КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (12), 2021
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2020.12.163171
УДК 004.056

Коршун Наталія Володимирівна
доктор технічних наук, доцент,
професор кафедри інформаційної та кібернетичної безпеки
Київський університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0000-0003-2908-970X
n.korshun@kubg.edu.ua

Літвінчук Ірина Сергіївна
Науковий співробітник
Військова частина А1906, Київ, Україна
ORCID: 0000-0002-0854-5393
Litvinchuk.irina94@gmail.com

Корчомний Руслан Олександрович
Науковий співробітник
Військова частина А1906, Київ, Україна
ORCID: 0000-0002-2457-6675
Rra30@ukr.net

Борисов Ігор Володимирович
Кандидат технічних наук, доцент
Науковий співробітник
Військової частини А1906, Україна, Київ
ORCID: 0000-0003-2276-9913
borisov_viti@ukr.net

РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО МІНІМІЗАЦІЇ РИЗИКІВ ЗЛОМІВ ОБЛІКОВИХ ЗАПИСІВ НА ОСНОВІ АНАЛІЗУ НАЙПОШИРЕНІШИХ МЕТОДІВ ЗЛОМУ

Анотація. В умовах розповсюдження Інтернету, соціальних мереж, месенджерів тощо та їх проникнення до усіх сфер життя сучасної особистості все збільшується кількість спроб отримання несанкціонованого доступу до особистої інформації користувачів. Облікові записи є найуразливішою мішенню для злому. Серед найпоширеніших видів атак – фішинг, крадіжка файлів cookie, використання кейлоггерів, брутфорс. Техніки соціальної інженерії набули великої популярності серед зловмисників. Використання паролю у вигляді набору букв, цифр та спеціальних символів вже не достатньо для забезпечення необхідного рівня захищеності облікових записів. Впровадження комбінованих систем збільшує кількість ідентифікаційних ознак і підвищує безпеку даних. У якості додаткових механізмів захисту можуть використовуватися системи на базі безконтактних смарт-карт, USB-ключів, гібридних смарт-карт, біоелектронні системи. Однією з основних рекомендацій щодо уникнень наслідків шахрайських дій є подвійна або багатофакторна аутентифікація з метою перевірки ідентичності клієнта (вимоги до користувачів надати дані, пароль з використанням інших факторів, наприклад, текстового повідомлення/SMS-коду або відбитків пальців). На всіх доступних інтернет-сервісах, де це можливо, для забезпечення прийнятного рівня безпеки необхідно використовувати багатофакторну аутентифікацію. Існує два основних типи багатофакторної аутентифікації: додаток MFA - процес аутентифікації, який активується, коли користувач намагається отримати доступ до одного або декількох додатків, та пристрій MFA - процес аутентифікації, який негайно активує MFA в точці входу в систему. Одним з найбільш поширених чинників аутентифікації є номер телефону. Застосовуються також коди електронної пошти, текстові токени, біометрична перевірка, апаратні токени, секретні питання та інше.

Ключові слова: багатофакторна аутентифікація; фішинг; парольний захист; біометрична аутентифікація.

ВСТУП

Постановка проблеми. Двадцять перше століття - це великий крок технологічного розвитку людства. Напевне, вже і не згадати, як давно та як міцно у наше життя ввійшли цифрові технології, а з ними і нові кіберзагрози.

Комп'ютери, смартфони, ноутбуки - це далеко не весь список ґаджетів, якими ми користуємось щодня, передаючи та отримуючи інформацію. Прокинувшись зранку, одразу переглядаємо пошту, соціальні мережі, месенджери, вводячи логіни та паролі, а щомісяця оплачуємо комунальні та інші послуги, вводячи номер банківської картки для оплати нових покупок в Інтернеті. Найпопулярнішим сервісом, яким доводиться користуватись кожному власнику ґаджета, є електронна пошта: хоча на перший погляд так не здається, однак, у більшості додатків та соціальних мережах вона використовується для реєстрації.

Щоб введена інформація (логіни, паролі, персональні дані, адреса проживання, відомості про стан здоров'я, а також уся банківська інформація) в мережі Інтернет не перестала бути конфіденційною, необхідно використовувати всі можливі способи захисту, таким чином забезпечивши свою інформаційну безпеку. В умовах стрімкого розповсюдження Інтернет на противагу відомим технологіям забезпечення безпеки постає людський чинник [1]. Соціальна інженерія активно використовується для отримання несанкціонованого доступу до захищених інфокомунікаційних систем. А оскільки облікові записи - це найуразливіша мішень для злому, ніколи не буде зайвим встановити додатковий рівень захисту багатофакторної аутентифікації (multi-factor authentication, MFA) як одного з основних і найдієвіших способів боротьби зі зломом та іншими кіберзагрозами.

