УДК 004.056

Особенности использования ролевой модели безопасности (модель взаимоисключающих ролей) в вузе

Корниенко Светлана Владимировна — канд. техн. наук, доцент кафедры «Информатика и информационная безопасность». Научные интересы: информационная безопасность, защита информации. E-mail: sv.diass99@yandex.ru

Протасов Максим Сергеевич — студент 3-го курса направления 10.05.03 «Информационная безопасность автоматизированных систем». Научные интересы: информационная безопасность, разработка защищенной серверной части приложений, реализация защищенных серверных интерфейсов. E-mail: protasima@bk.ru

Петербургский государственный университет путей сообщения Императора Александра I, Россия, 190031, Санкт-Петербург, Московский пр., 9

Для цитирования: Корниенко С. В., Протасов М. С. Особенности использования ролевой модели безопасности (модель взаимоисключающих ролей) в вузе // Интеллектуальные технологии на транспорте. 2025. № 4 (44). С. 5–16. DOI: 10.20295/2413-2527-2025-444-5-16

Аннотация. *Практическое применение базовой модели ролевого разграничения доступа в современных информационных системах, в том числе информационных системах высших учебных заведений, с каждым годом становится критической проблемой безопасности этих систем. Для повышения уровня безопасности информационной системы при использовании модели ролевого разграничения доступа необходимо вводить дополнительные ограничения на использование ролей, что позволяет при построении системы ограничить количество ролей путем внедрения ограничений привилегий пользователя в сеансе работы.* ***Цель:*** *модификация модели ролевого разграничения доступа с введением ограничений по взаимоисключению ролей для повышения уровня безопасности информационной системы высшего учебного заведения.* ***Методы:*** *применены методы статического и динамического взаимного исключения ролей, методы статического и динамического количественного ограничения на обладание ролью и правами доступа.* ***Результаты:*** *разработана модель ролевого разграничения доступа с добавлением взаимоисключающих ролей, выполнена программная реализация тестовой модели.* ***Практическая значимость:*** *заключается в повышении уровня безопасности при применении модели ролевого разграничения доступа в информационных системах, которым свойственна сложная архитектура системы ролей.*

Ключевые слова: *ролевое разграничение доступа, модель взаимоисключающих ролей, политика разграничения доступа, информационная безопасность*

2.3.6 *— методы и системы защиты информации, информационная безопасность (технические науки)*

Введение

В условиях стремительного развития информационных технологий и цифровизации всех сфер жизнедеятельности общества особую актуальность приобретает проблема обеспечения безопасного и дифференцированного доступа к данным, циркулирующим в информационных системах. Одной из самых гибких и понятных моделей разграничения доступа является ролевая модель, которая учитывает не только внутреннюю иерархию пользователей информационной системы, но и иерархию организации, в которой применяется информационная система [1].

При этом базовая модель ролевого разграничения доступа имеет один существенный недостаток. При использовании такой модели в классическом варианте перед администратором безопасности возникает дилемма: при определении небольшого количества ролей с широкими полномочиями существенно снижается безопасность модели, при создании большого количества ролей возникают сложности управления моделью. Для решения этой проблемы возможно строить различные модификации базовой ролевой модели [2]. Одним из простых, но эффективных решений является добавление в базовые механизмы различного рода ограничений на использование ролей.

Ролевая модель разграничения доступа

Базовая модель ролевого разграничения доступа (РРД) определяет самые общие принципы построения моделей РРД. В базовой модели РРД основными элементами являются множества пользователей U, множество ролей R, множество полномочий (прав доступа на объекты компьютерной системы) P, множество сессий пользователей S, а также функции:

- PA: $R \rightarrow 2^P$ — функция, определяющая для каждой роли множество прав доступа; при этом для каждого $p \in P$ существует $r \in R$ такая, что $p \in PA(r)$;
- UA: $U \rightarrow 2^R$ — функция, определяющая для каждого пользователя множество ролей, на которые он может быть авторизован;
- user: $S \rightarrow U$ — функция, определяющая для каждой сессии пользователя, от имени которого она авторизована;
- roles: $S \rightarrow 2^R$ — функция, определяющая для пользователя множество ролей, на которые он авторизован в данной сессии, при этом в каждый момент времени для каждого $s \in S$ выполняется условие: $\text{roles}(s) \subseteq UA(\text{user}(s))$.

В базовой модели РРД определены следующие принципы [3, 4]:

- одному субъекту (пользователю) может быть присуще множество ролей;
- одна роль может относиться к множеству пользователей;
- одной роли может быть присуще множество прав доступа;
- одно право доступа может относиться к множеству ролей;
- может быть роль, не присущая ни одному пользователю;
- может быть право доступа, не присущее ни одной роли.

Для обеспечения возможности большего соответствия реальным информационным системам, каждый пользователь которых занимает определенное положение в служебной иерархии организации, на множестве ролей в модели также реализуется иерархическая структура. Данный механизм обеспечивается введением отношения частичного порядка «≤».

В «классической» модели РРД предполагается, что все множества и функции не изменяются с течением времени. Множество ролей, на которые авторизуется пользователь в течение одной сессии, модифицируется самим пользователем. Также в базовой модели отсутствуют механизмы, позволяющие одной сессии активизировать другую сессию — все сессии активизируются пользователем.

Применение базовой модели в вузе

Вопрос эффективности разграничения прав доступа в информационной системе высшего учебного заведения периодически поднимается в научных работах [5–8]. Применение базовой модели РРД в вузе (без дополнительных модификаций) является возможным, но неэффективным и в какой-то мере менее удобным для конечного пользователя. Это связано с тем, что внутренняя иерархия вуза является сложной. Пример построения схемы иерархии вуза на примере ПГУПС приведен на рис. 1 [9].

