

Д. А. Остриков¹✉

Метод адаптивного контроля привилегированного доступа на основе мультипликативной агрегации рисков

¹Национальный исследовательский ядерный университет «МИФИ»,
г. Москва, Российская Федерация
e-mail: denis.ostrikov.01@mail.ru

Аннотация. В статье предложен метод адаптивного контроля привилегированного доступа к серверам Linux-инфраструктуры, основанный на количественной оценке рисков. Разработана мультипликативная модель агрегации пяти контекстных факторов запроса доступа: истории аномалий пользователя, критичности запрашиваемых ролей, подсети источника, геолокации и времени запроса. Модель обладает свойством вето: единственный критический фактор приводит к максимальной оценке риска независимо от остальных. Проведено сравнение трёх методов агрегации на публичном датасете из 31 млн записей аутентификации; мультипликативная модель показала AUC-ROC = 0,883, сопоставимый с взвешенной суммой (0,885), при наличии теоретически обоснованных преимуществ. На основе интегральной оценки риска система динамически определяет параметры выдаваемого SSH-сертификата: срок действия по экспоненциальной функции, уровень верификации по ступенчатой функции с двумя порогами и режим записи сессии. Метод интегрирован с подсистемой PAM операционной системы Linux. Реализован программный прототип, валидированный на виртуальном стенде. Показано сокращение срока действия аутентификационных данных на 64–82% по сравнению со статическими политиками. Симуляция работы 50 пользователей на протяжении 7 дней подтвердила корректное разделение профилей и адаптацию системы к изменениям поведения через механизм обратной связи.

Ключевые слова: адаптивный контроль доступа, оценка рисков, Linux-инфраструктура, SSH-сертификаты, PAM, Zero Trust

D. A. Ostrikov¹✉

Adaptive privileged access control method based on multiplicative risk aggregation

¹National Research Nuclear University MEPhI, Moscow, Russian Federation
e-mail: denis.ostrikov.01@mail.ru

Abstract. The paper proposes a method for adaptive privileged access control in Linux infrastructure based on quantitative risk assessment. A multiplicative aggregation model combining five contextual request factors is developed: user anomaly history, requested role criticality, source subnet, geolocation, and request time. The model features a veto property where a single critical factor forces maximum risk regardless of others. Three aggregation methods are compared on a public dataset of 31 million authentication records; the multiplicative model achieved AUC-ROC of 0.883, comparable to the weighted sum (0.885), while offering theoretically grounded advantages. Based on the integral risk score, the system dynamically determines SSH certificate parameters: validity period via an exponential function, verification level via a step function with two thresholds, and session recording mode. The method integrates with the Linux PAM subsystem. A software prototype has been implemented and validated on a virtual testbed, demonstrating 64–82% reduction in authentication creden-

tial validity period compared to static policies. A 7-day simulation with 50 users confirmed correct profile separation and behavioral adaptation through a feedback mechanism.

Keywords: adaptive access control, risk assessment, Linux infrastructure, SSH certificates, PAM, Zero Trust

Введение

Управление привилегированным доступом к серверам корпоративной инфраструктуры остаётся одной из ключевых задач информационной безопасности. Компрометация привилегированной учётной записи позволяет злоумышленнику выполнять произвольные команды на серверах, извлекать данные и перемещаться по инфраструктуре. Согласно отчёту Verizon DBIR 2024, злоупотребление привилегиями присутствует в 82% успешных инцидентов [1], а среднее время обнаружения компрометации составляет 207 дней [2].

Традиционный подход к управлению доступом основан на статических политиках: пользователю назначается фиксированный набор ролей, а параметры сеанса – срок действия удостоверяющих данных, уровень верификации, режим аудита – одинаковы для всех запросов. Такой подход не учитывает контекст: подключение в рабочее время из корпоративной сети и подключение ночью с неизвестного адреса оцениваются одинаково. Архитектура Zero Trust [3, 13] требует непрерывной верификации каждого запроса, однако на практике её реализация сводится к фиксированным многофакторным проверкам без количественной оценки риска.

Исследования в области интеллектуальной поддержки принятия решений в информационной инфраструктуре [4, 5] и методология интеллектуально-адаптивного управления [6] показали эффективность адаптивных подходов к обеспечению безопасности. Модели риск-ориентированного контроля доступа [7, 8] позволяют принимать градуированные решения, однако используют взвешенную сумму факторов [7, 15], которая допускает компенсацию критического фактора благоприятными значениями остальных. Кроме того, существующие решения либо ориентированы на специфические домены [9, 14], либо не имеют практической реализации, интегрированной с механизмами операционной системы [10].

