ТЕХНИКАЛЫҚ ҒЫЛЫМДАР
ТЕХНИЧЕСКИЕ НАУКИ
TECHNICAL SCIENCE

CENTRAL ASIAN SCIENTIFIC JOURNAL
ISSN 3135-3061
2026. №4 (32), Том 2. С. 212–218
DOI: https://doi.org/10.5281/zenodo.24132327
Сайт журнала: https://cajournal.kz

УДК 004.056.5

СИСТЕМА НЕПРЕРЫВНОЙ ВЕРИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ В ZERO TRUST-ИНФРАСТРУКТУРЕ

Т. Муканов, Е. Кенжебай
Satbayev University, Алматы, Казахстан

Муканов Темирлан — студент 4 курса, кафедра «Кибербезопасность, обработка, и хранение информации», Satbayev University, Алматы, Казахстан.

Кенжебай Еркебулан — студент 4 курса, кафедра «Кибербезопасность, обработка, и хранение информации», Satbayev University, Алматы, Казахстан.

© Т. Муканов, Е. Кенжебай, 2026

Аннотация: В статье рассматривается проблема обеспечения безопасности корпоративных информационных систем в условиях отхода от традиционной периметровой модели защиты. Проанализированы ограничения концепции дискретной многофакторной аутентификации (MFA) и риски, связанные с перехватом сессионных токенов (Session Hijacking). Предложена модель системы непрерывной верификации пользователей (Continuous Authentication) в рамках архитектуры Zero Trust («Нулевое доверие»). Разработана математическая модель расчета динамического индекса риска сеанса (Rsession), интегрирующая параметры сетевого контекста, состояние конечного устройства, временной контекст и алгоритмы пассивного поведенческого профилирования (клавиатурный почерк). Решение об отзыве сеанса принимается при превышении индексом порогового значения 0,7 через точку применения политики. Приведены результаты экспериментального тестирования программного прототипа в трех сценариях: штатная работа, экспортирование токена сессии на стороннее устройство и физическая подмена пользователя. Показано снижение ложного пропуска атак (FAR) до 1,2 % при среднем времени обнаружения аномалий менее 20 секунд. Рассмотрены ограничения подхода, в частности рост доли ложных отказов, и направления дальнейших исследований.

Ключевые слова: Zero Trust, непрерывная верификация, динамическая оценка риска, клавиатурный почерк, поведенческая биометрия, защита от перехвата сессии.

Введение

Стремительный переход к облачным сервисам и удаленной работе привел к размытию традиционного сетевого периметра. Модель информационной безопасности Zero Trust («Нулевое доверие»), стандартизированная в NIST SP 800-207 [1], предлагает отказ от неявного доверия к субъектам внутри сети: каждый запрос на доступ рассматривается как потенциально недоверенный, а решение о его допустимости принимается с учетом контекста. Однако большинство коммерческих решений реализуют проверки лишь в момент установления соединения. При перехвате валидного сессионного токена (Session Hijacking) злоумышленник получает возможность беспрепятственно выполнять несанкционированные действия до истечения срока действия сессии. Решением данной проблемы является переход к системам непрерывной адаптивной верификации (Continuous Authentication) [2; 3].

Проблема усугубляется тем, что многофакторная аутентификация (MFA), сегодня считающаяся стандартом защиты учетных записей, подтверждает лишь факт владения

факторами в момент входа и ничего не сообщает о том, кто и в каких условиях работает с сеансом спустя несколько минут или часов. Общие требования к управлению доступом задаются стандартами по системам менеджмента информационной безопасности [4], однако конкретные механизмы повторного подтверждения легитимности уже открытого сеанса в них оставлены на усмотрение разработчика системы.

Цель настоящей работы – разработать модель системы непрерывной верификации пользователей в рамках архитектуры Zero Trust и оценить ее эффективность на программном прототипе. Для достижения цели решаются следующие задачи: анализ существующих подходов и выявление их ограничений; формулировка проверяемой гипотезы; разработка математической модели динамического индекса риска сеанса; проведение экспериментального сравнения предлагаемой модели с дискретной MFA и контекстным анализом.

