Документальное отражение в бухгалтерском учете коммерческих организаций информации об утечке информации

Documentary reflection of information leakage in the accounting records of commercial organizations

УДК 332.012
Получено: 20.02.2026 Одобрено: 23.03.2026 Опубликовано: 25.04.2026

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
В условиях стремительной цифровизации и постоянном обмене информацией между экономическими субъектами появляются угрозы безопасности информации, где одним из ключевых этапов обеспечения защиты информации является обоснованность понесённого ущерба в результате негативных воздействий со стороны мошенников. Статья посвящена исследованию вопросов документального оформления информационных потерь в целях бухгалтерского учета в условиях дестабилизирующих воздействий угроз безопасности информации. В работе использовались общенаучные методы исследования, а также методы бухгалтерского учета (двойная запись, документирование). Представлена авторская последовательность отражения информации об информационном ущербе в системе бухгалтерского учета, и разработан авторский регистр учета, который позволит формировать информация об ущербе в результате информационных потерь и отражать ее в учете. Предложенные мероприятия являются элементами механизма управления информационной безопасностью организаций. Практическая значимость данного исследования заключается в возможности использовать авторские результаты в учетно-аналитической работе предприятий, а также для дальнейших научных исследований в области информационной и экономической безопасности.
Ключевые слова: бухгалтерский учет, документы, утечка данных, информация, экономическая безопасность.

Abstract
In the context of rapid digitalization and the constant exchange of information between economic entities, threats to information security are emerging. One of the key stages of ensuring information security is the justification of damage incurred as a result of negative impacts from fraudsters. This article examines the documentation of information losses for accounting purposes in the face of the destabilizing effects of information security threats. General scientific research methods, as well as accounting techniques (double entry, documentation), were used in the study. The author presents a sequence for reflecting information on information losses in the accounting system and

develops an accounting register that will enable the compilation of information on damage resulting from information losses and its reflection in accounting. The proposed measures are elements of an organizational information security management mechanism. The practical significance of this study lies in the potential use of the author's results in the accounting and analytical work of enterprises, as well as for further scientific research in the field of information and economic security.
Keywords: accounting, documents, data leakage, information, economic security.

Введение

Информация в современном мире стала аналогом валюты, ее ценность неоспорима и повышается с каждым днем. Знаменитая фраза о том, кто владеет информацией – владеет миром становится уже не просто крылатым выражением, а отражает экономические законы современного мира. Информация окружает человека везде, любая коммуникация невозможна без современных средств передачи данных: гаджетов, социальных сетей, навигаторов и иных информационных устройств, с помощью которых люди обмениваются информацией. Вместе с тем недобросовестные пользователи пользуются достижениями прогресса и используют информационные носители для похищения данных, их продажи, распространения, фальсификации. Утечка информации стала настоящей проблемой в современном мире, что создает угрозы не только для обычных людей, но и для экономического сообщества. Отдельные предприятия несут большие убытки из-за хищения данных своих клиентов, распространения фейковой информации в сети и многих других незаконных действий мошенников. В этой связи возникает необходимость отражения в учете потерь об утечке информации, чтобы оценить убытки, если таковая ситуация сложилась у экономического субъекта. Это обуславливает актуальность темы исследования и подчеркивает необходимость всестороннего изучения вопросов информационной безопасности в бизнес-пространстве и отражения этого в бухгалтерском учете [1].

Важно отметить, что изучением вопросов отражения в бухгалтерском учете информационных потерь посвящено немногочисленное количество трудов, так, интересны исследования Токмаковой Е.Г., Юхтановой Ю.А. и Скипина Д.Л. [2], Винтайкиной Д.А. и Астанаевой Ю.Р. [3], Глазовой М.В. и Курцадзе Н.И. [4], Нахаевой М.Р. [5], Яковлевой Л.Я. [6], Старенко А.Ю. [7], Бирулиной В.В., Шмониной К.С. [8], Никифоровой А.А. [9], Алибекова Ш.И., Морунова В.В., Бичурина А.А. [10] и т.д. Отмечая важный вклад в развитие информационной безопасности и ее взаимосвязь с бухгалтерским учетом, следует отметить, что современной экономической литературе недостаточно работ, которые были бы посвящены вопросам документального отражения информационных потерь в бухгалтерском учете, в этой связи изучение проблем документального оформления фактов хищения/потери информации в условиях цифровизации представляется теоретически и практически значимым.

