УДК 338

ОЦЕНКА СИСТЕМЫ КОНТРОЛЯ ДАННЫХ И СОБЛЮДЕНИЯ НОРМАТИВНЫХ ТРЕБОВАНИЙ В ЭКОСИСТЕМЕ ТЕЛЕКОМ ОПЕРАТОРА: СБОР И ХРАНЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

[1]С.В. Пелькова, [2]Е.С. Соколова, [1]М.А. Стародубова
[1] Тюменский государственный университет, Тюмень

[2] Тюменское высшее военно-инженерное командное училище имени маршала инженерных войск А.И. Прошлякова, Тюмень, email: sok-evgenia@yandex.ru

Аннотация. *Данная статья посвящена исследованию системы внутреннего контроля обработки персональных данных (ПДн) в условиях развития многофункциональных цифровых экосистем телеком-операторов. На примере ПАО «МТС» проанализированы современные вызовы, связанные с расширением экосистемы за счет подключения новых партнёров, что приводит к увеличению точек доступа к данным и усложнению инфраструктуры.*

Ключевые слова: *внутренний контроль, контроль данных, цифровые экосистемы.*

EVALUATION OF THE DATA CONTROL SYSTEM AND COMPLIANCE WITH REGULATORY REQUIREMENTS IN THE TELECOM OPERATOR ECOSYSTEM: COLLECTION AND STORAGE OF PERSONAL DATA

[1]S.V. Pelkova, [2]E.S. Sokolova, [1]M.A. Starodubova
[1] Tyumen State University, Tyumen

[2] Tyumen Higher Military Engineering Command School named after Marshal of the Engineering Troops A.I. Proshlyakov, Tyumen, email: sok-evgenia@yandex.ru

Abstract. *This article is devoted to the study of the system of internal control of personal data processing (PD) in the context of the development of multifunctional digital ecosystems of telecom operators. Using the example of MTS PJSC, modern challenges related to the expansion of the ecosystem by connecting new partners are analyzed, which leads to an increase in data access points and a more complex infrastructure.*

Keywords: *internal control, data control, digital ecosystems.*

Дата поступления статьи в редакцию: 04.12.2025
Дата принятия статьи в печать: 15.01.2026

Введение

За последнее десятилетие в России телекоммуникационная отрасль прошла путь от предоставления базовых услуг связи до формирования многофункциональных цифровых экосистем. Это развитие обусловлено не только ростом спроса на услуги связи, но и непрерывным технологическим прогрессом. Современная цифровая экосистема в телекоме представляет собой целостную среду, где пользователь получает доступ к образованию, финансовым услугам, развлечениям и другим сервисам, используя единую авторизацию на основе персональных данных. Однако стремительное расширение экосистем за счет подключения новых партнеров и создания специализированных бизнес-подразделений создает принципиально новую проблему. Каждое новое звено в этой цепи увеличивает количество точек доступа к персональным данным и усложняет инфраструктуру телеком оператора.

Цель исследования

Цель исследования – анализ системы внутреннего контроля обработки персональных данных в условиях развития многофункциональных цифровых экосистем телеком-операторов; выявление возможных направлений по внедрению улучшений системы внутреннего контроля.

Материал и методы исследования

Объектом исследования послужило ПАО «МТС», его структура управления, организационная структура и годовые отчеты о произведенной деятельности. Теоретическая и методологическая основа исследования сформирована: нормативно-правовой базой, регулирующей деятельность операторов связи,

нормативно правовой базой, регулирующей деятельность системы внутреннего контроля, анализом программных продуктов, задействованных в системе контроля.

Результаты исследования

Объектом исследования в статье послужило ПАО «МТС», в ходе анализа которого изучены современные вызовы, связанные с расширением экосистемы за счет подключения новых партнёров, что является основой увеличения точек доступа к данным и усложнению инфраструктуры. На рисунке 1 представлена карта цифровой экосистемы (на примере ПАО «МТС»).

