостачи и потери от порчи ценностей», иметь субсчета: 93.1 — потери при уплате штрафов, пенни, неустоек, 93.2 — потери от брака, 93.3 — потери от простоев, 93.4 — потери при недостачах сверх норм естественной убыли, 93.5 — потери от списания дебиторской задолженности по истечении срока исковой давности, 93.7 — прочие потери [12].

Изучение мнений различных специалистов показало, что как такового понятия информационных потерь нету, что обуславливает необходимость уточнения этого понятия в целях оценки в бухгалтерском учете (рис. 4).

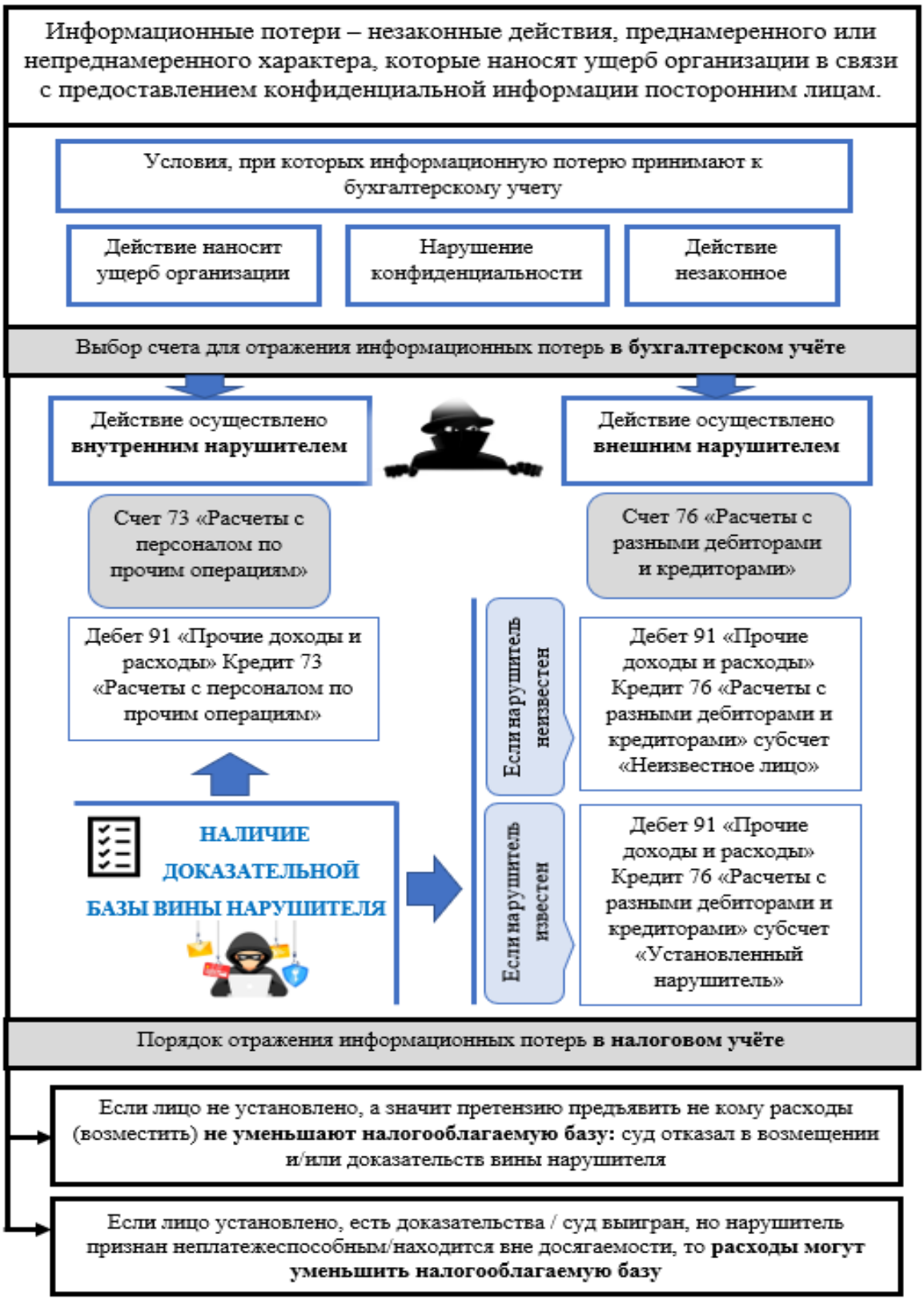

Рис. 4. Понимание информационных потерь и их отражение в учете
Источник: составлено автором

