

СИСТЕМА АУТЕНТИФИКАЦИИ НА ОСНОВЕ ИНТЕЛЛЕКТУАЛЬНОЙ МОДЕЛИ БЕЗОПАСНОСТИ RBA

С.А. Зайкова

*Учреждение образования «Гродненский государственный университет
им. Янки Купалы», Гродно, Беларусь*

Для ИТ-компаний и организаций, занятых разработкой программных средств и систем несанкционированный доступ к конфиденциальной информации может привести к утечке данных и потере доверия клиентов, что может существенно повлиять на их прибыль. Учитывая важность защиты личной и конфиденциальной информации, крайне важно иметь надежные системы для аутентификации пользователей и обеспечения доступа к конфиденциальной информации только уполномоченных лиц. Аутентификация на основе риска (RBA, Risk-Based Authentication) – это метод, который использует алгоритмы искусственного интеллекта и машинного обучения для оценки уровня риска запроса на вход в систему на основе широкого спектра информации о пользователе и запросе. Информация может включать местоположение

пользователя, его устройство, историю просмотров и поведение. Модели безопасности аутентификации на основе риска – это новый тип метода аутентификации, который направлен на устранение ограничений традиционных методов аутентификации. Такие модели работают путем анализа различных факторов риска для определения уровня риска, связанного с конкретной попыткой аутентификации [1, 2].

Новая система может определить соответствующий уровень аутентификации, необходимый для предоставления доступа к конфиденциальной информации сотрудников ИТ-компании. Кроме того, она может также обеспечить более высокий уровень удобства для администратора и пользователя, минимизируя количество попыток аутентификации, и уменьшая неудобство традиционных методов (таких как пароли, секретные вопросы и маркеры). Анализируя различные факторы риска, аутентификация на основе риска обеспечивает точную оценку риска, связанного с конкретной попыткой аутентификации. Это позволяет реагировать на потенциальные угрозы безопасности различного типа, включая фишинг. Предлагаемые программные инструменты обеспечивают более высокий уровень безопасности, чем традиционные методы аутентификации, которые уязвимы для подобных атак. Разработка может улучшить пользовательский опыт и повысить степень принятия пользователем системы аутентификации. Аутентификация на основе риска позволяет осуществлять динамическую аутентификацию, которая может регулировать уровень необходимой аутентификации в зависимости от оцененного уровня риска, это повышает безопасность и гибкость системы. Согласно проведенному исследованию, аутентификация RVA обеспечивает более совершенный и безопасный метод аутентификации по сравнению с традиционными методами аутентификации, а также обеспечивает более высокий уровень удобства.

Список литературы

1. Зайкова С.А. Комплексная защита конфиденциальной информации // Информационно-телекоммуникационные системы и технологии. ИТСиТ-2017: материалы Всеросс. научн.-практ. конф., Кемерово, 12–13 октября 2017 г. С. 217–218.
2. Нестерович Е.А., Зайкова С.А. Обеспечение безопасного хранения и защиты информации базы данных от несанкционированного доступа // Технические средства защиты информации: тез. докл. XV Белорусско-российской науч.-техн. конф., Минск, 6 июня 2017 г. С. 64–65.