Рис. 1. *Карта цифровой экосистемы ПАО «МТС»*

Источник: составлено авторами по данным официального годового отчета ПАО «МТС» за 2024 год [8].

Многогранность представленной цифровой экосистемы требует от операторов непрерывного масштабирования и адаптации систем защиты информации, а от регуляторов – ужесточения и развития нормативных требований в области обработки ПДн, которые должны охватывать всю расширяющуюся экосистему, а не только ее ядро. В связи с этим закономерно возникает вопрос: «Насколько добросовестно операторы обеспечивают конфиденциальность данных в условиях такой сложной и динамичной структуры?». Практически каждый пользователь сталкивался с последствиями утечек: назойливыми звонками, спам-рассылками и другими нарушениями приватности. Таким образом, актуальность темы защиты персональных данных сегодня крайне высока, поскольку телеком-операторы, являясь ядром цифровых экосистем, несут полную юридическую ответственность за безопасность информации, доверенной им миллионами пользователей.

Нормативная база, как набор обязательных требований к контролю

Сегодня процессы цифровизации в сфере телеком интенсивно развиваются повсеместно в общественном масштабе привлекая все больше и больше источников информации, а именно персональные данные абонентов. Персональные данные передаются абонентом на этапе заключения договора. Оператор и партнеры его экосистемы используют эти данные для оказания услуг в течение всего периода обслуживания абонента. Оператор обязан обеспечить безопасность обработки ПДн путем согласованной работы в соответствии с законодательством. В нашем случае ключевым нормативно правовым актом, регулирующим безопасность ПДн, будет выступать Федеральный закон «О персональных данных» от 27.07.2006 г. № 152-ФЗ. Согласно закону, персональные данные – это информация, которая прямо

или косвенно определяет физическое лицо. Данный акт регулирует отношения, связанные с обработкой ПДн в сфере телеком. Целью закона является обеспечение защиты прав и свобод человека при обработке его ПДн, с использованием средств автоматизации или без использования таких средства, а также защиту прав на неприкосновенность частной жизни, личную и семейную тайну, что прописано в ст. 2 № 152-ФЗ. Закон регулирует обработку ПДн, осуществляемую федеральными органами государственной власти, органами местного самоуправления, юридическими лицами и физическими лицами. Стоит упомянуть и другие нормативно правовые акты в сфере связи, такие как федеральные законы, постановления правительства РФ, нормативные документы федеральных органов исполнительной власти:

– Федеральный закон от 07.07.2003 г. № 126-ФЗ «О связи»;

– Федеральный закон от 26.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Постановление Правительства РФ от 29.06.2021 г. № 1045 «О федеральном государственном контроле (надзоре) в области связи»;

– Постановление Правительства РФ от 28.05.2022 г. № 968 «Об утверждении Правил оказания услуг телеграфной связи»;

– Приказ Министерства цифрового развития, связи массовых коммуникаций РФ от 13.08.2021 г. № 832 «Об утверждении Требований к построению телефонной сети связи общего пользования» и др.

Полный перечень правовой базы установлен и активен на сайте Роскомнадзора, которые ведут государственный контроль в сфере связи, информационных технологий и массовых коммуникациях.

В международной практике используется нормативный акт «General Data Protection Regulation» (GDPR) – Общий регламент по защите данных. Это нормативный акт Евросоюза, который определяет правила сбора, обработки и хранения, а также распространения ПДн на его территории. Применение GDPR к деятельности российских телеком-операторов обусловлено не территориальным принципом, а характером обработки данных. В соответствии со ст. 3 GDPR, регламент применяется, если обработка персональных данных касается субъектов данных, находящихся в ЕС, даже если сам оператор не учрежден на территории Евросоюза.

Для телеком-оператора, развивающего экосистему услуг, соблюдение требований как российского, так и европейского законодательства о персональных данных становится критически важным. Это связано с наличием абонентов – граждан ЕС, использованием сервисов и инфраструктуры, расположенных в Европе, или работой с международными партнерами. В таблице 1 приведено сравнение по ключевым критериям законодательных актов.