Цель статьи – разработка системы мероприятий, направленных на совершенствование механизма документального оформления информационных потерь в бухгалтерском учете организации.

При написании статьи использовались общенаучные методы познания (анализ, синтез, индукция, дедукция, сравнение), статистический, логический, а также специальные методы (метод двойной записи, документальный).

Объектом исследования – учетно-аналитическое обеспечение бухгалтерского учета организаций в условиях цифровизации.

Научная новизна статьи состоит в разработке и обосновании документального оформления информационных потерь в системе бухгалтерского учета организаций.

Основные результаты исследования

Наиболее желаемой для хищения информацией по данным экспертно-аналитического центра InfoWath в 2024 г. стали персональные данные – около 70%, аутентификационная информация достигла почти трети всех инцидентов – 29%, платежная информация составила порядка 1%.

Проблема утечки данных актуально для любой сферы деятельности, отраслевые особенности безусловно влияют на интерес злоумышленников (рис. 1).

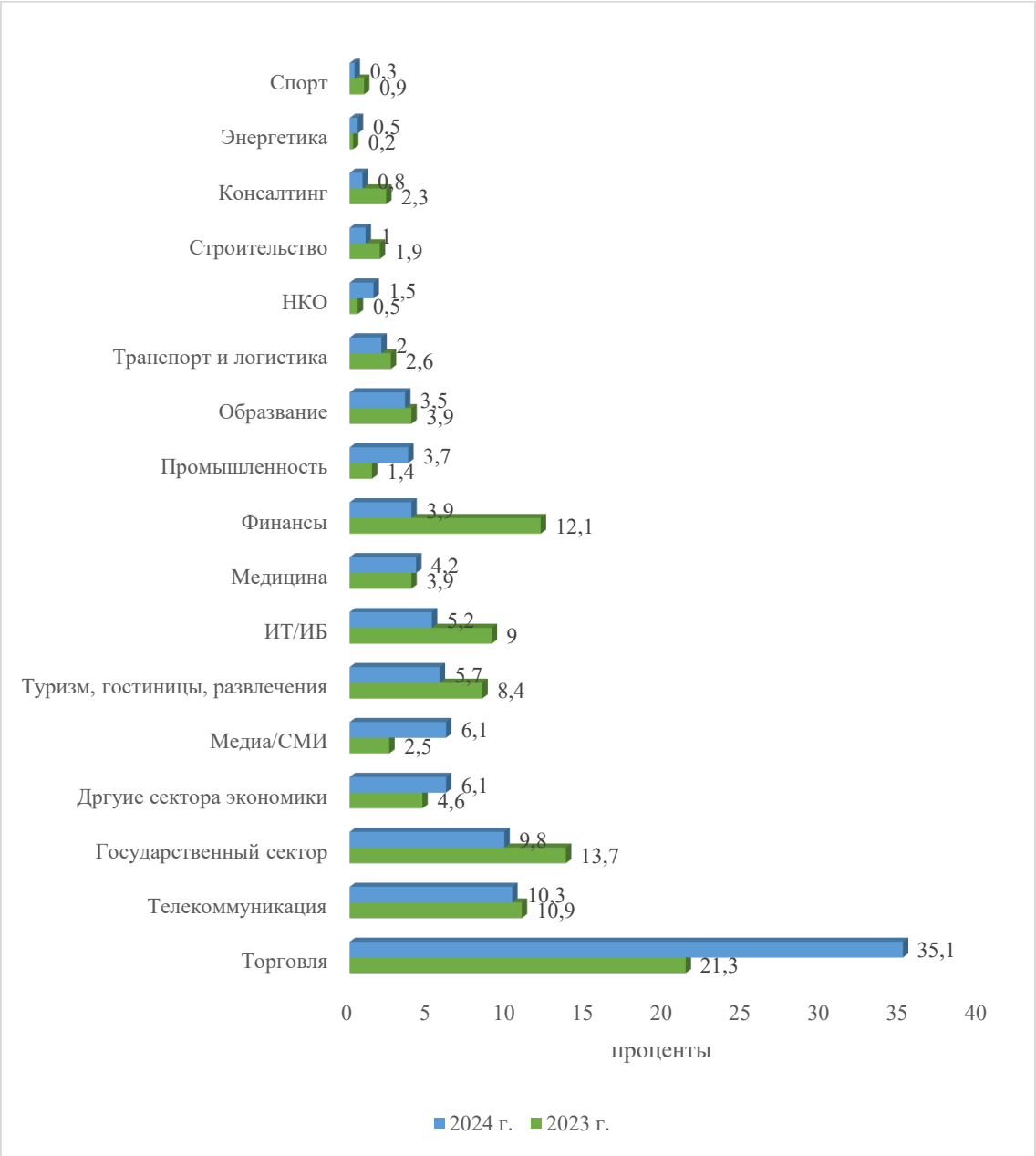

Рис. 1. Утечка персональных данных по отраслям в 2023-2024 гг. в РФ
Источник: составлено по данным [11]

Важным моментом является выяснение того, что является источником утечки/хищения информации: внешние угрозы или внутренние. Это может повлиять на ход внутреннего расследования и отражения в учете результатов потерь информации. По данным отчетов центра InfoWath в 2024 г. подавляющее большинство случаев являются вторжением внешних угроз в деятельность предприятий.

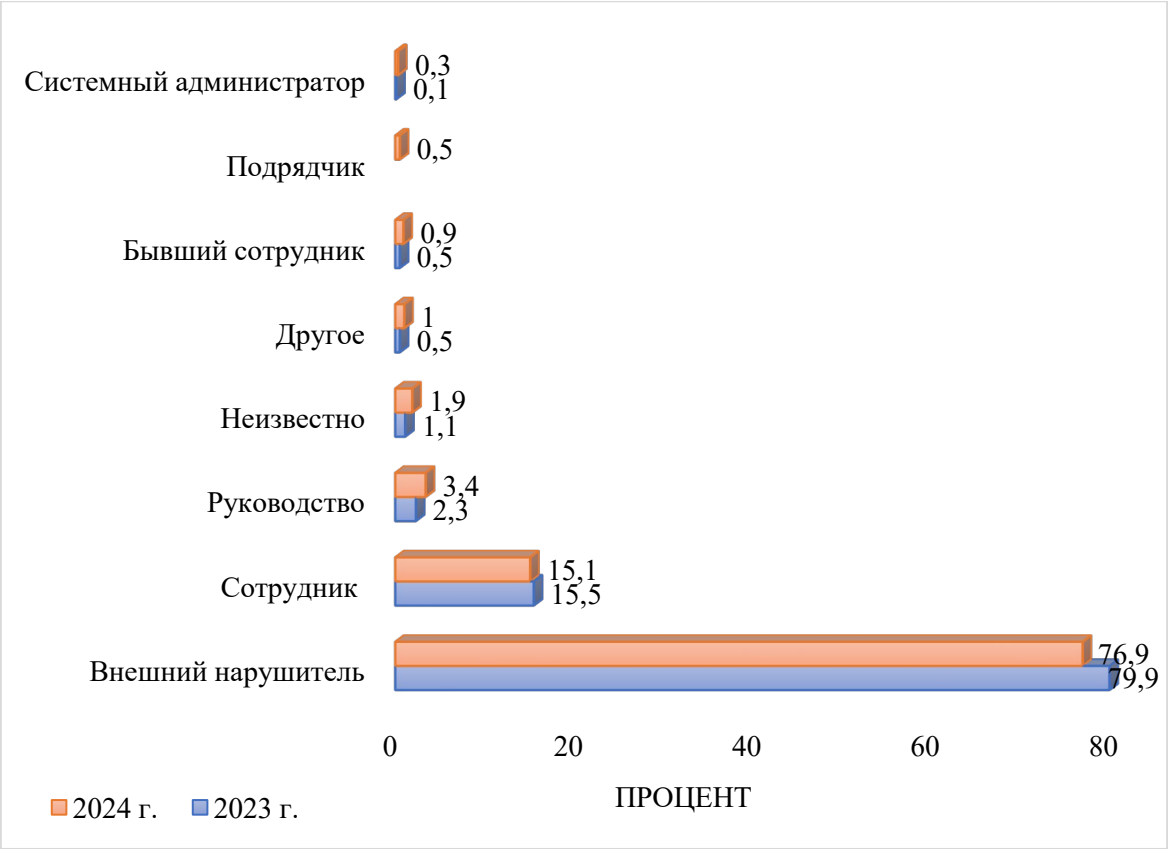

Рис. 2. Распределение утечек информации в России по типам нарушителей, 2023-2024 гг. Источник: составлено по данным [11]

Эта аналитика (рис. 2) подтверждает необходимость учета информационных потерь при документальном оформлении.

