СРАВНИТЕЛЬНЫЙ АНАЛИЗ РЕАЛИЗАЦИИ JIT-ДОСТУПА В СОВРЕМЕННЫХ PAM-СИСТЕМАХ

В.В. Сингуров[1], *выпускник специалитета*
А.С. Сафронов[2], *магистрант*
Н.У. Тагиров[2], *магистрант*
Научный руководитель: *А.В. Осин[2], канд. техн. наук, доцент*
[1]МИРЭА – Российский технологический университет
[2]Московский технический университет связи и информатики
[1,2](Россия, г. Москва)

DOI:10.24412/2500-1000-2026-4-2-97-102

Аннотация. *В статье рассмотрен механизм JIT-доступа как инструмент сокращения постоянных привилегий в системах PAM. Проведен сравнительный анализ реализации JIT-подхода в решениях Solar SafeInspect, СКДПУ НТ и CyberArk по критериям временного предоставления прав, согласования, отзыва привилегий и аудита действий. Показано, что исследуемые PAM-системы различаются по глубине реализации JIT-механизмов, сочетанию их с контролем сессий и аналитическими средствами. Результаты могут быть использованы при выборе PAM-решений для защищенных информационных систем.*

Ключевые слова: *управление привилегированным доступом; доступ «точно в срок»; контроль доступа; концепция нулевого доверия; привилегированные учетные записи; аудит и мониторинг сессий; информационная безопасность.*

В современных информационных системах контроль привилегированного доступа остается одной из ключевых задач обеспечения информационной безопасности, поскольку сохранение постоянных административных полномочий повышает риск злоупотребления правами, компрометации учетных записей и последующей эскалации привилегий. Развитие систем управления доступом и идентификацией, а также концепции Zero Trust (нулевое доверие), привело к распространению более гибких подходов, ориентированных на сокращение постоянных привилегий и предоставление доступа с учетом контекста, уровня риска и характера выполняемой задачи [1-6].

Одним из таких подходов является доступ «точно в срок» (Just-in-Time, JIT), предполагающий предоставление привилегий по запросу, на ограниченный срок и в объеме, необходимом для выполнения конкретной операции. Вместе с тем современные системы управления привилегированным доступом (Privileged Access Management, PAM) различаются по способам реализации данного механизма, включая порядок согласования доступа, использование временных учетных записей и автоматический отзыв привилегий. В связи с этим целью настоящей статьи является сравнительный анализ реализации JIT-доступа в современных PAM-системах и выявление ключевых различий между существующими подходами [5, 7-10].

Обзор научных подходов к динамическому и привилегированному доступу

Современные исследования в области контроля доступа показывают, что статические модели назначения прав все в меньшей степени соответствуют условиям распределенных корпоративных и облачных инфраструктур. Управление доступом все чаще рассматривается не как разовая процедура авторизации, а как непрерывный контур, включающий управление цифровыми идентичностями, аутентификацией, полномочиями и контролем корректности политик доступа. Одновременно отмечается, что сложность систем управления идентификацией и доступом (Identity and Access Management, IAM) сама по себе становится источником уязвимостей, а реализация принципа наименьших привилегий рассматривается как одно из ключевых направлений повышения их устойчивости [1, 2].

Привилегированный доступ в этой логике выступает наиболее чувствительным сегментом общей системы управления доступом, поскольку ошибки в назначении ролей, избы-

точные права и несогласованность жизненного цикла учетных записей в данной области приводят к наиболее тяжелым последствиям для безопасности. Исследования, посвященные межсистемному управлению идентификационными данными и ролевой модели разграничения доступа (Role-Based Access Control, RBAC) в рамках системы междоменного управления идентификацией (System for Cross-domain Identity Management, SCIM), показывают, что для современной инфраструктуры принципиальное значение имеют согласованность ролей, управляемость создания и отзыва учетных записей, а также совместимость различных сервисов и доменов [2, 7]. В современной литературе PAM рассматривается как специализированный уровень IAM, ориентированный на контроль наиболее критичных полномочий и сокращение постоянных привилегий.

Существенное влияние на развитие этих подходов оказала концепция Zero Trust, в которой доступ не связывается с неявным доверием к субъекту или устройству, а предоставляется после проверки набора атрибутов и может пересматриваться при изменении контекста. Исследования последних лет развивают эту логику в сторону динамической, риск-ориентированной и атрибутивной авторизации [3-6, 11, 12]. На этом фоне JIT-доступ рассматривается как прикладной механизм минимизации постоянных привилегий: доступ предоставляется по запросу, на ограниченный срок и в рамках конкретной задачи, а его реализация зависит от зрелости механизмов идентификации, управления учетными записями и автоматизированного применения политик. При этом в рассмотренных источниках сравнительные исследования, посвященные реализации JIT именно в PAM-системах, представлены ограниченно, что и определяет актуальность дальнейшего анализа [5, 7, 8].