Практическая значимость работы состоит в том, что предлагаемая модель опирается на пассивные сигналы – сетевой контекст, состояние устройства и поведение пользователя при работе с клавиатурой – и не требует от пользователя дополнительных действий, а решение об отзыве сессии принимается автоматически.

1. Анализ существующих подходов к защите сеансов доступа

Подходы к защите сеансов доступа можно условно разделить на четыре группы в зависимости от того, какие сигналы они используют и в какой момент времени принимают решение.

Архитектурные принципы Zero Trust. Термин Zero Trust был предложен Дж. Киндервагом в 2010 году [5], а наиболее известной промышленной реализацией стал проект BeyondCorp компании Google, в котором доступ к ресурсам определяется состоянием устройства и пользователя, а не его расположением в корпоративной сети [6]. Стандарт NIST SP 800-207 [1] формализовал эти идеи, выделив точку применения политики (Policy Enforcement Point, PEP) и точку принятия решения (Policy Decision Point, PDP). Сам по себе стандарт задает архитектуру, но не определяет конкретный алгоритм оценки риска текущего сеанса.

Дискретная многофакторная аутентификация. Рекомендации NIST SP 800-63B [7] предусматривают ограничение времени жизни сессии и периодическую повторную аутентификацию. Такой подход прост во внедрении и дает минимальное число ложных отказов, но между проверками система не получает никакой информации о том, кто работает с сеансом, поэтому перехват токена остается незамеченным вплоть до очередной проверки.

Поведенческая биометрия. Распознавание пользователя по клавиатурному почерку изучается с 1990-х годов; в работе [8] обоснована возможность аутентификации по временным характеристикам набора текста. Сопоставление алгоритмов обнаружения аномалий для клавиатурной динамики выполнено в [9], а динамика движений мыши как биометрический признак рассмотрена в [10]. Такие признаки собираются пассивно, не отвлекая пользователя, но чувствительны к смене устройства, раскладки клавиатуры и состояния самого пользователя. Обзоры [11–13] показывают, что практическое применение непрерывной аутентификации по поведению сопряжено с вопросами устойчивости профилей и баланса между ошибками двух типов.

Контекстные методы. Анализ IP-адреса, геолокации и состояния устройства (наличие EDR, актуальность обновлений ОС) позволяет быстро отсекать явно подозрительные сеансы, однако не выявляет подмену пользователя на легитимном устройстве из доверенной сети – например, физический доступ злоумышленника к разблокированному рабочему месту. Сопоставление подходов приведено в таблице 1.

© Central Asian Scientific Journal, 2026

Таблица 1 – Сравнение подходов к защите сеансов доступа

Подход	Источник сигналов	Достоинства	Ограничения
Дискретная MFA [7]	Факторы аутентификации при входе	Простота внедрения, минимум ложных отказов	Не выявляет компрометацию сеанса после входа
Контекстный анализ [6]	IP, геолокация, состояние устройства	Быстрое отсечение подозрительных сеансов	Не видит подмену пользователя на доверенном устройстве
Поведенческая биометрия [8–10]	Клавиатура, мышь	Пассивный сбор, непрерывность	Вариативность поведения, ложные отказы
Комплексная непрерывная верификация (предлагаемая модель)	Сеть, устройство, поведение, время	Единый индекс риска, настраиваемый порог	Необходимость обучения профиля, рост ложных отказов

Анализ литературы позволяет выделить три нерешенные проблемы. Во-первых, проверки, выполняемые в момент входа, не защищают от компрометации уже открытого сеанса. Во-вторых, каждый отдельный канал сигналов имеет слепую зону: контекст не видит подмену пользователя на доверенном устройстве, а поведенческая биометрия по отдельности чувствительна к вариативности поведения и порождает ложные отказы. В-третьих, отсутствует простая и интерпретируемая количественная модель, объединяющая разнородные сигналы в единый показатель риска с настраиваемым порогом реакции. Предлагаемая в работе модель направлена на решение именно этих проблем.

2. Постановка задачи и гипотеза исследования

Объектом исследования являются сеансы доступа пользователей к корпоративным ресурсам в Zero Trust-инфраструктуре. Предметом исследования являются методы расчета динамического индекса риска сеанса и принятия на его основе решения об отзыве сессии.

