

УДК 004.4

**ПРОГРАММНО-ТЕХНИЧЕСКИЕ АСПЕКТЫ СЕРВИСА «ЭЛЕКТРОННАЯ
ЗАЧЕТНАЯ КНИЖКА СТУДЕНТА»**

Домбровский Я.А.

старший преподаватель

*Калужский государственный университет им. К.Э. Циолковского,
Калуга, Россия*

Комаров К.А.

магистрант

*Калужский государственный университет им. К.Э. Циолковского,
Калуга, Россия*

Аннотация.

В статье исследуются программно-технические аспекты сервиса «Электронная зачетная книжка студента», ориентированного на предоставление гражданам сведений о статусе обучающегося и результатах освоения образовательной программы в электронном виде. Актуальность обусловлена государственным экспериментом по формированию электронных сведений о студенческих документах и последующей институционализацией практики использования электронных студенческих билетов и зачетных книжек [5,9]. С учетом нормативных требований к обработке персональных данных и юридической значимости академических записей обоснованы нефункциональные требования к сервису: надежность, отказоустойчивость, масштабируемость, интероперабельность и защищенность. Предложена целевая архитектурная модель (уровни представления, прикладных сервисов, интеграции и хранения данных) и набор инженерных практик сопровождения (мониторинг, журналирование, резервное копирование, тестирование). В качестве исследовательского результата приведена расчетная оценка пиковых нагрузок

для типового вуза и показано, какие архитектурные механизмы позволяют удерживать требуемые показатели доступности и времени отклика.

Ключевые слова: электронная зачетная книжка, электронный студенческий билет, цифровая трансформация, архитектура информационной системы, интеграция, отказоустойчивость, масштабируемость, информационная безопасность, персональные данные, эксплуатация.

SOFTWARE AND HARDWARE ASPECTS OF THE "ELECTRONIC STUDENT RECORD BOOK" SERVICE

Dombrovsky Y.A.

Senior Lecturer

Kaluga State University named after K.E. Tsiolkovsky,

Kaluga, Russia

Komarov K.A.

Master's student

Kaluga State University named after K.E. Tsiolkovsky,

Kaluga, Russia

Abstract.

The paper examines the software and hardware aspects of the “Electronic Student Record Book” service aimed at providing citizens with information about student status and learning outcomes in digital form. The relevance is driven by the governmental experiment on generating digital records for student documents and the subsequent institutionalization of electronic student IDs and record books in Russia [5,9]. Considering regulatory requirements for personal data processing and the legal significance of academic records, we derive non-functional requirements for the service: reliability, fault tolerance, scalability, interoperability, and secure data exchange. A target architectural model (presentation, application services, integration,

and data layers) and a set of operational engineering practices (monitoring, logging, backup, testing) are proposed. As a research contribution, a workload model is presented for a typical university during peak periods, demonstrating how architectural mechanisms help meet availability and latency targets.

Keywords: electronic record book, digital student ID, digital transformation, information system architecture, integration, fault tolerance, scalability, information security, personal data, operations.

Переход к электронным формам фиксации результатов обучения является устойчивым направлением цифровой трансформации высшего образования. В России переход к электронным студенческим документам был реализован через эксперимент, установленный постановлением Правительства РФ №509 (период 25.04.2024–31.12.2025), предусматривающий формирование электронных сведений о студенческих билетах и зачетных книжках и их отображение на Едином портале государственных услуг [9]. Дальнейшее развитие подхода закреплено федеральным законом №539-ФЗ от 29.12.2025, который ввел возможность использования электронных версий студенческого билета и зачетной книжки наряду с бумажными [5].

Для образовательных организаций и разработчиков ИС это означает смещение акцента с локальных «учетных» решений к распределенному межсистемному контуру, в котором электронная зачетная книжка становится сервисом, интегрированным с вузовскими системами управления учебным процессом и государственными цифровыми каналами [8,14]. Следовательно, ключевыми становятся программно-технические вопросы: архитектура и интеграция, модели обеспечения надежности и масштабирования, информационная безопасность и эксплуатация при пиковых нагрузках.

Сервис обрабатывает персональные данные обучающихся, поэтому проектирование должно учитывать требования федерального закона №152-ФЗ «О персональных данных» [15], а также подзаконные акты, регламентирующие

требования к защите персональных данных в ИСПДн и состав организационно-технических мер (в частности, постановление Правительства РФ №1119 и приказ ФСТЭК России № 21) [7, 12]. При межведомственном взаимодействии и интеграции с государственными информационными системами следует учитывать подходы к защите информации в государственных ИС, закрепленные в требованиях ФСТЭК России (приказ №17) [10].