JIT-доступ как механизм минимизации постоянных привилегий

JIT-доступ в современных подходах к управлению доступом понимается как предоставление полномочий не на постоянной основе, а по факту возникновения служебной необходимости, на ограниченный срок и в объеме, достаточном для выполнения конкретной операции. Такая логика соответствует развитию динамического и риск-ориентированного управления доступом, характерного для архитектур Zero Trust, где решение о допуске связывается не только с ролью пользователя, но и с контекстом запроса, текущим уровнем доверия и параметрами среды [3-6, 11, 12]. В применении к системам PAM JIT ориентирован прежде всего на сокращение числа постоянных административных полномочий и уменьшение окна времени, в течение которого такие полномочия вообще существуют.

Содержательно JIT-доступ характеризуется несколькими признаками. Во-первых, доступ инициируется по запросу, а не сохраняется за пользователем постоянно. Во-вторых, полномочия ограничиваются по времени и подлежат отзыву после завершения задачи. В-третьих, доступ обычно связывается с конкретной операцией, ресурсом или сценарием администрирования, что позволяет реализовать принцип наименьших привилегий не только на уровне ролей, но и на уровне фактического использования прав. Наконец, JIT-механизм предполагает прослеживаемость действий пользователя и включенность в общий жизненный цикл учетных записей и политик доступа. Именно поэтому в современной литературе временное предоставление прав рассматривается в тесной связи с динамической авторизацией, автоматизированным управлением учетными записями и созданием либо активацией учетной записи в момент санкционированного обращения [5, 7, 8].

При этом JIT-доступ не следует смешивать с любым временным допуском или с ручным согласованием доступа. Само по себе ограничение доступа по времени еще не образует полноценный JIT-механизм, если пользователь сохраняет избыточные права вне рамок конкретной задачи либо если выдача временного доступа не сопровождается автоматизированным отзывом привилегий. Аналогично ручное одобрение заявки не является достаточным признаком JIT, если после согласования пользователь получает широкие и слабо ограниченные полномочия без привязки к операции, ресурсу и сроку действия. В научной литературе акцент делается именно на сочетании краткосрочности, контекстной обусловленности, управляемости жизненного цикла прав и встроенности такого доступа в

общую архитектуру динамического контроля [5, 7, 8].

С учетом этого для последующего сравнительного анализа современных PAM-систем целесообразно использовать следующие критерии: наличие доступа по запросу; ограничение срока действия полномочий; наличие процедуры согласования; использование временных или специализированных учетных записей; автоматический отзыв прав; ограничение привилегий рамками конкретной задачи или ресурса; а также возможность аудита и прослеживания действий пользователя. Такая совокупность признаков позволяет отличать полноценную реализацию JIT от частичных решений, в которых временный доступ или согласование присутствуют лишь как отдельные элементы, но не образуют целостного механизма минимизации постоянных привилегий [5,7,8].

Сравнительный анализ реализации механизмов JIT-доступа в современных PAM-решениях

Сравнительный анализ реализации JIT-доступа в современных системах управления привилегированным доступом целесообразно проводить по следующим критериям: предоставление доступа по запросу, ограничение срока действия полномочий, наличие согласования, использование временных или специализированных учетных записей, автоматический отзыв прав, ограничение доступа рамками конкретной задачи, а также аудит действий пользователя [5, 7-10]. По указанным критериям в работе сопоставляются решения Solar SafeInspect [13], СКДПУ НТ [14] и CyberArk Privileged Access Manager [15].

Анализ открытых материалов показывает, что рассматриваемые решения различаются по степени формализации JIT-механизмов и по набору сопутствующих функций. Solar SafeInspect реализует гибкую организацию привилегированного доступа, включая различные режимы предоставления полномочий, и сочетает отдельные элементы JIT-подхода с координацией доступа и контролем сессий [13]. СКДПУ НТ позиционируется прежде всего как средство контроля действий привилегированных пользователей, мониторинга и аналитики, однако открытая документация также позволяет выделить ряд признаков JIT-подхода, включая предоставление доступа по запросу, ограничение его срока действия, согласование через механизм коллективного одобрения (голосования администраторов), а также отзыв доступа при нарушении установленных политик автоматически либо вручную [14]. CyberArk, напротив, наиболее последовательно акцентирует JIT-подход и концепцию Zero Standing Privileges: в открытых материалах заявлены временное предоставление полномочий, их отзыв после использования и настройка параметров согласования [15].