Багатофакторна аутентифікація — це метод аутентифікації, який вимагає від користувача надання двох або більше доказів особистості, щоб отримати доступ і увійти у свій обліковий запис. І тільки після введення всієї необхідної інформації користувач отримає доступ до свого облікового запису. Це може бути номер телефону, адреса електронної пошти або відповідь на якесь (відоме лише користувачу) секретне питання [2]. Сьогодення диктує нові правила при роботі в мережі. В умовах пандемії роботодавці змушені переводити своїх співробітників на домашню віддалену роботу, часто забуваючи при цьому про елементарні правила кібербезпеки. У такий вразливий для світу час кіберзлочинці мають більше можливостей заволодіти інформацією та ресурсами тієї чи іншої компанії. Елементарно - через малозахищені облікові записи співробітників.

Використання лише паролю не є гарантією безпеки. Як відомо, є безліч способів, як легко його зламати, викрасти, вгадати чи підібрати потрібну комбінацію. Використавши багатофакторну аутентифікацію, можна уникнути значних втрат.

Аналіз останніх досліджень і публікацій. В роботі [3] пропонується перелік показників, за якими можна здійснити порівняльну оцінку методів аутентифікації користувачів. Серед них, зокрема, стійкість до перебору, захищеність від підглядання, від викрадення, завадозахищеність системи аутентифікації, а також вартість, простота використання та зміни аутентифікатора, вартість системи аутентифікації.

Одна з провідних українських компаній KPMG, що належить до міжнародної мережі фірм-членів KPMG International, яка надає аудиторські та консультаційні послуги

з податкових та фінансових питань клієнтам, провела дослідження на тему «Глобальне дослідження з питань шахрайства у банківській сфері». У ньому підняте питання протидії внутрішнім та зовнішнім загрозам шахрайства. І от до яких рекомендаційних заключень прийшли експерти:

— необхідно навчити користувачів розпізнавати фішингові повідомлення, що надходять електронною поштою, текстові/SMS-повідомлення та телефонні дзвінки;

— часто змінювати паролі;

— ігнорувати спливаючі вікна;

— розпізнавати електронний спам через орфографічні помилки, відсутність надійної інформації про веб-сайт, підозрілі посилання та адреси електронної пошти, інші, ніж в організації, від імені якої нібито надійшло повідомлення;

— пам'ятати, що представник реальної організації ніколи не запитуватиме паролі;

— стерегтися спуфінгової атаки на автоматичний визначник номера (Caller ID spoofing), коли шахраї намагаються імітувати номер установи, за яку вони себе видають [4].

А однією з основних рекомендацій щодо уникнень наслідків шахрайських дій є подвійна або багатофакторна аутентифікація з метою перевірки ідентичності клієнта (вимоги до користувачів надати дані, наприклад, пароль, з використанням інших факторів, наприклад, текстового повідомлення/SMS-коду або відбитків пальців) [4].

Експерти з кіберзахисту української компанії Datami у своїй статті пояснили, чим небезпечний злом облікового запису. Фахівці вважають, що облікові записи соціальних мереж містять чимало важливих особистих даних. Люди часто надсилають одне одному номери банківських карток чи іншу приватну інформацію. Хакери можуть легко знайти цю інформацію і використати у своїх інтересах. І справа не тільки у банківській картці — всі дані, що передаються через Інтернет, включаючи особисті повідомлення та фотографії, можуть бути під загрозою. Тобто будь-яка інформація може стати засобом шантажу [5].

Разом з тим, експерти надають користувачам рекомендації щодо захисту облікових записів, зокрема:

– не варто відкривати підозрілі повідомлення, електронні листи або переходити за посиланнями (навіть якщо вони були надіслані людиною, котрій довіряєте) — вони можуть містити шкідливі програми;

– якщо отримано щось підозріле від знайомих, краще написати текстове повідомлення або зателефонувати «відправнику», щоб перевірити, чи справді він надсилав це повідомлення;

– слід створювати надійні паролі;

– не можна використовувати один пароль для різних акаунтів;

– користуватися багатофакторною аутентифікацією всюди, де це можливо.