На рис. 1 пунктиром обозначены косвенные (непрямые) связи. Фигурами одного цвета обозначены большие структуры и их составляющие (например, ректорат и различные проректоры).

Необходимо отметить, что для каждого факультета также свойственна определенная иерархия. Общая схема такой иерархии приведена на рис. 2.

На рис. 2 контрастными цветами обозначены непрямые связи между различными уровнями ие-

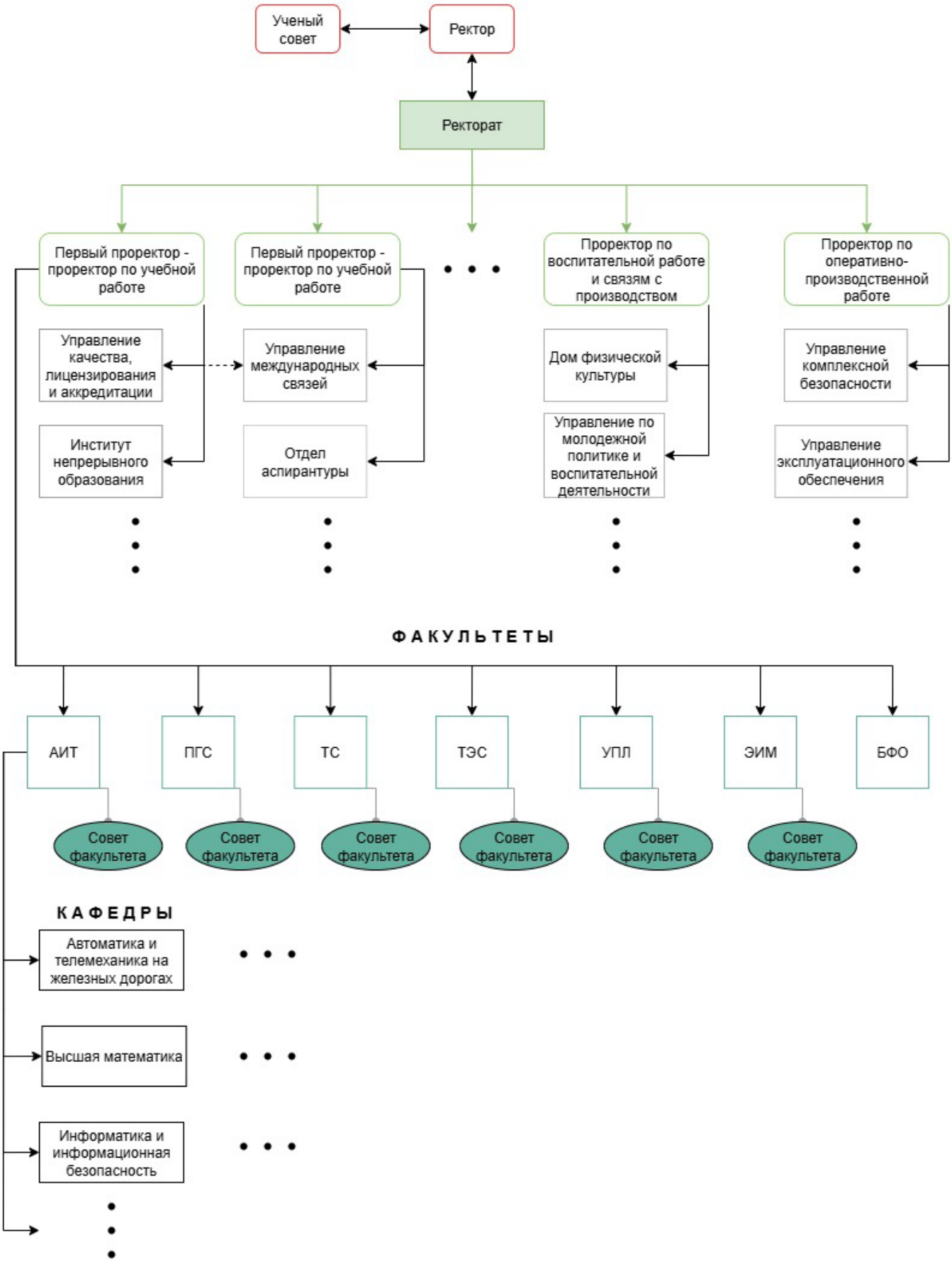

Рис. 1. Общая иерархия вуза на примере ПГУПС

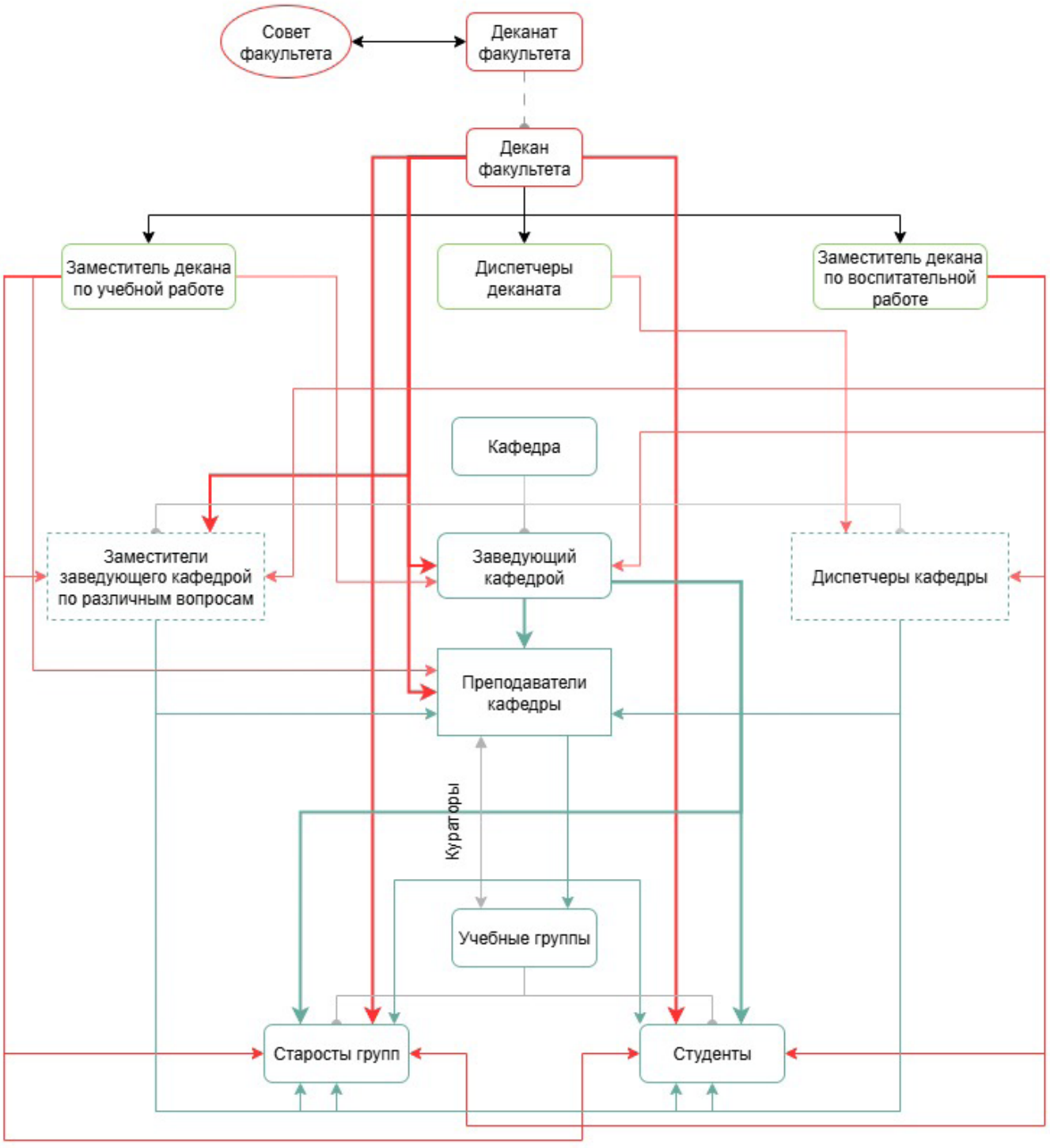

Рис. 2. Общая схема внутренней иерархии факультета

рархии: например, темно-красным выделена связь между деканом факультета и студентами, темно-зеленым — между заведующим кафедрой и старостами групп и т. д.

Из построенных схем видно, что мощность множества ролей большая, кроме того, необходимо учитывать иерархию. Наряду с этим сами связи являются сложными: так, например, ректор может иметь прямую связь с деканом какого-либо факультета, минуя проректора, а деканы — с преподавателями, минуя заведующих кафедрами. Построение приближенной схемы иерархии, которая учитывает все возможные связи, является объемной и трудоемкой задачей.

Построение множества пользователей U на основе внутренней иерархии вуза, которое будет удовлетворять следующим условиям:

1) каждому пользователю соответствует только одна роль,

2) каждый пользователь в определенный момент времени имеет только те права, которые ему действительно нужны в этот момент времени,

не представляется возможным. Возможно лишь определение конечного множества пользователей, при этом каждый пользователь будет авторизован со всеми ролями одновременно, то есть будет иметь все права, присущие ему, в любой момент времени.

Иными словами, данную проблему можно описать так: при построении базовой модели РРД для реальной организации необходимо учитывать не только прямые связи, которые показаны на иерархии организации, но и так называемые косвенные связи, которые реализуются между различными уровнями иерархии, минуя промежуточные уровни.