В основу данного понятия, по мнению автора, необходимо положить принципы законности, конфиденциальности, ущерба и получения выгоды (если это преднамеренное действие). Автор считает, что информационные потери можно разделить на умышленные и непреднамеренные, что может лечь в основу отражения на счетах бухгалтерского учёта.

Преднамеренные действия связаны с незаконными действиями третьих лиц и могут быть отнесены на счета прочих доходов и расходов. Автор считает, что потери, связанные с ошибками и непреднамеренными действиями, и не имеющие доказательств вины в этом третьих лиц, не должны уменьшать расходы в целях налогообложения налога на прибыль, а действия третьих лиц, которые привели к информационным потерям и имеющие доказательства, могут быть включены в НК РФ в перечень расходов, уменьшающих налогооблагаемую прибыль. Автор считает возможным отражение информационных потерь без открытия новых счетов, а потери отражать в зависимости от вида нарушителя. Внутренним нарушителем признается лицо, работающее в организации, внешним нарушителем признается постороннее лицо, не работающее на предприятии и вероятно даже незнакомое. Авторское понятие информационных потерь базируется на принципах соблюдения законности и конфиденциальности, отсутствия ущерба. Если данные принципы были нарушены, то информационную потерю можно признать как объект учета. В бухгалтерском учете в случае установления нарушителя как внутреннего расчета с ним можно осуществлять на счете 73 «Расчеты с персоналом по прочим операциям», открыв субсчет «Расчеты по информационным потерям или претензиям», если предприятие решит не переносить вину на такого нарушителя, то и расходы в налоговом учете не могут быть признаны в целях налогообложения налога на прибыль. Если же лицо установлено и это внешний нарушитель, то расчеты можно производить на счете 76 «Расчеты с разными дебиторами и кредиторами» субсчет «Расчеты по претензиям» можно открыть субсчет второго порядка «Расчеты с установленным/неустановленным нарушителем». Безусловно, для обоснования наличия вины предприятие должно предъявить достаточные доказательства, что важно не только для открытия дела в правоохранительных органах или в суде, но и для бухгалтерского учета. Если же внешний нарушитель находится вне досягаемости, например, скрылся в неизвестном направлении или имеются доказательства его смерти, то расходы, по мнению автора, могут уменьшать налогооблагаемую прибыль.

Авторский порядок оценки может быть возможен лишь при условии внесения соответствующих правок в нормативные документы РФ на всех уровнях регулирования (четырехуровневая система нормативного регулирования). Вносить изменения необходимо начинать с первого уровня и до четвертого, последовательно (рис. 5).

Так, на первом уровне необходимо вписать понятие информационных потерь в законы РФ как объект учета, а также прописать в НК РФ возможность включить при наличии доказательной базы в состав прочих расходов информационные потери.

На втором уровне нормативного регулирования по аналогии с НК РФ, но уже в целях бухгалтерского учёта в состав прочих расходов целесообразно было бы включить расходы на информационные потери. Другим, более оптимальным вариантом была бы разработка отдельного стандарта по учету информации, поскольку в современном мире информация становится наряду с остальными активами и обязательствами ценным источником получения дохода или формирования убытков. В настоящее время это могло бы быть отражено в ПБУ 10 «Расходы организации», но с 2027 г. станет обязательным его прототип ФСБУ 10/25 «Расходы».

На третьем уровне нормативного регулирования в качестве пояснений к стандарту можно было бы разработать какие-либо рекомендации, указания по оценке информационных потерь, их документальному отражению в учете.

На четвёртом уровне регулирования необходимо все важные для предприятия моменты отразить в учетной политике.

