УДК 004.622
DOI: 10.26102/2310-6018/2025.51.4.010

# Определение модели управления доступом для телекоммуникационной системы

**Д.С. Калининский, Л.А. Тремасова, Д.В. Гадасин**✉

*Московский технический университет связи и информатики, Москва, Российская Федерация*

***Резюме.*** В статье проведено исследование и сравнительный анализ современных моделей управления доступом, применяемых в телекоммуникационных системах. Рассмотрены три основные модели: управления доступом на основе ролей (RBAC), управления доступом на основе атрибутов (ABAC), управления доступом на основе полномочий (PBAC). В качестве примера использована телекоммуникационная инфраструктура банка, включающая 800 рабочих станций, 200 серверов, 800 сотрудников в офисной зоне и центр обработки данных с 50 серверами, обрабатывающими критические приложения. Пропускная способность между офисами и центром обработки данных составляет 10 Гбит/с, в публичной зоне – 1 Гбит/с. Для обеспечения безопасности используется Active Directory с поддержкой Kerberos и система мониторинга SIEM. В ходе исследования оценивались показатели производительности, такие как время отклика, пропускная способность и устойчивость к пиковым нагрузкам. Был проведен эксперимент безопасности, который включал в себя устойчивость к атакам, гибкость реагирования и уровень защиты в различных сценариях функционирования системы: при ежедневной нагрузке, отражающей стандартную работу сотрудников; при пиковой нагрузке, возникающей в моменты массового обращения к ресурсам (например, в конце отчетного периода); а также в условиях аварийной нагрузки, связанных с инцидентами безопасности или сбоями оборудования. Такой подход позволил выявить различия в эффективности моделей доступа в реальных эксплуатационных ситуациях.

***Ключевые слова:*** модели управления доступом, телекоммуникационные системы, модель управления доступом на основе ролей, модель управления доступом на основе атрибутов, модель управления доступом на основе полномочий.

***Для цитирования:*** Калининский Д.С., Тремасова Л.А., Гадасин Д.В. Определение модели управления доступом для телекоммуникационной системы. *Моделирование, оптимизация и информационные технологии.* 2025;13(4). URL: https://moitvivt.ru/ru/journal/pdf?id=2047 DOI: 10.26102/2310-6018/2025.51.4.010

# Defining an access control model for a telecommunication system

**D.S. Kalininsky, L.A. Tremasova, D.V. Gadasin**✉

*Moscow Technical University of Communications and Informatics, Moscow, the Russian Federation*

***Abstract.*** The article presents a study and comparative analysis of modern access control models used in telecommunication systems. Three main models are considered: role-based access control (RBAC), attribute-based access control (ABAC), and privilege-based access control (PBAC). The bank's telecommunications infrastructure, including 800 workstations, 200 servers, 800 employees in the office area, and a data center with 50 servers processing critical applications, is used as an example. The bandwidth between the offices and the data center is 10 Gbit/s, and in the public area it is 1 Gbit/s. Active Directory with Kerberos support and a SIEM monitoring system are used to ensure security. The study assessed performance metrics such as response time, throughput, and resilience to peak loads. A security experiment was conducted that tested attack resilience, response flexibility, and protection

 

levels under various system operating scenarios: under daily loads reflecting typical employee work; under peak loads occurring during periods of high resource usage (e.g., at the end of a reporting period); and under emergency loads associated with security incidents or equipment failures. This approach allowed us to identify differences in the effectiveness of access models in real operational situations.

***Keywords:*** access control models, telecommunication systems, role-based access control model, attribute-based access control model, authority-based access control model.

***For citation:*** Kalininsky D.S., Tremasova L.A., Gadasin D.V. Defining an access control model for a telecommunication system. *Modeling, Optimization, and Information Technology*. 2025;13(4). (In Russ.). URL: https://moitvivt.ru/ru/journal/pdf?id=2047 DOI: 10.26102/2310-6018/2025.51.4.010

## Введение

Управление доступом к инфокоммуникационным ресурсам играет ключевую роль для предотвращения несанкционированного использования данных и обеспечения безопасности пользователей и инфраструктуры. В последние годы число угроз, связанных с кибератаками и утечками данных, значительно возросло, что требует внедрения современных и эффективных моделей управления доступом, так по данным компании RED Security, в 2024 году количество кибератак на российские компании увеличилось в 2,5 раза по сравнению с 2023 годом, достигнув 130 000 инцидентов [1, 2]. Из них 26000 были высококритичными, способными привести к финансовым потерям или остановке работы организаций [3].

Кроме того, в первом полугодии 2024 года в России было зафиксировано 415 утечек конфиденциальной информации, что на 10,1 % больше по сравнению с аналогичным периодом 2023 года. В результате этих инцидентов было скомпрометировано почти 1 млрд записей персональных данных, что на 33,8 % больше, чем в первом полугодии 2023 года. Эти данные подчеркивают необходимость разработки и внедрения современных и эффективных моделей управления доступом, которые способны противостоять возрастающим киберугрозам и обеспечить безопасность в информационных системах[1] [4].

При организации управления доступом можно выделить следующие широко используемые подходы управления доступом на основе ролей (Role-Based Access Control, RBAC), атрибутов (Attribute-Based Access Control, ABAC) и полномочий (Policy-Based Access Control, PBAC). Инфокоммуникационные системы предъявляют высокие требования к надежности и скорости обработки данных, исходя из этого, эффективность применения определенной модели зависит от ограничений, накладываемых окружающей средой, что определяет преимущества использования той или иной модели[2] [5]. Необходимость разработки гибких и безопасных моделей управления доступом отмечается в таких современных работах в области управления доступом на основе атрибутов (ABAC) для облачных систем, анализ применения RBAC в системах Интернета вещей для повышения управляемости и производительности, а также отчета Национального института стандартов и технологий (NIST), посвященного использованию методов машинного обучения для проверки политик управления доступом [6, 7].

В настоящей работе проводится анализ основных моделей управления доступом, с целью выявления их сильных стороны и оценки степени применимости в инфокоммуникационных средах. Особое внимание необходимо уделить таким аспектам,

[1] Щеглов А.Ю. *Модели, методы и средства контроля доступа к ресурсам вычислительных систем.* Санкт-Петербург: Университет ИТМО; 2014. 95 с.

[2] Hu V.C. Machine Learning for Access Control Policy Verification. Internal Report 8360. National Institute of Standards and Technology. URL: https://doi.org/10.6028/NIST.IR.8360 (дата обращения: 20.06.2025).

как производительность и безопасность, также обосновать целесообразность применения той или иной модели при реализации стратегии защиты данных в зависимости от условий [8].

## Материалы и методы

Для подробного анализа и дальнейшего изменения структурной схемы системы контроля и управления доступом (СКУД) необходимо рассмотреть ее функциональные элементы и взаимосвязи между ними в логической последовательности. Структурная схема СКУД представлена в виде обобщенной схемы (Рисунок 1).