Проблема заключается в том, что существующие методы агрегации рисков не гарантируют, что единственный критический фактор – например, запрос привилегированной роли – приведёт к максимальному уровню защиты. Кроме того, отсутствуют готовые решения, связывающие количественную оценку риска с параметрами SSH-сертификатов через стандартные механизмы операционной системы Linux.

Постановка задачи

Целью исследования является повышение безопасности Linux-инфраструктуры за счёт разработки методов динамического управления привилегированным доступом на основе оценки рисков. Под динамическим управлением понимается адаптивное определение параметров каждого сеанса доступа – требуе-

мого уровня верификации, срока действия удостоверяющих данных и детальности аудита – в зависимости от контекста запроса.

Для достижения цели необходимо решить следующие задачи: разработать математическую модель многофакторной агрегации рисков, обеспечивающую свойство вето – невозможность компенсации критического фактора; разработать метод динамического определения параметров сеанса доступа на основе вычисленной оценки; обеспечить интеграцию метода с подсистемой РАМ операционной системы Linux; провести экспериментальное сравнение с альтернативными подходами к агрегации.

Новизна предлагаемого решения заключается в применении мультипликативной модели агрегации со свойством вето для задачи контроля привилегированного доступа и её интеграции с подсистемой РАМ через стандартные SSH-сертификаты, что обеспечивает практическую реализуемость без модификации существующей инфраструктуры.

Предлагаемое решение

Модель агрегации рисков. Для каждого запроса привилегированного доступа система вычисляет интегральную оценку риска $R \in [0, 1]$ на основе пяти контекстных факторов, каждый из которых нормализуется в оценку $r_i \in [0, 1]$. Агрегация выполняется по мультипликативной формуле:

$$R = 1 - \prod_{i=1}^d (1 - r_i)^{w_i} \quad (1)$$

где $w_i > 0$ – вес i -го фактора. Принципиальное отличие от взвешенной суммы состоит в свойстве вето: если хотя бы один $r_i = 1$, то $R = 1$ независимо от остальных факторов. Запрос с критической ролью не может быть «компенсирован» низкими значениями остальных факторов, что соответствует требованиям модели безопасности.

Контекстные факторы сгруппированы по категориям NIST SP 800-162 [11]: субъект (r_1 – агрегированная оценка аномальности прошлых сессий с экспоненциальным затуханием), объект (r_2 – максимальная критичность запрашиваемых ролей), окружение (r_3 – принадлежность IP-адреса к зоне доверия; r_4 – типичность геолокации; r_5 – принадлежность времени к рабочему периоду). Выбор факторов обоснован экспериментально: на датасете RBA (31 млн записей) [12] подсеть и страна источника показали наибольшую взаимную информацию с меткой атаки ($I = 0,127$ и $I = 0,094$), а на датасете LANL Cyber1 (1,05 млрд событий) подтверждена информативность временного фактора в корпоративной среде.

Адаптивные параметры сеанса. На основе R определяются четыре параметра выдаваемого SSH-сертификата. Срок действия задаётся экспоненциальной убывающей функцией:

$$T(R) = T_{min} + (T_{max} - T_{min}) \cdot e^{-k \cdot R} \quad (2)$$

где $T_{\min} = 1$ ч, $T_{\max} = 12$ ч, $k = 3$. Уровень верификации определяется ступенчатой функцией с двумя порогами: $\theta_1 = 0,10$ (пароль + ОТР $\rightarrow$ аппаратный ключ) и $\theta_2 = 0,65$ (аппаратный ключ $\rightarrow$ аппаратный ключ с одобрением администратора). Режим записи сессии и уведомление администратора определяются аналогичными пороговыми функциями.

Интеграция с операционной системой. Прототип состоит из трёх компонентов: сервер сертификатов, модуль аутентификации и клиент командной строки. Модуль аутентификации вызывается подсистемой PAM при каждом SSH-подключении. Адаптивные параметры (срок действия, режим записи, уведомление) передаются через поле расширений стандартного сертификата OpenSSH, что обеспечивает совместимость с существующей инфраструктурой без модификации серверного программного обеспечения.