Таблица 1

Сравнительный анализ 152-ФЗ и GDPR

Критерий	Федеральный закон № 152-ФЗ «О персональных данных»	General Data Protection Regulation (GDPR)	Практические сложности для экосистемы телеком-оператора
1. Правовое основание обработки	Чёткий перечень оснований	Свободное, информированное, несвязанное с основной услугой	Риск признания согласия недействительным при его привязке к договору
2. Право на перенос данных (Data Portability)	Не предусмотрен в машиночитаемом формате	Прямое право на передачу данных другому оператору	Необходимость разработки дорогостоящих технических решений
3. Сроки ответа на запросы субъекта	30 дней	30 дней с возможностью продления	Риск нарушения GDPR из-за внутренних регламентов
4. Ответственность и штрафы	До 20 млн руб.	До 20 млн евро или 4% оборота	Экзистенциальные риски для бизнеса

Источник: составлено авторами.

Для успешного и безопасного функционирования экосистемы телеком-оператора необходимо внедрять единую систему контроля и управления данными, гибко настраивающую политику в зависимости от юрисдикции субъекта данных. Базовое требование по внедрению системы внутреннего контроля определяется федеральным законом «О бухгалтерском учете» от 06.12.2011 г. № 402-ФЗ. Однако для акционерных обществ и крупных компаний в качестве корпоративного стандарта, описывающего требования к системе внутреннего контроля, можно обозначить два документа:

1. Кодекс корпоративного управления Банка России. Документ содержит рекомендации по построению эффективной системы управления для публичных компаний. Крупным операторам с публичным

статусом кодекс предписывает внедрить лучшие практики: обеспечить независимость и работу советов директоров, повысить прозрачность для акционеров, выстроить систему управления рисками и внутреннего контроля. Это необходимо для привлечения инвестиций и соответствия стандартам регулятора.

2. Указание Банка России от 28.12.2020 г. № 5683-У «О требованиях к системе внутреннего контроля профессионального участника рынка ценных бумаг». Документ описывает обязательные требования к организации системы внутреннего контроля для профессиональных участников рынка ценных бумаг. Однако, если оператор создает или управляет финансовыми дочерними структурами (например, онлайн банком), то для них соблюдение этого указания становится обязательным. Оно предписывает выявление рисков, процедуры контроля и противодействие недобросовестным практикам.

Таким образом нормативная база в сфере связи содержит широкий спектр вопросов и ответов на них, связанных с деятельностью операторов связи, и включает документы определяющие требования не только в российском законодательстве, но и в зарубежном.

Жизненный цикл персональных данных: от сбора до уничтожения

Совокупность этапов обработки ПДн с момента их сбора до уничтожения называют жизненным циклом персональных данных. Этапы жизненного цикла персональных данных при обработке отражены на рисунке 2.