Понятие конфиденциальности закреплено в Федеральном законе Российской Федерации от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», также предприятие может использовать понятие коммерческой тайны, которое регламентируется Федеральным законом от 29.07.2004 г. № 98-ФЗ «О коммерческой тайне». Если же речь идет о персональных данных сотрудников, то здесь основным документом, регулирующим эти вопросы, является Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», он же регулирует работу с владельцами веб-сайтов, которые у многих организаций имеются. Для описания работы организации с персональными данными (информацией), способах обеспечения ее защиты составляется политика конфиденциальности, что, по сути, представляет собой документ, устанавливающий отношения между организацией и клиентом в сфере обработки данных, его часто размещают на сайтах организаций. Форма данного документа не установлена, поэтому каждая организация составляет ее самостоятельно (или с привлечением специалистов) [12]. По мнению автора, политика конфиденциальности и учетная политика должны быть между собой взаимосвязаны в части закрепления, что относится к конфиденциальной информации (рис. 3).

Рис. 3. Отражение в учетной политике сведений об информационных потерях
Источник: составлено автором

Важным моментом для грамотного ведения бухгалтерского учета является необходимость отражения в учетной политике предприятия всех элементов конфиденциальности, которая будет в последствии отражаться в учете в виде возможных расходов в результате информационных потерь. Если предприятие этим будет пренебрегать, то это может помешать сформировать правомерную доказательную базу, что негативно скажется на финансовом состоянии, поскольку суд или налоговые органы могут не признать такие расходы и посчитать их не правомерными [13].

Бухгалтерский учет информационных потерь предполагает отражение информации в документах. В альбоме унифицированных форм первичной документации нет подобного рода документов, да и он не является в настоящее время обязательным, однако, в условиях цифровизации и повсеместного обмена информацией документы отражающие информационные потери стали необходимостью. Основные требования к составлению документов отражены в Законе «О бухгалтерском учете» №402-ФЗ (ст. 9) и ФСБУ 27/2021 «Документы и документооборот в бухучете». Говоря о документальном отражении факта утечки информации важно отметить, что на сегодняшний момент в целях бухгалтерского учета не существует хотя бы шаблона документа, который служил бы основной для отражения информационных потерь.

Последовательность действий оператора в случае потери персональных данных отражена некоторыми авторами. Специалисты сайта Клерк отмечают, что если произошла утечка персональных данных, то согласно Закону «О персональных данных» №152-ФЗ, необходимо в течение 24 часов проинформировать Роскомнадзор о таком факте, при условии, что это произошло без согласия владельца таких данных. Сделать это можно через сайт Госуслуг. Также в последующие 72 часа нужно провести внутреннее расследование и его результаты отправить в Роскомнадзор. Обязательно нужно уведомить пострадавших, чьи данные пострадали и предложить им мероприятия для минимизации рисков (поменять пароли, быть внимательным к звонкам и т.д.) [14].

Специалисты Актион Право рекомендуют оценивать вред по шкале: высокий, средний, низкий, и даже предлагают чек лист для оценки такого вреда, который представляет собой анкету с вопросами, с разбивкой по степеням вреда. После этого можно оформить Акт оценки вреда персональных данных, содержание которого предполагает существование в организации специализированной комиссии по таким вопросам, которая утверждается администрацией [15]. Аналогичные действия описывает Салита А., но с поправкой уже не просто на персональные данные, а на информацию. Автор схемой описывает последовательность действий, где изначально фиксируется факт утечки, затем одновременно создаётся рабочая группа внутри предприятия (юристы, сотрудники IT-отдела и ИБ-специалисты, PR-служба) и уведомляется Роскомнадзор, следом происходит информирование клиентов, правоохранительных органы через юридическую службу и PR-отдел. Автор к политике конфиденциальности добавляет необходимость разработки политики информационной безопасности и парольной политики [16].

