УДК 528.71

Д. А. Кондрашин[1], Г. А. Казанцев[1]✉, Е. В. Рыжкова[1]

Универсальный аудит безопасности обработки персональных данных

[1]Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: engrab66@gmail.com

Аннотация. В статье рассматривается концепция универсального аудита безопасности обработки персональных данных (ПДн) для субъектов малого и среднего предпринимательства (МСП). Проведен анализ действующего нормативно-правового поля (включая 152-ФЗ, 149-ФЗ, постановления Правительства РФ № 687-ПП и № 1119-ПП, приказы ФСТЭК № 17, № 21 и др.). Определены типовые риски и нарушения при обработке ПДн МСП (например, отсутствие правовых оснований обработки, неполучение согласий, использование несертифицированных средств и отсутствие доступа контроля) и сформирован базовый набор критериев для аудита. Предложена концепция системы аудита в виде набора чек-листов, разделенных на правовые, организационные и технические меры с пояснениями и ссылками на нормы, позволяющих организациям самостоятельно выявлять несоответствия и получать рекомендации. Результаты проекта подтверждают востребованность простого и доступного инструмента аудита ПДн для МСП, однако требуют дальнейшей проработки.

Ключевые слова: персональные данные, аудит, МСП, информационная безопасность, чеклисты, 152-ФЗ

D. A. Kondrashin[1], G. A. Kazantsev[1]✉, E.V. Ryzhkova[1]

Universal audit of personal data processing security

[1]Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: engrab66@gmail.com

Abstract. The article presents the concept of a universal audit of personal data processing security for small and medium-sized enterprises (SMEs). An analysis of the current regulatory framework was conducted, including Federal Laws No. 152-FZ and No. 149-FZ, Russian Government Decrees No. 687 and No. 1119, and FSTEC orders No. 17 and No. 21, among others. Typical risks and violations in SMEs' personal data processing were identified – such as lack of legal grounds for processing, absence of consent, use of uncertified tools, and lack of access control – and a basic set of audit criteria was developed. The proposed audit concept is structured as a set of checklists divided into legal, organizational, and technical measures, each with explanations and references to relevant regulations. This approach enables organizations to independently identify noncompliance and receive recommendations. The project results confirm the demand for a simple and accessible personal data audit tool for SMEs, although further refinement is needed.

Keywords: personal data, audit, SME, information security, checklists, 152-FZ

Введение

Защита персональных данных (ПДн) – одна из приоритетных задач информационной безопасности и законодательства. В России основной нормативный акт – Федеральный закон № 152-ФЗ «О персональных данных» (ред. от 08.08.2024) устана-

вливает принципы обработки ПДн и обязует операторов принимать «необходимые правовые, организационные и технические меры» для их защиты [1].

Однако малые и средние предприятия (МСП) часто испытывают трудности с соблюдением этих требований. У большинства небольших компаний нет в штате специалистов по ИБ или юристов по ПДн, и требования закона либо игнорируются, либо выполняются формально. Это создает серьезные риски – утечки данных, штрафы и потерю доверия клиентов. Согласно современному законодательству, обработка ПДн допускается только при наличии правового основания (например, согласия субъекта или иного юридического факта). При отсутствии такого основания (нарушении ст. 6 152-ФЗ) наступает административная ответственность (штрафы для юридических лиц до 100 тыс. руб. по ст. 13.11 КоАП РФ) [2]. К типичным нарушениям также относится невыполнение требований по конфиденциальности (ст. 7 152-ФЗ), неуведомление Роскомнадзора о начале обработки (ст. 22), отсутствие договоров с «обработчиками» и несоблюдение организационных и технических мер (ст.19 152-ФЗ). Сложность ситуации усугубляется частыми изменениями законодательства и появлением новых требований (например, с 2025 г. вступают в силу значительные поправки в 152-ФЗ). Существующие методы аудита обработки ПДн обычно предполагают привлечение дорогих экспертов или сложные технические инструменты, что делает их недоступными для МСП. Вместе с тем бизнес нуждается в простом понятном инструменте для самостоятельной проверки соответствия требованиям и минимизации рисков. Цель данного исследования – разработать концепцию универсального аудита безопасности обработки ПДн, который позволит МСП без привлечения внешних специалистов выявлять проблемные места в процессах обработки данных и получать ясные рекомендации по устранению нарушений.