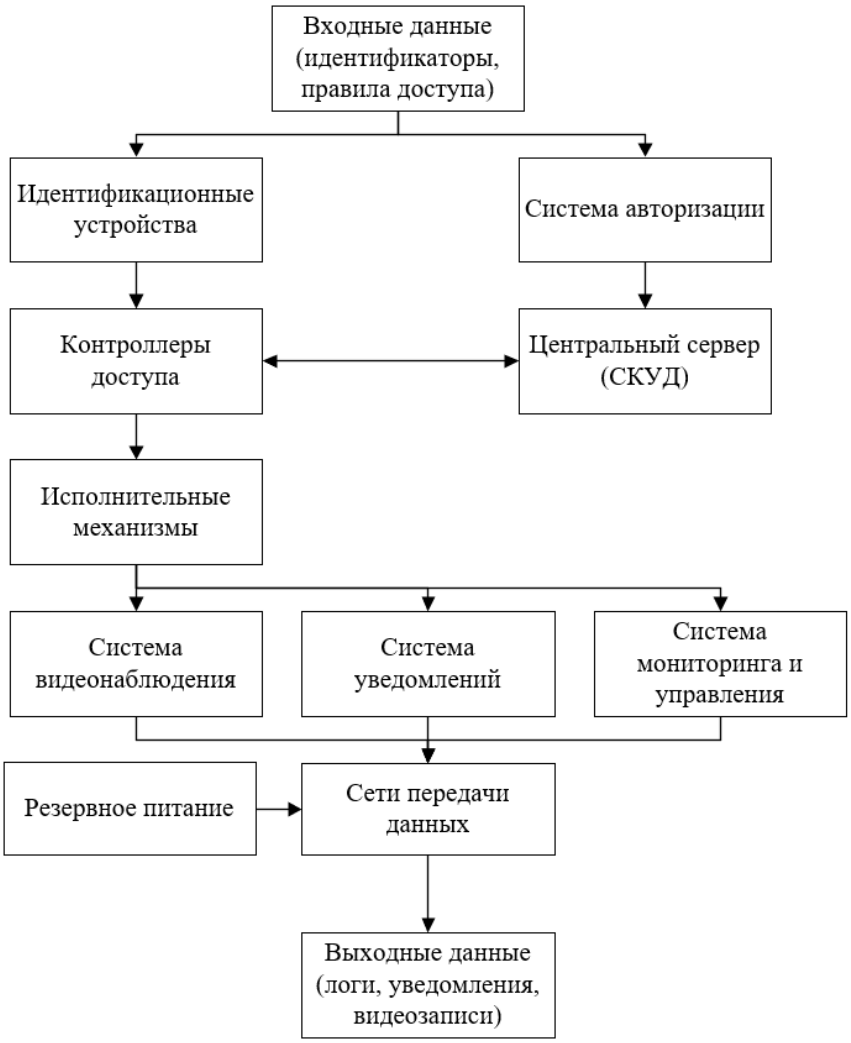


Рисунок 1 – Структурная схема СКУД
Figure 1 – Structural diagram of the access control system

На вход системы поступают данные, с помощью которых возможно провести идентификацию пользователей: данные с удостоверяющих документов, биометрические данные, данные карты или PIN-коды, а также правила доступа, задаваемые администраторами. На следующем шаге происходит передача исходных данных в идентификационные устройства, которые служат точками первичного сбора информации. После выполнения процесса идентификации информация поступает в контроллеры доступа, играющие ключевую роль в обработке запросов на доступ.

Контроллеры взаимодействуют с центральным сервером СКУД, где осуществляется проверка данных, на основе которых возможно запустить процесс авторизации. Центральный сервер, опираясь на заданные политики доступа, полученные от системы авторизации, принимает решение о разрешении или отказе в доступе, после чего, принятое решение возвращается в контроллеры, которые, в случае положительного исхода, активируют исполнительные механизмы (такие как замки, турникеты и т. д.) для предоставления физического доступа.

Одновременно осуществляется фиксация действий системой видеонаблюдения, что обеспечивает визуальный контроль над точкой доступа. Параллельно проводится регистрация событий и их передача в систему уведомлений, которая может оповестить ответственных лиц о попытке несанкционированного доступа, тревожных ситуациях или нарушениях. Дополнительно, система мониторинга и управления позволяет операторам в реальном времени отслеживать состояние всех компонентов системы, управлять событиями и получать доступ к аналитической информации.

Функционирование системы в едином информационном пространстве происходит благодаря сетям передачи данных, которые позволяют обеспечить обмен информацией между элементами системы. Для повышения надежности работы все активные компоненты подключаются к системе резервного питания, что позволяет сохранять работоспособность даже при перебоях в электроснабжении.

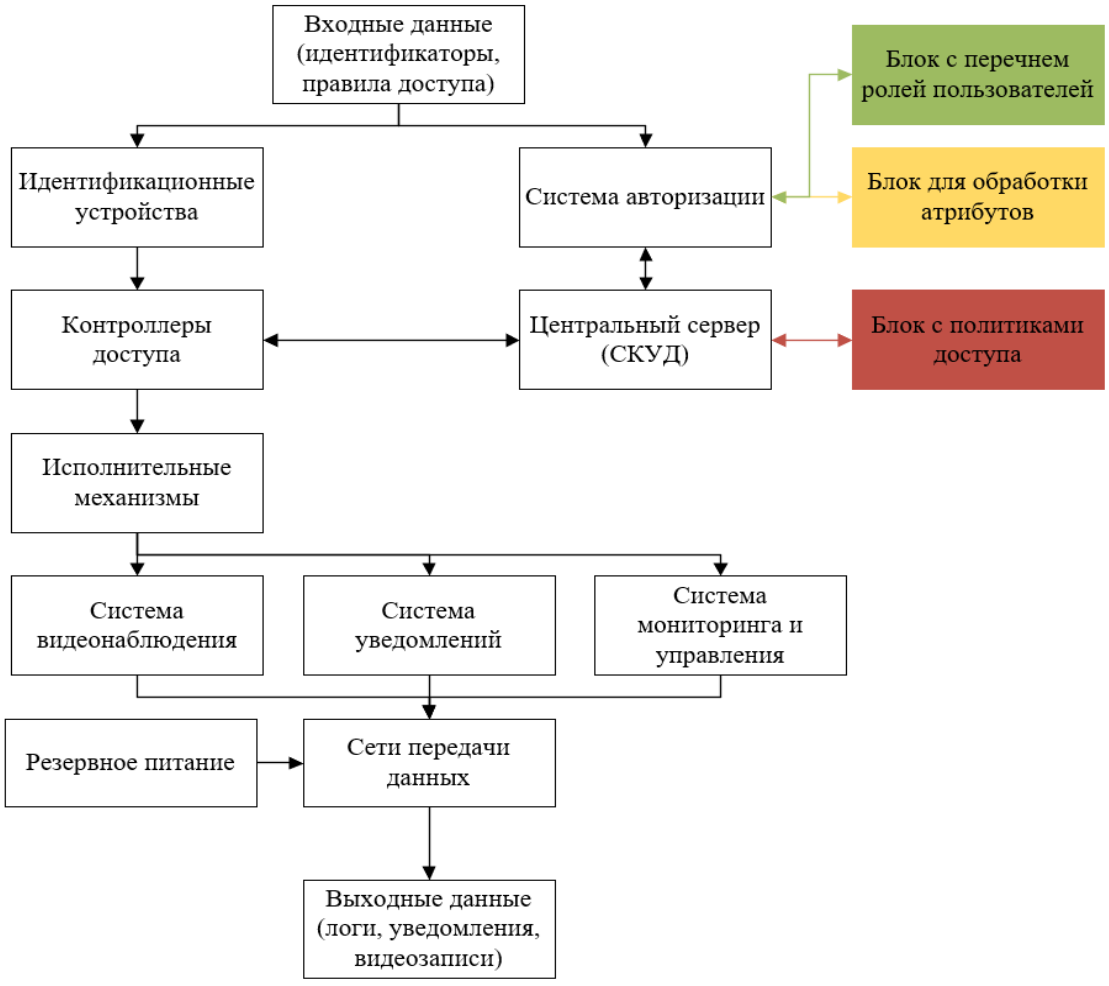


Рисунок 2 – Схема СКУД с моделями управления доступом
Figure 2 – Scheme of access control system with access control models

На выходе системы происходит формирование итоговых документов: журналы событий, видеозаписи, уведомления и отчеты, которые могут использоваться для последующего анализа, аудита и принятия решений по безопасности.