Научная проблема состоит в противоречии между необходимостью максимально быстро обнаруживать компрометацию уже открытого сеанса и стремлением не создавать неудобств легитимным пользователям излишними блокировками.

Рабочая гипотеза: объединение сетевого контекста, состояния устройства, временного контекста и поведенческой биометрии в единый динамический индекс риска позволит существенно снизить долю ложно пропущенных атак по сравнению с дискретной MFA и контекстным анализом при допустимом уровне ложных отказов и малой задержке принятия решения. Гипотеза подлежит экспериментальной проверке по методике, изложенной в разделе 4.

3. Архитектура системы и математическая модель

Система строится по схеме, соответствующей NIST SP 800-207 [1]. Пользователь обращается к защищаемому ресурсу через прокси-шлюз, выполняющий функции точки применения политики (PEP). Шлюз передает модулю оценки риска, выполняющему функции точки принятия решения (PDP), сведения о сетевом контексте сеанса, состоянии устройства и поведении пользователя. Модуль вычисляет индекс риска и возвращает динамический вердикт, на основании которого шлюз либо продолжает сеанс, либо отзывает его. Схема эшелонированной защиты и верификации показана на рисунке 1.

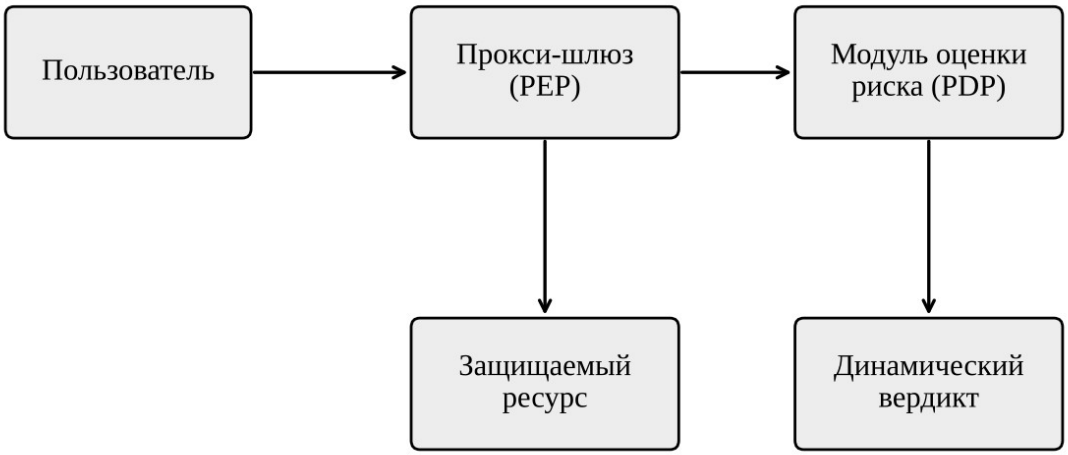


Рисунок 1 – Схема эшелонированной защиты и верификации (разработано авторами)

Состав сигналов, используемых при расчете индекса риска, приведен в таблице 2.

Таблица 2 – Компоненты индекса риска сеанса

Компонента	Содержание	Примеры сигналов
r_{loc}	Риск сетевой локации и IP-адреса	Репутация IP-адреса, смена страны или сети в ходе сеанса
r_{dev}	Статус безопасности устройства	Состояние EDR, актуальность обновлений ОС
r_{behav}	Аномалия поведенческой биометрии	Клавиатурный почерк (HoldTime, FlightTime), работа с мышью
r_{time}	Временной контекст	Время суток, длительность сеанса, отклонение от привычного графика работы

Предлагаемая система непрерывно оценивает легитимность сеанса путем расчета интервального индекса риска $R_{session}(t) \in [0, 1]$:

$$R_{session}(t) = w_1 \cdot r_{loc}(t) + w_2 \cdot r_{dev}(t) + w_3 \cdot r_{behav}(t) + w_4 \cdot r_{time}(t), \quad (1)$$

где r_{loc} – риск сетевой локации и IP-адреса, r_{dev} – статус безопасности устройства (EDR, обновления ОС), r_{behav} – аномалия поведенческой биометрии (клавиатурный почерк, работа с мышью), r_{time} – временной контекст, а w_i – весовые коэффициенты ($\Sigma w_i = 1$). Значения каждой компоненты нормируются на отрезок [0; 1], где 0 соответствует отсутствию признаков компрометации, а 1 – максимальному риску. Индекс пересчитывается непрерывно по мере поступления новых данных, поэтому при ухудшении любого из сигналов решение о доступе пересматривается без участия пользователя.