Методы и материалы

В рамках исследования проведен комплексный анализ нормативно-правовой базы по защите ПДн. Основное внимание уделялось как федеральному закону 152-ФЗ (и связанным поправкам), так и подзаконным актам: постановлениям Правительства РФ № 687-ПП «Об утверждении Положения об особенностях обработки ПДн, осуществляемой без использования средств автоматизации» (применяется, когда обработка ПДн ведется вручную) и № 1119-ПП «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», а также нормативным актам ФСТЭК (приказам № 17 и № 21) и рекомендациям Роскомнадзора [2]. Это позволило выделить ключевые требования к правовым, организационным и техническим мерам защиты ПДн. Параллельно изучались типовые риски и уязвимости МСП в части обработки ПДн. Основными источниками стали отчеты Роскомнадзора о проверках, публикации в области ИБ и результаты предварительных интервью с представителями бизнеса.

Выявлено, что наиболее часто встречаются: отсутствие согласий и уведомлений, недостатки договорной работы с подрядчиками (иногда используются облачные сервисы без договора), отсутствие разграничения прав доступа и кон-

троля действий пользователей, неприменение сертифицированных средств защиты и систем контроля утечек и т.д. Эти нарушения формируют «поля риска» для МСП. На основе анализа требований и рисков были определены критерии оценки для аудита. Предложен подход чек-листов: вопросы разбиты на три блока (правовые, организационные, технические меры).

Каждый вопрос чек-листа формулируется простым языком, к нему дается пояснение и ссылка на конкретную норму закона или регламента. По результатам заполнения (ответы «да»/«нет», «не уверены») генерируются индивидуальные рекомендации и план корректирующих действий. Методология сочетает в себе элементы классического аудита (выявление несоответствий) и принципа самоаудита: инструменты рассчитаны на непрофессионала без глубоких юридических или технических знаний. Для предварительной оценки предложенной концепции проведены обсуждения с представителями малого бизнеса из сфер услуг и онлайн-торговли. Это позволило уточнить, что целевой аудитории действительно нужен простой формат проверки «поставил галочку – узнал, что делать дальше». Кроме того, было опрошены представители нескольких предприятий о конкретных проблемах в области ПДн и информационной безопасности, что помогло сформировать примеры вопросов и рекомендаций.

Результаты

В результате исследования сформирована базовая структура универсального аудита обработки ПДн, включающая три направления мер: правовые, организационные и технические. Ниже приведены основные находки и концептуальные решения, полученные в ходе работы.

Правовые меры. В этой части проверяется наличие правовых оснований для обработки ПДн. контролируется, есть ли у организации согласия субъектов ПДн, договоры с контрагентами (например, договора поручения обработки ПДн с облачными сервисами по ст. 6,19 152-ФЗ) и соответствующие локальные нормативы. Установлено, что МСП часто не заключают договоры на обработку ПДн с внешними ИТ-сервисами (например, при использовании «1С в облаке», CRM-систем, облачных почтовых сервисов). Положительный ответ на вопрос чек-листа («Договор заключен») сопровождается ссылкой на статьи 6 и 19 152-ФЗ о требованиях к оформлению обработки по поручению. При отрицательном ответе или «не уверен» выводится рекомендация срочно заключить договор в соответствии с законодательством. Например, несоблюдение требований договорной работы влечет штраф до 100 тыс. руб. и риски имущественной ответственности в случае инцидента [3].

Организационные меры. Проверяются внутренние регламенты, политики и процедуры. Это касается назначения ответственных за ИБ и ПДн, регламентов работы с информацией, контроля исполнения требований. Например, среди типичных нарушений выявлено отсутствие разграничения доступа к системам (не разработаны политики ролей и привилегий). Проверяется наличие регламента резервного копирования, журналирования действий сотрудников, обработки инцидентов. Несоблюдение организационных мер прямо противоречит общим принципам

ст. 19 152-ФЗ и рекомендациям ГОСТ, ФСТЭК, а также может привести к штрафу (КоАП 13.11). В чек-листе задаются вопросы вида «Разработаны ли внутренние регламенты безопасности ПДн?» или «Проводится ли вводный инструктаж по ПДн для сотрудников?» – с объяснением роли этих мер.

Технические меры. Проверяется применение средств защиты информации, сертифицированных по приказам ФСТЭК № 17 и № 21. Это включает использование антивирусного ПО, средств шифрования, межсетевых экранов, систем обнаружения вторжений, DLP-систем, а также правильная настройка учетных записей и права доступа. В частности, по п.3 ст. 19 ФЗ-152 обработка ПДн в ИСПДн должна проводиться с применением «средств защиты информации, прошедших процедуру оценки соответствия».

