НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ПОЛТАВСЬКА ПОЛІТЕХНІКА
ІМЕНІ ЮРІЯ КОНДРАТЮКА

ЗБІРНИК МАТЕРІАЛІВ

77-Ї НАУКОВОЇ КОНФЕРЕНЦІЇ ПРОФЕСОРІВ, ВИКЛАДАЧІВ, НАУКОВИХ ПРАЦІВНИКІВ, АСПІРАНТІВ ТА СТУДЕНТІВ УНІВЕРСИТЕТУ

16 травня – 22 травня 2025 р.

Криптографія може бути інтегрована в інші цифрові системи. Наприклад, вивчіть основи шифрування за допомогою безпечної комунікації та мобільних додатків на освітніх платформах.

Крім того, невелика кількість інформації про нестандартні канали може бути адаптована до потреб середовища IoT, де передача (звук, візуальна) є нагальним завданням.

Запропонована система не тільки дозволяє ефективні приховані повідомлення, але й дозволяє перетворити процес шифрування на культурні та мистецькі вчинки. Надалі це можна розглядати як частину більш широкої платформи для прихованого обміну інформацією, яка поєднує естетику, функціональність та безпеку.

Література:

1. *with music21. URL: https://web.mit.edu/music21/doc/usersGuide/usersGuide_26_encoding.html (дата звернення – 20.04.2024 р.)*
2. *MIDIUtil – A Python library for creating MIDI files. URL: https://github.com/MarkCWirt/MIDIUtil (дата звернення – 20.04.2024 р.)*
3. *Encoding Text in Music Scores. URL: https://www.researchgate.net/publication/340578475_Musical_Cryptography (дата звернення – 20.04.2024 р.)*

УДК 004.056.53

Ю.М. Здоренко, к.т.н.,
І.В. Ромашко, старший викладач
В.Ф. Пенц, доцент, к.т.н.,
Національний університет «Полтавська політехніка імені Юрія Кондратюка»
С. В. Любарський, к.т.н., доцент
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут

МЕТОД КІБЕРЗАХИСТУ ОБ'ЄКТІВ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ НА ОСНОВІ НЕЧІТКИХ МОДЕЛЕЙ БАГАТОФАКТОРНОЇ АУТЕНТИФІКАЦІЇ

Захист інформаційних ресурсів, які знаходяться на об'єктах інформаційної діяльності з багатокористувальницьким доступом потребує надійних механізмів розмежування прав користувачів. Забезпечення конфеденційності інформації є одним з пріоритетних завдань такого спрямування. Засоби парольного захисту на даний час є недосконалими та

потребують подальшого розвитку. Це пов’язано з низькою стійкістю слабких паролів до брутфорс-атак, складністю запам’ятовування складних паролів користувачами, атаками фішингового типу та інших форм соціальної інженерії, внаслідок чого пароль може бути викрадений, втрачений або забутий. Тому існує потреба в пошуку підходів для удосконалення традиційних систем парольної аутентифікації. Так, в комерційній сфері широко використовується двохфакторна аутентифікація на основі парольного захисту та коду, який отримується з використанням мережевих технічних засобів (наприклад, мобільного зв’язку). Однак такий спосіб захисту та забезпечення конфеденційності інформації також не є повністю безпечним, оскільки передбачає використання сторонніх технічних засобів, які можуть потрапити під контроль інших осіб. Тому подальші дослідження пропонується проводити на основі доповнення механізмів парольної аутентифікації індивідуальними біометричними складовими кожного окремого користувача. Так, кожен користувач, має множину відносно постійних індивідуальних ознак біометричного характеру, а саме: статура тіла, індивідуальні відбитки пальців, обличчя, райдужну оболонку ока, голос, частоту серцебиття, тиск та поведінкові характеристики за різних обставин (міміку, рухи під час пересування або виконання певних операцій тощо). Деякі з цих ознак та характеристик потребують додаткових засобів для їх вимірювання, що може ускладнити процес такої багатофакторної аутентифікації. Наприклад, розпізнавання за відбитком пальця потребує наявність скануючого з відповідною точністю пристрою, чистоту рук користувача. А деякі загальнодоступні ознаки легко компрометуються, наприклад, голос користувача, на даний час може бути згенерований засобами штучних нейронних мереж на основі попередніх його записів та підмінений. Тому пропонується зосередити увагу на поведінкових характеристиках користувачів, які не потребують додаткових технічних засобів для вимірювання та не можуть бути скопійовані. Так, людський мозок здатний ідентифікувати інших людей з великою точністю на великій відстані лише за окремими рухами під час їхнього пересування, при цьому обличчя може бути прихованим. Подібний підхід пропонується використати для удосконалення існуючих систем багатофакторної аутентифікації. При цьому для уникнення некоректних блокувань існуючих користувачів до інформаційних ресурсів пропонується надавати до них доступ при співпадінні двох факторів, а саме: паролю та одного з факторів поведінкової біометрії.

Перспективним напрямком поведінкової біометрії при цьому є рухи під час набору тексту (клавіатурний почерк користувача) [1]. Перевагою такої біометричної складової при удосконаленні механізмів аутентифікації є відсутність потреби в додаткових технічних засобах вимірювання та можливістю реалізації під час процедури парольної аутентифікації (при введенні паролю). Однак розглянутий в роботі [1] підхід для оцінки

клавіатурного почерку не враховує різних психоемоційних станів користувача (наприклад, стресових ситуацій) в яких може перебувати користувач, що може значно вплинути на його почерк та призвести до некоректних блокувань. Тому для цього пропонується використовувати підходи на основі інтелектуальних систем з нечіткою логікою та можливістю постійного їх навчання, що дозволяє врахувати ці аспекти. Так, підходи для використання таких систем наявні в літературі. Наприклад, в [2] авторами пропонується використовувати fuzzy-системи для аутентифікації користувачів по клавіатурному почерку на основі експертного налаштування їхніх параметрів. Пропонується удосконалити налаштування таких систем шляхом поєднання fuzzy-системи з технологією штучних нейронних мереж. Очікується, що такий підхід дозволить розвинути існуючі механізми аутентифікації та покращити захист інформації.

Література:

1. Є.О. Башков, Т.В. Алтухова, Є.О. Єжова Розробка методу аутентифікації користувача на основі клавіатурного почерку / Наукові праці ДонНТУ, №2 (35), 2022-№1(36), (2023). Серія "Інформатика, кібернетика та обчислювальна техніка", ISSN 1996-1588

2. V.Fesokha, N. Fesokha Модель нечіткої автентифікації користувачів інформаційних систем органів військового управління на основі поведінкової біометрії / Захист інформації. НАУ. Том 23 № 2 (2021). DOI: 10.18372/2410-7840.23.15728

УДК 004.896

М.О. Толочин, асистент
А.О. Мізік, асистент
О.С. Скорбатюк, асистент
Національний університет «Полтавська політехніка імені Юрія Кондратюка»

ІНТЕЛЕКТУАЛЬНА СИСТЕМА ДЛЯ РОЗПІЗНАВАННЯ ЕМОЦІЙ ЛЮДИНИ НА ЗОБРАЖЕННЯХ З ВИКОРИСТАННЯМ БІБЛІОТЕКИ DEEPFACE

В епоху швидкої цифровізації та штучного інтелекту здатність машин сприймати та інтерпретувати людські емоції стає все більш актуальною. Автоматичне розпізнавання емоцій за зображеннями є одним із найперспективніших напрямків розвитку інтелектуальних систем, що може сприяти покращенню взаємодії людини з комп'ютером, вдосконаленню