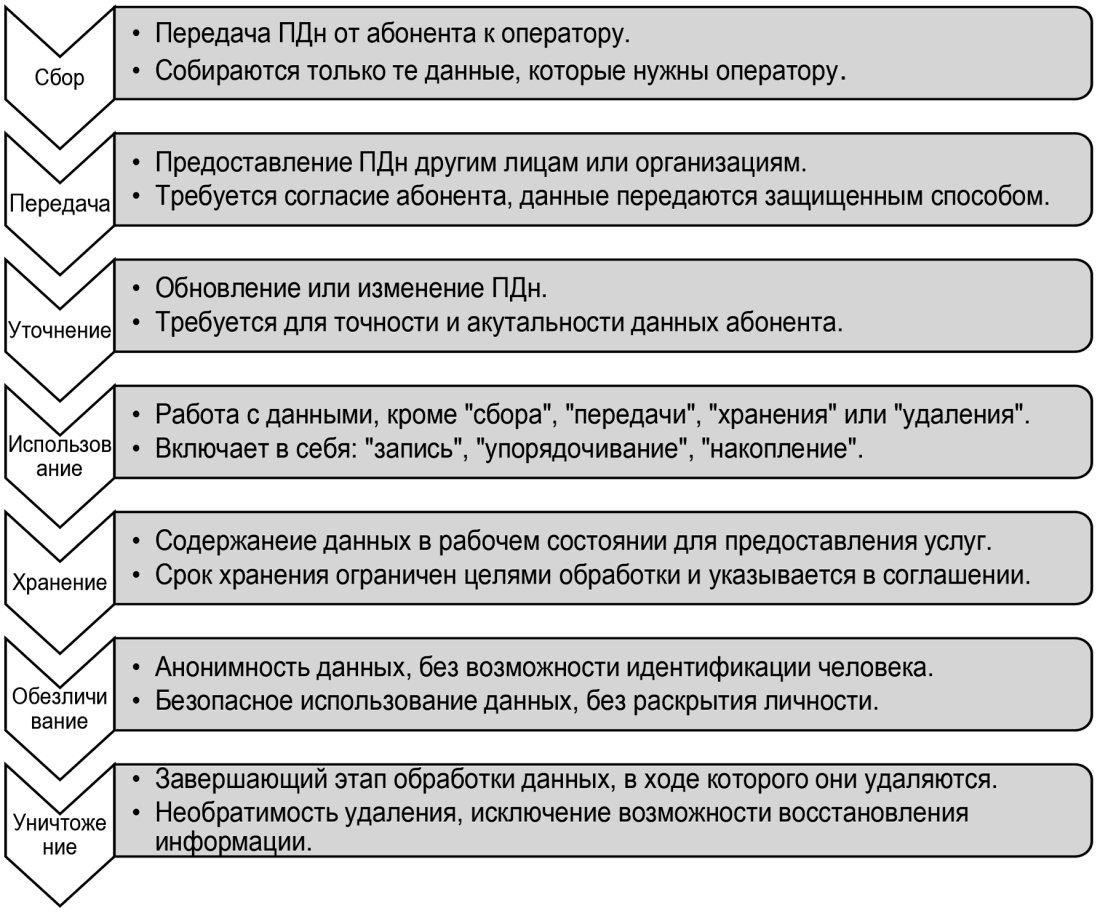

Рис. 2. *Этапы жизненного цикла*

Источник: составлено авторами по данным методических рекомендаций ПАО «Сбербанк» [3].

Понимание жизненного цикла ПДн помогает осуществлять грамотное управление потоками данных на всех этапах.

Идентификация ПДн является неотъемлемой частью работ, выполняемых в рамках жизненного цикла ПДн. Контроль осуществляется через совокупность организационных и технических мер. Ответственность лежит на руководителе телеком оператора, а также на закрепленном документально, ответственном лице за обработку ПДн, службе информационной безопасности.

На примере ПАО «МТС», на этапе «Сбор» технической мерой является не просто DLP, а специализированный шлюз (API Gateway), через которого все партнеры обязаны получать данные. Этот шлюз автоматически проверяет валидность полученного от абонента согласия именно для той услуги, которую запрашивает партнер. Таким образом, нормативное требование о конкретности и информированности согласия (ст. 6 152-ФЗ) реализуется на техническом уровне. Контроль этапов жизненного цикла персональных данных включает в себя разнообразные методы контроля на каждом этапе жизненного цикла ПДн.

В целом, контроль процесса идентификации жизненных циклов ПДн это не просто набор разнообразных мер, а согласованный комплекс методов и действий способный регулировать слаженную работу каждого из этапов. Нарушение на любом из этапов контроля свидетельствует о неэффективности всей системы и ставит под сомнение целесообразность ее применения на последующих стадиях.

