УДК 519.87

Я. О. Король[1]
В. С. Озеранський[1]
С.І. Перевозніков[1]

АНАЛІЗ ТА РЕАЛІЗАЦІЯ ЗАСОБІВ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧА

[1]Вінницький національний технічний університет

Анотація

Розглянуто поняття автентифікації, авторизації та ідентифікації, розглянуто їхні види та вказано на їх недоліки. Запропоновано реалізацію систему автентифікації та авторизації для програм, які матимуть обмежений доступ у користуванні.

Ключові слова: автентифікація, автоматизовані системи, захист, інформаційна технологія**.**

Abstract

The concepts of authentication, authorization and identification are considered, their types are considered and their shortcomings are pointed out. The implementation of the system of authentication and authorization for programs that will have limited access in use.

Keywords: authentication, automated systems, security, information technology.

Вступ

В сьогоднішньому світі, всюди використовуються автоматизовані системи які розрослися до дуже серйозних масштабів і охоплюють практично всі етапи життя людей, компаній, підприємств. Загалом, такі системи складаються з персоналу і комплексу засобів автоматизації його діяльності та реалізують інформаційну технологію виконання установлених функцій. Однією з найскладніших напрямків для впровадження автоматизованих інформаційних систем, є робота з електронним документообігом.

Результат досліджень

Інформаційні технології, програмного реалізовані в інформаційну систему можуть в рази збільшити ефективність роботи персоналу, у випадку правильної організації взаємодії між людьми та автоматизованими інформаційними системами. Але це супроводжується багатьма недоліками які потрібно виправити для запобігання помилок, але перед цим, потрібно впевнитись в тому, що з цією системою працює людина, яка має на це дозвіл і потрібні вміння.

Об’єктом розгляду є процес авторизації. Предмет роботи – системи авторизації та автентифікації.

Проаналізувавши різні види автентифікації, ідентифікації та авторизації, можна зробити висновок, що краще всього для використання підходить двофакторний метод ідентифікації з використанням біометрії користувача та трибічний метод автентифікації, який використовує третю, довірену сторону для підтвердження особи.

Оцінивши матеріальні можливості та потреби програми, яку потрібно захистити від несанкціонованого доступу, було вирішено зробити двофакторну автентифікацію, усунувши проблему вартості.

Двофакторні методи аутентифікації отримують в результаті комбінації двох різних однофакторних методів, частіше всього ідентифікаційного та логічного. Наприклад: “пароль + дискета”, “магнітна карта + PIN”.

Кожен клас методів має свої переваги і недоліки. Майже всі методи автентифікації мають один недолік – вони, насправді, автентифікують не конкретного суб’єкта, а лише фіксують той факт, що аутентифікатор суб’єкта відповідає його ідентифікатору. Тобто всі відомі методи не захищені від компрометації аутентифікатора.

В якості ідентифікатора було вирішено вказувати гешований серійний номер флешки, а також логін користувача та пароль, реалізувавши метод мандатного керування доступом.

В результаті авторизації, що реалізована в програмі, користувачу достатньо під'єднати "флешку" до комп'ютера на якому він буде працювати, щоб авторизуватися в системі. В такому випадку цей процес, в залежності від якості з'єднання, буде займати від 0.5 до 2.0 секунд, що є практично непомітним і одночасно відповідає всім вимогам безпеки і зручності під час роботи.

Висновки

Згідно з проведеним дослідженнями встановлено, що програмний продукт в розробці дозволить вирішити поставлену задачу. Подальша розробка програмного продукту вважається актуальною. Реалізація системи автентифікації та авторизації програми було виконано в повному обсязі, та показало хороші результати.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Про основні засади забезпечення кібербезпеки України : Закон України від 21 червня 2018 р. № 2469-VIII URL: https://zakon.rada.gov.ua /laws/show/2163-19 (дата звернення: 20.02.2021).

2. Applying Cyber Kill Chain® Methodology to Network Defense : GAINING THE ADVANTAGE Lockheed Martin. Режим доступу: https://www. lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the _Advantage_Cyber_Kill_Chain.pdf.

3. Носенко К. М., Півторак О. І., Ліхоузова Т. А. Огляд систем виявлення атак в мережевому трафіку : Міжвідомчий науково-технічний збірник "Адаптивні системи автоматичного управління", 2014. 67–75с.

4. Арсенюк І. Р.Застосування апарату нечіткої логіки для оцінки якості графічних растрових зображень./ І. Р. Арсенюк, О. В. Сілагін, С. О. Кукунін // Матеріали IX Міжнародної науково-практичної конференції "Інтернет-Освіта-Наука" (ІОН-2014). –Вінниця: УНІВЕРСУМ-Вінниця, 2014. – С. 223 - 225

Король Яна Олександрівна – студентка групи 2КН-17б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, email: korol3854@gmail.com.

Науковий керівник: ***Озеранський Володимир Сергійович*** - кандидат технічних наук, старший викладач, Вінницький національний технічний університет, м. Вінниця, e-mail: ozeransky@ukr.net

Перевозніков Сергій Іванович— доктор технічних наук, професор кафедри комп'ютерних наук, Вінницький національний технічний університет, м. Вінниця, email: perevoznikov@ukr.net

Korol Yana Oleksandrivna – Department of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: korol3854@gmail.com.

Supervisor: ***Ozeransky Volodumur*** - Ph.D., senior lecturer, Vinnytsia National Technical University, Vinnytsia, email: ozeransky@ukr.net

Perevoznikov Serhiy - professor, Department of Computer Science, Vinnytsia National Technical University, Vinnytsia, email: perevoznikov@urk.net.