Багатофакторна аутентифікація допоможе захистити акаунт. Система її роботи наступна: перший крок — увійти в соціальну мережу тощо з ім'ям користувача і паролем, другий – отримати повідомлення з пін-кодом на телефон, а третій – заповнити відповідний рядок отриманим кодом. І лише після цього можна увійти в обліковий запис. Іноді замість повідомлення на телефон використовується відповідь на секретне питання, відбиток пальця чи то FaceID.

Не рекомендується входити в акаунти через загальнодоступний Wi-Fi. Якщо таки доведеться – обов'язково використовувати VPN.

Слід завжди оновлювати свої додатки, адже хакеру набагато простіше зламати застарілий додаток. Кожне оновлення – це виправлення вразливостей, тож зламати акаунт стає складніше [5].

Мета статті. Виходячи з наведеного вище, метою статті є розробити рекомендації щодо захисту облікових записів від зломів та несанкціонованого доступу на основі аналізу існуючих способів захисту облікових записів, оцінивши найпопулярніші види несанкціонованого доступу.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

У 2021 році вийшла приголомшлива стаття з заголовком «Хакер з України розробив найбільший у світі фішинг-сервіс для атак на фінустанови». Повідомляється, що:

- хакер розробив фішинг-пакет і спеціальну адміністративну панель до нього. Вони були націлені на веб-ресурси більше сотні банківських установ та їхніх клієнтів у країнах Європи, а також в Австралії.
- Зокрема, адмінпанель дозволяла контролювати облікові записи користувачів, зареєстрованих на скомпрометованих ресурсах. Платіжні дані, які вводили клієнти, у подальшому використовували хакерські угрупування у власних цілях.
- Крім фішингових інструментів для атак на фінустанови, хакер розробляв ресурси, орієнтовані на злом поштових сервісів, якими користується понад 1,5 млрд осіб [6].

Таким чином, хакер зумів розробити один з найбільших у світі фішинг-сервіс для атак на фінансові установи та поштові сервіси, завдавши шкоди одинадцятьом країнам світу на суму збитків, що перевищує десятки мільйонів доларів. Нажаль, такі статті не є поодинокими. Отже, розглянемо найпопулярніші кіберзагрози.

1. *Фішинг.* Як говорить статистика, фішинг є найчастіше використовуваною зброєю хакерів. Фішинг базується на відправленні користувачу повідомлення, електронного листа для залучення уваги та викрадення паролів та доступу до облікових даних. Зазвичай хакери у таких фішинг-листах використовують попереджувальні повідомлення, призи або все, що дійсно змушує користувача натискати на посилання у листі [7]. Справа в тому, що ці посилання приводять користувача на сайти, створені для атаки - так звані сайти підміни. Сайти за своїм стилем, дизайном можуть не сильно різнитись від тих, під які мімікрують, однак, коли користувач вводить дані, то вони надходять на сервер, керований хакерами. І це лише один з видів фішингу.
2. *Крадіжка файлів cookie.* Атаки на браузер дуже часті. Крадіжка файлів cookie, введення шкідливого коду застосовується, щоб перенаправити користувача на сторінки, які можуть бути небезпечними, або на помилкові розширення тощо. Крадіжка файлів cookie широко використовується для отримання інформації та даних від користувачів.
3. *Кейлоггер.* Техніка злому, що використовується для крадіжки паролів, використовує шкідливе програмне забезпечення під назвою keylogger, яке має функцію запису всіх натискань клавіш. Таким чином хакери можуть збирати ключі та облікові дані, отримуючи доступ до облікових записів [7].
4. *Брутфорс.* Брут (брутфорс) використовується з метою зламати чужі акаунти, в тому числі і скриньки електронної пошти. Під брутфорсом розуміють сукупність методів заволодіння чужими акаунтами шляхом підбору всіх теоретично можливих варіантів логіна і пароля. У такому формулюванні брут здається злегка примітивним і малоефективним заняттям. Однак існує можливість звузити рамки

підбору логіна і пароля до таких обсягів, де результати вже стають реальними і їх не варто чекати днями \ тижнями \ місяцями. Злом пошти може відбуватися за двома схемами: злом конкретної скриньки і злом множини скриньок.

У разі злому множини скриньок процедура брутфорса мало чим відрізняється від процедури брута сторінок. У спеціальну програму завантажуються бази е-мейлів, паролів, і програма починає працювати, відбираючи «гуди» (позитивні результати). Відсоток зламаних скриньок виявляється не великим, але цього цілком вистачає, якщо пошта зламувалася з метою розсилки спаму по адресах контактів [8].