Существенные различия проявляются и в сопутствующих возможностях решений. Solar SafeInspect делает акцент на проксировании, изоляции и контроле привилегированных сессий, СКДПУ НТ – на сочетании механизмов контроля действий привилегированных пользователей, мониторинга, поведенческой аналитики и управляемого предоставления доступа по запросу, тогда как CyberArk ориентирован на наиболее глубокой интеграции JIT-доступа с концепцией отказа от постоянных привилегий. Для российской практики значим и нормативный аспект: отечественные решения ориентированы на использование в регулируемой среде, тогда как CyberArk в представленных открытых материалах не позиционируется как решение, ориентированное на требования российского регулируемого контура. В целом различия между сравниваемыми PAM-системами определяются не столько наличием базовых функций управления привилегированным доступом, сколько глубиной реализации временного и управляемого предоставления привилегий. Сводные результаты сравнения представлены в таблице 1. При этом для СКДПУ НТ часть признаков JIT выявляется не столько из кратких обзорных материалов, сколько из более детализированной открытой документации по механизмам согласования, временного предоставления и отзыва доступа [14].

Таблица 1. Сравнительная характеристика реализации JIT в современных PAM-решениях (оценка авторов по данным открытых материалов вендоров)

Критерий	Solar SafeInspect	СКДПУ НТ	CyberArk
Доступ по запросу	Реализован, в том числе через политики и сценарии согласования	Реализован; доступ инициируется по запросу	Реализован как базовый принцип JIT
Ограничение срока действия доступа	Декларируется изменение сроков доступа, в том числе автоматически	Поддерживается; доступ предоставляется на ограниченный срок	Явно реализовано
Согласование доступа	Поддерживается; в открытых материалах акцентирован механизм «четырех глаз»	Поддерживается; возможно коллективное согласование (голосование администраторов)	Явно поддерживается через approval-настройки
Временные / эфемерные учетные записи	Частично отражено в открытых материалах, без явного акцента на эфемерности	В открытой документации акцент сделан не на эфемерных учетных записях, а на управляемом предоставлении временного доступа	Явно поддерживаются
Автоматический отзыв привилегий	Частично отражен в открытых материалах	Поддерживается отзыв доступа; при нарушении политик доступ может быть прекращен автоматически или вручную	Явно поддерживается
Аудит и контроль сессий	Явно акцентировано в открытых материалах	Явно акцентировано в открытых материалах	Явно акцентировано в открытых материалах
Поведенческая аналитика	Частично отражена в открытых материалах	Явно акцентирована в открытых материалах	Явно акцентирована в открытых материалах
Применимость в регулируемой среде РФ	Ориентировано на применение в регулируемой среде РФ	Ориентировано на применение в регулируемой среде РФ	В открытых материалах не акцентировано как решение для регулируемой среды РФ

Заключение

Проведенный анализ показал, что JIT-доступ является одним из наиболее значимых механизмов снижения уровня постоянных привилегий в современных системах управления привилегированным доступом. В отличие от статического назначения административных полномочий, JIT-подход ориентирован на предоставление доступа по запросу, на ограниченный срок и в объеме, необходимом для выполнения конкретной задачи, что соответствует современным направлениям развития динамического и риск-ориентированного управления доступом.

Сравнение современных PAM-решений показало, что они существенно различаются по глубине реализации данного подхода. По результатам анализа открытых материалов наиболее формализованная и явно артикулированная реализация JIT-механизма выявлена у CyberArk, где временный доступ рассматривается как базовый элемент архитектуры управления привилегиями. Solar SafeInspect занимает промежуточное положение, сочетая отдельные элементы JIT с развитым контролем сессий и политиками доступа. СКДПУ НТ, наряду с выраженной ориентацией на мониторинг и аналитику, также поддерживает значимые элементы JIT-подхода, включая предоставление доступа по запросу, временное ограничение полномочий, процедуры согласования и отзыв доступа при нарушении политик. Следовательно, различия между PAM-системами определяются не только наличием базовых функций управления привилегированным доступом, но и степенью формализации, автоматизации и контекстной управляемости временного предоставления привилегий.

