БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2026. – № 1 (120). – 54–68

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004.6 DOI: 10.17212/2782-2230-2026-1-54-68

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ УПРАВЛЕНИЯ ПРАВАМИ ДОСТУПА В ИНФОРМАЦИОННОЙ СИСТЕМЕ УЧЕБНОГО ЦЕНТРА*

Г.В. ТРОШИНА[1], М.К. БАЮКОВ[2]

[1] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, кандидат технических наук, доцент кафедры вычислительной техники. E-mail: troshina@corp.nstu.ru*
[2] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, лаборант кафедры вычислительной техники E-mail: bayukov.2019@stud.nstu.ru*

В настоящее время учебные центры активно используют информационные системы для организации и сопровождения образовательного процесса в условиях как очного, так и дистанционного обучения. Расширение спектра образовательных услуг и рост объемов обрабатываемой информации, включая персональные данные обучающихся и сотрудников, учебную, организационную и финансовую информацию, обусловливают повышенные требования к обеспечению информационной безопасности. Данная работа посвящена вопросам обеспечения информационной безопасности в информационной системе учебного центра на основе управления правами доступа. В работе выделены основные группы данных, подлежащие хранению и обработке в процессе оказания образовательных услуг. Особое внимание уделено архитектуре информационной системы, построенной по клиент-серверному принципу. Рассмотрены особенности взаимодействия компонентов системы и роль серверной части в реализации механизмов защиты информации и контроля доступа к ресурсам. Значительная часть работы посвящена вопросам безопасности системы и организации уровней доступа пользователей. Описана ролевая модель управления доступом, позволяющая разграничить права пользователей в соответствии с их функциональными обязанностями. Доступ к функционалу системы реализован с помощью двух последовательных этапов: процедуры аутентификации и процедуры авторизации. Логическое разделение данных, нормализованная структура таблиц, использование идентификаторов вместо персональных данных, а также применение ограничений целостности позволяет повысить уровень защищенности базы данных и снизить риски утечки, искажения и несанкционированного изменения информации. Показано, что применение принципа наименьших привилегий и контроль доступа на уровне программных интерфейсов способствуют снижению рисков несанкционированного доступа и повышению надежности функционирования системы.

* Статья получена 12 февраля 2026 г.

Ключевые слова: информационная безопасность, управление правами доступа, ролевая модель доступа, информационная система учебного центра, аутентификация, авторизация, защита персональных данных

ВВЕДЕНИЕ

В условиях цифровизации образовательной деятельности информационные системы учебных центров играют ключевую роль в организации и сопровождении учебного процесса. Учебные центры реализуют широкий спектр образовательных услуг в формате очного и дистанционного обучения.

Основными направлениями деятельности являются:

- подготовка к школьным экзаменам (ОГЭ, ЕГЭ);
- курсы по школьным предметам (математика, русский язык, физика, информатика и др.);
- дополнительное образование для детей младшего возраста;
- курсы для взрослых – переподготовка, повышение квалификации, обучение современным цифровым навыкам;
- языковые курсы (английский и другие иностранные языки);
- онлайн-курсы и вебинары как в записи, так и в прямом эфире;
- индивидуальные занятия и мини-группы в зависимости от потребностей обучающихся.

Каждая образовательная программа имеет определенную длительность, расписание, преподавательский состав и стоимость обучения. Ведение и отслеживание таких данных вручную становится всё более трудоемким при росте числа клиентов, преподавателей и программ. Это создает потребность в комплексной информационной системе, способной обеспечить автоматизацию и интеграцию всех ключевых процессов учебного центра.

Такие системы обеспечивают хранение и обработку значительных объемов данных, включая персональные данные обучающихся и сотрудников, учебно-методическую информацию, а также сведения финансового и организационного характера. В связи с этим вопросы обеспечения информационной безопасности приобретают особую актуальность.

1. КЛАССИФИКАЦИЯ ДАННЫХ

Учебный центр, как организация, предоставляющая образовательные услуги, ежедневно работает с большим объемом структурированной и неструктурированной информации.

В рамках деятельности учебного центра подлежат сбору, хранению, обновлению и аналитической обработке следующие групп данных (табл. 1).