Найрозповсюдженішою системою аутентифікації є використання паролю у вигляді набору букв, цифр та спеціальних символів [3]. З метою підвищення рівня захищеності інформаційних ресурсів відділи безпеки компаній зазвичай висувають до паролів певні вимоги, яких мають дотримуватися співробітники. Наприклад, встановлення обмеження на мінімальну довжину пароля, комбінація регістрів та символів, періодичність зміни паролів та заборона на використання слів, словосполучень тощо.

Достатньо розповсюджені графічні паролі (особливо для портативних пристроїв). При використанні таких паролів в якості парольної інформації зберігаються координати пікселів екрану. Як і у випадку символьного паролю, цю інформацію можна підібрати або викрасти за допомогою програмної закладки.

В роботі [9] серед загроз безпеки парольних систем вказані наступні: розголошування параметрів облікового запису через, наприклад, підбір, навмисну передачу пароля його власником іншій особі або перехоплення інформації при передаванні по мережі, втручання у функціонування компонентів парольної системи шляхом впровадження програмних закладок, використання помилок, допущених на стадії розробки, виведення з ладу парольної системи.

Отже, парольний захист не може вважатися надійним без використання додаткових механізмів захисту. Впровадження комбінованих (комплексних, багатофакторних) систем збільшує кількість ідентифікаційних ознак і тим самим підвищує безпеку [9]. Існують такі комбіновані системи: на базі безконтактних смарт-карт і USB-ключів, з використанням гібридних смарт-карт, біоелектронні системи.

Серед біометричних методів аутентифікації найбільш практичними вважаються методи, що використовують такі ознаки, як відбитки пальців, райдужна оболонка ока, риси обличчя. Системи розпізнавання облич застосовуються та суттєво підвищують рівень безпеки, наприклад, при реєстрації пасажирів в аеропортах, при ідентифікації розшукуваних осіб, для запобігання несанкціонованому доступу до периметру безпеки сторонніх осіб тощо [10].

З’являються також оригінальніші методи, такі, як розроблений в [11] метод автентифікації користувачів за їх рукописним почерком, який забезпечує високий рівень значень імовірності правильного розпізнавання користувачів та може застосовуватися при наявності пристроїв із сенсорним екраном.

Визначивши найпопулярніші методи злому облікових записів та проаналізувавши шляхи їх реалізації, можна оцінити та рекомендувати найбільш ефективні способи захисту облікових записів, а саме:

- Не ігнорувати попередження про спам чи «підозрілі листи» в електронній пошті та не переходити за незнайомими посиляннями. Перед переходом за посиланням варто звернути увагу на назву посилання: чи немає помилок у назві, самому листі та інше (зазвичай такі листи вимагають негайних дій від користувача).

- Логін та пароль, фінансові дані можна вводити лише тоді, коли сторінка (URL) використовує протокол HTTPS (де «s» означає secure, тобто «безпечне»), а не просто HTTP.
- Що стосується власне ключових моментів авторизації – логіну та паролю, то їх робити максимально стійкими, не вказувати в них особисту інформацію (Ivanov.Ivan_Ivanovich21.06.97@gmail.com), для всіх облікових записів генерувати свої унікальні логіни та паролі, бажано раз на місяць змінювати паролі.
- Пам'ятати, що кожна соціальна мережа чи електронна пошта має свої налаштування щодо захисту облікового запису, звернути на це увагу та використовувати рекомендовані налаштування.
- Потрібно постійно та скрізь, де це можливо, використовувати багатофакторну аутентифікацію - на всіх доступних інтернет-сервісах (соціальні мережі, особиста пошта та інше).

Існує два основних типи багатофакторної аутентифікації. Додаток MFA: процес аутентифікації, який активується, коли користувач намагається отримати доступ до одного або декількох додатків. Пристрій MFA: процес аутентифікації, який негайно активує MFA в точці входу в систему. Хоча вони є окремими процесами, MFA в основному однакова для обох типів. Коли користувач намагається отримати доступ до будь-чого (телефону, ноутбука, сервера), він стикається з багатофакторною аутентифікацією і змушений вводити два або більше факторів аутентифікації. Якщо основний постачальник посвідчень (IdP) підтвердить ці чинники, користувачу буде надано доступ.