Библиографический список

1. Parkinson S., Khan S. A Survey on Empirical Security Analysis of Access Control Systems: A Real-World Perspective // ACM Computing Surveys. 2022. Vol. 55, № 6. Art. 123. 28 p. DOI: 10.1145/3533703.

2. Glöckler J., Sedlmeir J., Frank M., Fridgen G. A Systematic Review of Identity and Access Management Requirements in Enterprises and Potential Contributions of Self-Sovereign Identity // Business & Information Systems Engineering. 2024. Vol. 66, № 4. P. 421-440. DOI: 10.1007/s12599-023-00830-x.

3. Liu C., Tan R., Wu Y., Feng Y., Jin Z., Zhang F., Liu Y., Liu Q. Dissecting Zero Trust: Research Landscape and Its Implementation in IoT // Cybersecurity. 2024. Vol. 7. Art. 20. DOI: 10.1186/s42400-024-00212-0.

4. Cao Y., Pokhrel S. R., Zhu Y., Doss R., Li G. Automation and Orchestration of Zero Trust Architecture: Potential Solutions and Challenges // Machine Intelligence Research. 2024. Vol. 21, № 2. P. 294-317. DOI: 10.1007/s11633-023-1456-2.

5. Wang R., Li C., Zhang K., Tu B. Zero-Trust Based Dynamic Access Control for Cloud Computing // Cybersecurity. 2025. Vol. 8. Art. 12. DOI: 10.1186/s42400-024-00320-x.

6. Ma Y.-W., Chiu P.-H. A Novel Risk-Based Access Control Engine in Zero Trust Architecture for IoT Network // International Journal of Information Security. 2025. Vol. 24. Art. 124. DOI: 10.1007/s10207-025-01030-2.

7. Baumer T., Müller M., Pernul G. System for Cross-Domain Identity Management (SCIM): Survey and Enhancement With RBAC // IEEE Access. 2023. Vol. 11. P. 86872-86894. DOI: 10.1109/ACCESS.2023.3304270.

8. Gudu D., Hardt M., Brocke L., Zachmann G. Enabling Secure Shell Access with OpenID Connect // Computing and Software for Big Science. 2025. Vol. 9. Art. 5. DOI: 10.1007/s41781-025-00136-5.

9. ГОСТ Р 71753-2024. Защита информации. Системы автоматизированного управления учетными записями и правами доступа. Общие требования. – Москва, 2024.

10. Приказ ФСТЭК России от 11.04.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений» (зарегистрирован в Минюсте России 16.06.2025 № 82619).

11. Zubair M., Sabzevari M., Khatri V., Tarkoma S., Hätönen K. Access Control for Trusted Data Sharing // EURASIP Journal on Information Security. 2024. Vol. 2024. Art. 30. DOI: 10.1186/s13635-024-00178-z.

12. Mao Y., Fu W., Zhao Y., Yuan Z., Sun Z., Zhao Y. A Zero-Trust Access Control Model Based on Attribute and Dynamic Trust Evaluation for Cloud Environments // Symmetry. 2025. Vol. 17, № 12. Art. 2059. DOI: 10.3390/sym17122059.

13. Solar SafeInspect: полнофункциональная PAM-система. – Москва: Solar, 2024. – 10 с.

14. АйТи Бастион. Скат: система контроля привилегированного доступа. – Москва: АйТи Бастион, 2024. – 74 с.

15. CyberArk. CyberArk Privileged Access Management Solutions: whitepaper. – 2024. – 13 p.

COMPARATIVE ANALYSIS OF JIT ACCESS IMPLEMENTATION IN MODERN PAM SYSTEMS

V.V. Singurov[1], *Specialist Degree Graduate*
A.S. Safronov[2], *Graduate Student*
N.U. Tagirov[2], *Graduate Student*
Supervisor: *A.V. Osin[2], Candidate of Technical Sciences, Associate Professor*
[1]MIREA – Russian Technological University
[2]Moscow Technical University of Communications and Informatics
[1,2](Russia, Moscow)

Abstract. *The article examines the JIT access mechanism as a tool for reducing standing privileges in PAM systems. A comparative analysis of JIT implementation in Solar SafeInspect, SKDPU NT, and CyberArk is carried out using the criteria of time-limited privilege provision, approval procedures, privilege revocation, and action auditing. The study shows that the PAM systems under consideration differ in the depth of JIT implementation and in the way JIT mechanisms are combined with session control and analytical capabilities. The results may be used in the selection of PAM solutions for secure information systems.*

Keywords: *privileged access management; just-in-time access; access control; zero trust concept; privileged accounts; session auditing and monitoring; information security.*