УДК: 004.056.52; 004.056.53

Комплекс программно-алгоритмических средств интеллектуальной аутентификации пользователя

Иогансон И. Д., Тихомиров А. В., Чернов Р. И.

Научный руководитель - доцент Гришенцев А. Ю.

Национальный исследовательский университет ИТМО

Данная статья подготовлена при финансовой поддержке Министерства науки и высшего образования Российской Федерации в рамках соглашения № 075-15-2019-1707 от 22.11.2019 г. (идентификатор RFMEFI60519X0189, внутренний номер 05.605.21.0189).

В настоящее время разграничение прав доступа в операционных системах – это важная часть обеспечения информационной безопасности персональных компьютеров. В большинстве современных операционных систем есть встроенная функция аутентификации по паролю, однако порой этого бывает недостаточно.

Большую степень защищенности могут обеспечить аппаратные средства аутентификации, такие как USB-токен. Преимущества таких средств очевидны: для проникновения в систему злоумышленнику необходимо иметь физический экземпляр данного устройства, что сложно реализуемо при правильной организации делопроизводства.

На сегодняшний день на рынке существует множество реализаций USB-токенов, однако ни одна из них не использует интеллектуальные алгоритмы, которые бы обучались во время работы.

Целью данного научно-практического исследования является разработка интеллектуального алгоритма для USB-токена, который позволил бы учитывать индивидуальные особенности пользователя и режима на предприятии.

В качестве фактора определяющего особенности конкретного пользователя и режима на предприятии было принято время, в которое происходит аутентификация с помощью токена.

Идея состоит в том, чтобы устройство запоминало время, в которое пользователь обычно аутентифицируется в разные моменты дня: по приходу на работу, после обеденного перерыва, после перекура и прочее. Далее при следующих попытках аутентификации токен будет принимать решение о том, является ли настоящее время – обычным временем, в которое пользователь возвращается к работе. Если да, то происходит обыкновенная процедура аутентификации, иначе у пользователя запрашивается дополнительный фактор аутентификации.

Вероятность того, что злоумышленник получит несанкционированный доступ к USB-токену выше именно в то время, когда настоящий пользователь токена не пользуется им. Таким образом данный алгоритм повысит защищенность токена в то время, когда пользователь его не использует.

Авторы: Иогансон И. Д., Тихомиров А. В., Чернов Р. И.
Научный руководитель: Гришенцев А. Ю.