Нужно отметить, что все действия не сопряжены с отражением данного факта в бухгалтерском учете, кроме попытки оценить вред от пропажи персональных данных специалистами Актион Право. Для ведения бухгалтерского учета необходим специализированный документ, в котором отразится факт нарушения и связь с содержанием учётной политики в отношении информационных потерь, сформируются бухгалтерские записи.

Обобщая вышесказанное, автор считает, что в сложившихся условиях возникает необходимость формирования регистра по отражению информационных потерь в учете предприятия. Регистр предполагается оформлять на любые информационные потери, с обязательным указанием какая именно это потеря: персональные данные, база данных 1С, промышленные образцы какого-то изделия, которое носит секретный характер и т.д. [17]. Также важным моментом является определение в процессе служебного расследования установления факта кто является виновным лицом, что предопределяет отражение на соответствующих счетах учета операций по формированию суммы ущерба. Так, если это работник организации (внутренний нарушитель), то отражение можно провести через счет 73, открыв к нему субсчет «Расчеты по информационным потерям», а если это сторонне лицо (внешний нарушитель), то в таком случае можно применить 76 счет в зависимости от возможности идентификации личности 76.1 «Неизвестное лицо» (если лицо установить не представляется возможным), или 76.2 «Установленный нарушитель» (если лицо установлено). Все расходы будут относиться на счет 91 с открытием субсчетов «Доходы/расходы по информационным потерям» (рис. 4).

ООО «Литейные композиции», г. Омск, ул. Мира, 24, корпус 2, литера Е
(наименование организации)
Конструкторское бюро
(наименование структурного подразделения)

Акт отражения утечки информации	Номер документа	Дата составления
	1	13.02.2026

Документ, уведомляющий Роскомнадзор	Дата информирования
Уведомление №1	12.02.2026
Акт о результатах внутреннего расследования №1	13.02.2026

Информация об разновидности ущерба

Вид пропавшей информации (указать)		Нарушитель (указать по результатам расследования)		Счета	Субсчет	Формируемая бухгалтерская запись
Персональные данные		внутренний		Счет 73 «Расчеты с персоналом по прочим операциям»	Субсчет «Расчеты по информационным потерям»	Дебет 91 «Прочие доходы и расходы» Кредит 73 субсчет «Расчеты по информационным потерям»
Информация, причисляемая к государственной тайне	V					
Чертежи …		внешний	V	Счет 76 «Расчеты с разными дебиторами и кредиторами»	Субсчет «Неизвестное лицо»	Дебет 91 «Прочие доходы и расходы» Кредит 76 «Расчеты с разными дебиторами и кредиторами» субсчет «Неизвестное лицо»
База данных поставщиков					Субсчет «Установленный нарушитель»	
Прочее…						

Информация о сумме ущерба:

Сумма ущерба, руб.	Метод оценки	Комиссия, оценившая ущерб
3 000 000	Стоимость расходов на создание образца детали, оценка ее дефектов, испытательные работы	Петрова П.П., начальник планово-экономического отдела; Иванова И.И., начальник конструкторского бюро; Сидоров С.С., инженер по технике безопасности; Шутов О.Ш., ведущий ИТ-специалист; Семенов С.С., начальник отдела безопасности.

Главный бухгалтер _____ / С.С. Старова/
Руководитель предприятия _____ / П.П. Павлов/

Рис. 4. Авторская форма документа по отражению информационных потерь в бухгалтерском учете
Источник: составлено автором

Как выше было отмечено при обнаружении факта информационных потерь законом установлена последовательность действий для экономического субъекта, что положено в основу авторского алгоритма отражения информационных потерь в бухгалтерском учете (рис. 5). Данная схема построена на основании нормативных документов, иных авторских наработок [14, 15, 16], а также дополнена автором и оформлена в последовательность формирования информации об информационных потерях в целях бухгалтерского учета, поскольку вся информация между собой взаимосвязана.