Данный фактор является серьезной угрозой безопасности защищаемой системы в целом. К тому же контроль такой системы практически невозможен из-за большого количества пользователей.

Решением этой проблемы является создание статических и динамических ограничений прав доступа или ролей, то есть использование модификации классической модели РРД — модели взаимоисключающих ролей.

Модель взаимоисключающих ролей

При проектировании модели взаимоисключающих ролей множество ролей и множество прав доступа разбиваются на непересекающиеся подмножества. При этом каждый пользователь может обладать не более чем одной ролью из каждого подмножества ролей, а каждая роль — не более чем одним правом доступа из каждого подмножества прав доступа.

Модель взаимоисключающих ролей включает в себя следующие принципы [3, 4]:

1. Статическое взаимное исключение ролей или прав доступа обеспечивается путем разделения множества ролей и множества прав доступа на непересекающиеся подмножества, которые удовлетворяют условиям:

$$R = R_1 \cup R_n,\ R_i \cap R_j = \varnothing \text{ для } 1 \le i < j \le n;$$

$$\left|UA(u) \cap R_i\right| \le 1 \text{ для } u \in U, i = 1,2,\ldots,n;$$

$$P = P_1 \cup \ldots \cup P_m, P_i \cap P_j = \varnothing \text{ для } 1 \le i < j < m;$$

$$\left|PA(r) \cap P_i\right| \le 1 \text{ для } p \in U, i = 1,2,\ldots,m.$$

Статическое взаимоисключение ролей (прав доступа) выполняется при проектировании и разработке системы разграничения доступа. Суть данного метода заключается в определении структуры множества ролей, а также основных ролей и присущих им прав доступа.

Как правило, на данном этапе выделяются такие роли, удаление которых недопустимо, а изменение прав доступа, присущих этим ролям, будет производиться при модернизации или обновлении всей системы защиты в целом, то есть при приостановке функционирования системы на короткий промежуток.