В основе обеспечения производительности и защиты данных в системах СКУД лежат модели управления доступом, каждая из которых обладает уникальными характеристиками, подходами к распределению прав доступа и способами реализации (Рисунок 2).

Выделяют три основные модели: на основе ролей, атрибутов и полномочий.

1) Модель управления доступом на основе ролей (RBAC) – одна из наиболее широко используемых моделей управления доступом, которая предоставляет гибкость и простоту в управлении правами доступа. В основе RBAC лежит концепция назначения пользователям ролей, каждая из которых обладает определенным набором прав и полномочий. Пользователи получают доступ к ресурсам на основании своих ролей, что упрощает администрирование и управление доступом.

Для взаимодействия СКУД с моделью управления доступом на основе ролей организуется блок, в котором указываются роли пользователей и соответствующие им права доступа, на Рисунке 2 изображен зеленым цветом. Центральный сервер применяет политики доступа на основе ролей, а контроллеры доступа запрашивают у сервера разрешение на доступ.

2) Модель управления доступом на основе атрибутов (ABAC) – предоставляет более высокую гибкость и детализированное управление доступом за счет использования большого количества дополнительных атрибутов. В ABAC доступ определяется на основе атрибутов пользователей, объектов и условий среды. Правила доступа формируются динамически, что позволяет учитывать множество факторов при принятии решений о предоставлении доступа. Интеграция СКУД с моделью управления доступом на основе атрибутов происходит посредством блока обработки атрибутов, на Рисунке 2 данный блок выделен желтым цветом. На центральном сервере хранятся политики доступа, зависящие от атрибутов (местоположение, время, устройство), идентификационные устройства могут собирать дополнительные атрибуты (например, тип устройства), а система авторизации проверяет атрибуты пользователя.

3) Модель управления доступом на основе полномочий (PBAC) – фокусируется на реализации правил и политик, обеспечивая точное определение доступа на основе политики безопасности. Модель PBAC использует централизованные политики для определения доступа пользователей. Эти политики описывают условия предоставления доступа и применяются ко всем объектам системы. Если модели RBAC и ABAC взаимодействовали с СКУД через систему авторизации, то PBAC взаимодействует непосредственно с центральным сервером СКУД, на Рисунке 2 выделена красным цветом. На центральном сервере хранятся и интерпретируются политики доступа, система авторизации выполняет централизованную проверку полномочий, а контроллеры доступа передают запросы на сервер и получают решения.

## Результаты

Для определения наиболее приемлемых условий применения той и ли иной модели необходимо провести практические испытания. Логика проведения эксперимента включает в себя пять последовательных этапов:

1. Подготовка тестовых сред.
2. Определение ограничений на модели управления доступом.
3. Определение производительности системы.
4. Проведение тестирования безопасности системы.

5. Сбор и анализ полученных результатов.

*Подготовка тестовых сред.* Для определения параметров производительности и безопасности методов управления доступом была создана специализированная изолированная тестовая среда, с небольшими исключениями отличающейся от реальной сети передачи данных, которая обеспечивает устойчивую работу финансовой организации (Рисунок 3). Таким образом было достигнуто максимальное соответствие проведенных тестов практическим условиям. Основные параметры организованной сети:

1) количество рабочих станций, используемых сотрудниками в офисной зоне для выполнения повседневных задач – 800;

2) количество серверов, предназначенных для поддержки различных приложений и внутренних систем банка – 200;

3) центр обработки данных (ЦОД) представляет собой 50 серверов, на которые установлены критически важные приложения, такие как системы управления транзакциями, клиентские базы данных и аналитические платформы;

4) для имитации процессов аутентификации и авторизации применяется служба каталогов Active Directory с поддержкой Kerberos, а для мониторинга событий и обнаружения угроз система SIEM (Security Information and Event Management);

5) каналы связи поддерживают скорости до 100 Мбит/с для публичной сети и скорости от 1 до 10 Гбит/с на других отрезках.

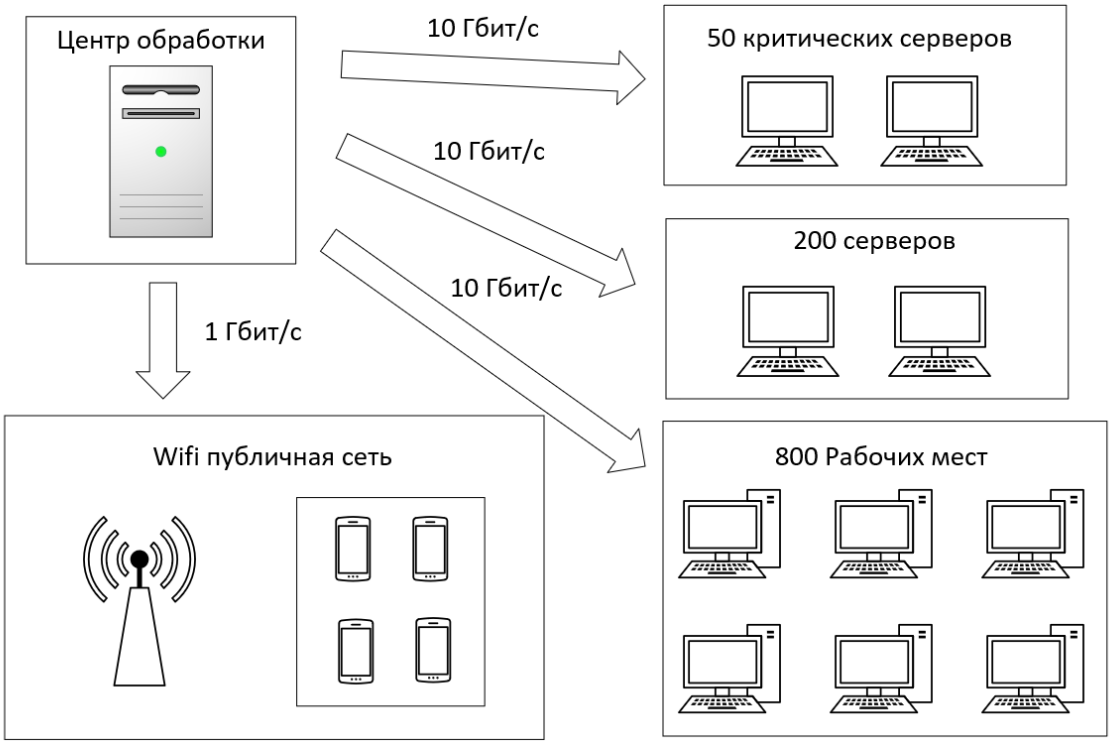


Рисунок 3 – Схема тестовой среды
Figure 3 – Test environment diagram

*Определение ограничений на модели управления доступом.* При построении и тестировании моделей управления доступом необходимо учитывать факторы, влияющие на производительность и надежность системы в условиях реальной телекоммуникационной инфраструктуры:

1. Архитектура телекоммуникационной сети оказывает значительное влияние на эффективность. Структура сети определяет, каким образом распределяется нагрузка между компонентами системы аутентификации и авторизации. Сложная или фрагментированная архитектура может привести к узким местам, особенно в узлах, выполняющих функции централизованной проверки прав доступа. Это ограничивает масштабируемость системы и может вызывать задержки при увеличении числа пользователей или при подключении дополнительных сегментов сети.

2. Централизованная служба каталогов Active Directory с поддержкой протокола Kerberos предъявляет высокие требования к вычислительным ресурсам, особенно в моменты высокой активности, таких как начало рабочего дня, когда множество пользователей одновременно проходит аутентификацию. Это создает нагрузку на контроллеры домена, снижает устойчивость к пиковым обращениям и увеличивает время отклика системы, что критично для приложений с жесткими требованиями к времени доступа.

