



# Многофакторная аутентификация по времени

УДК 004.056.5

**Д.П. НЕЧАЕВ, сотрудник ФГКВООУ ВО “Краснодарское высшее военное училище имени генерала армии С.М. Штеменко” Министерства обороны РФ, А.В. АКИШИН, сотрудник ФГКВООУ ВО “Краснодарское высшее военное училище имени генерала армии С.М. Штеменко” Министерства обороны РФ кандидат технических наук, М.А. КАПЛИН, сотрудник ФГКВООУ ВО “Краснодарское высшее военное училище имени генерала армии С.М. Штеменко” Министерства обороны РФ кандидат технических наук, А.А. КУЗЬМИЧ, сотрудник ФГКВООУ ВО “Военная академия связи имени Маршала Советского Союза С.М. Буденного” Министерства обороны РФ кандидат технических наук**

## Многофакторная аутентификация по времени *Time-based multi-factor authentication*

Многофакторная аутентификация является важным элементом современной системы безопасности, обеспечивающим дополнительный уровень защиты пользовательских аккаунтов. Одним из интересных и перспективных ее подходов является использование временных интервалов для ограничения возможности авторизации.

В данной статье рассматривается концепция многофакторной аутентификации, основанная на временных интервалах, где для успешного входа в систему пользователь должен выполнить аутентификацию в определенный временной промежуток в пределах минуты. Этот подход повышает защищенность системы, предотвращая злоупотребление или кражу данных, так как даже при наличии корректных учетных данных и пароля время для входа в систему ограничено.

Данный подход в свою очередь реализует группу мер защиты по отношению к идентификации и аутентификации, таких как аутентификация пользователей с применением логина и пароля, аутентификация пользователей с применением одноразового пароля и многофакторная (двухфакторная) аутентификация пользователей.

Статья включает описание принципов работы подхода, его преимуществ и возможных проблем, а также предполагаемых сценариев применения.

*Multifactor authentication is an important element of modern security systems, providing an additional layer of protection for user accounts. One of the interesting and promising approaches to multifactor authentication is the use of time intervals to limit the possibility of authorization.*

*This article considers the concept of multifactor authentication based on time intervals, where, to successfully log into the system, the user must complete authentication within a certain time frame, within one minute. This approach enhances system security by preventing abuse or data theft, since even if the correct credentials and password are available, the time allowed for system access is limited.*

*This approach, in turn, implements a group of security measures related to identification and authentication, such as user authentication using login and password, user authentication using a one-time password, and multifactor (two-factor) user authentication.*

*The article includes a description of the operating principles of the approach, its advantages and potential issues, as well as proposed application scenarios.*

**Ключевые слова:** многофакторная аутентификация, временные интервалы, защита учетных данных, ограничение времени, системы аутентификации, одноразовый пароль.

**Keywords:** multifactor authentication, time intervals, credential protection, time restriction, authentication systems, one-time password.

## Актуальность и анализ существующих решений многофакторной аутентификации

Цель статьи — раскрыть концепцию многофакторной аутентификации на основе временных интервалов, показать принципы ее работы, привести примеры практического применения, а также рассмотреть преимущества и потенциальные риски данного подхода.

Многофакторная аутентификация признана одним из наиболее эффективных способов защиты от несанкционированного доступа. Согласно исследованию Google, ее внедрение снижает риск компрометации аккаунтов на 99 процентов для целевых атак [2].

**Статью целиком читайте  
в бумажной версии журнала**