Юридическая значимость записей об успеваемости предопределяет требования к целостности и прослеживаемости изменений. Минимальный состав «аудитного следа» включает идентификаторы дисциплины и периода, дату/время, субъекта внесения, основание выставления/изменения оценки и результат операции. В целях снижения рисков спорных ситуаций целесообразно хранить версионную историю и использовать неизменяемые журналы событий (append-only) с контролем целостности.

Нормативный контекст использования электронных студенческих документов задается законом №273-ФЗ «Об образовании в Российской Федерации» [11] с учетом изменений, внесенных законом №539-ФЗ [5]. Наличие государственных каналов доступа к сведениям повышает требования к унификации интерфейсов и безопасности соединений. В частности, при интеграции с инфраструктурой «Госуслуг» и ЕСИА применимы регламентные документы, описывающие требования к защищенным соединениям и механизмам аутентификации [6,13].

Исследование выполнено на основе комбинированной методики, включающей: анализ нормативных документов и публичных описаний сервиса [5,8,9,14]; контент-анализ научных публикаций по тематике электронного документооборота и цифровых сервисов в университетах [1,4]; сопоставление архитектурных вариантов (монолит, модульный монолит, микросервисы) по критериям надежности, сопровождений и интеграционной гибкости с опорой на общие подходы проектирования ИС [3]; расчетное моделирование пиковых нагрузок на основе предположений о численности контингента и сценариях

использования; экспертную декомпозицию рисков и мер защиты с опорой на требования ПП РФ и ФСТЭК [7,9,10].

Расчетные сценарии не претендуют на измерение производительности конкретного промышленного экземпляра сервиса, их назначение – показать порядок величин и связать архитектурные решения с достижением целевых показателей (SLO) по времени отклика и доступности.

Исследования внедрения электронного документооборота в образовательных организациях показывают, что устойчивость решения в эксплуатации во многом определяется нефункциональными требованиями и соответствием инженерных практик установленным регламентам [1,4]. Для сервиса целесообразно выделять функциональные требования (просмотр сведений, подтверждение статуса, выгрузка/печать выписок и т.п.) и нефункциональные требования, определяющие качество и устойчивость решения. Таблица 1 фиксирует рекомендуемое соответствие между нефункциональными требованиями и механизмами их достижения.

Таблица 1 – Соответствие нефункциональных требований и механизмов реализации

Нефункциональное требование	Показатель (пример)	Механизмы реализации
Доступность	SLO: 99,5–99,9%/мес	резервирование; балансировка; автоперезапуск; раздельные зоны отказа
Производительность	P95 1–2 с	кэширование; оптимизация БД; асинхронная обработка; CDN/edge
Масштабируемость	рост нагрузки без остановки	горизонтальное масштабирование; контейнеризация; очереди сообщений
Целостность данных	версионность; аудит	транзакции; неизменяемые журналы; контроль целостности; сверка данных
Безопасность	снижение рисков утечек/искажений	RBAC/ABAC; MFA; шифрование каналов; журналирование; сегментация
Интероперабельность	подключение ИС разных вендоров	версирование API; адаптеры; ETL; контрактное тестирование

Сопровождаемость	обновления без простоев	CI/CD; feature flags; blue-green/canary; наблюдаемость
------------------	-------------------------	--

С учетом межсистемного характера решения рационально применять многослойную архитектуру с разделением контуров ответственности: 1) слой представления (веб/мобильные клиенты, виджеты государственных порталов); 2) слой прикладных сервисов (бизнес-логика, правила формирования представлений); 3) интеграционный слой (адаптеры к системам вуза и внешним сервисам, маршрутизация, трансформация форматов); 4) слой хранения и аналитики (операционные БД, журнал событий, витрины данных). Для снижения связности между источниками данных и каналами предоставления информации рекомендуется выделять доменные контексты: учебные результаты, справочники, идентификация и права доступа, журнал аудита.

Практически целевая архитектура может быть реализована как модульный монолит или как набор микросервисов. Микросервисный подход дает преимущества по горизонтальному масштабированию и независимому обновлению компонентов, но повышает сложность наблюдаемости и управления конфигурациями. Для большинства вузов оптimalен модульный монолит с выделенным интеграционным контуром и последующей эволюцией отдельных модулей в микросервисы по мере роста нагрузки и зрелости DevOps-процессов [3].

Интеграция с системами управления учебным процессом (электронные ведомости, расписание, контингент), LMS и учетными системами является критическим фактором актуальности данных. Для каждой сущности необходимо определить источник истины (system of record) и режим синхронизации: событийный (push), пакетный (batch ETL) или запросный (pull) с кэшированием.