3. Системы мониторинга и аналитики SIEM в режиме реального времени обрабатывает журналы событий и анализирует сетевой трафик для выявления потенциальных угроз. Интенсивная корреляция событий и анализ данных увеличивают нагрузку на вычислительные ресурсы серверов, что может привести к задержкам в реагировании на инциденты. Кроме того, появляется необходимость в грамотной балансировке нагрузки между средствами мониторинга и основной инфраструктурой доступа, чтобы избежать конкуренции за ресурсы и обеспечить стабильность функционирования системы в целом.

Предполагается, что в практической задаче будут использованы все три модели доступа, но на них буду наложены следующие ограничения:

1) ролевая модель – используется для 80 % сотрудников с фиксированными ролями (операционист, менеджер, IT-администратор);

2) атрибутная модель – применяется к сотрудникам, работающим удаленно или с высокими правами доступа. Параметры: время (доступ с 9:00 до 18:00), местоположение (внутренняя сеть);

3) модель на основе полномочий – тестируется с динамическим созданием правил для управления доступом к критически важным данным.

Данные ограничения были наложены из-за того, чтобы при внедрении и масштабировании моделей управления доступом, особенно в условиях высоконагруженных телекоммуникационных систем, их необходимо учитывать при разработке.

*Определение производительности системы.* Для тестирования производительности необходимо провести комплексные измерения в целях оценки работоспособности применяемых методов управления доступом и степени обеспечения стабильности системы. Должны быть оценены следующие параметры:

1) время отклика системы на запросы пользователей;

2) пропускная способность: какое количество запросов система способна обрабатывать за единицу времени;

3) устойчивость к пиковым нагрузкам: способна ли система сохранить стабильную работу при резком увеличении количества одновременных подключений.

Производительность – это способность системы управления доступом обрабатывать пользовательские запросы с минимальной задержкой при сохранении устойчивости к пиковым нагрузкам. Для количественной оценки общей эффективности ($E_p$) используем следующую формулу:

$$E_p = \frac{P}{T}, \quad (1)$$

где $P$ – пропускная способность (запросов/сек), $T$ – время отклика (мс).

*Проведение тестирования безопасности.* Безопасность – это способность системы противостоять внешним и внутренним угрозам, обеспечивать конфиденциальность, целостность и доступность данных при доступе пользователей.

Для получения агрегированной оценки безопасности ($E_s$) используем формулу:

$$E_S = \frac{S+U+G}{3}, \quad (2)$$

где $S$ – уровень защиты (%), $U$ – устойчивость к атакам (%), $G$ – гибкость реагирования (%).

В рамках проведения тестирования безопасности необходимо дать оценку возможностям системы противостоять угрозам и предотвращать утечки данных. В рамках настоящего тестирования будут применяться методы: пен тестирование – имитация реальных атак, направленных на выявление слабых мест в системе, использование инструментов IDS/IPS – представляющие из себя систему обнаружения и предотвращения вторжений и служащие для контроля активности в сети и предотвращения подозрительных действий.

Основными точкам тестирования являются:

1) тестирование процесса аутентификации сотрудников и клиентов банка – проверка устойчивости системы к атакам, таким как перебор паролей и атаки типа «атака посредника»;

2) тестирование процессов авторизации пользователей – определение, насколько эффективно система управления доступом и предотвращает несанкционированный доступ к критически важным данным;

3) тестирование реакции системы на инциденты – необходимость оценивания скорости и точности, с которой система реагирует на выявленные угрозы и предотвращает их.

Тестирование будет проводиться с помощью инструментов LoadRunner и JMeter. Данные инструменты позволяют подключать к сети до нескольких тысяч пользователей и одновременно выполнять запросы к программному обеспечению (ПО).

В рамках этапа тестирования были разработаны следующие сценарии:

Сценарий 1. Проверка пригодности ПО к использованию – ежедневные операции сотрудников, от доступа к локальным или удаленным файлам и до отправки требований в базы данных.

Сценарий 2. Сценарий пиковых нагрузок – когда СКЗИ испытывает воздействие на всю систему, например, утренний час наибольшей нагрузки, когда практически весь персонал компании в начале рабочего дня подключается к ней.

Сценарий 3. Аварийные сценарии – проверка ситуаций использования ПО, когда в сеть поступает «черный» поток данных.

*Сбор и анализ результатов.* Для дальнейшего анализа результатов все полученные данные тестирования должны быть систематизированы и проанализированы.

На первом этапе проводится анализ производительности, что позволяет оценить время отклика, средние и пиковые показатели пропускной способности, а также выявить потенциальные места, где необходимы изменения.

Вторым этапом проводится оценка безопасности. Проверяется эффективность обнаружения угроз и способность системы предотвращать атаки.

На заключительном шаге проводится анализ полученных данных с установленными нормативами, чтобы определить, соответствуют ли протестированные модели управления доступом с установленными начальными параметрами требованиям безопасности и производительности.

## Обсуждение

*Анализ производительности.* Время отклика (мс) – это метрика, показывающая, за какой промежуток система обрабатывает поступивший запрос и возвращает результат пользователю или приложению.

В повседневной эксплуатации наиболее быстро реагировала RBAC: в среднем 280 мс. Чуть медленнее срабатывал ABAC – около 380 мс, а PBAC замыкал тройку с показателем 420 мс. Когда нагрузка возрастала до пиковых значений, задержки увеличивались: RBAC – до 500 мс, ABAC – до 600 мс, PBAC – до 650 мс. В аварийных ситуациях, имитирующих нетипичные перегрузки, время реакции выросло еще сильнее – 550 мс, 650 мс и 700 мс соответственно (Рисунок 4).

Из этого можно заключить, что RBAC обрабатывает запросы заметно быстрее в любых условиях, что особенно важно в средах с большим количеством динамичных обращений.

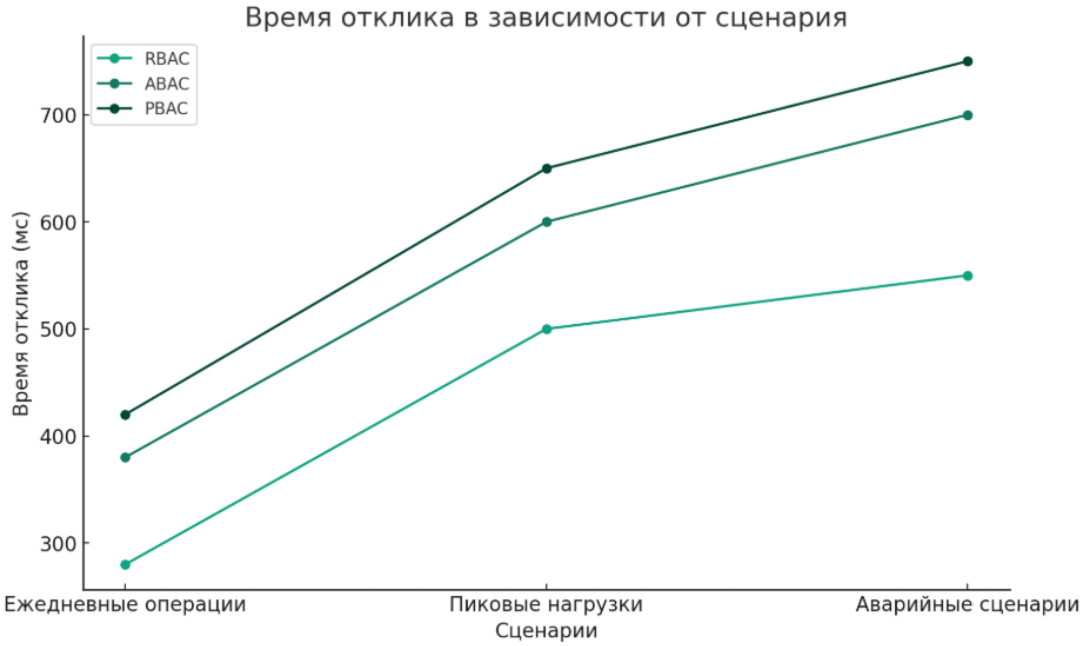


Рисунок 4 – Графики тестирования времени отклика
Figure 4 – Response time testing graphs

Пропускная способность (запросы/сек) отражает, сколько запросов система способна обработать за одну секунду.