Экспериментальная методика

Для обоснования выбора мультипликативной модели проведено сравнение с двумя альтернативами: взвешенной суммой с логистической функцией и двухуровневой агрегацией по категориям NIST. Веса каждого метода определены из данных методом лог-линеаризации. Оценка выполнена на тестовой выборке из 400 тыс. записей датасета RBA по метрике AUC-ROC; статистическая значимость различий проверена тестом Делонга.

Прототип валидирован на виртуальном стенде с реальной операционной системой. Проведены три серии экспериментов: оценка адаптивности срока действия сертификата для 500 сессий с различным профилем риска; нагрузочное тестирование при 1, 10 и 50 параллельных клиентах; 7-дневная симуляция с 50 пользователями трёх поведенческих профилей (нормальный, необычный, вредоносный). Вредоносные пользователи генерировали аномальные оценки сессий, поступающие в фактор r_1 через механизм обратной связи.

Результаты

Сравнение методов агрегации. Результаты сравнения трёх методов на датасете RBA представлены в табл. 1. Все три метода показали сопоставимые значения AUC-ROC; различие между взвешенной суммой и мультипликативной моделью составило 0,002 (тест Делонга: $p = 0,002$). Мультипликативная модель выбрана как единственная, обладающая свойством вето.

Таблица 1. Сравнение методов агрегации рисков

Метод	AUC-ROC	Recall	Свойство вето
Взвешенная сумма	0,885	0,894	Нет
Мультипликативная	0,883	0,901	Да
Двухуровневая	0,881	0,894	Нет

Адаптивность срока действия. В табл. 2 показано, как предложенный метод дифференцирует срок действия сертификата в зависимости от профиля риска. При статической политике все пользователи получают одинаковый срок (ти-

пично 12–24 ч); предложенный метод сокращает его от 5,78 ч для низкого риска до 1,55 ч для критического. Среднее сокращение относительно фиксированного срока 12 ч составляет 64%.

Таблица 2. Зависимость срока действия сертификата от уровня риска

Профиль запроса	Средний R	Срок действия, ч
Низкий риск (непривилегированная роль, доверенная подсеть)	0,28	5,78
Умеренный риск (привилегии на промежуточную среду)	0,44	3,48
Высокий риск (привилегированная роль, внешняя подсеть)	0,76	2,05
Критический риск (аномальная история, внешняя подсеть)	0,99	1,55

Нагрузочное тестирование (табл. 3) показало, что латентность принятия решения остаётся приемлемой даже при значительной параллельной нагрузке: при 50 одновременных клиентах 99-й перцентиль составляет 95 мс при пропускной способности 1210 запросов в секунду.

Таблица 3. Латентность принятия решения

Параллельных клиентов	p_{99} , мс	Запросов/с
1	9	129
10	22	647
50	95	1210

Симуляция. Результаты 7-дневной симуляции (табл. 4) демонстрируют, что система корректно дифференцирует три класса пользователей исключительно на основе контекстных факторов. Нормальные пользователи получают минимальные ограничения, вредоносные – максимальные. Особенно показателен механизм обратной связи: средний R вредоносных пользователей вырос с 0,989 в первый день до 1,000 к третьему дню за счёт накопления аномальных оценок в факторе r_1 , что свидетельствует об адаптации системы к устойчивым угрозам.

Таблица 4. Результаты 7-дневной симуляции

Профиль	Средний R	Верификация	Срок, ч	Запись, %
Нормальный (n=840)	0,278	100% L1	5,78	0
Необычный (n=98)	0,642	67% L1, 33% L2	2,70	67
Вредоносный (n=84)	0,998	100% L2	1,55	100

Обсуждение

Предложенный метод отличается от существующих подходов к риск-ориентированному контролю доступа [7, 8] в двух аспектах. Во-первых, мультипликативная агрегация обеспечивает свойство вето, отсутствующее у методов на основе взвешенной суммы [7]. Сравнительный эксперимент на 31 млн записей подтвердил, что это свойство достигается без потери качества классификации (AUC-ROC 0,883 против 0,885). Во-вторых, метод интегрирован с подсистемой РАМ через стандартные SSH-сертификаты, что отличает его от теоретических моделей [8, 10], не имеющих практической реализации.