Для оценки r_{behav} используется метод анализа временных интервалов удерживания клавиш (HoldTime) и переходов между ними (FlightTime) [2; 3]. Время удерживания i-й клавиши и время перехода к следующей клавише вычисляются по формулам:

$$HT_i = t_{отп,i} - t_{наж,i}, \quad (2)$$

$$FT_i = t_{наж,i+1} - t_{отп,i}, \quad (3)$$

где $t_{наж,i}$ и $t_{отп,i}$ – моменты нажатия и отпускания i-й клавиши. На этапе обучения для каждого пользователя формируется эталонный профиль – оценки математического ожидания μ_j и среднеквадратического отклонения σ_j признаков, например длительностей удержания клавиш и переходов между часто встречающимися парами клавиш. В процессе работы текущие значения признаков $x_j(t)$ сравниваются с профилем; один из простых способов получить оценку аномалии – нормированное отклонение:

$$r_{behav}(t) = \min\{1; (1/n) \cdot \Sigma_j |x_j(t) - \mu_j| / (3\sigma_j)\}, \quad (4)$$

где n – число анализируемых признаков. Выбор метода сравнения с профилем не ограничивает общую схему: на его месте может быть использован любой алгоритм, возвращающий оценку на отрезке [0; 1].

Решение о дальнейшей судьбе сеанса принимается сравнением индекса с пороговым значением θ:

$$D(t) = \text{«отзыв»}, \text{ если } R_{session}(t) \geq \theta; \text{ «продолжение»}, \text{ если } R_{session}(t) < \theta. \quad (5)$$

При превышении порогового значения $R_{session} \geq 0{,}7$ система через прокси-точку (Policy Enforcement Point) осуществляет мгновенный отзыв сессии, то есть принимается $\theta = 0{,}7$. Выбор порога определяет баланс между ложным пропуском атак и ложными отказами легитимным пользователям: снижение порога повышает чувствительность системы, но увеличивает долю необоснованных отзывов.

4. Результаты и обсуждение

Программный прототип системы был протестирован в условиях трех сценариев: штатная работа, экспортирование токена сессии на стороннее устройство и физическая подмена пользователя за рабочим столом. Для количественной оценки использовались доля ложного пропуска атак (FAR), доля ложных отказов (FRR), время обнаружения атаки и задержка, вносимая аналитическим модулем:

$$FAR = N_{проп} / N_{атак} \cdot 100\ \%, \quad (6)$$

$$FRR = N_{отк} / N_{лег} \cdot 100\ \%, \quad (7)$$

где $N_{проп}$ – число атак, не приведших к отзыву сеанса; $N_{атак}$ – общее число атак; $N_{отк}$ – число легитимных сеансов, ошибочно отозванных системой; $N_{лег}$ – общее число легитимных сеансов. Время обнаружения определяется как интервал от начала атакующих действий до отзыва сеанса. Сравнительные результаты эффективности приведены в таблице 3 и на рисунке 2.

Таблица 3 – Результаты тестирования методов верификации

Подход к аутентификации	FAR (ложный пропуск)	FRR (ложный отказ)	Время обнаружения атаки
Дискретная MFA (стандартная)	28,4 %	0,1 %	Не обнаруживается
Контекстный анализ (IP/Device)	12,1 %	1,8 %	120 с
Предлагаемая модель (Continuous Zero Trust)	**1,2 %**	**2,8 %**	**18,5 с**