На практике МСП часто игнорируют сертификацию ПО, что приводит к уязвимостям. Чек-лист содержит вопросы: «Используются ли сертифицированные средства шифрования/антивируса?» и «Есть ли разграничение по паролям и аудит доступа?». Если ответ «нет», генерируются рекомендации по обновлению паролей, внедрению двухфакторной аутентификации, резервированию данных и т.п.

Все вышеописанные данные (типы нарушений и соответствующие меры) обобщены в табл. 1. Она демонстрирует пример того, какие нарушения чаще всего встречаются и какие требования на них накладывает законодательство РФ. В таблице показана связь между видом нарушения, соответствующей нормой закона и видом необходимых мер (правовых, организационных, технических) для его устранения.

Обсуждение

Предложенная модель универсального аудита обработки ПДн сочетает формальные требования законодательства с практичным упором на доступность. Сравнительный анализ с традиционными аудитами показал, что ключевое отличие состоит в упрощении процедуры: вместо комплексного обследования привлекается принцип чек-листа. Это снижает стоимость и время проведения проверки, однако требует корректной формулировки вопросов (на понятном языке) и адекватной интерпретации ответов. Соответствие правовой части чек-листа базируется на нормах 152-ФЗ и смежных актов [1].

Таблица 1

Типичные нарушения при обработке ПДн и соответствующие требования

№	Нарушение	Норма\Требование	Рекомендуемые меры
1	Обработка ПДн без правового основания	ст. 6 ФЗ-152; КоАП 13.11	Срочно оформить согласия/уведомления; заключить договоры (п.5 ст.6 ФЗ-152)
2	Нет добровольного согласия на обработку специальных ПДн	ст. 23 ФЗ-152; КоАП 13.11	Получить письменные согласия; при необходимости прекратить незаконную обработку.

Окончание таблицы 1

№	Нарушение	Норма\Требование	Рекомендуемые меры
3	Нет договора с внешним оператором (сервисом)	ст. 6, 19 ФЗ-152; КоАП 13.11	Заключить «договор поручения» ПДн с сервисом (на основе шаблона РКН)
4	Отсутствие политики безопасности (и регламентов)	ст. 19 ФЗ-152; ГОСТ 57580.1	Разработать и документировать регламенты ИБ, инструкции, роль АПДн, обучить персонал.
5	Нет систем контроля и мониторинга (журналирования)	ст. 19 ФЗ-152; ГОСТ 57580.1	Внедрить системы логирования, регулярно проверять и контролировать доступ к ПДн.
6	Использование непроверенного ПО для обработки ПДн	Приказы ФСТЭК №17, 21	Использовать только сертифицированное ПО; провести оценку соответствия ИСПДн.
7	Неограниченное хранение ПДн дольше положенного	ст. 5, 18 ФЗ-152; КоАП 13.11	Удалять или анонимизировать устаревшие данные; соблюдать сроки хранения.
8	Неуведомление РКН об ИСПДн или утечке	ст. 22, 22.1 ФЗ-152; КоАП 13.11	Сообщать в РКН о начале обработки и/или фактах утечки в установленные сроки.

Например, обязательность заключать договоры поручения при передаче ПДн указана прямо в законе и подтверждается разъяснениями Роскомнадзора. По организационным и техническим мерам концепция соответствует рекомендациям ГОСТ и ФСТЭК: базовые меры ИБ на уровне ГОСТ Р 57580.1-2017 охватывают создание политики безопасности, определение ответственных, организацию доступа и применение сертифицированных средств.

На практике же небольшие фирмы часто не имеют оформленной политики ИБ, что отражает потребность в подобных инструментах. В ходе обсуждений с представителями МСП подтвердился интерес к подходу. Компании признали, что им важно минимизировать риски, не тратя большие ресурсы на аудит: «Нам нужна простая проверка – поставить галочку, и знать, что делать дальше» (один из опрошенных руководителей). Этот запрос совпал с выводом исследования о том, что проект востребован, но требует доработки: отмечена необходимость адаптации чек-листов под разные сферы бизнеса (услуги, торговля, производство и т.д.), уточнения критериев оценки и формата рекомендаций.

Также обсуждались потенциальные форматы реализации: одна из идей – выпуск методических материалов (печатное руководство с чек-листами и шаблонами договоров) или создание онлайн-сервиса с автоматическим формированием отчета. Оценка экономической эффективности предварительно показала, что при мини-

мальных затратах на разработку (как программного продукта, так и контента) такая услуга может быть коммерчески привлекательной – если она действительно упрощает решение проблем и не требует найма юриста или аудитора. С точки зрения риска, важно отметить динамику законодательства. К 2024–2025 годам 152-ФЗ подвергся значительным изменениям (последние поправки приняты Федеральным законом № 233-ФЗ от 08.08.2024, вступающим в силу 01.09.2025) [1].