Таблица 1

Table 1

Группы и виды данных

Groups and types of data

Группа данных	Вид данных
Обучающиеся (клиенты учебного центра)	• ФИО, контактные данные. • Дата рождения, пол. • История обучения: список пройденных курсов, посещаемость, успеваемость. • Финансовая информация. • Канал привлечения, анкеты, отзывы
Преподаватели	• ФИО, контактная информация. • Образование, опыт, специализация. • Закрепленные курсы, расписание занятий. • Заработная плата и рабочая нагрузка. • Рейтинги и отзывы обучающихся
Курсы и учебные программы	• Название, описание, длительность. • Программа обучения, расписание. • Требования к обучающимся. • Стоимость и формат обучения
Расписание	• Временные слоты, аудитории / онлайн-ссылки. • Назначенные преподаватели и группы. • Изменения, замены, отмены занятий
Успеваемость и посещаемость	• Оценки по модулям и итоговая аттестация. • Посещение занятий, причины пропусков. • Динамика успеваемости по времени
Финансы	• Счета, оплаты, задолженности. • Абонементы, скидки, акции. • Отчёты по доходам и расходам
Административные и вспомогательные данные	• Пользовательские роли и права доступа. • История взаимодействия с клиентами. • Внутренняя документация, задачи и обращения

Все эти данные должны быть надежно защищены, логически организованы, доступны для поиска, анализа и оперативной обработки.

2. АРХИТЕКТУРА СИСТЕМЫ

Архитектура системы основывается на использовании фронтенд-приложения на Nuxt и бэкенд-приложения на Django REST framework с использованием PostgreSQL в качестве системы управления базами данных. Критически важные функции контроля доступа реализованы на стороне бэкенд-приложения, что исключает возможность обхода ограничений на уровне клиентского приложения. В состав системы входят следующие ключевые компоненты.

- Прокси/веб-сервер NGINX – функционирует как «передний экран» приложения: принимает все входящие HTTP(S)-запросы и на основе конфигурации маршрутизации либо направляет их к фронтенду или к API-бэкенду, либо обслуживает статические файлы и обеспечивает TLS-termination [1].
- Nuxt – отвечает за генерацию HTML на стороне сервера: при получении запроса, требующего рендеринга интерфейса, Nuxt инициирует жизненный цикл, в котором делает запросы к API, получает данные и формирует финальный HTML.
- Django и Django REST framework – реализует бизнес-логику, обрабатывает запросы к REST-эндпоинтам, осуществляет валидацию, сериализацию/десериализацию данных, взаимодействует с базой данных. В рамках серверной части используется механизм сериализации и маршрутизации, что упрощает использование CRUD-операций и структуру кода [2].
- PostgreSQL – выступает как надежное решение для хранения данных. Django посредством своего ORM обеспечивает взаимодействие с PostgreSQL как с реляционной СУБД, а DRF гарантирует корректное представление данных для Nuxt [3].

Общая архитектура системы представлена на рис. 1. Схема отражает взаимосвязь между основными компонентами системы: прокси-/веб-сервером NGINX, клиентской частью на Nuxt, серверной частью на Django REST Framework и СУБД PostgreSQL [4].

Логика потоков данных

1. Пользователь направляет HTTP-запрос из браузера.
2. NGINX перенаправляет запрос на Nuxt-сервер.
3. Nuxt обращается к REST API Django для получения данных.
4. Формируется внутренний запрос API.
5. Django инициирует обращение к PostgreSQL.
6. PostgreSQL принимает запрос.
7. База данных возвращает результаты Django.
8. API отправляет данные обратно Nuxt.

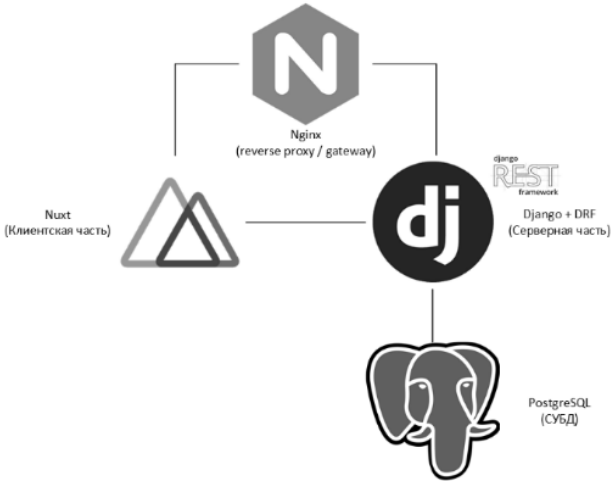

Рис. 1. Архитектура системы

Fig. 1. System architecture

9. Nuxt передает сгенерированный HTML NGINX, который отправляет страницу клиенту.

10. Запросы, относящиеся непосредственно к API, могут направляться NGINX сразу на Django.

