МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Одеська національна академія харчових технологій
Університет Інформатики і прикладних знань, м.Лодзь, Польща
Національний технічний університет України «Київський політехнічний інститут»
Навчально-науковий інститут комп'ютерних систем і технологій «Індустрія 4.0» ім. П.М. Платонова

XXI Всеукраїнська науково-технічна конференція молодих вчених, аспірантів та студентів

«СТАН, ДОСЯГНЕННЯ ТА ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ»

Матеріали конференції

Одеса

22-23 квітня 2021 р.

Стан, досягнення та перспективи інформаційних систем і технологій / Матеріали XXI Всеукраїнської науково-технічної конференції молодих вчених, аспірантів та студентів. Одеса, 22-23 квітня 2021 р**.** - Одеса, Видавництво ОНАХТ, 2021 р. – 229 с.

Збірник включає матеріали доповідей учасників конференції, які об'єднані за тематичними напрямками конференції.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Матеріали подано українською, російською та англійською мовами.
Редактор збірника Котлик С.В.

UDC 00:45:004.056.5 (043.2)

DEVELOPMENT OF MODELS AND ALGORITHMS FOR THREE-FACTOR AUTHENTICATION SYSTEM

DONETS O.V. (*xa11867818@student.karazin.ua*),
V. N. Karazin Kharkiv National University
RADOUTSKA A.K. (*anna.radoutska@nure.ua*),
Kharkiv National University of Radio Electronics

The thesis demonstrates the need to create an additional authentication factor that will be independent of additional devices and will operate on the principle of a single password.

Nowadays, there is a rapid digitalization of society: the transition from paper to digital, and then, the integration of disparate systems into a single cloud network. There is a change in established control mechanisms of systems for which the necessary condition is the direct presence on systems with remote controls. This is due to the fact that the level of development of information technology has reached a level where it becomes possible and profitable to move from established systems management technologies to computer systems. This transition creates both many opportunities and many additional problems, without the solution of which the implementation of computer systems does not make sense. One of such problems is the problem of organizing access to the system - authentication [1]. Namely, it is necessary to provide access to the system to users to whom this access is provided, and to prohibit all others. It is necessary to provide ease of access and, at the same time, a sufficient level of security against hacking.

Multiple password authentication is the most common type of authentication in which the knowledge factor is used. However, due to the fact that this type of authentication has significant disadvantages: multiple passwords can be intercepted, multiple passwords can be picked up by brute force, the use of multiple passwords as a single link authentication is not a sufficient condition to protect systems with high security requirements [2,3]. Other examples of the use of one-factor authentication are the use of the ownership factor (tokens, authentication via SMS, mobile applications on the phone), or the use of the user property factor (biometric authentication). Each type of authentication has its advantages and disadvantages, but the disadvantages of each individual factor are sufficient to break the system. Therefore, using only one authentication factor is not desirable. The next step in the development of authentication systems was the simultaneous use of several types of authentication - multifactor authentication. Multifactor authentication involves the use of several different authentication factors [2,3]. As a simple and widespread example, we can use as the first factor the login and password, and as the second factor in the use of SMS code that comes to the mobile number of the user. In this way, the information owned by the user (password) and things owned by the user (SIM card) are checked. The highest level of protection is authentication systems that use all 3 types of authentication (knowledge, ownership, property). And the least secure approach is to use 2 different types of authentication out of 3 possible [3].

The problem is that existing knowledge factors have the least security, namely: usually the knowledge factor involves the transfer of the same information to the authentication server at each authentication attempt. This has the same disadvantages as using a multiple password. Therefore, it was decided to develop a knowledge factor that will get rid of the existing shortcomings inherent in this type of factors. To solve this problem, the following requirements were created: the factor must be created on the basis of a one-time password (user with different authentication attempts transmits different data), the factor must be a factor of knowledge (lack of hardware as opposed to ownership factor), provide the minimum possible synchronizations, provide the ability to configure the complexity factor.

The authentication factor was developed, the main idea of which is as follows: 1) at the synchronization stage, the user creates a mathematical formula for authentication and transmits this formula to the authentication server; 2) at the authentication stage, the server generates random values for the arguments of the function and transmits these values to the user. The user calculates the value of the function with these arguments and passes this value to the authentication server. As a result, an authentication factor has been developed that uses the knowledge factor and has the necessary characteristics. This increases the security of systems that use the knowledge factor.

Sources:

1. What is E-Authentication? [Electronic resource]. - 2021. Resource access mode: https://www.easytechjunkie.com/what-is-e-authentication.htm

2. Authentication and Lifecycle Management [Electronic resource]. - 2021. Resource access mode: https://pages.nist.gov/800-63-3/sp800-63b.html

3. Authentication at Scale [Electronic resource]. - 2018. Resource access mode: https://www.computer.org/cms/Computer.org/ComputingNow/pdfs/AuthenticationAtScale.pdf

УДК 004.418

КОМП'ЮТЕРИЗОВАНИЙ ВІДБІР ОПЕРАТОРІВ БПЛА

МАРУЩАК А. В., ШМАЛЮХ В. А., РОМАНЮК О. Н., КОВАЛЬ Л. Г.
(*rom8591@gmail.com*)
Вінницький національний технічний університет

Метою статті є аналіз схеми та алгоритму відбору операторів безпілотних літальних апаратів за станом психофізіологічного здоров'я. У роботі наведено важливість проведення спеціалізованого тестування для операторів БПЛА та обґрунтовано необхідність їх психофізіологічного відбору. Зображено переваги та недоліки певних методик таких підходів. Проведення професійного відбору за такими результатами дозволить значно підвищити ефективність використання безпілотних літальних апаратів і рівень керування ними.

Тестування проводиться у вигляді комп'ютерного тесту, що дозволяє

Спеціалізований тест «Адаптивність – 200» призначений для вивчення адаптаційних можливостей військовослужбовців на основі оцінки деяких соціально-психологічних і психологічних характеристик особистості, що відображують інтегральні особливості психічного та соціального розвитку. Нова версія БОО «Адаптивність-200» містить 200 запитань. Крім традиційних градацій: ПР (психічна регуляція), КП (комунікативний потенціал) і МН (моральна нормативність) до версії опитувальника увійшли додаткові шкали ВПС (військово-професійна спрямованість), ДАП (схильність до девіантних форм поведінки) і СР (суїцидальний ризик).

Безпосередньо перед проведенням обстеження дається коротка інструкція, що вказує про те, що дане дослідження спрямоване на виявлення індивідуальних особливостей. Опитувальник містить 200 тверджень (запитань) про життя, роботу, відносини у сім'ї, інтереси та схильності. Завдання полягає у тому, щоб визначити своє відношення до кожного твердження, тобто погодитися або не погодитися з ним. Якщо, оператор погоджуєтеся із твердженням, то при комп'ютерному опитуванні у клітці з номером даного питання ставиться «+» а якщо ж не згодні – ставиться «–». Для обробки отриманих даних необхідно мати набір ключів, які відповідають основним і додатковим шкалам БОО «Адаптивність-

XXI Всеукраїнська науково-технічна конференція молодих вчених, аспірантів та студентів

«СТАН, ДОСЯГНЕННЯ ТА ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ»

Одеса

22-23 квітня 2021 р.

Збірник включає доповіді учасників конференції. Тези доповідей публікуються у вигляді, в якому вони були подані авторами.

Відповідальність за зміст і форму подачі матеріалу несуть автори статей.

Редакційна колегія: Котлик С.В., Корнієнко Ю.К.

Комп'ютерний набір і верстка: Соколова О.П.

Відповідальний за випуск: Котлик С.В.