Оценка политики в области обработки персональных данных и ее соблюдения

После разработки и внедрения системы внутреннего контроля в ту или иную организацию телеком оператора возникает необходимость проанализировать и подтвердить её функциональность и результативность. Для этого Федеральным законом № 152 предусмотрена оценка эффективности мер по обеспечению внутреннего контроля ПДн – комплекс мероприятий организационно-технического характера, по итогам которого составляется официальный протокол. На его основании можно начинать эксплуатацию системы внутреннего контроля ПДн.

Оценочные мероприятия внутреннего контроля организации телеком оператора может осуществляться как в добровольном, так и в обязательном порядке. Проводятся усилиями самой организации, либо путем привлечения сторонних специалистов. Внутри организации оценка строится по модели «Трех линий защиты», каждая из которых играет свою роль:

1. Первая линия – операционный менеджмент – это непосредственное управление операционными рисками и выполнение контрольных процедур. Включает в себя: финансовый отдел, отдел продаж и обслуживания.

2. Вторая линия – функции управления рисками и внутреннего контроля – это подразделения разрабатывающие стандарты, координирующие и оценивающие работу первой линии. Включает в себя: служба безопасности, юридический отдел, служба внутреннего контроля.

3. Третья линия – внутренний аудит – независимая и объективная оценка первых двух линий. Включает в себя: служба внутреннего аудита.

Эффективность модели зависит от четкого разграничения ролей и налаженного взаимодействия между линиями защиты. Это позволяет оценить, насколько продуктивно функционирует система и справляются ли предусмотренные меры защиты с поставленными задачами. Оценочные мероприятия включают в себя анализ:

– структурных особенностей системы внутреннего контроля ПДн;

– достаточности внутренней документации, ее соответствия прописанным в нормативно-правовых актах требованиям;

– технологических нюансов обработки ПДн абонентов, состава программно-технологической базы;

– верное определение уровня защиты ПДн и способы защиты для каждого из них;

– уровня подготовки персонала, осведомленности и распределения ответственности;

– состояния выполнения работ по поддержанию стабильного функционирования системы внутреннего контроля.

Для составления окончательного вердикта специалистам необходимо проанализировать соответствие организационно-техническим требованиям и произвести испытания внедренных защитных мер от потенциальных угроз. По итогам каждого теста и этапа заполняются протоколы, а выводы отражаются в итоговом заключении.

Оценка технических средств контроля, мониторинга и реагирования

В целях предупреждения несанкционированного проникновения, утечки данных и прочих угроз собственными силами организации, либо привлеченными специалистами с помощью специализированного оборудования и программного обеспечения проводятся испытания всех технических средств контроля, мониторинга и реагирования. Проверка проводится по тем программным продуктам, которые задействованы в системе контроля. Например, такие программы как:

– DLP-система – это специализированное программное обеспечение, предназначенное для предотвращения утечки данных;

– RBAC-система – это модель управления доступом, в которой администраторы предоставляют разрешения отдельным пользователям в зависимости от их ролей и обязанностей в организации;

– SEIM-система – выполняет мониторинг, анализ и корреляцию событий безопасности. В экосистеме телеком-оператора, такой как МТС, ее роль особенно критична для контроля доступа партнеров. Например, SEIM-платформа может агрегировать логи аутентификации с портала партнеров, логи доступа к базам данных и события от сетевых экранов. Корреляция этих событий позволяет выявлять сложные атаки, такие как попытка доступа к данным абонентов из нехарактерного географического местоположения в ночное время, что может свидетельствовать о компрометации учетных данных партнера. Таким образом, SEIM трансформирует разрозненные данные в actionable intelligence для службы безопасности.

Испытания и тестирование программных продуктов помогут удостовериться в том, что системы хранения и передачи ПДн надежно защищены от угроз. Испытания по техническим средствам контроля, мониторинга и реагирования проводятся по следующим подсистемам:

– антивирусная защита и действующая лицензия на него;
– контроль доступа к ПДн у определенных лиц;
– поддержание целостности ПДн, их группировка по критериям сбора и хранения;
– степень защищенности каналов связи для передачи данных;
– тест на возможные вторжения в систему;
– оценка защищенности системы и данных.