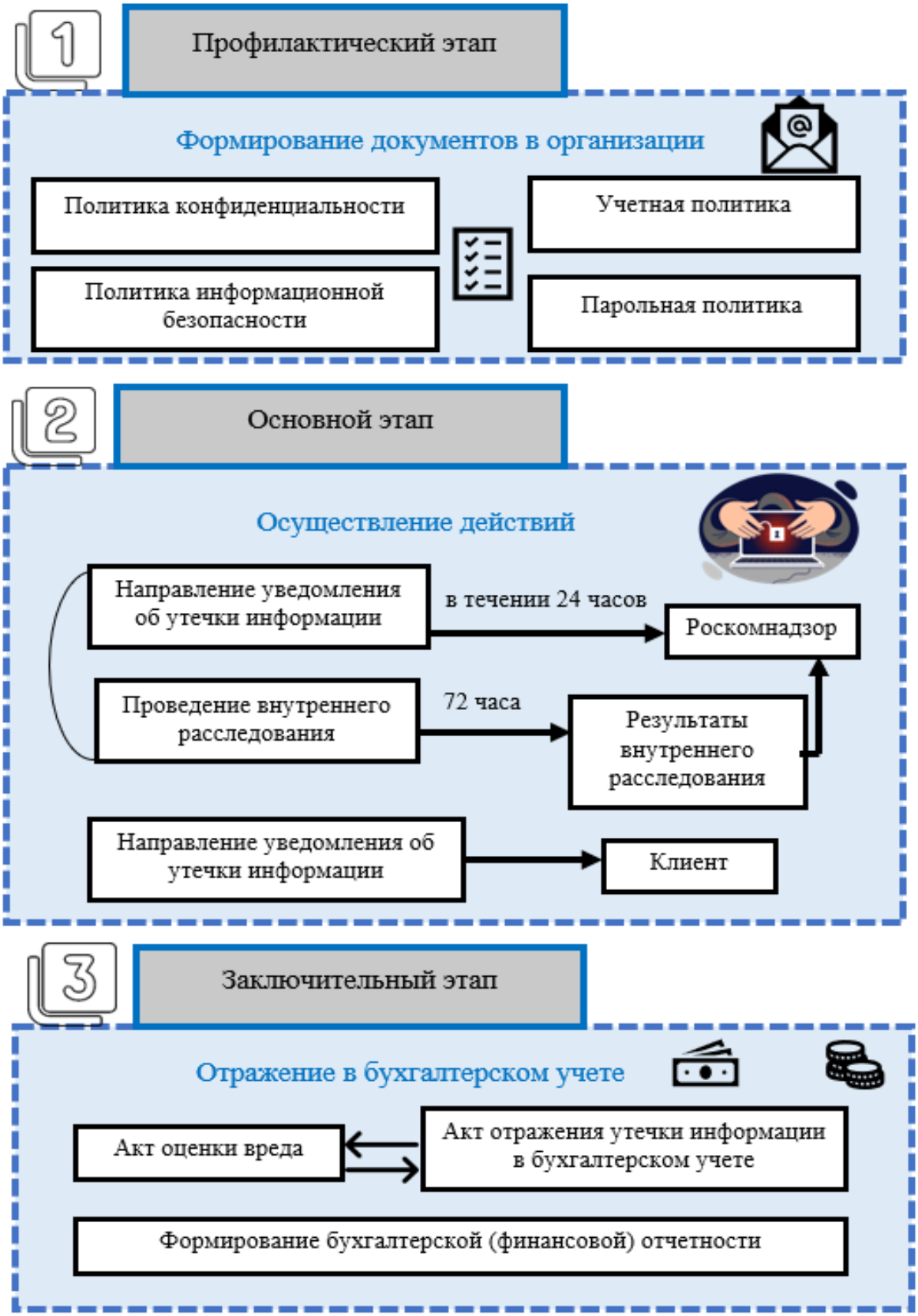

Рис. 5. Авторский алгоритм формирования данных об информационных потерях в бухгалтерском учете
Источник: составлено на основании [14, 15, 16] и дополнено автором

Схема включает в себя не только авторский регистр, но и иные действия, документы, которые на данный момент обязательны для применения. Данный алгоритм позволит

однозначно идентифицировать факт хищений информации и его отражение в учете и отчетности предприятия.

