Министерство образования Республики Беларусь
Учреждение образования
«Брестский государственный технический университет»
Кафедра ИИТ

Лабораторная работа №2
По дисциплине: «Технологии и инструментальные средства разработки ИС»
Тема: «Концептуализация»

Выполнил:
Студент 4 курса
Группы ИИ-23
Швороб В. А.
Проверил:
Кулеша В. И.

Брест 2025

Цель работы: Освоить этапы инженерии знаний, включающие извлечение, структурирование и концептуализацию знаний из предметной области интеллектуальной авторизации пользователей в веб-системах.

Ход работы:

Задание 1. Описание предметной области

Интеллектуальная авторизация — это процесс предоставления доступа пользователю на основе не только стандартных учетных данных (логин/пароль), но и анализа поведенческих, контекстных и биометрических характеристик.

Система интеллектуальной авторизации использует модели машинного обучения, чтобы распознавать типичные шаблоны входа, местоположение, устройство, скорость ввода, а также поведенческие метрики (например, почерк на клавиатуре).

Цель такой системы — повысить безопасность и удобство входа на сайт за счёт адаптивной проверки подлинности, когда пользователю не требуется вводить сложные коды, если его поведение соответствует привычному профилю.

Задание 2. Ключевые понятия

Ключевые понятия показаны в таблице 2.1.

Таблица 2.1. - Ключевые понятия

Понятие	Определение
Пользователь	Зарегистрированное лицо, получающее доступ к системе.
Сессия	Интервал активности пользователя между входом и выходом.
Поведенческий профиль	Набор характеристик, описывающих привычки пользователя (скорость ввода, движение мыши, время активности и т.п.).
Модель авторизации	Алгоритм, определяющий степень доверия к пользователю на основе входных данных.
Биометрический модуль	Подсистема, анализирующая биометрические данные (отпечаток, лицо, голос).
Контекстная проверка	Анализ внешних факторов (устройство, IP, время суток, геолокация).
Уровень доверия	Числовой показатель вероятности, что пользователь — настоящий.

Доступ	Разрешение на выполнение действий в системе.

Задание 3. Атрибуты понятий
Атрибуты понятий показаны в таблице 3.1.

Таблица 3.1. - Атрибуты понятий

Понятие	Атрибуты
Пользователь	ID, логин, роль, история входов.
Сессия	ID, время начала/окончания, IP-адрес, устройство.
Поведенческий профиль	Средняя скорость ввода, количество ошибок, распределение времени между действиями.
Модель авторизации	Тип модели (MLP, SVM, Decision Tree), точность, ROC-AUC.
Биометрический модуль	Тип данных (отпечаток/лицо/голос), точность распознавания, время отклика.
Контекстная проверка	Геолокация, тип устройства, уровень риска.
Уровень доверия	Значение (0–1), порог аутентификации, дата обновления.
Доступ	Тип доступа (чтение/запись/администрирование), приоритет.

Задание 4. Основные правила:

1. Если поведенческий профиль пользователя совпадает с предыдущими сессиями ≥ 80%, то уровень доверия повышается.
2. Если IP-адрес и устройство совпадают с последними 3 входами, авторизация проходит без дополнительной проверки.
3. Если обнаружено новое устройство или страна, активируется двухфакторная аутентификация.
4. Если время отклика биометрического модуля превышает допустимый порог, происходит fallback к паролю.
5. Если уровень доверия < 0.5, то доступ блокируется и создаётся запись о подозрительном входе.
6. Если активность пользователя выходит за типичный диапазон (по времени суток), уровень доверия снижается.
7. Если попытки входа превышают 3 подряд, пользователь проходит дополнительную проверку по email/SMS.
8. Если контекстная проверка возвращает высокий риск, система предлагает пройти повторную биометрию.
9. Если пользователь имеет роль "Администратор", то применяется усиленная аутентификация.

10. Если аномалий не выявлено, вход завершается мгновенно, без дополнительных проверок.

Задание 5. Концепции и сравнение концепций
Концепции приведены в таблице 5.1.

Таблица 5.1. - Концепции

Концепция	Описание
A. “Интеллектуальный фильтр доступа”	Система анализирует поведение пользователя и контекст входа, автоматически определяя необходимость дополнительных проверок.
B. “Адаптивный защитник”	Система использует самообучающиеся алгоритмы, которые динамически обновляют модели риска и поведения, обеспечивая постоянное улучшение точности аутентификации.

Сравнение концепций
Сравнение концепций приведены в таблице 5.2

Таблица 5.2. - Сравнение концепций

Критерий / Концепция	A. Интеллектуальный фильтр доступа	B. Адаптивный защитник
Скорость авторизации	Очень высокая	Средняя
Глубина анализа	Средняя	Высокая
Сложность реализации	Средняя	Высокая
Точность распознавания	0.85	0.93
Требования к ресурсам	Низкие	Повышенные
Гибкость под разные системы	Высокая	Средняя
Обучаемость модели	Ограниченная	Автоматическая
Масштабируемость	Отличная	Средняя
Объяснимость решений	Хорошая	Сложная
Уровень безопасности	Средний–высокий	Очень высокий

Вывод: После анализа концепций можно сделать вывод, что наиболее сбалансированным и практичным решением является Концепция А — “Интеллектуальный фильтр доступа”, так как она сочетает скорость, безопасность и простоту внедрения.