2. Динамическое взаимное исключение ролей обеспечивается разделением множества ролей на непересекающиеся подмножества, которые удовлетворяют условиям:

$$R = R_1 \cup \ldots \cup R_n,\ \ R_i \cap R_j = \varnothing \text{для } \ 1 \le i < j \le n;$$

$$\left|\text{roles}(s) \cap R_i\right| \le 1 \text{ для } s \in S, i = 1, 2, \ldots, n.$$

При этом в каждой сессии пользователь может обладать не более чем одной ролью из каждого подмножества ролей.

Динамическое взаимное исключение ролей обеспечивается специальным механизмом (например, скриптом), который в зависимости от того, какую сессию активизировал пользователь, выдает ему ту или иную роль. В большинстве реализаций данный механизм предусматривает выбор пользователем одной из присущих им ролей и работает в реальном времени.

3. Задание статического количественного ограничения на обладание ролью или правом доступа, то есть определение двух функций:

$$\alpha : R \to N_0;$$

$$\beta : P \to N_0,$$

где N_0 — множество натуральных чисел с нулем, при выполнении условий:

$$\left|UA^{-1}(r)\right| \le \alpha(r) \text{ для } r \in R;$$

$$\left|PA^{-1}(p)\right| \le \beta(p) \text{ для } p \in P.$$

Для каждой (или определенной) роли устанавливается максимальное число пользователей, которые могут быть на нее авторизованы, а для каждого права доступа — максимальное число ролей, которые могут им обладать.

Такое ограничение бывает полезно, когда при разработке или проектировании системы необходимо ограничить количество пользователей, у которых может быть определенная роль (например, роль администратора безопасности системы должна быть только у одного пользователя) или ограничить количество прав, которое может быть у ролей (например, когда мощность множества прав доступа велика).

4. Задание динамического количественного ограничения на обладание ролью, то есть определение функции

$$\gamma : R \to N_0$$

при выполнении условия

$$\left|\text{roles}^{-1}(r)\right| \le \gamma(r) \text{ для } r \in R.$$

Для роли устанавливается максимальное число сессий, которые могут быть одновременно на нее авторизованы.

Динамическое ограничение обеспечивает дополнительную защиту от сбоев системы, способных привести к искажению или потере данных. В качестве примера можно привести ограничение на одновременную активность: разрешена только одна сессия администратора безопасности системы.

На рис. 3 представлена общая модель взаимоисключающих ролей, которая включает в себя как статическое, так и динамическое взаимное исключение ролей.

В приближении статическое взаимоисключение ролей представлено на рис. 4.

Динамическая модель взаимоисключающих ролей в приближении может иметь различную структуру, что зависит от ее конкретной реализации.

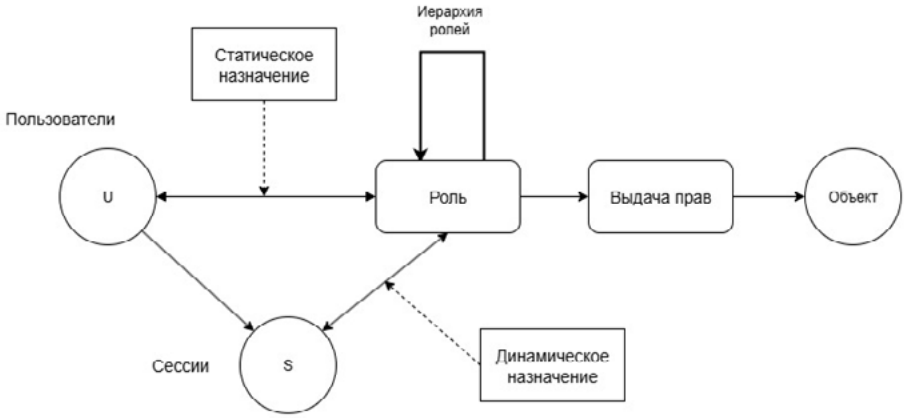

Рис. 3. Модель взаимоисключающих ролей

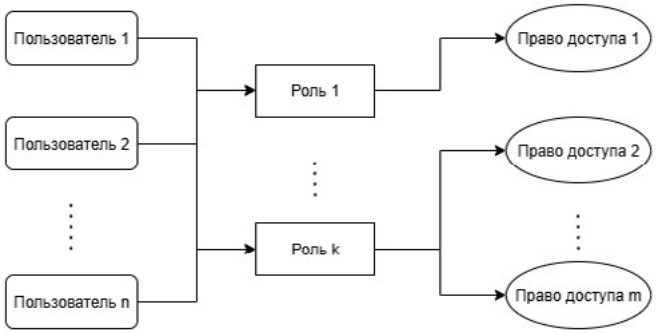

Рис. 4. Общая схема статического взаимного исключения ролей

Особенности применения модели взаимоисключающих ролей в вузе

В связи со сложной структурой иерархии вуза, которая была рассмотрена ранее, следует выделить следующие особенности построения модели взаимоисключающих ролей для разграничения доступа.

Перед описанием особенности построения модели взаимоисключающих ролей следует отметить следующие пункты, свойственные большинству процессов построения моделей разграничения доступа:

1. Необходимо описать объекты, которые находятся в информационной системе, и субъекты, через которые происходит взаимодействие с объектами.

2. Определить пользователей, которые обеспечивают и поддерживают функционирование системы (технические специалисты, администраторы безопасности и др.) и выделить присущие им роли.

3. Для описанных ранее ролей необходимо задать количественные ограничения и реализовать жесткую привязку этих ролей к конкретным пользователям.