Выводы. Цифровая экономика открывает множество возможностей для предприятий и населения, но одновременно сопряжена со множеством рисков, что обусловлено хищением информации. Новые вызовы заставляют не только общество искать способы защиты данных, но и осуществлять их компенсации, что в бухгалтерском учёте возможно только при наличии доказательной базы, которой выступают грамотно оформленные документы, подтверждающие факт информационных потерь. Эта сфера еще не сформирована, есть много нюансов, которые необходимо предусмотреть, чтобы претендовать на право отражения в составе расходов информационных потерь. Количество инцидентов по хищению информации хоть и сокращается, но существует, а значит необходимо разрабатывать не только новые способы противодействия мошенникам, но и способы фиксации этих фактов и их компенсацию через нормативные инструменты, документальное оформление, в противном случае экономические субъекты становятся незащищенными от неправомерных действий нарушителей.

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. 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
3. Винтайкина Д.А. Сравнительный анализ учета конфиденциальности информации / Д.А. Винтайкина, Ю.Р. Астанаева // Научно-исследовательский центр "Technical Innovations". 2021. № 2. С. 38-43.
4. Глазова М.В. Управленческий учет в обеспечении экономической безопасности организации / М.В. Глазова, Н.И. Курцадзе // Финансово-экономическая безопасность Российской Федерации и ее регионов: Сборник материалов V Международной научно-практической конференции, Симферополь, 30 сентября 2020 года. – Симферополь: ФГАОУ ВО «Крымский федеральный университет имени В.И. Вернадского», 2020. С. 129-130.
5. Нахаева М.Р. Бухгалтерский учет и внутренний контроль в системе обеспечения экономической безопасности организации // Актуальные вопросы современной экономики. 2021. № 1. С. 190-193. DOI 10.34755/IROK.2021.65.43.025.
6. Яковлева Л.Я. Роль бухгалтерского учета в системе экономической безопасности хозяйствующего субъекта // Инновационное развитие экономики. 2020. № 6(60). С. 404-406.
7. Старенко А.Ю. Роль бухгалтерского учета в обеспечении экономической безопасности предприятия // Научный вестник государственного образовательного учреждения Луганской Народной Республики "Луганский национальный аграрный университет". 2020. № 8-3. С. 438-443.
8. Бирулина В.В. Роль налогового учета в обеспечении экономической безопасности организации / В.В. Бирулина, К.С. Шмонина // Учетно-аналитическое и правовое обеспечение экономической безопасности организации: Материалы III Всероссийской студенческой научно-практической конференции в 4-х ч., Воронеж, 24 апреля 2021 года. Том Часть 1. – Воронеж: Воронежский государственный университет, 2021. – С. 163-166.
9. Никифорова А.А. Бухгалтерский учет в обеспечении финансовой безопасности компании // Международная научно-техническая конференция молодых ученых, Белгород, 25–27 мая 2020 года. Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, 2020. С. 5566-5569.

10. Алибеков Ш.И. Конфиденциальность учетно-экономической и контрольной информации как инструмент обеспечения экономической безопасности / Ш.И. Алибеков, В.В. Морунов, А.А. Бичурин // Управленческий учет. 2024. № 2. С. 19-24. DOI 10.25806/uu2202419-24.
11. 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 13.02.2026).
12. Суровцев А. Зачем нужна политика конфиденциальности и как ее составить// Т-бизнес секреты. URL: https://secrets.tbank.ru/glossarij/chto-takoe-politika-konfidencialnosti/?internal_source=copypaste (дата обращения 13.02.2026).
13. Голова Е.Е., Витковский Е.О. Анализ финансового состояния организации-участника внешнеэкономической деятельности // Электронный научно-методический журнал Омского ГАУ. 2020. № 1 (20). С. 14.
14. Что делать при утечке персональных данных в 2025 году: памятка для бизнеса // Клерк. URL: https://www.klerk.ru/blogs/data-sec/672641/#chapter-chto-takoe-utechka-personalnyh-dannyh-i-kakie-posledstviya-ona (дата обращения 15.02.2026).
15. Утечка персданных: план действий для юриста компании // Актион Право. URL: https://www.law.ru/news/36577-utechka-persdannyh-plan-deystviy-dlya-yurista-kompanii (дата обращения 15.02.2026).
16. Салита А. Утечки информации: виды, причины и каналы // Академия Selektel. URL: https://selectel.ru/blog/information-leaks/
17. Голова Е.Е. Финансовая инклюзия: новые задачи в современных условиях // Экономика, предпринимательство и право. 2023. Т. 13, № 5. С.1663-1682. DOI 10.18334/epp.13.5.117575 URL: https://1economic.ru/lib/117575 (дата обращения 16.02.2026).