Рекомендуется реализовать интеграционный слой как API-шлюз и набор адаптеров, которые нормализуют форматы (JSON/XML), обеспечивают версионирование контрактов, поддерживают гарантированную доставку

событий (очереди сообщений) и идемпотентность операций. Для взаимодействия с внешними государственными каналами применимы регламенты подключения к API ЕПГУ и методические материалы по использованию ЕСИА, включающие требования к защищенным соединениям и механизмам аутентификации [6,13]

Для первичной оценки требуемой производительности рассмотрим сценарии массового обращения к ЭЗК в период сессии. Пиковый поток запросов можно оценить выражением: $RPS = (N \times a \times k) / (60 \times t)$, где N - количество обучающихся, a - доля активных пользователей в пиковом окне, k - среднее число запросов на пользователя за окно (открытие списка дисциплин, просмотр деталей, обновления), t - длительность пикового окна в минутах. Полученные значения не являются результатом измерений, а используются как расчетная постановка для выбора класса инфраструктуры и для последующего нагружочного тестирования (таблица 2).

Таблица 2 – Расчетная оценка пиковой нагрузки (RPS) для сервиса «Электронная зачетная книжка студента» по сценариям масштаба

Сценарий	N, чел.	a	k, запросов	t, мин	RPS (расчет)
S1 (региональный вуз)	12000	0.25	8	10	40.0
S2 (крупный вуз)	35000	0.30	10	10	175.0
S3 (федеральный масштаб/агрегация)	100000	0.35	12	10	700.0

Даже при умеренных параметрах активности расчет показывает, что система должна устойчиво обрабатывать десятки-сотни запросов в секунду, причем с существенным преобладанием операций чтения. Это обосновывает применение кэширования на уровне представлений (например, «текущий семестр»), а также использование оптимизированных запросов к БД и предвычисленных агрегатов. Для верификации расчетных оценок рекомендуется проводить нагружочное тестирование с профилем, приближенным к реальному, и контролем метрик времени отклика, ошибок и ресурсоемкости.

Основные узкие места обычно формируются в трех контурах: 1) СУБД (конкуренция за блокировки и I/O), 2) интеграционные вызовы к внешним системам (латентность и лимиты), 3) генерация агрегированных представлений и выписок. Соответственно рекомендуется: кэшировать справочники и часто запрашиваемые представления; использовать асинхронные очереди для операций, не требующих немедленного ответа; минимизировать количество сетевых вызовов за счет пакетирования; разделять транзакционные и аналитические нагрузки (OLTP/OLAP) с помощью реплик и витрин.

Для сервисов, влияющих на учебный процесс, следует задавать явные показатели надежности (SLO) и параметры восстановления: допустимую потерю данных (RPO) и целевое время восстановления (RTO). Базовые практики: кластеризация критических компонентов (БД, кэш), автоматическое переключение, резервные копии с проверкой восстановления, раздельные контуры тестовой и производственной сред, непрерывный мониторинг метрик и трассировка запросов.

Наблюдаемость должна строиться на трех источниках: метрики (нагрузка, латентность, ошибки), логи (технические и аудитные) и трассы распределенных запросов. Журнал аудита должен фиксировать: субъект действия, объект (запись/оценка), время, основание изменения и результат операции. Для предотвращения подмены записей рекомендуется неизменяемое хранение журналов и контроль целостности (хеш-цепочки) в сочетании с регламентами доступа и архивирования.

Угрозы для электронной зачетной книжки целесообразно группировать по трем направлениям: 1) нарушение конфиденциальности (утечки персональных данных); 2) нарушение целостности (несанкционированное изменение оценок, подмена записей); 3) нарушение доступности (DDoS, отказ инфраструктуры в пиковые периоды). Меры защиты должны формироваться с учетом требований к ИСПДн (ПП РФ № 1119) и перечня организационно-технических мер (приказ ФСТЭК № 21) [7,12].

Контроль доступа рекомендуется реализовать как минимум в модели RBAC с учетом категорий пользователей (студент, преподаватель, сотрудник деканата, администратор). Для операций с повышенным риском (изменение записей, выгрузка массовых данных, администрирование интеграций) целесообразны многофакторная аутентификация и расширенное журналирование. Для защищенного обмена данными используется TLS, а при необходимости применения российских криptoалгоритмов – соответствующие стандарты, включая ГОСТ Р 34.12-2015 [2].

В дополнение к защите канала важны меры обеспечения целостности данных: транзакционные механизмы, проверка согласованности при синхронизации с системами-источниками, идемпотентные обработчики событий, а также процедуры периодической сверки между сервисом и учетной системой вуза.

Практические рекомендации по внедрению и сопровождению:

- 1) Выполнить инвентаризацию данных и регламентов: какие сущности ведутся в каких ИС, каковы правила пересдач и апелляций, кто и когда имеет право вносить изменения.
- 2) Зафиксировать интеграционные контракты (модели данных, версии API, коды ошибок) и сопровождать их автоматическими тестами.
- 3) До ввода в эксплуатацию выполнить нагрузочное тестирование для сценариев сессий и массовых обновлений; заложить резерв по производительности и предусмотреть деградацию по функциональности без полного отказа.
- 4) Ввести практики SRE: мониторинг SLI/SLO, управление инцидентами, постмортемы, регулярные учения по восстановлению.
- 5) Проектировать меры безопасности по принципу security by design: минимизация прав, сегментация, аудит, шифрование, регулярное обновление зависимостей.