В штатном режиме RBAC уверенно удерживала лидерство, обрабатывая примерно 10500 запросов в секунду. ABAC оказывалась на уровне 8200 запросов/сек, а PBAC – около 9200 запросов/сек. При пиковых нагрузках значения несколько снижались, но RBAC по-прежнему показывала 10000 запросов/сек, что выше, чем у PBAC (9000 запросов/сек) и ABAC (8000 запросов/сек). В экстремальных условиях разрыв сохранялся: 9500 против 8500 и 7800 запросов/сек соответственно (Рисунок 5).

Таким образом, RBAC демонстрирует наибольшую пропускную способность и стабильность при росте нагрузки, тогда как ABAC и PBAC снижают производительность из-за дополнительных затрат на анализ атрибутов и политик.

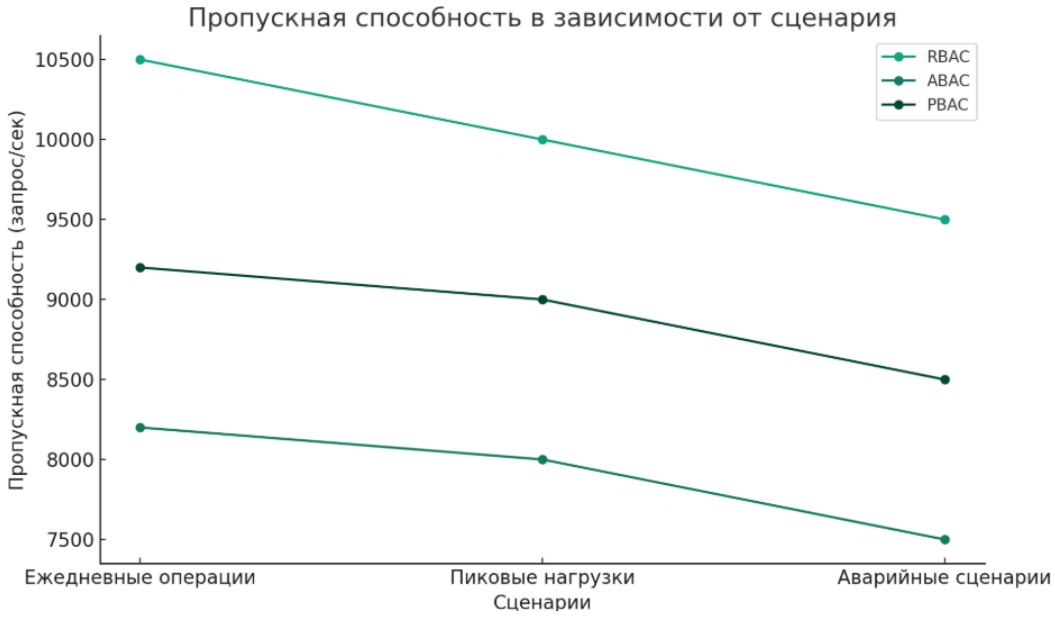


Рисунок 5 – Графики тестирования пропускной способности
Figure 5 – Throughput testing graphs

Устойчивость к пиковым нагрузкам (подключения) характеризует способность системы сохранять работоспособность при увеличении числа одновременных соединений.

В типичном режиме работы RBAC без проблем выдерживала до 10200 активных подключений. Для PBAC этот показатель составил 9200, а для ABAC – 8100. При нагрузке, приближенной к максимальной, RBAC поддерживала работу при 10000 подключениях, PBAC – при 9000, ABAC – при 8000. В аварийных сценариях, где нагрузка была нестабильной и превышала обычные значения, RBAC сохраняла работу до 9700 подключений, тогда как PBAC и ABAC показывали 8700 и 7900 соответственно (Рисунок 6).

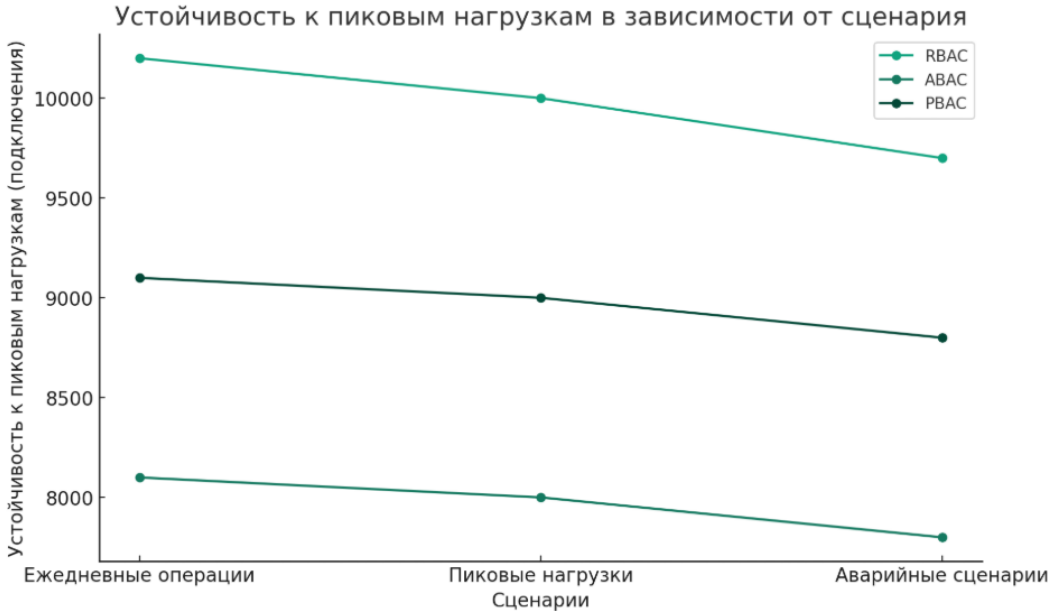


Рисунок 6 – Графики тестирования устойчивости к пиковым нагрузкам
Figure 6 – Peak load resistance test graphs

Эти данные показывают, что RBAC лучше справляется с резким ростом числа пользователей, в то время как ABAC теряет стабильность быстрее.

Таким образом, по всем ключевым параметрам – скорости отклика, объему обрабатываемых запросов и устойчивости при повышенных нагрузках – RBAC в исследованных сценариях оказалась наиболее эффективной.

Результаты количественной оценки общей производственной эффективности ($E_p$) по каждой модели представлен в Таблице 2.

Таблица 2 – Количественная оценка производительности
Table 2 – Quantitative performance assessment

| **Модель** | **Сценарий** | **Время отклика (мс)** | **Пропускная способность (запрос/сек)** | $\mathrm{E_p} = \frac{P}{T}$ |
|---|---|---|---|---|
| RBAC | Ежедневный | 280 | 10500 | 37,5 |
| | Пиковый | 500 | 10000 | 20 |
| | Аварийный | 550 | 9500 | 17,27 |
| ABAC | Ежедневный | 380 | 8200 | 21,57 |
| | Пиковый | 600 | 8000 | 13,33 |
| | Аварийный | 650 | 7800 | 12 |
| PBAC | Ежедневный | 420 | 9200 | 21,91 |
| | Пиковый | 650 | 9000 | 13,85 |
| | Аварийный | 700 | 8500 | 12,14 |

Модель RBAC, обеспечивает наименьшее время отклика и наибольшую пропускную способность. ABAC и PBAC показали более низкие значения, что объясняется сложностью вычислений, связанных с анализом атрибутов и политик соответственно.