3. БЕЗОПАСНОСТЬ СИСТЕМЫ

Доступ к функционалу системы реализуется в два последовательных этапа: аутентификация и авторизация. Аутентификация выполняется на серверной стороне с использованием встроенных механизмов Django REST Framework и заключается в проверке корректности представленных пользователем учетных данных. После успешного подтверждения личности инициируется процесс авторизации, в ходе которого определяется, обладает ли пользователь с назначенной ролью необходимыми правами для выполнения запрашиваемой операции.

Проверка прав доступа осуществляется на уровне серверных эндпоинтов, каждый из которых связан с определенным набором разрешенных действий. При попытке выполнения операции через интерфейс клиентского приложения доступ будет отклонен, если эндпоинт не допускает выполнение данной операции пользователем [5].

Фронтенд, реализованный на Nuxt, осуществляет дополнительную проверку прав доступа для корректного отображения пользовательского интерфейса, включая скрытие недоступных разделов и элементов управления. Однако такие проверки носят вспомогательный характер и не используются как основной механизм защиты.

Рис. 2. Настройки доступа в клиентском приложении

Fig. 2. Access settings in the client application

Безопасность базы данных, представленной на рис. 3, обеспечивается не только средствами программной защиты. Логическое разделение данных, нормализованная структура таблиц, использование идентификаторов вместо персональных данных, а также применение ограничений целостности позволяет повысить уровень защищенности базы данных и снизить риски утечки, искажения и несанкционированного изменения информации.

4. ОРГАНИЗАЦИЯ УРОВНЕЙ ДОСТУПА

Для разграничения доступа в системе используется ролевая модель управления доступом (RBAC). В рамках такой модели каждому пользователю назначается одна из ролей, определяющая его права и допустимые действия в системе. Реализация RBAC позволяет централизованно управлять правами доступа, упростить администрирование и повысить общий уровень защищенности информационной системы [6].

В системе предусмотрены следующие роли пользователей: администратор, руководитель, преподаватель и студент (обучающийся, клиент учебного центра). Диаграмма прецедентов, представленная на рис. 4, отражает совокупность доступных действий для каждой роли и демонстрирует логику разграничения прав в соответствии с их функциональными обязанностями.

Рис. 3. Структура базы данных

Fig. 3. Database structure

Также в целях повышения уровня информационной безопасности в системе реализован принцип минимальных привилегий [7], согласно которому каждой роли предоставляется минимально необходимый набор прав.

Администраторы – пользователи с максимальным набором прав, отвечающие за общую конфигурацию и настройку платформы, управление пользователями и контроль ее работоспособности. Перечень доступных эндпоинтов для роли администратора представлен в табл. 2.

Цели и задачи

- Управлять учетными записями пользователей (регистрировать и удалять учетные записи, назначать роли, восстанавливать права доступа).
- Настраивать модули системы: создавать или изменять справочники (например, перечень учебных программ, виды платежей).
- Обеспечить интеграцию системы с внешними сервисами.