Результаты симуляции показывают, что доминирование фактора критичности ролей обеспечивает чёткое разделение классов пользователей, что соответствует принципу наименьших привилегий [3] и рекомендациям по интеллектуально-адаптивному управлению инфраструктурой [6]. Механизм обратной связи через r_1 позволяет системе адаптироваться к устойчивым угрозам без переобучения модели.

Ограничением метода является зависимость качества от экспертного назначения значений факторов. В дальнейших исследованиях планируется автоматическое определение значений из данных, а также интеграция нейросетевой модели обнаружения аномалий в последовательностях привилегированных команд.

Заключение

В работе предложен метод адаптивного контроля привилегированного доступа, основанный на мультипликативной агрегации пяти контекстных факторов риска. Метод обеспечивает свойство вето, отсутствующее у альтернативных подходов на основе взвешенной суммы, при сопоставимом качестве классификации (AUC-ROC 0,883 против 0,885 на датасете из 31 млн записей). На основе интегральной оценки риска система динамически определяет срок действия SSH-сертификата, уровень верификации и режим записи сессии. Реализованный прототип интегрирован с подсистемой РАМ Linux и валидирован на виртуальном стенде: показано сокращение срока действия удостоверяющих данных на 64% относительно статической политики, а 7-дневная симуляция подтвердила адаптацию системы к изменениям поведенческого профиля пользователей.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Verizon. 2024 Data Breach Investigations Report [Электронный ресурс]. – URL: <https://www.verizon.com/business/resources/reports/dbir/> (дата обращения: 15.04.2026).
2. IBM. X-Force Threat Intelligence Index 2024 [Электронный ресурс]. – URL: <https://www.ibm.com/reports/threat-intelligence> (дата обращения: 15.04.2026).
3. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture : NIST SP 800-207. – National Institute of Standards and Technology, 2020. – 59 p.
4. Басыня Е. А. Интеллектуальная поддержка при принятии технических решений в информационной инфраструктуре предприятия // Защита информации. Инсайд. – 2020. – № 4. – С. 68–73.
5. Басыня Е. А., Худяков Д. С. Комплексный мониторинг информационной инфраструктуры предприятия // Защита информации. Инсайд. – 2020. – № 6. – С. 28–33.

6. Басыня Е. А. Комплексная методология интеллектуально-адаптивного управления информационной инфраструктурой предприятия // Защита информации. Инсайд. – 2021. – № 5 (101). – С. 16–25.
7. Kandala S., Sandhu R., Bhamidipati V. An Attribute Based Framework for Risk-Adaptive Access Control Models // Proceedings of the 6th International Conference on Availability, Reliability and Security. – IEEE, 2011. – P. 236–241.
8. Chen L., Crampton J. Risk-Aware Role-Based Access Control // Proceedings of the 7th International Workshop on Security and Trust Management. – Springer, 2012. – P. 140–156.
9. Atlam H. F., Wills G. B. IoT Security, Privacy, Safety and Ethics // Digital Twin Technologies and Smart Cities. – Springer, 2020. – P. 123–149.
10. Магомедов Ш. Г. Модели и методы интеллектуально-адаптивного управления доступом в образовательных вычислительных сервисах : дис. ... д-ра техн. наук. – М., 2024. – 312 с.
11. Hu V. C. et al. Guide to Attribute Based Access Control (ABAC) Definition and Considerations : NIST SP 800-162. – National Institute of Standards and Technology, 2014. – 54 p.
12. Wiefeling S., Lo Iacono L., Dürmuth M. Is This Really You? An Empirical Study on Risk-Based Authentication Applied in the Wild // IFIP Annual Conference on Data and Applications Security and Privacy. – Springer, 2019. – P. 134–152.
13. Syed N. F. et al. Zero Trust Architecture (ZTA): A Comprehensive Survey // IEEE Access. – 2022. – Vol. 10. – P. 57143–57179.
14. Ramezanpour K., Jagannath J. Intelligent Zero Trust Architecture for 5G/6G Networks // IEEE Communications Standards Magazine. – 2022. – Vol. 6. – No. 4. – P. 60–67.
15. Xiao S., Ye Y., Kanwal N., Neue T., Lee B. SoK: Context and Risk Aware Access Control for Zero Trust Systems // Security and Communication Networks. – 2022. – Vol. 2022. – P. 1–14.

© Д. А. Остриков, 2026