Сервис «Электронная зачетная книжка студента» в силу массовости и юридической значимости предъявляет повышенные требования к программно-технической реализации. На основе анализа нормативного контекста и научных публикаций по цифровизации документооборота в образовании обоснованы нефункциональные требования и предложена архитектурная модель, ориентированная на интеграцию и эксплуатационную устойчивость [1,4,5,9]. Расчетные сценарии показывают, что достижение целевых показателей доступности и времени отклика возможно при использовании кэширования, асинхронной обработки, разделения нагрузок и кластеризации критических компонентов. Представленные рекомендации могут быть использованы при проектировании и сопровождении вузовских и межведомственных решений, обеспечивающих предоставление электронных студенческих документов через государственные цифровые каналы.

Библиографический список:

1. Абдусаламов, Р. А. Правовые основы внедрения электронного документооборота в вузе // Юридический Вестник Дагестанского государственного университета. 2023. URL: <https://cyberleninka.ru/article/n/pravovye-osnovy-vnedreniya-elektronnogo-dokumentooborota-v-vuze> (дата обращения: 11.01.2026).
2. ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры. - М.: Стандартинформ, 2015.
3. Корнилова, И. В. Электронный документооборот в образовательной организации / И. В. Корнилова // Проблемы реализации прав человека и гражданина в условиях современных социальных трансформаций : Материалы XIV Всероссийской научно-практической конференции с международным участием, посвященной памяти профессора Ф.М. Рудинского, Москва, 20 апреля 2023 года. – Саратов: Издательство "Саратовский источник", 2023. – С. 280-284.

4. Коцюба, И. Ю. Основы проектирования информационных систем [Текст] : учебное пособие / И. Ю. Коцюба, А. В. Чунаев, А. Н. Шиков. – СПб. : [б. и.], 2015. – 206 с.

5. Методические рекомендации по использованию ЕСИА. Минцифры России. URL:

<https://digital.gov.ru/uploaded/files/metodicheskierekomendatsiipoispolzovaniyuesiav348-1.pdf> (дата обращения: 11.01.2026).

6. Минцифры России. Электронные студенческие билеты и зачётные книжки (проект на Госуслугах). URL:

<https://digital.gov.ru/activity/gosuslugi/elektronnye-studencheskie-bilety-i-zachyotnye-knizhki> (дата обращения: 11.01.2026).

7. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». URL:
<https://base.garant.ru/70252506/> (дата обращения: 11.01.2026).

8. Постановление Правительства РФ от 20.04.2024 № 509 «О проведении эксперимента по формированию в электронном виде сведений о студенческих билетах и сведений о зачетных книжках...». Официальное опубликование: 22.04.2024. URL: <https://publication.pravo.gov.ru/document/0001202404220030> (дата обращения: 11.01.2026).

9. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». URL:
https://www.consultant.ru/document/cons_doc_LAW_147084/ (дата обращения: 11.01.2026).

10. Приказ ФСТЭК России от 18.02.2013 № 21 (ред. от 14.05.2020) «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных...». URL:

https://www.consultant.ru/document/cons_doc_LAW_146520/ (дата обращения: 11.01.2026).

11. Регламент подключения к API Единого портала государственных и муниципальных услуг (ЕПГУ). Версия 1.8. URL: https://gu-st.ru/content/partners/api_for_gu/Reglament_podklyucheniya_k_API_Gosuslug_1_8.docx (дата обращения: 11.01.2026).

12. Сервис «Электронный студенческий»: справка портала «Госуслуги». URL: https://www.gosuslugi.ru/help/faq/lk_education/102154 (дата обращения: 11.01.2026).

13. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (действующая редакция). Официальный интернет-портал правовой информации. URL: <https://pravo.gov.ru/proxy/ips/?docbody=&nd=102108261> (дата обращения: 11.01.2026).

14. Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» (действующая редакция). Официальный интернет-портал правовой информации. URL: <https://pravo.gov.ru/proxy/ips/?docbody=&nd=102162745> (дата обращения: 11.01.2026).

15. Федеральный закон от 29.12.2025 № 539-ФЗ «О внесении изменений в Федеральный закон “Об образовании в Российской Федерации”» (электронные студенческие билеты и зачетные книжки). Официальное опубликование: 29.12.2025. URL: <https://publication.pravo.gov.ru/document/0001202512290027> (дата обращения: 11.01.2026).