Например, усилились требования к обеспечению информзащиты, уточнены основания обработки и усилены санкции. Это означает, что любой инструмент аудита должен быть обновляемым: чек-листы должны отражать текущую редакцию законов и новые постановления (в частности, в ближайшее время ожидаются новые правила о трансграничной передаче ПДн и ужесточении ответственности).

Сравнение с работами других авторов. Хотя в специализированной литературе универсальные чек-листы под МСП встречаются редко, общий подход аудитирования описан в нескольких руководящих документах. В частности, Роскомнадзор публикует Методические рекомендации по организации защиты ПДн, где рекомендовано подразделять меры на организационные и технические (что совпадает с нашей моделью) и проводить регулярную оценку угроз. Цитируемые ГОСТы (например, 57580.1–2017) также делят меры на категории, близкие к нашим блокам.

Таким образом, предложенный универсальный чек-лист во многом следует отработанным принципам, однако «упаковывает» их в более простой и понятный для МСП формат.

Ограничения исследования:следует отметить, что разработанная концепция на данном этапе является теоретической моделью и апробирована лишь частично (пилотные обсуждения с ограниченным числом компаний). Реальная эффективность чек-листа зависит от корректности ответов и мотивации руководства к честному заполнению. Кроме того, некоторые технические положения (например, требования к криптостойкости средств шифрования или пожарным резервированием) требуют дополнительного пояснения, которое пока обеспечивается лишь общими ссылками. Отсутствие реальных кейсов усложняет количественную оценку качества: пока можно привести только качественные примеры и предположительные сценарии использования (как показано выше).

Заключение

Проведенное исследование подтвердило возможность создания доступного инструмента аудита безопасности обработки персональных данных для малого и среднего бизнеса. Основные выводы работы таковы:

– разработана концепция универсального аудита, включающая структурированные чек-листы по правовым, организационным и техническим аспектам защиты ПДн. Такая структура позволяет охватить требования 152-ФЗ и смежных нормативов в понятном виде, что упрощает проверку соответствия требованиям законодательства [1, 4–9];

– на основе анализа законодательства и практики проверок выявлены типичные нарушения обработки ПДн (см. табл. 1). Для них предложены конкретные рекомендательные меры – юридические и технические, что снижает риск санкций (например, штрафов по ст.13.11 КоАП) и инцидентов утечек [3];

– первичная оценка концепции со стороны представителей МСП показала востребованность простого и понятного инструмента. Хотя проект требует дальнейшей доработки (учет отраслевых особенностей, тестирование на реальных данных, разработка программной реализации), сформулированы следующие перспективные направления: адаптация чек-листов для разных типов бизнес-процессов, формализация критериев оценки («балльная» система), а также подготовка электронного или бумажного справочника с автоотчетом.

Таким образом, идея «универсального» аудита безопасности ПДн оказалась актуальной и получила предварительное подтверждение значимости. Успех дальнейшей работы будет зависеть от практической реализации (например, создания веб-сервиса с автоформированием отчета) и постоянного обновления контента в соответствии с новейшими нормативами (ГОСТами, законами и рекомендациями Роскомнадзора). В дальнейшем планируется расширить исследования: протестировать разработанный чек-лист на реальных предприятиях (получить и проанализировать результаты аудита), интегрировать дополнительные инструменты анализа (например, автоматизированный сканер уязвимостей) и выпустить методические материалы.

Благодарности

Авторы выражают благодарность научному руководителю – Е. В. Рыжковой, а также представителям малого бизнеса за участие в обсуждении концепции.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных» (ред. от 08.08.2024).
2. Роскомнадзор. Методические рекомендации и данные об инициативах в области защиты ПДн.
3. Кодекс РФ об административных правонарушениях, ст.13.11 (ред. 2025).
4. Постановление Правительства РФ от 01.06.2012 N 687-ПП «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
5. Постановление Правительства РФ от 01.11.2012 N 1119-ПП «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
6. Приказ ФСТЭК России от 11.02.2013 N 17 «Об утверждении Порядка применения криптографических (или иных) средств защиты информации».
7. Приказ ФСТЭК России от 18.02.2013 N 21 «Об утверждении Порядка проведения аттестации объектов информатизации».
8. ГОСТ Р 57580.1-2017 «Безопасность финансовых операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер»
9. КоАП РФ, ст.13.11