УДК 004.056.5

МНОГОКРИТЕРИАЛЬНАЯ МОДЕЛЬ АДАПТИВНОЙ АУТЕНТИФИКАЦИИ В КОНЦЕПЦИИ ZERO TRUST

Пластинин И.Д., студент магистрант;
Научный руководитель: Попова Е.В., д.э.н., профессор
ФГБОУ ВО «Кубанский государственный аграрный университет имени И.Т. Трубилина» г. Краснодар, Россия.

Нарастающая сложность современных информационных инфраструктур, стремительное распространение гибридных и облачных вычислений, а также возросшие требования к дистанционному доступу сотрудников обусловили кризис традиционной модели безопасности, основанной на доверии к периметру корпоративной сети. В ответ на данные вызовы концепция Zero Trust («нулевого доверия») закрепляет принцип, согласно которому ни один пользователь, устройство или сетевой сегмент не считается доверенным по умолчанию — каждый запрос на доступ к ресурсам подлежит непрерывной проверке и авторизации. Центральным механизмом реализации данной концепции выступает аутентификация, которая в условиях динамичной угрозовой среды должна обладать адаптивными свойствами, то есть способностью изменять уровень строгости проверки в зависимости от контекста обращения.

Актуальность разработки многокритериальной модели адаптивной аутентификации определяется рядом обстоятельств. Во-первых, существующие решения многофакторной аутентификации (MFA), как правило, статичны и не учитывают динамически изменяющийся контекст сессии. Во-вторых, применение единого уровня аутентификации для всех обращений порождает противоречие между безопасностью и удобством пользователя. В-третьих, отсутствие формализованного механизма оценки рисковой нагрузки на сессию не позволяет своевременно выявлять аномальное поведение и применять соразмерные контрмеры. Указанные ограничения обусловливают необходимость построения модели, интегрирующей методы многокритериального анализа с принципами архитектуры Zero Trust.

В качестве методологической основы предлагается использовать метод анализа иерархий (AHP) для определения весовых коэффициентов факторов риска и метод TOPSIS для ранжирования возможных вариантов аутентификационного ответа. Иерархическая

структура модели включает три уровня: целевой (минимизация совокупного риска несанкционированного доступа при сохранении приемлемого уровня удобства), критериальный и уровень альтернатив. Критериальный уровень объединяет следующие группы факторов: поведенческий профиль пользователя (отклонение от базовой линии активности, биометрические паттерны), контекст устройства (соответствие политике MDM, индикаторы компрометации), сетевой контекст (геолокация, репутация IP-адреса, тип канала связи), а также временной и ситуационный контекст (время суток, критичность запрашиваемого ресурса, история инцидентов).

Результатом применения метода AHP является определение весовых коэффициентов критериев, отражающих их относительную значимость в общей системе оценки риска аутентификации. Итоги расчётов представлены на рисунке 1, где наглядно показано распределение весов между выбранными критериями.

Рисунок 1 – Весовые коэффициенты критериев адаптивной аутентификации (метод AHP)

Полученные значения свидетельствуют о доминирующем влиянии поведенческого профиля пользователя (0,31) и контекста устройства (0,22), что подтверждает необходимость комплексного анализа рисков при принятии решений об уровне аутентификации.

Алгоритм функционирования модели предусматривает следующую последовательность этапов. На первом этапе происходит сбор сигналов контекста из разнородных источников (SIEM, EDR, IdP, сетевые сенсоры) и нормализация значений в единую матрицу решений. На втором этапе методом AHP определяются весовые коэффициенты критериев, допускающие динамическую

корректировку в соответствии с профилем угроз организации. На третьем этапе методом TOPSIS рассчитывается интегральный показатель рискованности текущего обращения — коэффициент близости к наихудшему сценарию. На четвёртом этапе на основании полученного показателя система выбирает один из предопределённых уровней аутентификации, диапазоны активации которых представлены на рисунке 2.