После выполнения вышеописанных пунктов следует построить формальное описание основных групп пользователей и присущих им ролей, полномочий, а также дополнительных ограничений, называемых атрибутами, на каждую роль, выделить несовместимые роли [10, 11]. Рекомендуется выполнять проектирование модели взаимоисключающих ролей снизу вверх, то есть начиная с самых нижних уровней иерархии, которые обладают меньшим количеством полномочий.

В качестве атрибутов ролей можно определить для роли студента номер его группы, курс обучения и т. д. Несовместимыми ролями на примере вуза являются роли студента и преподавателя, заведующего кафедрой. Никакая роль из внутренней иерархии организации несовместима с ролями пользователей, отвечающих за функционирование системы.

Проверку на наличие у пользователей несовместимых ролей (например, при компрометации базы данных учетных записей) можно реализовать

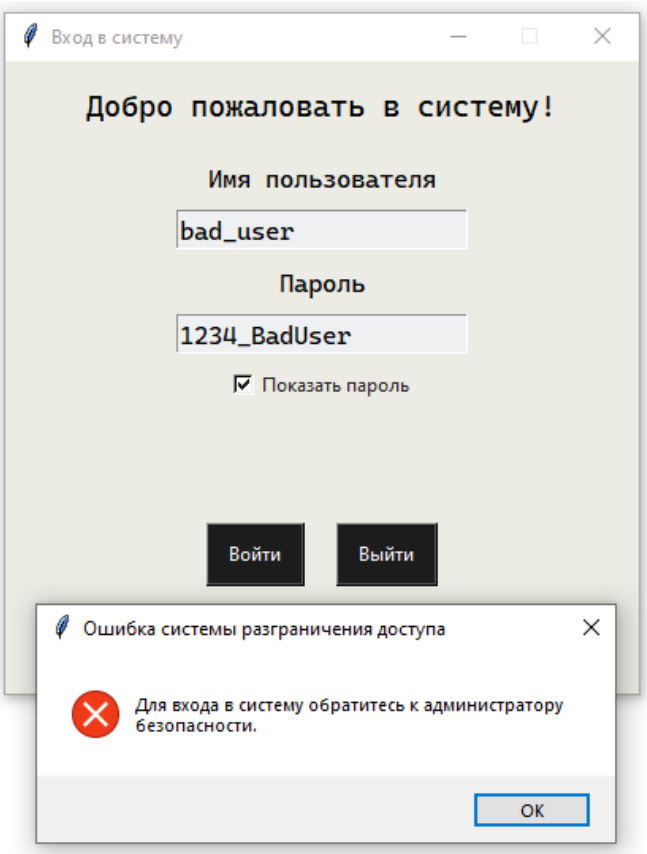

Рис. 5. Отказ в доступе пользователю с несовместимыми ролями

путем отказа в доступе в систему и формирования запроса к администратору безопасности системы (рис. 5).

Стоит отметить, что статическое взаимное исключение ролей подойдет только для двух групп пользователей: «студенты» и «старосты учебных групп». Во-первых, это обусловлено тем, что данные группы пользователей обладают наименьшим количеством полномочий (находятся на нижнем уровне иерархии). Во-вторых, то, что роль «староста учебной группы» обладает полномочиями роли «студент», не является уязвимостью. Напротив, это более удобно и эффективно для конечного пользователя. Однако обратная ситуация недопустима: роль «студент» не может обладать полномочиями роли «староста».

На основе построенного описания основных групп пользователей и присущих им ролей выполняется статическое определение ролей и полномочий. Лучше всего реализовать это в виде таблицы или любой другой структуры данных (табл. 1).

Таблица 1

Статическое определение ролей и полномочий

Группы пользователей	Название ролей	Основные полномочия	Атрибуты
Студент	Студент (student)	Просмотр учебных курсов Просмотр успеваемости …	Специальность Номер группы Курс
Староста	Староста (head_student)	Полномочия роли «Студент» + Редактирование журналов посещаемости …	Как у «Студент»
Преподаватель	Преподаватель (coach)	Редактирование учебных курсов Редактирование журналов успеваемости …	Ученое звание Преподаваемые дисциплины Кафедра …
Заведующий кафедрой	Заведующий кафедрой (department_head)	Назначение преподавателей на курсы …	Ученая степень Ученое звание Кафедра …

Безусловно, для реальной организации такая таблица будет содержать в себе намного больше информации, но использование принципа структурирования данных упростит в дальнейшем реализацию и внедрение системы разграничения доступа в информационную систему организации.

Для передачи полномочий (прав доступа) субъектам системы, через которые пользователь взаимодействует с объектами, формируется множество активируемых пользователем сессий путем выстраивания связей между полномочиями, субъектами и объектами. Права доступа при этом можно разграничить так, чтобы при выборе роли и активации сессии пользователь напрямую не видел те объекты, на взаимодействие с которыми у него недостаточно полномочий.

Например, наполнение рабочего окна для пользователя с ролью «староста группы» (рис. 6, *а*) и присущими этой роли полномочиями отличается от наполнения рабочего окна для пользователя с ролью «преподаватель» (рис. 6, *б*), но при этом они имеют доступ к одинаковым объектам, различаются лишь полномочия, присущие ролям этих пользователей. Рабочее окно для администратора безопасности системы отличается от других, поскольку он работает с другими объектами — базой данных учетных записей, ролями и полномочиями, журналами логирования и ошибок.

На данном этапе также поможет принцип построения снизу вверх: использование такого подхода может облегчить построение элементов множества сессий для ролей, больших по иерархии, поскольку многие наборы (роль, права доступа, активируемая сессия) уже были реализованы, а для пользователя, который обладает ролями разных уровней иерархии, останется определить только набор с ролью большей иерархии. Пример построения множества сессий для двух пользователей приведен на рис. 7.