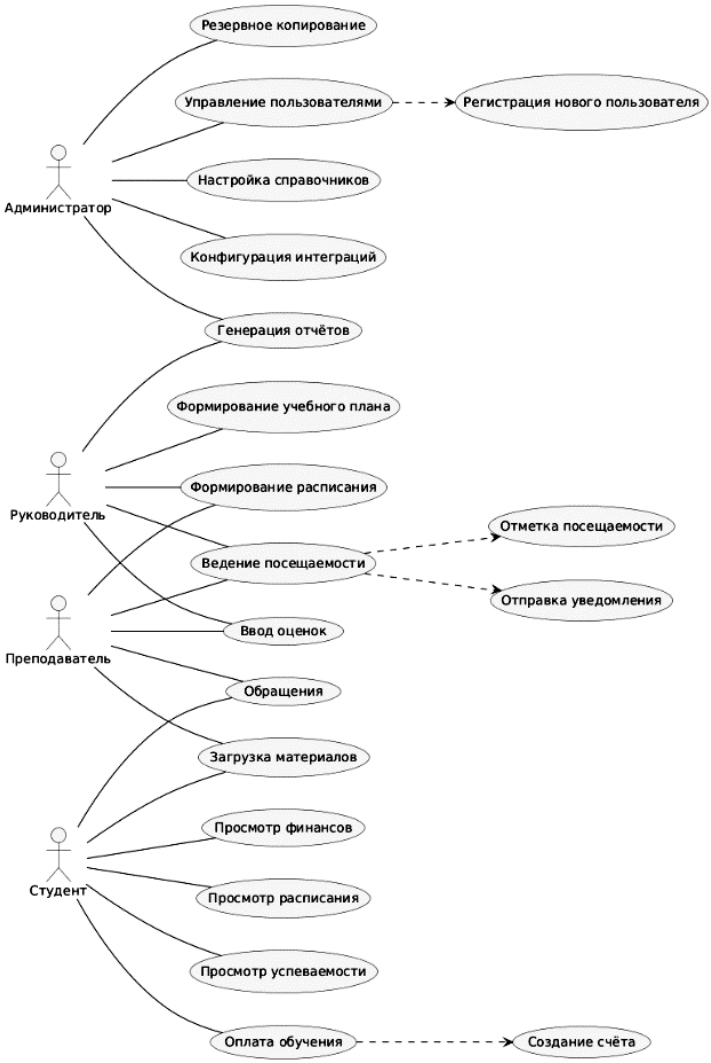

Рис. 4. Диаграмма прецедентов

Fig. 4. Use Case Diagram

Таблица 2

Table 2

Доступные эндпоинты для администратора

Available endpoints for the administrator

Эндпоинт	Доступ
/api/auth/login/, /api/auth/logout/	Полный
/api/users/, /api/users/{id}/	Полный
/api/logs/	Просмотр
/api/branches/, /api/branches/{id}/	Полный
/api/lesson-types/, /api/lesson-types/{id}/	Полный
/api/task-templates/, /api/task-templates/{id}/	Полный
/api/accounts/, /api/accounts/{id}/	Полный
Все остальные эндпоинты	Полный

Руководители учебных подразделений (заведующие отделениями, методисты) отвечают за качество и своевременность образовательных программ, контроль планирования учебного процесса и принятие управленческих решений. Перечень доступных эндпоинтов для роли руководителя представлен в табл. 3.

Цели и задачи

- Планирование обучения: определять перечень курсов, назначать преподавателей и корректировать расписание.
- Контроль успеваемости: получать агрегированные данные по посещаемости и результатам студентов, выявлять проблемные группы или преподавателей.
- Анализ показателей эффективности: просматривать дашборды с графиками загрузки аудиторий, динамикой продаж курсов, коэффициентом удержания студентов.
- Формирование отчетности: готовить отчеты о результатах учебного процесса для руководства центра, инвесторов или органов контроля.

Таблица 3

Table 3

Доступные эндпоинты для руководителя

Available endpoints for the supervisor

Эндпоинт	Доступ
/api/auth/login/, /api/auth/logout/	Полный
/api/clients/, /api/clients/{id}/	Полный
/api/interactions/, /api/interactions/{id}/	Полный
/api/programs/, /api/programs/{id}/	Полный
/api/courses/, /api/courses/{id}/	Полный
/api/groups/, /api/groups/{id}/	Полный
/api/groups/{id}/members/	Полный
/api/schedule/, /api/schedule/{id}/	Полный
/api/subscription-plans/, /api/subscription-plans/{id}/	Полный
/api/client-subscriptions/, /api/client-subscriptions/{id}/	Полный
/api/invoices/, /api/invoices/{id}/	Полный
/api/payments/, /api/payments/{id}/	Полный
/api/tasks/, /api/tasks/{id}/	Полный

Преподаватели непосредственно взаимодействуют со студентами (обучающимися, клиентами учебного центра), оценивают их успехи и вносят данные о посещаемости и результатах в систему, проводят занятия. Перечень доступных эндпоинтов для роли преподавателя представлен в табл. 4.

Цели и задачи

- Получение актуального расписания занятий и информации о студентах в своих группах.
- Ведение статистики посещаемости и проставление оценок.
- Просмотр учебных материалов (если они загружены в систему) и загрузка собственных раздаточных материалов или ссылок на внешние ресурсы.
- Обмен сообщениями со студентами: рассылка уведомлений, ответ на вопросы, размещение объявлений о дополнительных занятиях или консультациях.