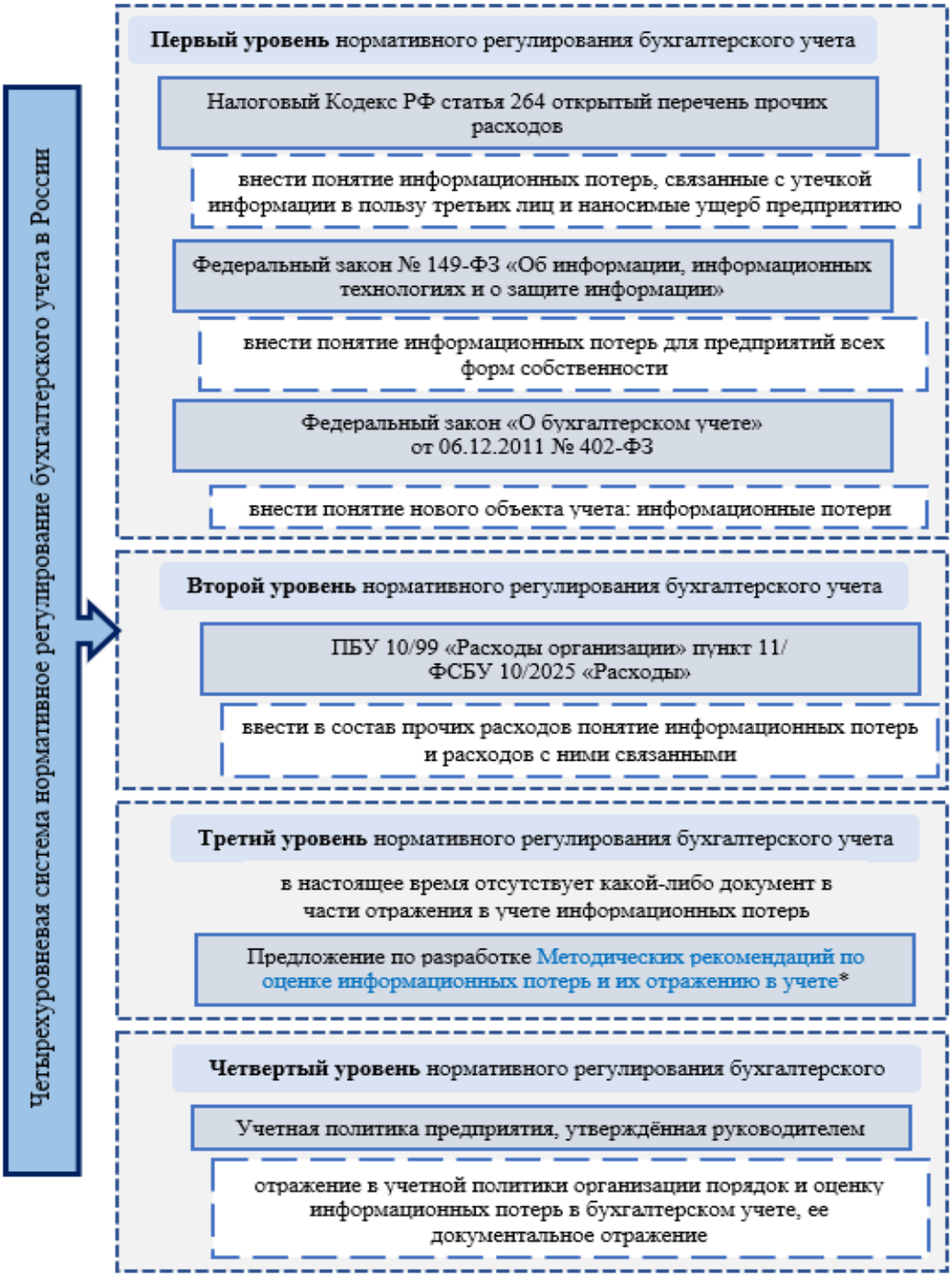

Рис. 5. Понимание информационных потерь и их отражение в учете
Источник: составлено автором

Внесение поправок и уточнений в нормативные документы является обязательным этапом для формирования нового объекта учета, но, по мнению автора, важным, поскольку информация становится наряду с денежными средствами основным ресурсом в экономической среде. Без законодательной основы эти понятия будут размыты и не будут иметь единого методического обеспечения, что позволит повысить качество учёта и отчетности.