а *б*

Рис. 6. Рабочее окно пользователя:
а — с ролью «староста группы»; *б* — с ролью «преподаватель»

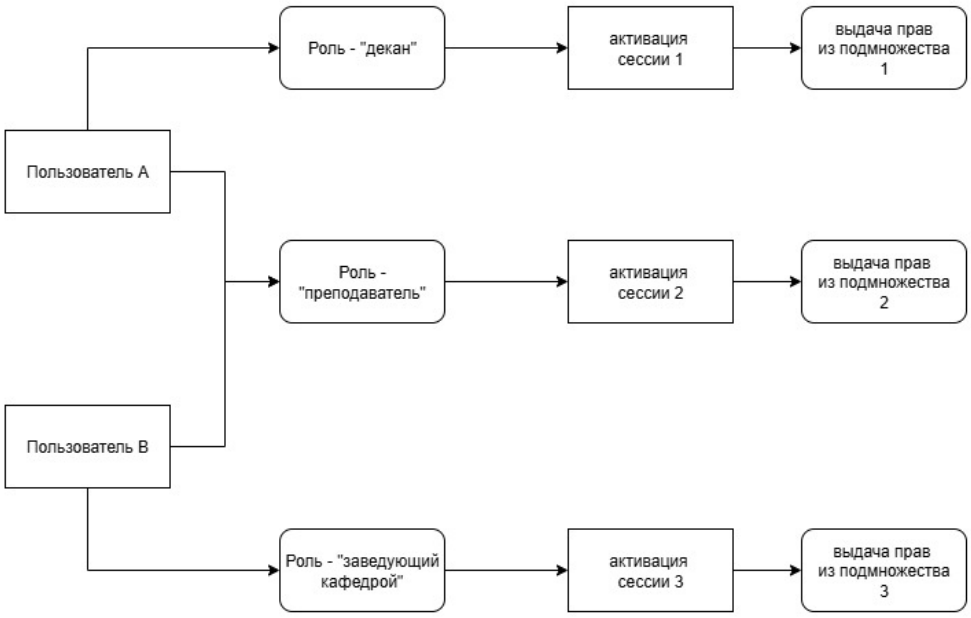

Рис. 7. Пример построения множества сессий

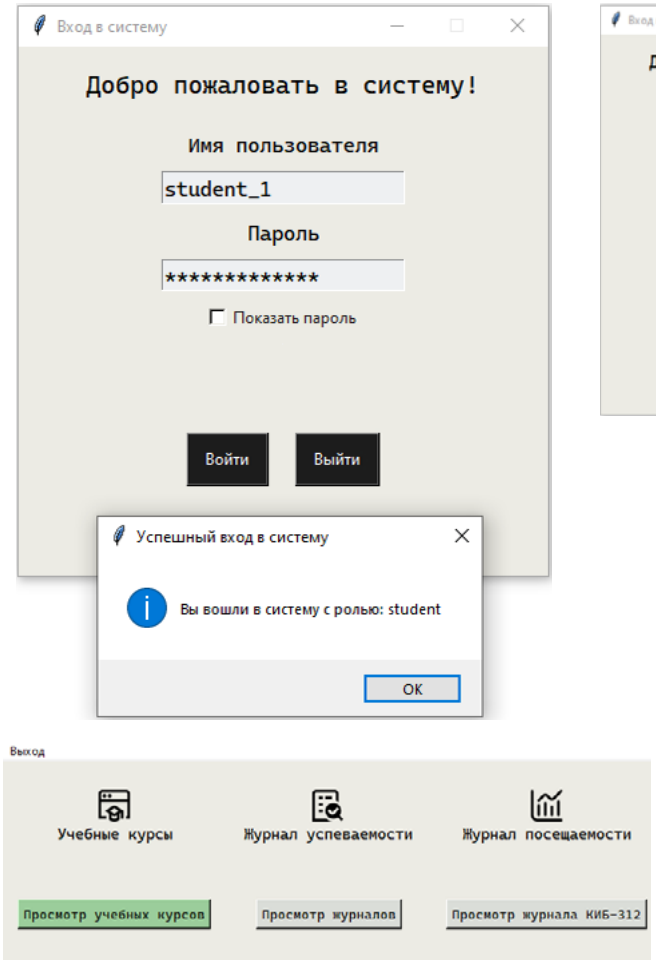

Рис. 8. Активация сессии для пользователя с одной ролью

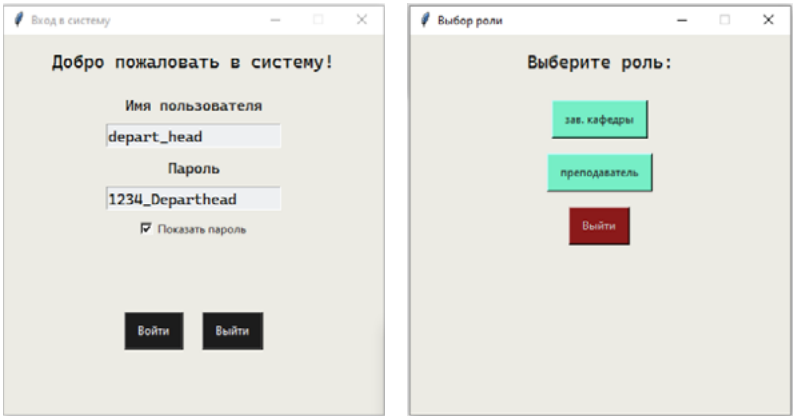

Рис. 9. Выбор пользователем роли при входе в систему

После авторизации пользователя в системе происходит активация сессии, при этом возможны две ситуации:

1. Пользователь не обладает взаимоисключающими ролями или ему присуща всего одна роль (рис. 8). В данном случае у пользователя student_1 имеется единственная роль «student» с атрибутами «group = КИБ-312» и «year = 3».