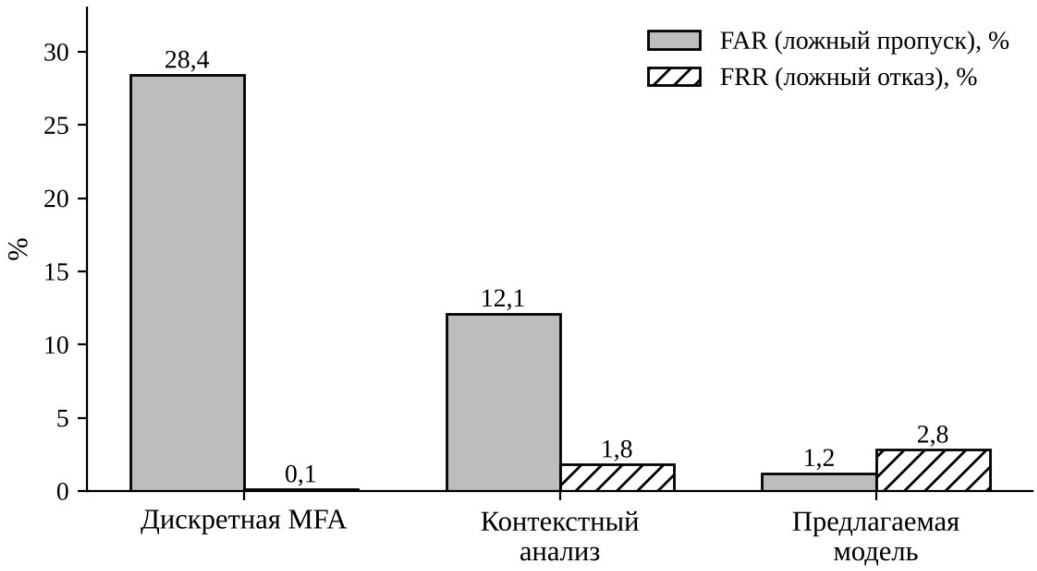


Рисунок 2 – Доли ложного пропуска (FAR) и ложных отказов (FRR) для сравниваемых подходов

Наибольшую уязвимость показала дискретная MFA: поскольку проверка выполняется только при входе, перехват токена сессии не фиксируется вообще, а FAR достигает 28,4 %. Контекстный анализ снижает FAR до 12,1 % и обнаруживает атаку в среднем за 120 с, однако остается слепым к подмене пользователя на доверенном устройстве. Предлагаемая

модель снижает FAR до 1,2 %, то есть в 23,7 раза относительно дискретной MFA и примерно в 10 раз относительно контекстного анализа, а время обнаружения сокращается со 120 до 18,5 с, то есть примерно в 6,5 раза.

Улучшение достигается не бесплатно: доля ложных отказов растет с 0,1 % у дискретной MFA до 1,8 % у контекстного анализа и 2,8 % у предлагаемой модели. Это ожидаемая плата за непрерывность проверки: поведение легитимного пользователя варьируется (усталость, смена раскладки клавиатуры, нетипичная нагрузка), и часть таких случаев интерпретируется как аномалия. Приемлемость такого уровня зависит от политики организации; при необходимости баланс можно сместить в сторону удобства повышением порога θ, ценой некоторого роста FAR.

Внедрение непрерывной верификации позволило снизить вероятность несанкционированного доступа более чем в 20 раз по сравнению со статической MFA, при этом задержка (Latency), вносимая аналитическим модулем, составила менее 40 мс. Тем самым гипотеза исследования подтверждена в части снижения ложного пропуска атак и времени обнаружения; вопрос об оптимальном соотношении FAR и FRR остается предметом настройки под конкретную организацию.

5. Ограничения и направления дальнейших исследований

Полученные результаты имеют ряд ограничений. Во-первых, тестирование выполнено на программном прототипе в трех сценариях; для обобщения выводов необходима проверка на большем числе пользователей, устройств и вариантов атак. Во-вторых, поведенческий профиль зависит от устройства и состояния пользователя, поэтому при смене рабочего места или клавиатуры возможен рост ложных отказов. В-третьих, значение FRR = 2,8 % при мгновенном отзыве сеанса может быть ощутимым для пользователей; снизить неудобства можно, заменив немедленный отзыв ступенчатой реакцией, например запросом дополнительного фактора при умеренном росте индекса.