Таким образом, проверка и оценка эффективности внутреннего контроля в области политики обработки ПДн и технического оснащения помогает на раннем этапе выявить возможные пробелы и предотвратить их, что не допустить утечки информации или куда хуже несанкционированное вторжение в систему. В таблице 2 представлены существующие процедуры для защиты данных при работе с новыми партнерами.

Таблица 2

Процедуры защиты при работе с новыми партнерами

Процедура	Содержание	Механизм реализации
Типовой договор	Обязательство партнёра соблюдать стандарты оператора	Разработка типового договора с правом одностороннего обновления требований
Требования к интеграции	Использование безопасных каналов и шифрования	Сертификация ИТ-решений партнёра, внедрение защищённых шлюзов
Право на аудит	Проверка эффективности контроля у партнёра	Плановые аудиты, привлечение независимых экспертов
Тестирование на уязвимости	Регулярное сканирование систем партнёра	Разработка типовой программы тестирования

Источник: составлено авторами.

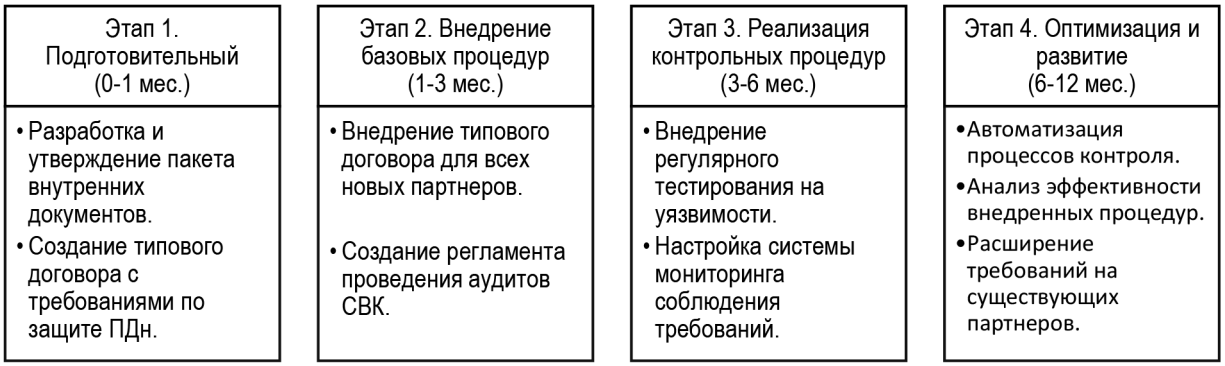

Рис. 3. *Дорожная карта внедрения процедур защиты Пдн*

Источник: составлено авторами.

Для минимизации рисков, построения и внедрения защитных процедур, которые усилят контрольную среду необходим комплексный подход, реализуемый через последовательное внедрение регламентированных процедур. На рисунке 3 представлена предлагаемая дорожная карта, описывающая поэтапное

создание системы для реализации контрольных процедур защиты ПДн при подключении новых партнеров. Каждый этап в ней детализирован с указанием конкретных мероприятий, ожидаемых результатов и ответственных сторон, что обеспечивает практическую применимость предлагаемых мер.

Достижение этой цели разбито на четыре ключевых этапа, которые раскрывают логику и содержание каждого шага:

Этап 1. Подготовительный (0-1 месяц).

Цель: создать нормативную базу для единой контрольной среды.

Мероприятия:

1. Сформировать рабочую группу для аудита текущих партнеров и выявления уязвимостей.

2. Разработать и утвердить пакет документов:

– Политика взаимодействия с партнерами (Due Diligence, классификация по рискам).

– Регламент передачи ПДн (процедуры, шифрование).

– Типовой договор (требования оператора, право на аудит, уведомление об инцидентах).

Результат: единый пакет документов для новых партнеров, устранение правовой неоднородности.

Этап 2. Внедрение базовых процедур (1-3 месяца).