Таблица 4

Table 4

Доступные эндпоинты для преподавателя

Available endpoints for the teacher

Эндпоинт	Доступ
/api/auth/login/, /api/auth/logout/	Полный
/api/groups/, /api/groups/{id}/	Просмотр (только свои)
/api/groups/{id}/members/	Просмотр
/api/schedule/, /api/schedule/{id}/	Просмотр
/api/tasks/, /api/tasks/{id}/	Полный

Клиенты учебного центра являются конечными потребителями образовательных услуг и используют систему преимущественно в режиме просмотра своих данных, взаимодействия с преподавателями и администрацией, а также для оплаты обучения и просмотра учебных материалов. Перечень доступных эндпоинтов для роли студент (обучающегося, клиента учебного центра) представлен в табл. 5.

Таблица 5

Table 5

Доступные эндпоинты для студентов

Available endpoints for the student

Эндпоинт	Доступ
/api/auth/login/, /api/auth/logout/	Полный
/api/client-subscriptions/, /api/client subscriptions/{id}/	Просмотр (только свои)
/api/invoices/	Просмотр (только свои)
/api/payments/	Просмотр (только свои)
/api/schedule/	Просмотр (только свои)
/api/tasks/	Просмотр (только свои)

Цели и задачи

- Просмотр личного расписания занятий, уведомлений об изменениях и сроков проведения контрольных модулей.
- Доступ к собственным учебным материалам.
- Введение статуса выполнения домашних заданий, мониторинг оценок и успеваемости.
- Оплата обучения через встроенные платежные сервисы и отслеживание статуса своих платежей и задолженностей.
- Коммуникация с администрацией и преподавателями.

ЗАКЛЮЧЕНИЕ

Были рассмотрены вопросы обеспечения информационной безопасности информационной системы учебного центра на основе управления правами доступа. Учитывая специфику деятельности учебных центров, связанную с обработкой персональных, учебных и финансовых данных, особое значение приобретает защита информации от несанкционированного доступа и неправомерного использования.

В ходе работы было обосновано применение ролевой модели управления доступом, позволяющей разграничить полномочия пользователей в соответствии с их функциональными обязанностями. Реализация механизмов аутентификации и авторизации обеспечивает контроль доступа к ресурсам системы и способствует соблюдению принципа наименьших привилегий. Это позволяет снизить риски утечки информации, искажения данных и нарушения целостности информационных ресурсов.

Разграничение доступа к функциональным возможностям системы, в том числе к REST-API, обеспечивает защиту серверной части приложения и исключает возможность обхода ограничений на уровне клиентского интерфейса. Дополнительное использование журналирования действий пользователей повышает прозрачность работы системы и создает условия для последующего аудита и анализа событий безопасности.

Таким образом, реализованные механизмы управления правами доступа обеспечивают необходимый уровень информационной безопасности информационной системы учебного центра, повышают надежность ее функционирования и соответствуют основным требованиям к защите информации в современных информационных системах.

СПИСОК ЛИТЕРАТУРЫ

1. Nginx: website. – URL: https://nginx.org/ (accessed: 26.02.2026).

2. Django REST framework: website. – URL: https://www.django-rest-framework.org/ (accessed: 26.02.2026).

3. PostgreSQL: The world's most advanced open source relational database: website. – URL: https://www.postgresql.org/ (accessed: 26.02.2026).

4. *Brian Caffey*. Building web applications with Django, Django REST Framework, Nuxt.js and docker. – URL: https://briancaffey.github.io/2020/12/27/building-web-applications-with-django-drf-and-nuxt/ (accessed: 26.02.2026).

5. Понимание API-эндпоинтов // LightNode. – 2024. – November 20. – URL: https://go.lightnode.com/ru/tech/api-end-point (дата обращения: 26.02.2026).

6. *Салихова Н.* Ролевая модель управления доступом (RBAC) // SpectrumData: сайт. – 2025. – 21 марта. – URL: https://spectrumdata.ru/blog/proverka-soiskatelya/rolevaya-model-upravleniya-dostupom-rbac-chto-eto-i-zachem-ona-nuzhna/ (дата обращения: 26.02.2026).

7. Сбербанк. Принцип минимальных привилегий. – URL: https://www.sberbank.ru/ru/person/kibrary/vocabulary/princip-minimalnykh-privilegij (дата обращения: 26.02.2026).