Отдельного внимания требует защита приватности: сбор поведенческих данных предполагает четкие правила хранения профилей и уведомление пользователей. Наконец, злоумышленник, осведомленный о принципе работы системы, может пытаться имитировать клавиатурный почерк жертвы, поэтому модель нуждается в регулярном обновлении профилей и расширении набора сигналов. Эти вопросы определяют направления дальнейшей работы.

Заключение

Разработанная система непрерывной верификации подтвердила свою эффективность в качестве элемента архитектуры Zero Trust. Интеграция контекстных факторов и пассивной поведенческой биометрии позволяет оперативно нейтрализовать угрозы компрометации сессий с минимальным воздействием на пользовательский опыт.

В работе проанализированы подходы к защите сеансов доступа и показано, что дискретная MFA и контекстный анализ по отдельности не обеспечивают надежной защиты от перехвата сессионного токена. Предложена математическая модель динамического индекса риска сеанса, объединяющая сетевой контекст, состояние устройства, временной контекст и поведенческую биометрию, и правило принятия решения об отзыве сеанса по порогу. По результатам тестирования прототипа предлагаемая модель снижает ложный пропуск атак с 28,4 % до 1,2 % и сокращает время обнаружения со 120 до 18,5 с при задержке менее 40 мс; платой за это является рост доли ложных отказов до 2,8 %.

Дальнейшая работа включает расширение выборки пользователей и сценариев атак, подбор весовых коэффициентов и порога θ под требования конкретной организации, переход от мгновенного отзыва к ступенчатой реакции и оценку устойчивости модели к целенаправленной имитации поведения.

Список литературы:

1. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture: NIST Special Publication 800-207. – Gaithersburg: NIST, 2020. – 59 p.

2. Acar A., Aksu H., Uluagac A. S. A Survey on Continuous Authentication using Behavioral Biometrics // ACM Computing Surveys. – 2021. – Vol. 54, № 2. – P. 1–36.

3. Кенжебай Е. М. Разработка моделей непрерывной аутентификации на основе поведенческой биометрии // Вестник КазНИТУ. – 2025. – № 4. – С. 112–119.

4. ГОСТ Р ИСО/МЭК 27001-2021. Информационная технология. Методы и средства обеспечения безопасности. – М.: Стандартинформ, 2021. – 32 с.

5. Kindervag J. No More Chewy Centers: Introducing The Zero Trust Model Of Information Security. – Cambridge, MA: Forrester Research, 2010.

6. Ward R., Beyer B. BeyondCorp: A New Approach to Enterprise Security // ;login:. – 2014. – Vol. 39, № 6. – P. 6–11.

7. Grassi P. A., Garcia M. E., Fenton J. L. Digital Identity Guidelines: Authentication and Lifecycle Management: NIST Special Publication 800-63B. – Gaithersburg: NIST, 2017.

8. Monrose F., Rubin A. D. Keystroke dynamics as a biometric for authentication // Future Generation Computer Systems. – 2000. – Vol. 16, № 4. – P. 351–359.

9. Killourhy K. S., Maxion R. A. Comparing Anomaly-Detection Algorithms for Keystroke Dynamics // Proceedings of the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). – 2009. – P. 125–134.

10. Ahmed A. A. E., Traore I. A New Biometric Technology Based on Mouse Dynamics // IEEE Transactions on Dependable and Secure Computing. – 2007. – Vol. 4, № 3. – P. 165–179.

11. Patel V. M., Chellappa R., Chandra D., Barbello B. Continuous User Authentication on Mobile Devices: Recent Progress and Remaining Challenges // IEEE Signal Processing Magazine. – 2016. – Vol. 33, № 4. – P. 49–61.

12. Abuhamad M., Abusnaina A., Nyang D., Mohaisen D. Sensor-Based Continuous Authentication of Smartphones' Users Using Behavioral Biometrics: A Contemporary Survey // IEEE Internet of Things Journal. – 2021. – Vol. 8, № 1. – P. 65–84. – DOI: 10.1109/JIOT.2020.3020076.

13. Stylios I., Kokolakis S., Thanou O., Chatzis S. Behavioral Biometrics & Continuous User Authentication on Mobile Devices: A Survey // Information Fusion. – 2021. – Vol. 66. – P. 76–99. – DOI: 10.1016/j.inffus.2020.08.021.