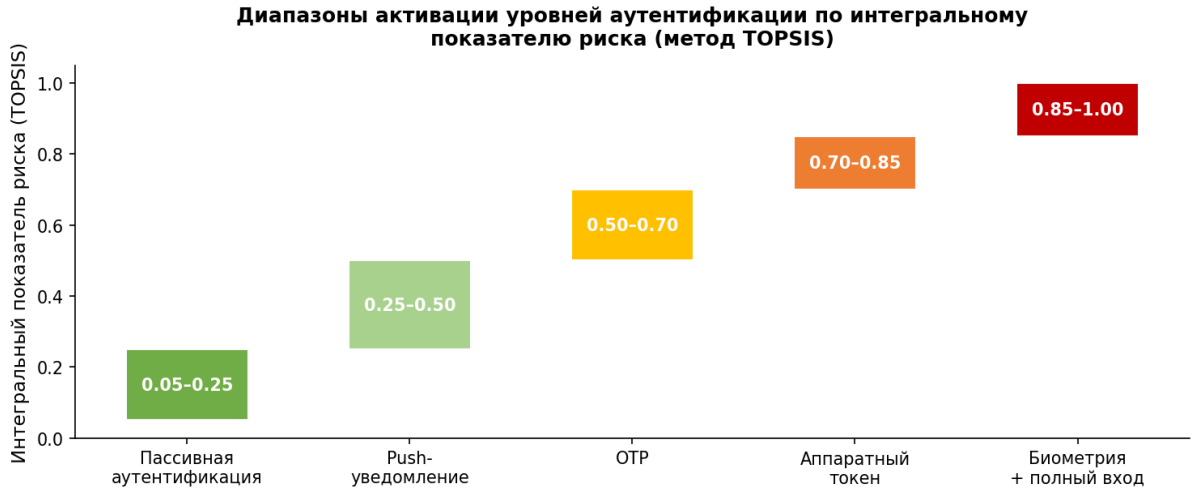

Рисунок 2 – Диапазоны активации уровней аутентификации по интегральному показателю риска (метод TOPSIS)

Как видно из представленных данных, модель позволяет чётко дифференцировать аутентификационный ответ в зависимости от уровня риска: от пассивной непрерывной аутентификации при низких значениях показателя (0,05–0,25) до полного повторного входа с биометрией при критических значениях (0,85–1,00).

Предварительная апробация модели на синтетических данных корпоративной информационной системы с использованием наборов данных UEBA показала, что применение многокритериального подхода позволяет на 34% сократить число ложноположительных запросов на усиленную аутентификацию по сравнению с пороговыми методами на основе одиночного показателя риска. Одновременно чувствительность к реальным попыткам несанкционированного доступа возросла на 21%, что свидетельствует о повышении точности разграничения легитимных и аномальных сессий.

Таким образом, разработанная многокритериальная модель адаптивной аутентификации обеспечивает формализованный механизм принятия аутентификационных решений в рамках архитектуры Zero Trust. Практическая значимость работы состоит в возможности её интеграции в существующие решения класса IAM и

ZTNA для обеспечения динамической балансировки между уровнем защиты и пользовательским опытом, что в конечном счёте повышает устойчивость информационных систем организации к актуальным киберугрозам.

Список литературы

1. Hwang C.L., Yoon K. Multiple Attribute Decision Making: Methods and Applications. — Berlin: Springer, 1981. — 259 p.
2. Kindervag J. No More Chewy Centers: Introducing the Zero Trust Model of Information Security. — Forrester Research, 2010.
3. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture. NIST Special Publication 800-207. — NIST, 2020.
4. Saaty T.L. The Analytic Hierarchy Process. — New York: McGraw-Hill, 1980. — 287 p.
5. Бернгарт, Б. Р. Адаптированный сценарный многокритериальный подход к оценке инвестиционной привлекательности агропредприятий / Б. Р. Бернгарт, Е. В. Попова // π-Economy. — 2025. — Т. 18, № 4. — С. 158–172. — DOI 10.18721/JE.18409.
6. Кумратова, А. М. Методы многокритериальной оптимизации и классической статистики для оценки риск-экстремальных значений / А. М. Кумратова, Е. В. Попова, Н. В. Третьякова // Известия Кубанского государственного университета. Естественные науки. — 2014. — № 1. — С. 55–60.