Одним з найбільш поширених чинників аутентифікації є номер телефону. Зазвичай за допомогою MFA користувач вводить свій логін та пароль при вході в систему, а потім унікальний код, який відправляється за допомогою текстового повідомлення на мобільний телефон. Це доводить, що користувач пам'ятає як логін і пароль, так і те, що у нього є смартфон, який «зареєстрований» як пристрій для отримання кодів цих типів [5]. До інших чинників аутентифікації належать: коди електронної пошти, текстові токени, біометрична перевірка, апаратні токени, питання безпеки (секретні питання) та інше.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Досить часто, використовуючи різні соціальні мережі, електронну пошту та інше, користувачі часто забувають про елементарні правила захисту інформації або просто ігнорують їх, хоча така необачність, як показує практика, стає ключовим моментом у втраті не лише інформаційних ресурсів, але і великих фінансових втратах. Декілька хвилин налаштувань не створює незручності, отже, завжди варто думати про більш високий рівень безпеки в довгостроковій перспективі.

У статті запропоновано перелік основних способів захисту облікових записів на основі аналізу реалізації способів злому та несанкціонованого доступу. Працездатність та способи реалізації рекомендацій можна перевірити кожному користувачу і переконатись в їх дієвості. Способи злому та несанкціонованого доступу не є вичерпними, а отже, перелік способів захисту від них може змінюватись. Рекомендації можна використовувати і в навчальних цілях. В подальшому планується створити підхід до оцінки ефективності методів аутентифікації, що застосовуються для додаткового захисту акаунтів, з урахуванням наведених вище показників.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа. Інформаційна та кібербезпека: соціотехнічний аспект: підручник.— К.: ДУТ, 2015. - 288 с.
2. Що таке MFA — багатофакторна аутентифікація? [Електронний ресурс] Режим доступу: https://datami.ua/shho-take-mfa-bagatofaktorna-autentifikatsiya/
3. С.І. Болобан, О.М. Перегуда, В.В. Умінський, «Методи аутентифікації користувачів інформаційно-комунікаційних систем», *Розроблення та модернізація ОВТ*, №2. С. 47-52, 2009.
4. КПМГ-Україна. Глобальне дослідження з питань шахрайства у банківській сфері [Електронний ресурс] Режим доступу: https://assets.kpmg/content/dam/kpmg/ua/pdf/2019/11/Global_Banking_Fraud_Survey.pdf
5. Datami. Як захистити власні соціальні мережі? [Електронний ресурс] Режим доступу: https://datami.ua/yak-zahistiti-vlasni-sotsialni-merezhi/
6. Хакер з України розробив найбільший у світі фішинг-сервіс для атак на фінустанови [Електронний ресурс] Режим доступу: https://banda.media/ru/haker-z-ukrayiny-rozrobyv-najbilshyj-u-sviti-fishyng-servis-dlya-atak-na-finustanovy-kiberpolicziya/
7. Назвіть найпоширеніші методи злому [Електронний ресурс] Режим доступу: https://uk.focuzcomputers.com/t-cnicas-de-hacking-comunes-que-debes-conocer
8. Взлом почты [Електронний ресурс] Режим доступу: https://brut4you.wordpress.com/2014/08/08/%D0%B2%D0%B7%D0%BB%D0%BE%D0%BC-%D0%BF%D0%BE%D1%87%D1%82%D1%8B/
9. О. С. Кульчицький, В. В. Грицюк, І. Г. Зотова, «Аналіз існуючих підходів при ідентифікації і аутентифікації користувачів в інформаційно-телекомунікаційних системах» , *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського*, №3. С. 60-64, 2016.
10. Я.П. Кісь В.М. Теслюк, «Методи і засоби автентифікації біометричних даних в інформаційних системах», *Актуальні проблеми економіки*, №12(138). С. 174-182, 2012.
11. О. Корченко, А. Давиденко, О. Висоцька, «Метод автентифікації користувачів інформаційних систем за їх рукописним почерком з багатокроковою корекцією первинних даних», *Захист інформації,* №1. С. 40-51, 2019.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (12), 2021
ISSN 2663 - 4023

Nataliia V. Korshun
Doctor of Technical Sciences, associate professor, Professor of the Department of Information and Cyber Security
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID ID: 0000-0003-2908-970X
n.korshun@kubg.edu.ua