Выводы. В современном мире спрос на информацию и ее качество растет, она является важным элементом учета и отчетности, однако, вместе с цифровизацией растёт число мошеннических схем по хищению информации и использовании ее в преступных целях, как

против физических, лиц, так и против предприятий и страны в целом. В этой связи информация может выступать как оружие и наносить ущерб другим организациям, что обуславливает необходимость учета потерь и их отражения в учете предприятия.

Литература

1. Голова Е.Е., Баетова Д.Р. Финансовая инклюзия в условиях цифровизации: состояние и перспективы // Фундаментальные исследования. 2022. № 10-1. С. 42-47.
2. Глухов Н.И., Наседкин П.Н., Милько Д.С. Онтологическая модель управления информационными потоками на предприятии с учетом уровней конфиденциальности // Информационные технологии и математическое моделирование в управлении сложными системами. 2021. № 3 (11). С. 59-66.
3. Винтайкина Д.А., Астанаева Ю.Р. Сравнительный анализ учета конфиденциальности информации // Научно-исследовательский центр "Technical Innovations". 2021. № 2. С. 38-43.
4. Сотникова В.А., Ивченко М.А. Механизм защиты учетно-аналитической информации на современном этапе // Учет, анализ и аудит: проблемы теории и практики. 2023. № 31. С. 163-168.
5. Москаленко Е.А. Безопасность данных в информационных системах бухгалтерского учета / Е.А. Москаленко, А.Д. Ветрова // Транспорт. Экономика. Социальная сфера (Актуальные проблемы и их решения): Сборник статей XII Международной научно-практической конференции, Пенза, 16–17 апреля 2025 года. – Пенза: Пензенский государственный аграрный университет, 2025. – С. 396-399. – EDN EIZTKN.
6. Бондарь А.С. Современные подходы к защите коммерческой тайны средствами бухгалтерского учета / А.С. Бондарь, Д.Ф. Дайнеко // Учетно-аналитическое и правовое обеспечение экономической безопасности организации: Сборник научных статей VII Всероссийской студенческой научно-практической конференции. В 3-х томах, Воронеж, 26 апреля 2025 года. – Воронеж: Воронежский государственный университет, 2025. – С. 152-156. – EDN JCDJXR.
7. Бабаева З.Ш., Гаджимагомедова А.Г. Обеспечение экономической безопасности предприятия при организации бухгалтерского учета// Журнал монетарной экономики и менеджмента. 2024. № 12. С. 30-40.
8. Сунгатуллина, З.А. Информационная безопасность в бухгалтерском учете / З. А. Сунгатуллина // Актуальные проблемы финансирования и налогообложения АПК в условиях глобализации экономики: Сборник статей XII Всероссийской научно-практической конференции, Пенза, 20–21 марта 2025 года. – Пенза: Пензенский государственный аграрный университет, 2025. – С. 153-157. – EDN ADAJJQ.
9. Кизилов А.Н. Защита учетной информации в условиях аутсорсинга с использованием информационно-коммуникационных технологий / А.Н. Кизилов, М.С. Кюсева // Дни Российской науки: сборник статей Всероссийской научно-практической конференции, Пенза, 07 февраля 2025 года. – Пенза: Наука и Просвещение (ИП Гуляев Г.Ю.), 2025. – С. 93-96. – EDN HYZDUY.
10. Гранкова АН. Обеспечение информационной безопасности при ведении бухгалтерского учета / А.Н. Гранкова, И.А. Кузьмина // Человек: преступление и наказание: Сборник материалов Международной научно-теоретической конференции адъюнктов, аспирантов, соискателей, курсантов и студентов. В 3-х частях, Рязань, 27 марта 2020 года. Том Часть 2. – Рязань: Академия права и управления Федеральной службы исполнения наказаний, 2020. – С. 79-86. – EDN WDJABS.
11. Кузьмина И.А. Угрозы информационной безопасности бухгалтерских данных и пути их устранения // Экономика и предпринимательство. 2020. № 5(118). С. 1137-1140. DOI 10.34925/EIP.2020.118.5.237.
12. Токмакова Е.Г. Формирование информации о потерях хозяйствующего субъекта в бухгалтерском учете для обеспечения его экономической безопасности / Е.Г. Токмакова,