*Анализ безопасности.* В рамках тестирования системы на безопасность были проанализированы способности защиты системы от различных типов угроз, таких как несанкционированный доступ, атаки с повышенной адаптивностью и попытки эксплуатации уязвимостей.

В сценарии ежедневных операций модель RBAC демонстрирует устойчивость к атакам на уровне 88 %, ABAC – 93 %, а PBAC – 96 %, при этом последняя обеспечивает наивысший уровень предотвращения несанкционированного доступа благодаря учету контекста, оценки рисков и поведенческих паттернов. При переходе к пиковым нагрузкам уровень устойчивости снижается: RBAC – до 85 %, ABAC – до 90 %, PBAC – до 94 %, что указывает на высокую надежность PBAC даже в условиях интенсивного пользовательского трафика, тогда как RBAC теряет эффективность из-за своей упрощенной модели ролей. В аварийных ситуациях, где система подвергается нетипичным угрозам, PBAC сохраняет лидерство с показателем 92 %, в то время как ABAC демонстрирует 87 %, а RBAC – 82 %, подтверждая, что PBAC обладает лучшими механизмами адаптации и защиты за счет динамического анализа поведения и гибкой настройки политик доступа (Рисунок 7).

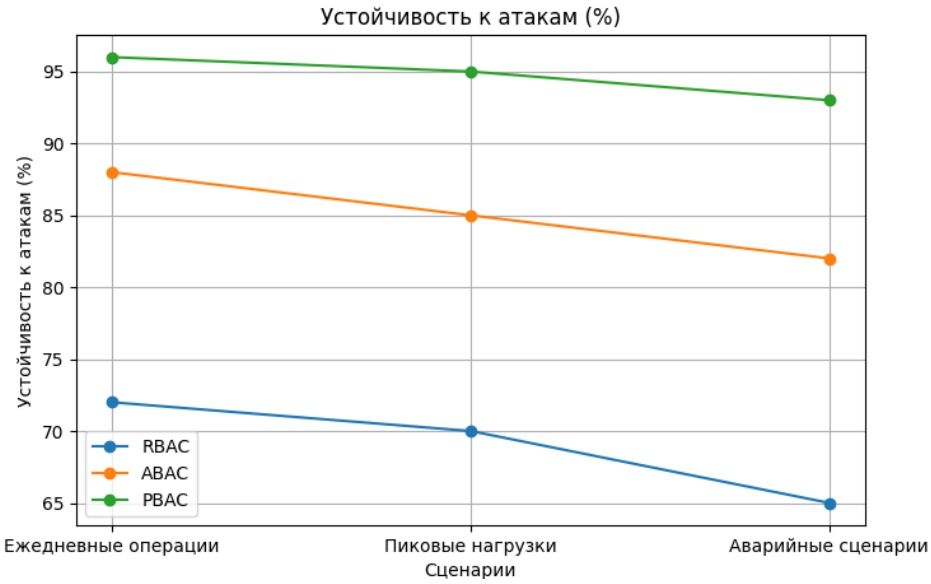


Рисунок 7 – Графики тестирования устойчивости к атакам
Figure 7 – Attack resilience testing graphs

Гибкость в реагировании (%) – способность системы адаптироваться к новым типам угроз, изменяя правила доступа без вмешательства в архитектуру.

В сценарии ежедневных операций модели демонстрируют следующую гибкость реагирования: RBAC – 60 %, ABAC – 85 %, PBAC – 95 %. Это свидетельствует о том, что PBAC и ABAC позволяют легко адаптировать политики доступа без необходимости перестраивать архитектуру системы, тогда как RBAC требует ручной корректировки ролей при изменениях. В условиях пиковых нагрузок показатели ожидаемо снижаются: RBAC – 55 %, ABAC – 80 %, PBAC – 93 %, что подчеркивает ограниченную адаптивность RBAC при росте числа событий, в то время как PBAC сохраняет высокую устойчивость благодаря динамической настройке. В аварийных ситуациях гибкость RBAC падает до 50 %, ABAC – до 75 %, тогда как PBAC остается наиболее адаптивной с результатом в 90 %, обеспечивая быстрое внесение изменений в политики и снижая риск ошибок при администрировании в критических условиях (Рисунок 8).

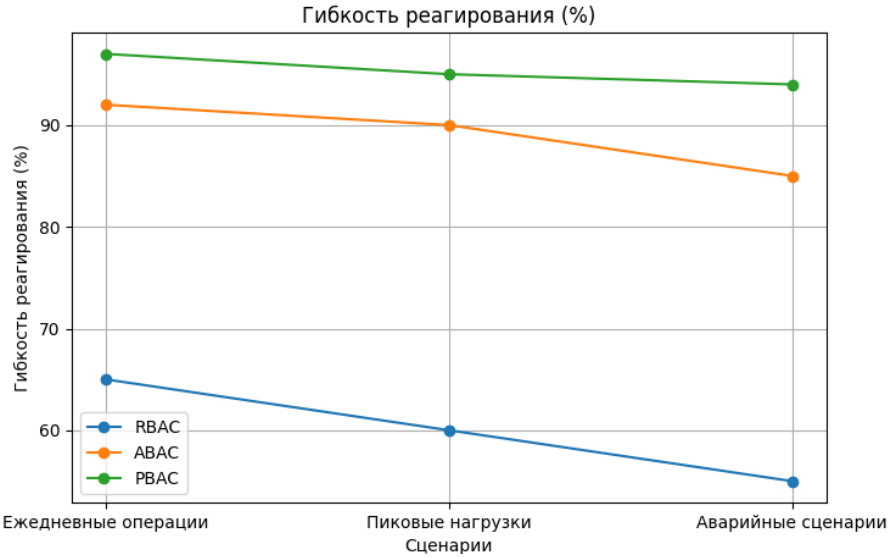


Рисунок 8 – Графики тестирования гибкости реагирования
Figure 8 – Responsiveness testing graphs

Уровень защиты (%) – обобщенная оценка мер защиты, включающая аутентификацию, контроль привилегий и аудит доступа.

В условиях повседневной нагрузки уровень защиты демонстрирует следующие значения: RBAC – 78 %, ABAC – 88 %, PBAC – 94 %. PBAC уверенно лидирует благодаря глубокой интеграции поведенческого анализа, контекстуальных данных и оценки рисков, что позволяет точнее идентифицировать угрозы. При пиковых нагрузках показатели снижаются, однако PBAC сохраняет преимущество: RBAC – 75 %, ABAC – 85 %, PBAC – 92 %. Это говорит о снижении точности RBAC из-за ограниченной структуры ролей, в то время как PBAC продолжает эффективно защищать систему. В аварийных ситуациях уровень защиты RBAC составляет 72 %, ABAC – 82 %, PBAC – 90 %, и вновь PBAC подтверждает свою надежность благодаря возможности проактивной адаптации к изменяющимся условиям и угрозам (Рисунок 9).