Iryna S. Litvinchuk
Researcher
Military base A1906, Kyiv, Ukraine
ORCID ID 0000-0002-0854-5393
litvinchuk.irina94@gmail.com

Ruslan O. Korchomnyi
Researcher
Military base A1906, Kyiv, Ukraine
ORCID ID 0000-0002-2457-6675
rra30@ukr.net

Ihor V. Borysov
PhD, Associate Professor
Researcher
Military base A1906, Kyiv, Ukraine
ORCID: 0000-0003-2276-9913
borisov_viti@ukr.net

DEVELOPMENT OF RECOMMENDATIONS FOR MINIMIZING THE RISKS OF ACCOUNT HACKING ON THE BASIS OF ANALYSIS OF THE MOST COMMON HACKING METHODS

Abstract. With the spread of the Internet, social networks, messengers, etc. and their penetration into all spheres of life of the modern individual, the number of attempts to obtain unauthorized access to personal information of users is increasing. Accounts are the most vulnerable target for hacking. Among the most common types of attacks - phishing, theft of cookies, use of keyloggers, brute force. Social engineering techniques have become very popular among attackers. Using a password in the form of a set of letters, numbers, and special characters is no longer sufficient to provide the required level of account security. The introduction of combined systems increases the number of identification features and increases data security. Systems based on contactless smart cards, USB keys, hybrid smart cards, bioelectronic systems can be used as additional protection mechanisms. One of the main recommendations for avoiding the consequences of fraudulent actions is double or multifactor authentication to verify the identity of the client (requiring users to provide data, such as a password, using other factors, such as a text message / SMS code or fingerprints). Multi-factor authentication should be used on all available Internet services, where possible, to ensure an acceptable level of security. There are two main types of multifactor authentication: the MFA application, an authentication process that is activated when a user tries to access one or more applications, and the MFA device, an authentication process that immediately activates the MFA at the login point. One of the most common authentication factors is the phone number. Email codes, text tokens, biometric verification, hardware tokens, security issues (secret issues) and more are also used.

Keywords: multifactor authentication; phishing; password protection; biometric authentication.

REFERENCES

1. V.L. Buryachok, V.B. Tolubko, V.O. Khoroshko, S.V. Tolyupa. Information and cybersecurity: socio-technical aspect.— K.: SUT, 2015. - 288 c.
2. What is MFA - Multifactor Authentication? [Electronic resource]. Available: https://datami.ua/shho-take-mfa-bagatofaktorna-autentifikatsiya/
3. S.I. Boloban, O.M. Pereguda, V.V. Uminsky, «Methods of authentication of users of information and communication systems», *Development and modernization of armaments and military equipment*, №2. Pp. 47-52, 2009.
4. KPMG-Ukraine. Global study on banking fraud [Electronic resource]. Available: https://assets.kpmg/content/dam/kpmg/ua/pdf/2019/11/Global_Banking_Fraud_Survey.pdf
5. Datami. How to protect your own social networks? [Electronic resource]. Available: https://datami.ua/yak-zahistiti-vlasni-sotsialni-merezhi/
6. A hacker from Ukraine has developed the world's largest phishing service for attacks on financial institutions [Electronic resource]. Available: https://banda.media/ru/haker-z-ukrayiny-rozrobyv-najbilshyj-u-sviti-fishyng-servis-dlya-atak-na-finustanovy-kiberpolicziya/
7. Name the most common methods of hacking [Electronic resource]. Available: https://uk.focuzcomputers.com/t-cnicas-de-hacking-comunes-que-debes-conocer
8. Mail hacking [Electronic resource]. Available: https://brut4you.wordpress.com/2014/08/08/%D0%B2%D0%B7%D0%BB%D0%BE%D0%BC-%D0%BF%D0%BE%D1%87%D1%82%D1%8B/
9. O.S. Kulchytsky, V.V. Hrytsiuk, I.G. Zotova, «Analysis of existing approaches to user identification and authentication in information and telecommunication systems» , *Collection of scientific works of the Center for Military Strategic Studies of the Ivan Chernyakhovsky National University of Defense of Ukraine*, №3. Pp. 60-64, 2016.
10. J.P. Kis, V.M. Teslyuk, «Methods and means of authentication of biometric data in information systems», *Current economic problems*, №12 (138). Pp. 174-182, 2012.
11. O. Korchenko, A. Davydenko, O. Vysotska, «Method of authentication of users of information systems by their handwriting with multi-step correction of primary data», *Information protection*, №1. Pp. 40-51, 2019.