Цель: интегрировать стандарты в операционную деятельность.

Мероприятия:

1. Обязательное использование типового договора для всех новых партнеров.

2. Обучение менеджеров новым правилам.

3. Создать регламент и чек-листы для аудитов партнеров (с периодичностью по категории риска).

Результат: новые партнеры подключаются на безопасных условиях, создан механизм проверки.

Этап 3. Реализация контрольных процедур (3-6 месяцев).

Цель: активное выявление и устранение уязвимостей.

Мероприятия:

1. Регулярное тестирование на уязвимости.

2. Настройка мониторинга: интеграция данных (SIEM, DLP) и оповещений о подозрительной активности.

Результат: снижение количества инцидентов за счет раннего обнаружения слабых мест.

Этап 4. Оптимизация и развитие (6-12 месяцев).

Цель: достичь максимальной эффективности и масштабируемости.

Мероприятия:

1. Автоматизация: дашборды с KPI безопасности, автоматизированные workflow (поток работы) согласования партнеров.

2. Анализ эффективности: Сравнение метрик «до/после», опросы стейкхолдеров.

3. Работа с существующими партнерами: Программа приведения старых договоров в соответствие с новыми стандартами.

Результат: создание самосовершенствующейся и масштабируемой системы контроля.

Выводы

Таким образом, реализация предложенной детализированной дорожной карты позволит оператору создать не фрагментарный, а целостный и надежный контур защиты ПДн. Такой подход трансформирует безопасность из затратной статьи в стратегический актив, который повышает доверие абонентов, укрепляет деловую репутацию и обеспечивает устойчивое развитие цифровой экосистемы в условиях ожесточающегося регуляторного давления.

Литература

1. Квятковская И.Ю., Фам Куанг Хиеп. Система показателей оценки качества телекоммуникационных услуг и метод их оценки // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2013. № 2. С. 98-103.

2. Кодекс корпоративного управления Банка России. [Электронный ресурс]. URL: https://cbr.ru/statichtml/file/59420/inf_apr_1014.pdf (дата обращения: 14.11.2025).

3. Обработка и защита персональных данных ПАО «Сбербанк». [Электронный ресурс]. URL: https://www.sberbank.ru/ru/person/kibrary/personal_data/processing (дата обращения: 17.11.2025).

4. Репников Н.И., Богомолова И.П., Василенко И.Н. Совершенствование управления образовательным процессом и взаимодействием с внешними партнерами на основе современных цифровых решений // Лидерство и менеджмент. 2025. Т. 12. № 4. С. 979-1002. DOI: 10.18334/lim.12.4.122816.

5. Роскомнадзор Нормативные правовые акты в сфере связи / Роскомнадзор. [Электронный ресурс]. URL: https://36.rkn.gov.ru/law/p30164/ (дата обращения: 14.11.2025).

6. Толстиков А. Новые правила обезличивания персональных данных. [Электронный ресурс]. URL: https://habr.com/ru/articles/931348/ (дата обращения: 14.11.2025).

7. Указание Банка России от 28.12.2020 г. № 5683-У «О требованиях к системе внутреннего контроля профессионального участника рынка ценных бумаг» (Зарегистрировано в Минюсте России 05.02.2021 N 62416). [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_377124/ (дата обращения: 14.11.2025).

8. Финансовые результаты ПАО «МТС». [Электронный ресурс]. URL: https://ir.mts.ru/investors/financial_center/financial_results (дата обращения: 17.11.2025).

9. Хайретдинов Р. Защита персональных данных на протяжении всего жизненного цикла. [Электронный ресурс]. URL:https://www.itsec.ru/articles/dlp-malovato-budet-zashchita-personalnyh-dannyh-na-protyazhenii-vsego-zhiznennogo-cikla (дата обращения: 14.11.2025).

10. GDPR для российского бизнеса. [Электронный ресурс]. URL: https://blog.infra-tech.ru/gdpr-zashchita-dannyh/ (дата обращения: 14.11.2025).