Ю. А. Юхтанова, Д. Л. Скипин // Учет. Анализ. Аудит. 2020. Т. 7, № 1. С. 49-57. DOI 10.26794/2408-9303-2019-7-1-49-57.
13. Мишучкова Ю.Г. Профессиональный контроль над рисками бухгалтерской (финансовой) отчетности в контексте экономической безопасности / Ю.Г. Мишучкова, М. С. Коське, И.В. Воюцкая // Вестник Московского гуманитарно-экономического института. 2022. № 4. С. 239-256. DOI 10.37691/2311-5351-2022-0-4-239-256.
14. Секирина Н.В. Порядок защиты коммерческой тайны, содержащейся в первичных документах строительных организаций: пути совершенствования // Бухучет в строительных организациях. 2024. № 4. С. 14-22.
15. Башкатов В.В. Кибербезопасность в бухгалтерии: важность защиты конфиденциальной информации от кибератак и способы её обеспечения / В.В. Башкатов, В.Е. Литун, О.Д. Вендина // Вестник Алтайской академии экономики и права. 2024. № 6-2. С. 206-213. DOI 10.17513/vaael.3520.
16. Голова Е.Е. Роль анализа бухгалтерской отчетности в анализе финансовых результатов / Е.Е. Голова, С.И. Гражданцев // Электронный научно-методический журнал Омского ГАУ. 2020. № 4(23). С. 12.
17. Утечки информации в России: отчет за прошедший год // InfoWatch. URL: https://www.infowatch.ru/analytics/analitika/utechki-informatsii-v-rossii-otchet-za-proshedshiy-god (дата обращения 10.01.2026)
18. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Справочно-правовая система «КонсультантПлюс» [Электронный ресурс]. URL: https://base.garant.ru/12148555/ (дата обращения 10.01.2026)
19. Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне» // Справочно-правовая система «КонсультантПлюс» [Электронный ресурс]. URL: https://base.garant.ru/12136454/ (дата обращения 10.01.2026)
20. Секретные материалы: какие сведения не может разглашать бухгалтерия // БУХ 1С: для современного бухгалтера. URL: https://buh.ru/articles/sekretnye-materialy-kakie-svedeniya-ne-mozhet-razglashat-bukhgalteriya-.html (дата обращения 11.01.2026)
21. Данные против Информации: В чем разница? / Getguru. URL: https://www.getguru.com/ru/reference/what-is-data-vs-information (дата обращения 11.01.2026)
22. Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Справочно-правовая система «Гарант» [Электронный ресурс]. URL: https://base.garant.ru/12148555/741609f9002bd54a24e5c49cb5af953b/ (дата обращения 11.01.2026)
23. Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. N 373-ст) // Справочно-правовая система «Гарант». URL: https://base.garant.ru/193664/ (дата обращения 11.01.2026)
24. Рекомендации в области стандартизации банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» // CBR.ru. URL: https://cbr.ru/statichtml/file/59420/rs-29-16.pdf (дата обращения 11.01.2026)
25. Потеря данных // РУВИКИ: интернет-энциклопедия. URL: https://ru.ruwiki.ru/wiki/%D0%9F%D0%BE%D1%82%D0%B5%D1%80%D1%8F_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85 (дата обращения 11.01.2026)
26. Потеря данных (Data Loss) // anti-malware. URL: https://www.anti-malware.ru/threats/data-loss (дата обращения 11.01.2026)
27. Защита от утечек данных // Solar Dozor. URL: https://rt-solar.ru/products/solar_dozor/blog/2587/ (дата обращения 11.01.2026)