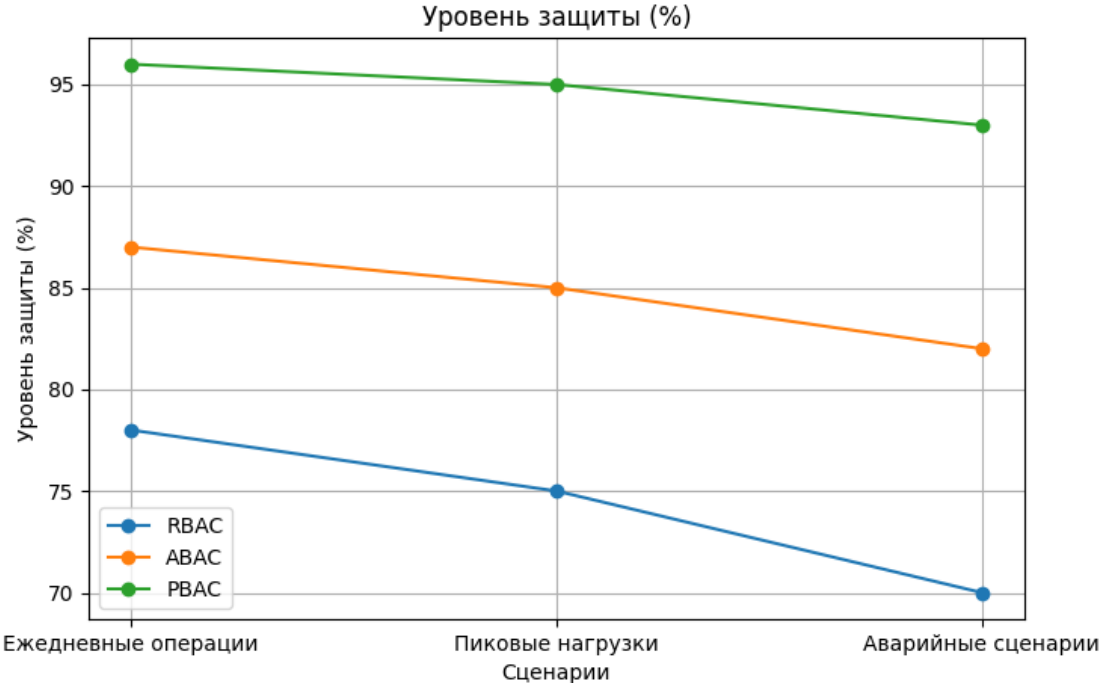


Рисунок 9 – Графики тестирования уровня защиты
Figure 9 – Protection level testing graphs

В целом, модель PBAC демонстрирует наивысшие показатели по всем ключевым аспектам безопасности (устойчивость к атакам, гибкость реагирования, уровень защиты) во всех сценариях – от повседневной эксплуатации до аварийных ситуаций, что обусловливает ее способность учитывать контекст, поведенческие факторы и риски в режиме реального времени. ABAC следует за ней, предлагая высокую гибкость и адаптивность без кардинальных изменений в архитектуре. RBAC, несмотря на простоту и высокую производительность, уступает по уровню защиты и адаптивности, особенно в условиях повышенной или нестандартной нагрузки.

Результаты агрегированной оценки безопасности по каждой модели представлен в Таблице 3.

Таблица 3 – Результаты расчета агрегированной оценки безопасности $E_s$
Table 3 – Results of calculating the aggregate safety assessment $E_s$

| Сценарий | Модель | Устойчивость, (%) | Гибкость, (%) | Уровень защиты, (%) | Es, (%) |
|---|---|---|---|---|---|
| Ежедневный | RBAC | 75 | 60 | 80 | 71,67 |
| | ABAC | 90 | 85 | 88 | 87,67 |
| | PBAC | 95 | 95 | 95 | 95,00 |
| Пиковый | RBAC | 65 | 55 | 70 | 63,33 |
| | ABAC | 83 | 88 | 85 | 85,33 |
| | PBAC | 93 | 93 | 94 | 93,33 |
| Аварийный | RBAC | 60 | 50 | 65 | 58,33 |
| | ABAC | 80 | 90 | 82 | 84,00 |
| | PBAC | 96 | 97 | 97 | 96,67 |

Подводя итог эксперимента безопасности с использованием различных моделей управления доступом, наивысшие показатели по всем параметрам безопасности продемонстрировала модель PBAC, благодаря контекстному анализу и политико-ориентированному подходу. ABAC также показала высокий уровень безопасности за счет гибкости и точности. RBAC, несмотря на стабильность, уступает остальным моделям в динамических сценариях угроз.

Таким образом, выбор модели управления доступом должен основываться на приоритетах системы:

1. В том случае, если основное требование – высокая производительность и предсказуемая структура пользователей (например, в операторской сети с большим количеством однородных клиентов), предпочтение стоит отдать RBAC.

2. Если критична адаптивность и безопасность (например, при доступе к конфиденциальным данным или в распределенных облачных системах), то более подходящими будут ABAC или PBAC, несмотря на их большую нагрузку на вычислительные ресурсы.

Формулы обобщенной производительности и безопасности, использованные в анализе, подтверждают данную зависимость, показывая, что рост одного параметра зачастую достигается за счет снижения другого. Это подчеркивает необходимость баланса между производительностью и уровнем защиты при проектировании архитектуры управления доступом [9, 10].

## Заключение

Для достижения цели работы был смоделирован виртуальный стенд, который имитирует телекоммуникационную сеть финансовой организации, в которой присутствует как подсеть для сотрудников организации, так и клиентская подсеть.

В качестве основы анализа приняты параметры производительности, такие как время отклика запроса пользователей на систему, пропускная способность и устойчивость к пиковым нагрузкам, и параметры безопасности: устойчивость к атакам, гибкость в реагировании на угрозы и уровень защиты.

Проведенный эксперимент показал, что выбор модели управления доступом зависит от потребностей в безопасности и производительности, а также от особенностей сетевой инфраструктуры:

1. Ролевая модель управления доступом подходит для систем с фиксированными ролями и задачами, где требуется стабильная работа при умеренной нагрузке. Однако для более гибкого управления доступом в условиях динамичных изменений и высоких

требований к безопасности, ABAC и PBAC предлагают более сложные, но более безопасные и адаптируемые решения.

2. Атрибутная модель управления доступом эффективно работает в сценариях, где важно учитывать различные атрибуты и контексты пользователя, но ее сложность настройки и необходимость обработки большого объема данных могут снижать производительность.

3. Модель, основанная на политиках, в свою очередь, позволяет создавать динамичные политики доступа и обеспечить высокий уровень безопасности, но требует значительных вычислительных ресурсов для обработки больших объемов данных.

Таким образом, можно сделать вывод, что для сетей, где критична как безопасность, так и гибкость, предпочтительным подходом будет являться подход использования гибридных моделей. Гибридной моделью доступа может считаться сочетание RBAC для рутинных задач и ABAC/PBAC для управления доступом к критически важной информации что должно позволить сбалансировать параметры производительность и безопасности, снизив при этом риски, связанные с управления доступом (Рисунок 10).