2. Пользователь имеет несколько взаимоисключающих ролей в системе. Реализуется принцип динамического взаимного исключения ролей: после авторизации в системе пользователь выбирает, под какой ролью он хочет работать (рис. 9), и активируется сессия с соответствующими полномочиями.

Заключение

В результате проведенного исследования были рассмотрены теоретические основы и практические аспекты применения модели взаимоисключающих ролей в информационной системе высшего учебного заведения.

Внедрение такой модификации базовой модели ролевого разграничения доступа является эффективным инструментом обеспечения информационной безопасности системы на основе следующих принципов:

1. Ограничение количества ролей и прав доступа в конкретный момент времени и на протяжении всего действия активной сессии.

2. Возможность динамического изменения ролей тем пользователям, у которых их несколько.

3. Возможна реализация механизмов, позволяющих добавлять/удалять новых пользователей без приостановки функционирования системы, построенной на основе описываемой модели: достаточно добавить новый элемент, состоящий из набора «пользователь, роль, права доступа» в множество сессий.

4. Возможна реализация механизмов, позволяющих добавлять/удалять роли или права доступа конкретных пользователей: достаточно добавить или удалить соответствующий элемент из множества сессий или убрать набор «пользователь, роль, права доступа» из этого элемента.

Основной задачей при реализации подобной модели является необходимость обработки большого объема данных, который нужно формализовать, разбить на множества и выстроить связи. При использовании принципа нисходящего проектирования данной модели задача существенно упрощается, и трудности могут возникнуть лишь при описании пользователей с уникальными ролями, которые не встречались ранее.

Практическая значимость исследования заключается в разработке принципов реализации модели взаимоисключающих ролей в информационных системах, которым свойственна сложная архитектура системы ролей. Данный подход может быть использован не только в учебных заведениях, но и в организациях других сфер деятельности с большим числом сотрудников, в которых необходим контроль конфликтных полномочий.

СПИСОК ИСТОЧНИКОВ

1. Ролевая модель разграничения прав // Блог компании «Солар». 2023. 31 мая. URL: http://rt-solar.ru/products/solar_inrights/blog/3481 (дата обращения: 08.11.2025).

2. Рахметов Р. Ролевая модель безопасности и ее отличия от атрибутной модели управления доступом // Блог компании Security Vision. 2024. 26 августа. URL: http://www.securityvision.ru/blog/rolevaya-model-bezopasnosti-i-eye-otlichiya-ot-atributnoy-modeli-upravleniya-dostupom/ (дата обращения: 08.11.2025).

3. Девянин П. Н. Модели безопасности компьютерных систем: учебное пособие для студентов вузов. М.: Академия, 2005. 144 с.

4. Гайдамакин Н. А. Теоретические основы компьютерной безопасности: учебное пособие. Екатеринбург: Уральский гос. ун-т им. А. М. Горького, 2008. 212 с.

5. Змеев А. А. Модели и метод разграничения доступа в образовательных информационных системах на основе виртуальных машин: автореферат дисс. … канд. техн. наук: 2.3.6 / Змеев Анатолий Анатольевич [Место защиты: Санкт-Петербургский Федеральный исследовательский центр Российской академии наук]. Тверь, 2022. 23 с.

6. Демурчев Н. Г. Проектирование системы разграничения доступа автоматизированной информационной системы на основе функционально-ролевой модели на примере высшего учебного заведения: автореферат дисс. … канд. техн. наук: 05.13.19 / Демурчев Никита Георгиевич [Место защиты: Таганрогский гос. радиотехнический ун-т]. Таганрог, 2006. 18 с.

7. Раецкий А. Д., Шлянин С. А., Ермакова Л. А. Реализация разграничения прав доступа в информационной системе «Портфолио СибГИУ» // Кибернетика и программирование. 2019. № 2. С. 44–54. DOI: 10.25136/2644-5522.2019.2.18530.

8. Разграничение прав при доступе к сервисам и ресурсам электронной информационно-образовательной среды вуза / А. Ю. Ужаринский, А. И. Фролов, В. Н. Волков [и др.] // Преподавание информационных технологий в Российской Федерации: материалы Девятнадцатой открытой Всероссийской конференции: сборник научных трудов (онлайн, 19–20 мая 2021 г.). М.: 1С-Паблишинг, 2021. С. 166–168.

9. Структура и органы управления // Петербургский гос. ун-т путей сообщения Императора Александра I. URL: http://www.pgups.ru/struct (дата обращения: 15.11.2025).

10. Севастьянова Л. Строим ролевую модель управления доступом. Часть первая, подготовительная // Хабр. 2020. 09 июля. URL: http://habr.com/ru/companies/solarsecurity/articles/509998 (дата обращения: 09.11.2025).

11. Attribute Based Access Control NIST SP 1800-3 Practice Guide Original Draft / B. Fisher, N. Brickman, S. Jha [et al.]. National Cybersecurity Center of Excellence, National Institute of Standards and Technology, 2016. 532 p. URL: http://www.nccoe.nist.gov/sites/default/files/legacy-files/abac-nist-sp1800-3-draft.pdf (дата обращения: 08.11.2025).