Трошина Галина Васильевна, кандидат технических наук, доцент кафедры вычислительной техники Новосибирского государственного технического университета. Направления научных исследований – базы данных, идентификация динамических объектов. Имеет более 95 публикаций. E-mail: troshina@corp.nstu.ru

Баюков Михаил Константинович, лаборант кафедры вычислительной техники Новосибирского государственного технического университета. Направления научных исследований – базы данных, информационные технологии. E-mail: bayukov.2019@stud.nstu.ru

DOI: 10.17212/2782-2230-2026-1-54-68

Information security ensuring based on access rights management in the information system of the training center*

G.V. Troshina[1], M.K. Bayukov[2]

[1] *Novosibirsk State Technical University, 20 K. Marx Prospekt, Novosibirsk, 630073, Russian Federation, candidate of technical sciences, associate professor of the computer engineering department. E-mail: troshina@corp.nstu.ru*
[2] *Novosibirsk State Technical University, 20 K. Marx Prospekt, Novosibirsk, 630073, Russian Federation, laboratory assistant of the computer engineering department. E-mail: bayukov.2019@stud.nstu.ru*

Currently, educational centers are actively using information systems to organize and support the educational process in conditions of both full-time and distance learning. The expansion of the range of educational services and the growth in the volume of processed information, including personal data of students and employees, educational, organizational and financial information, lead to increased requirements for information security ensuring. This work is devoted to the issues of information security ensuring in the information system of the training center based on access rights management. The paper highlights the main groups of data to be stored and processed in the process of educational services providing. Special attention is paid to the architecture of the information system based on the client-server principle. The interaction features of the components system and the role of the server part in the mechanism implementation of information protecting and access control to resources are considered. A significant part of the work is devoted to the system security issues and the organization of user access levels. A role-based access control model is described that allows you to differentiate user rights in accordance with their functional responsibilities. Access to the system functionality is implemented using two consecutive stages: authentication and authorization procedures. Logical separation of data, the normalized structure of tables, the use of identifiers instead of personal data, as well as the use of integrity restrictions can increase the level of database security and reduce the risks of leakage, distortion and unauthorized change of information. It has been shown that the application of the principle of least privileges and access control at the level of software interfaces contribute to reducing the risks of unauthorized access and increasing the reliability of the system.

Keywords: information security, access rights management, role-based access model, training center information system, authentication, authorization, personal data protection

REFERENCES

1. *Nginx*. Website. Available at: https://nginx.org/ (accessed 26.02.2026).

2. *Django REST framework*. Website. Available at: https://www.django-rest-framework.org/ (accessed 26.02.2026).

* *Received 12 February 2026.*

3. *PostgreSQL: The world's most advanced open source relational database*. Website. Available at: https://www.postgresql.org/ (accessed 26.02.2026).

4. *Brian Caffey*. *Building web applications with Django, Django REST Framework, Nuxt.js and docker*. Available at: https://briancaffey.github.io/2020/12/27/building-web-applications-with-django-drf-and-nuxt/ (accessed 26.02.2026).

5. Understanding API Endpoints: The Gateway to Web Services. *LightNode*, 2024, November 20. Available at: https://go.lightnode.com/ru/tech/api-end-point (accessed 26.02.2026).

6. Salikhova N. Rolevaya model' upravleniya dostupom (RBAC) [Role-based access control model (RBAC)]. *SpectrumData*. Website, 2025, March 21. (In Russian). Available at: https://spectrumdata.ru/blog/proverka-soiskatelya/rolevaya-model-upravleniya-dostupom-rbac-chto-eto-i-zachem-ona-nuzhna/ (accessed 26.02.2026).

7. SberBank. *Printsip minimal'nykh privilegii* [Principle of Least Privilege, PoLP]. (In Russian). Available at: https://www.sberbank.ru/ru/person/kibrary/vocabulary/princip-minimalnykh-privilegij (accessed 26.02.2026).

Для цитирования:

Трошина Г.В., Баюков М.К. Обеспечение информационной безопасности на основе управления правами доступа в информационной системе учебного центра // Безопасность цифровых технологий. – 2026. – № 1 (120). – С. 54–68. – DOI: 10.17212/2782-2230-2026-1-54-68.

For citation:

Troshina G.V., Bayukov M.K. Obespechenie informatsionnoi bezopasnosti na osnove upravleniya pravami dostupa v informatsionnoi sisteme uchebnogo tsentra [Information security ensuring based on access rights management in the information system of the training center]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2026, no. 1 (120), pp. 54–68. DOI: 10.17212/2782-2230-2026-1-54-68.