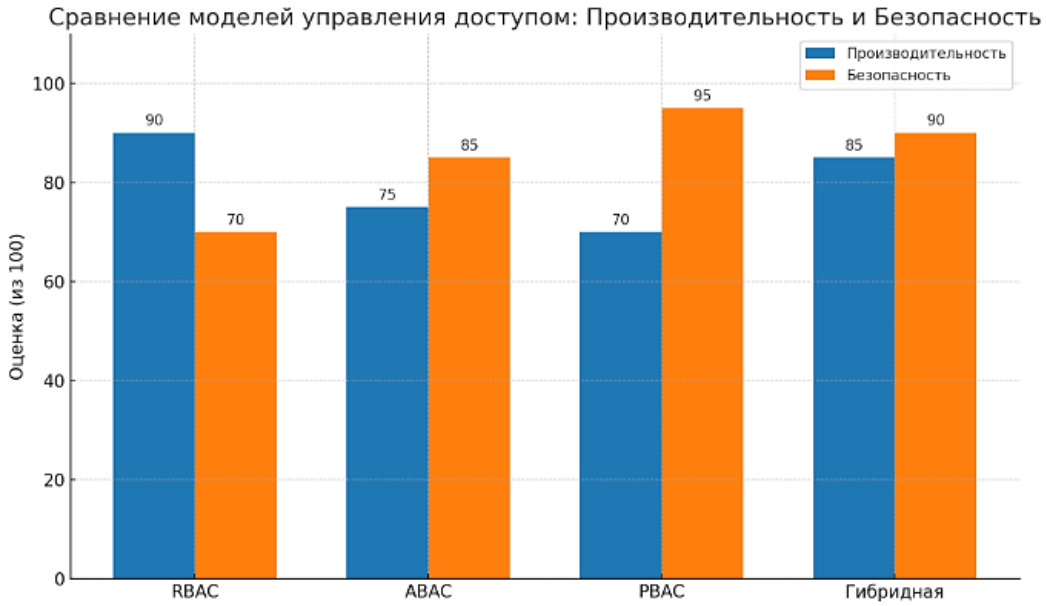


Рисунок 10 – Графики сравнения моделей управления доступом
Figure 10 – Access control model comparison charts

График демонстрирует сравнительный анализ моделей управления доступом RBAC, ABAC, PBAC и гибридной по двум показателям: производительность и безопасность (оценка от 0 до 100). RBAC показывает наибольшую производительность (90 %) при сравнительно низкой безопасности (70 %), ABAC имеет более сбалансированные значения (75 % и 85 % соответственно), PBAC достигает максимальной безопасности (95 %), но при этом обладает низшей производительностью (70 %). Гибридная модель сочетает высокую производительность (85 %) и высокий уровень безопасности (90 %), обеспечивая оптимальный баланс между эффективностью и защитой.

## СПИСОК ИСТОЧНИКОВ / REFERENCES


1. Гадасин Д.В., Шведов А.В. Применение транспортной задачи для балансировки нагрузки в условиях нечеткости исходных данных. *T-Comm: Телекоммуникации и транспорт.* 2024;18(1):13–20. https://doi.org/10.36724/2072-8735-2024-18-1-13-20
   Gadasin D.V., Schvedov A.V. Application of a Transport Task for Load Balancing in Conditions of Source Data Fuzziness. *T-Comm.* 2024;18(1):13–20. (In Russ.). https://doi.org/10.36724/2072-8735-2024-18-1-13-20
2. Гадасин Д.В. Построение бинарного дерева минимальной цены. *T-Comm: Телекоммуникации и транспорт.* 2024;18(11):38–44. https://doi.org/10.36724/2072-8735-2024-18-11-38-44
   Gadasin D.V. Building a Binary Tree of the Minimum Prices. *T-Comm.* 2024;18(11):38–44. (In Russ.). https://doi.org/10.36724/2072-8735-2024-18-11-38-44
3. Докучаев В.А., Нетребко А.В., Маклачкова В.В., Мытенков С.С. Механизмы обеспечения защищенности данных в распределенных информационных системах. *Экономика и качество систем связи.* 2025;(2):125–134.
   Dokuchaev V.A., Netrebko A.V., Maklachkova V.V., Mytenkov S.S. Mechanisms for Ensuring Data Security in Distributed Information Systems. *Ekonomika i kachestvo sistem svyazi.* 2025;(2):125–134. (In Russ.).
4. Ворона В.А., Тихонов В.А. *Системы контроля и управления доступом.* Москва: Горячая линия-Телеком; 2010. 272 с.
5. Singh Ja., Rani S., Kumar V. Role-Based Access Control (RBAC) Enabled Secure and Efficient Data Processing Framework for IoT Networks. *International Journal of Communication Networks and Information Security.* 2024;16(2). https://doi.org/10.17762/ijcnis.v16i2.6697
6. Сагидова М.Л. Современные системы контроля и управления доступом. *Международный журнал гуманитарных и естественных наук.* 2022;(9–1):64–68. https://doi.org/10.24412/2500-1000-2022-9-1-64-68
   Sagidova M.L. Modern Access Control and Management Systems. *International Journal of Humanities and Natural Sciences.* 2022;(9–1):64–68. (In Russ.). https://doi.org/10.24412/2500-1000-2022-9-1-64-68
7. Козлов А.Е. Система контроля и управления доступом на предприятие: понятие, характеристика и основные требования. *Вестник Воронежского государственного технического университета.* 2019;15(1):42–47. https://doi.org/10.25987/VSTU.2019.15.1.006
   Kozlov A.E. Control System and Access Control in the Enterprise: Concept, Characteristics and Basic Requirements. *Bulletin of the Voronezh State Technical University.* 2019;15(1):42–47. (In Russ.). https://doi.org/10.25987/VSTU.2019.15.1.006
8. Волковицкий В.Д., Волхонский В.В. *Системы контроля и управления доступом.* Санкт-Петербург: Экополис и культура; 2003. 164 с.
9. Докучаев В.А., Маклачкова В.В., Бойко А.А. Проблема актуализации данных в CRM-системах. *Экономика и качество систем связи.* 2025;(1):45–57.
   Dokuchaev V.A., Maklachkova V.V., Boiko A.A. The Problem of Updating Data in CRM Systems. *Ekonomika i kachestvo sistem svyazi.* 2025;(1):45–57. (In Russ.).
10. Докучаев В.А., Маклачкова В.В., Статьев В.Ю. Цифровизация субъекта персональных данных. *T-Comm: Телекоммуникации и транспорт.* 2020;14(6):27–32. https://doi.org/10.36724/2072-8735-2020-14-6-27-32
    Dokuchaev V.A., Maklachkova V.V., Statev V.Yu. Digitalization of the Personal Data Subject. *T-Comm.* 2020;14(6):27–32. (In Russ.). https://doi.org/10.36724/2072-8735-2020-14-6-27-32

## ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

**Калининский Даниил Сергеевич,** аспирант кафедры «Сетевые информационные технологии и сервисы», Московский технический университет связи и информатики, Москва, Российская Федерация.
*e-mail:* daniilblag28@mail.ru
ORCID: 0009-0005-3069-9566

**Daniil S. Kalininsky,** Postgraduate at the Department of Network Information Technologies and Services, Moscow Technical University of Communications and Informatics, Moscow, the Russian Federation.

**Тремасова Лилия Андреевна,** ассистент кафедры «Сетевые информационные технологии и сервисы», Московский технический университет связи и информатики, Москва, Российская Федерация.
*e-mail:* l.a.tremasova@mtuci.ru
ORCID: 0009-0004-6852-4131

**Lilia A. Tremasova,** Assistant Professor at the Department of Network Information Technologies and Services, Moscow Technical University of Communications and Informatics, Moscow, the Russian Federation.

**Гадасин Денис Вадимович,** кандидат технических наук, доцент, заместитель заведующего кафедрой «Сетевые информационные технологии и сервисы», Московский технический университет связи и информатики», Москва, Российская Федерация.
*e-mail:* dengadiplom@mail.ru
ORCID: 0000-0002-5601-7798

**Denis V. Gadasin,** Candidate of Engineering Sciences, Docent, Deputy Head of the Department of Network Information Technologies and Services, Moscow Technical University of Communications and Informatics, Moscow, the Russian Federation.

*Статья поступила в редакцию 15.08.2025; одобрена после рецензирования 15.09.2025; принята к публикации 27.09.2025.*

*The article was submitted 15.08.2025; approved after reviewing 15.09.2025; accepted for publication 27.09.2025.*