Дата поступления: 16.11.2025
Решение о публикации: 19.11.2025

Implementation of the Role-Based Access Control Model (Mutually Exclusive Roles Model) at Higher Education Institution

Svetlana V. Kornienko — PhD in Engineering, Associate Professor of the "Information Technology and IT Security" Department. Research interests: information security, information protection. E-mail: sv.diass99@yandex.ru

Maksim S. Protasov — 3rd year Specialist's Degree Student in 10.05.03 Information Security of Automated Systems. Research interests: information security, secure application server development, implementation of secure server interfaces. E-mail: protasima@bk.ru

Emperor Alexander I St. Petersburg State Transport University, 9, Moskovsky ave., St. Petersburg, 190031, Russia

For citation: Kornienko S. V., Protasov M. S. Implementation of the Role-Based Access Control Model (Mutually Exclusive Roles Model) at Higher Education Institution. *Intellectual Technologies on Transport*, 2025, No. 4 (44), Pp. 5–16. DOI: 10.20295/2413-2527-2025-444-5-16. (In Russian)

Abstract. *The practical implementation of the role-based access control model (RBAC) in contemporary information systems, particularly those within higher education institutions, has increasingly become a critical security concern. To enhance the security of an information system utilizing the RBAC model, it is essential to impose further restrictions on role usage. This approach will enable the limitation of the number of roles within the system's architecture by introducing constraints on user privileges during their session.* ***Purpose:*** *to modify the role-based access control model by introducing role exclusion constraints to enhance the security of information systems within higher education institutions.* ***Methods:*** *both static and dynamic mutual exclusion methods for managing roles, along with static and dynamic quantitative limitations on role possession and access privileges.* ***Results:*** *a role-based access control model featuring mutually exclusive roles has been created, and a software implementation of a test model has been successfully carried out.* ***Practical significance:*** *this research is expected to enhance security standards in the deployment of role-based access control models within information systems that feature intricate role architecture.*

Keywords: *role-based access control, model of mutually exclusive roles, access control policy, information security*

REFERENCES

1. Rolevaya model razgranicheniya prav [Role-Based Model of Delimitation of Rights], *Solar Company blog*. Available at: http://rt-solar.ru/products/solar_inrights/blog/3481 (accessed: November 08, 2025). (In Russian)

2. Rakhmetov R. Rolevaya model bezopasnosti i ee otlichiya ot atributnoy modeli upravleniya dostupom [Role-Based Security Model and Its Differences from the Attribute-Based Access Control Model], *Security Vision Company*

Blog. Available at: http://www.securityvision.ru/blog/rolevaya-model-bezopasnosti-i-eye-otlichiya-ot-atributnoy-modeli-upravleniya-dostupom/ (accessed: November 08, 2025). (In Russian)

3. Devyanin P. N. Modeli bezopasnosti kompyuternykh sistem: uchebnoe posobie dlya studentov vuzov [Computer System Security Models: A Tutorial for University Students]. Moscow, Akademiya Publishing House, 2005, 144 p. (In Russian)

4. Gaydamakin N. A. Teoreticheskie osnovy kompyuternoy bezopasnosti: uchebnoe posobie [Theoretical Foundations of Computer Security: a tutorial], Yekaterinburg, A. M. Gorky Ural State University, 2008, 212 p. (In Russian)

5. Zmeev A. A. Modeli i metod razgranicheniya dostupa v obrazovatelnykh informatsionnykh sistemakh na osnove virtualnykh mashin [Models and Method of Access Control in Educational Information Systems Based on Virtual Machines]: Abstract of the diss. on competition of a scientific degree PhD (Engin.). Tver, 2022, 23 p. (In Russian)

6. Demurchev N. G. Proektirovanie sistemy razgranicheniya dostupa avtomatizirovannoy informatsionnoy sistemy na osnove funktsionalno-rolevoy modeli na primere vysshego uchebnogo zavedeniya [Design of an Access Control System for an Automated Information System Based on a Functional-Role Model Using a Higher Education Institution as an Example]: Abstract of the diss. on competition of a scientific degree PhD (Engin.). Taganrog, 2006, 18 p. (In Russian)

7. Raeckiy A. D., Shlyanin S. A., Ermakova L. A. Realizatsiya razgranicheniya prav dostupa v informatsionnoy sisteme “Portfolio SibGIU” [The Implementation of the Differentiation of Access Rights in the “Portfolio SibGIU” Information System], *Kibernetika i programmirovanie [Cybernetics and Programming]*, 2019, No. 2, Pp. 44–54. DOI: 10.25136/2644-5522.2019.2.18530. (In Russian)

8. Uzharinskiy A. Yu., Frolov A. I., Volkov V. N., et al. Razgranichenie prav pri dostupe k servisam i resursam elektronnoy informatsionno-obrazovatelnoy sredy vuza [Differentiation of Rights When Accessing Services and Resources of the Electronic Information and Educational Environment of the University], *Prepodavanie informatsionnykh tekhnologiy v Rossiyskoy Federatsii: materialy Devyatnadtsatoy otkrytoy Vserossiyskoy konferentsii: sbornik nauchnykh trudov [Teaching Information Technology in Russia: Collection of Research Papers for the 19th Open All-Russian Conference], online, May 19–20, 2021*. Moscow, 1C-Publishing, 2021, Pp. 166–168. (In Russian)

9. Structure and Administration, *Emperor Alexander I St. Petersburg State Transport University*. Available at: http://www.pgups.ru/en/struct (accessed: November 15, 2025).

10. Sevastyanova L. Stroim rolevuyu model upravleniya dostupom. Chast pervaya, podgotovitelnaya [Building a Role-Based Access Control Model. Part One, Preparatory], *Khabr Habr*. Published online at July 09, 2020. Available at: http://habr.com/ru/companies/solarsecurity/articles/509998 (accessed: November 09, 2025). (In Russian)

11. Fisher B., Brickman N., Jha S., et al. Attribute Based Access Control NIST SP 1800-3 Practice Guide Original Draft. National Cybersecurity Center of Excellence, National Institute of Standards and Technology, 2016, 532 p. Available at: http://www.nccoe.nist.gov/sites/default/files/legacy-files/abac-nist-sp1800-3-draft.pdf (accessed: November 08, 2025)

Received: 16.11.2025
Accepted: 19.11.2025