

УДК 004.056.52

Адаптивная аутентификация и управление доступом: от статических политик к контекстно-зависимым системам с непрерывной верификацией

Ворона Ангелина Алексеевна^{1,2(*)}

angelinavorona@yandex.ru

SPIN-код: 8622-6746

Данилов Александр Сергеевич¹

danilovas@student.bmstu.ru

Лапшин Артем Александрович¹

lapshinartem01@gmail.com

¹ МГТУ им. Н.Э. Баумана, Москва, Россия² ООО «Технологии Доверия — Консультирование», Москва, Россия

Аннотация. Исследование посвящено построению адаптивных систем безопасности на основе интеграции гетерогенных контекстных данных. Центральная проблема — оценка эффективности машинного обучения для минимизации несанкционированного доступа при сохранении удобства для легитимных пользователей. Также рассмотрены практические аспекты внедрения, включая проблему ложных срабатываний и перспективы концепции «Непрерывного адаптивного доверия» (Continuous Adaptive Trust).

Ключевые слова: адаптивная аутентификация, управление доступом на основе рисков, контекстно-зависимая безопасность, поведенческая биометрия, машинное обучение

Введение. Цифровая трансформация и гибридный формат работы делают традиционные методы аутентификации уязвимыми. В ответ на это формируется тренд перехода к адаптивным системам, которые обеспечивают безопасность на основе непрерывной оценки рисков. В их основе лежит использование поведенческой биометрии, машинного обучения и анализа контекстных данных [1–3].

Методы и материалы; результаты. На основе анализа научных трудов исследованы принципы построения динамических систем безопасности. Рассмотрена интеграция контекстных данных и машинного обучения для реализации адаптивной аутентификации, риск-ориентированного управления и непрерывной верификации. Особое внимание уделено практическим аспектам: применению биометрии и снижению ложных срабатываний [4–7].

Сравнительный анализ подтверждает перспективность использования машинного обучения и контекстных данных для построения адаптивных систем безопасности. Ключевой проблемой их внедрения остается высокий уровень ложных срабатываний, требующий разработки механизмов балансировки [4, 5, 7]. Адаптивные системы, основанные на постоянной оценке поведения и контекста, формируют новый стандарт безопасности. Их развитие связано с интеграцией доверительных метрик, динамической настройкой порогов и защитой приватности данных [8].

Современная безопасность требует перехода от статической аутентификации к адаптивным системам, использующим поведенческую биометрию. Однако эти системы сталкиваются с проблемами ложных срабатываний, высоких вычислительных затрат и рисков при обработке данных.

Основные вызовы для адаптивных систем — это постепенное изменение поведения пользователей и целевые атаки, что требует более совершенных механизмов самокалибровки. Критически важен и баланс между безопасностью, приватностью и удобством. Перспективы развития связаны с концепцией «непрерывного адаптивного доверия», которая интегрирует технические решения с регуляторными нормами.

Заключение. Исследование показывает переход к новой парадигме информационной безопасности, основанной на адаптивной аутентификации и риск-ориентированном управлении. Ключевое преимущество — интеграция поведенческих и контекстных факторов для снижения рисков, однако проблемой остаются ложные срабатывания. Перспективы развития связаны с созданием архитектур динамического доверия и минимизацией ошибок. Дальнейшие усилия должны быть сосредоточены на повышении устойчивости к атакам, оптимизации нагрузки и создании прозрачных моделей.

Список источников

- [1] Шитов А.В., Стельмах Н.Е., Магомедов Ш.Г. Программный комплекс механизма управления доступом на основе риск ориентированной атрибутивной модели. *International Journal of Open Information Technologies*, 2024, № 6, с. 133–142.
- [2] Уймин А.Г., Никитин О.Р. Сравнение производительности алгоритмов классификации в рамках сетевой инфраструктуры. *Наукоемкие технологии в космических исследованиях Земли*, 2023, № 2. <https://doi.org/10.36724/2409-5419-2023-15-2-33-40>
- [3] Шиганова С.И., Аникина О.В., Шиганов Е.В. Алгоритмическая трансформация теоретической модели ux-исследования в адаптивную систему пользовательского опыта на базе когнитивных и поведенческих данных. *Вестник науки*, 2025, № 4 (85), с. 732–749.
- [4] Осин А.В., Мурашко Ю.В. Обзор методов идентификации пользователя на основе цифровых отпечатков. *Труды учебных заведений связи*, 2023, № 5. <https://doi.org/10.31854/1813-324X-2023-9-5-91-111>
- [5] Костогрызов А.И., Нистратов А.А. Анализ угроз злоумышленной модификации модели машинного обучения для систем с искусственным интеллектом. *Вопросы кибербезопасности*, 2023, № 5 (57). <https://doi.org/10.21681/2311-3456-2023-5-9-24>
- [6] Чарыев А.Б., Джуманазаров Е.Г., Гараева О.Г. Использование нейронных сетей в идентификации динамических параметров робота-манипулятора. *Символ науки*, 2024, № 10-1-1, с. 84–86.
- [7] Кураков В.И., Худадян А.С., Баева У.М. Анализ уязвимостей биометрических методов аутентификации. *Вестник науки*, 2022, № 5 (50), с. 87–98.
- [8] Полтавцева М.А., Платонов В.В., Супрун А.Ф., Семьянов П.В. Методы анонимизации персональных данных. *SAEC*, 2024, № 2. <https://doi.org/10.18720/SPBPU/2/id24-507>