УДК 004.93'1
DOI: https://doi.org/10.26642/ten-2020-1(85)-171-176

О.С. Бойченко, к.т.н.
І.В. Гуменюк, к.т.н.
К.В. Сметанін, к.т.н.
О.В. Некрилов, курсант
Житомирський військовий інститут ім. С.П. Корольова

Метод блокування доступу до інформаційно-телекомунікаційних систем на основі біометричної ідентифікації/аутентифікації користувачів

Встановлено, що гарантування безпеки інформаційно-телекомунікаційних систем (ІТС) суттєво залежить від високого рівня ефективності функціонування їхніх систем управління доступом та захисту даних. Разом з тим постійне зниження актуальності парольних та атрибутних методів ідентифікації/аутентифікації користувачів вимагає пошуку нових шляхів захисту інформації від несанкціонованого доступу до неї. Одним із перспективних підходів вважається розроблення методів біометричної ідентифікації/аутентифікації інсайдер-користувачів для блокування їхнього доступу до інформаційно-телекомунікаційних систем. Своєчасне виявлення несанкціонованого доступу до таких систем є необхідною складовою гарантування безпеки їх функціонування, особливо в умовах матеріального та нематеріального витоку інформації, та обумовлює необхідність розроблення методів блокування доступу до інформаційно-телекомунікаційних мереж інсайдер-користувачами. З цією метою у статті запропоновано метод блокування доступу до такого класу систем, в основу якого покладено алгоритм біометричної ідентифікації/аутентифікації за геометрією обличчя. Наведено результати верифікації методу для різних типів ідентифікації, зокрема одиночної (персональної) та групової, їхні порівняльні характеристики залежно від величини природньої освітленості. Показано, що застосування запропонованого методу дає змогу оперативно виявляти факти несанкціонованого доступу інсайдер-користувачами до інформаційно-телекомунікаційних систем та своєчасно запобігати витоку інформації. Окрім цього встановлено, що запропонований метод можливо реалізувати у мобільних додатках, що особливо актуально в умовах інформатизації сьогодення.

Ключові слова: *біометрична ідентифікація; аутентифікація; інформаційно-телекомунікаційна мережа; захист інформації; несанкціонований доступ; кібербезпека.*

Постановка проблеми у загальному вигляді. Останні події, які спостерігаються на світовій арені, супроводжуються процесом перерозподілу зон впливу у технологічному та економічному просторах, розвитком інформаційних технологій (ІТ), які породжують нові способи отримання інформації. У зв'язку з цим, забезпечення захисту секретної інформації є актуальним питанням та вимагає від держав, незалежно від їх розвитку, постійного зміцнення національної безпеки, а також спроможності протидіяти загрозам і мінімізувати ризики реального витоку важливих відомостей та даних.

З початком збройної агресії з боку Російської Федерації (РФ), яка безпрецедентно створює напружену оперативну обстановку як в Україні, так і навколо неї, потреба у впровадженні адекватної комплексної системи гарантування безпеки інформації та протидії кіберзагрозам й атакам набула особливої актуальності. Зважаючи на досвід технологічного розвитку ІТ, одним із потенційно можливих напрямів удосконалення методів захисту інформації від несанкціонованого доступу (НСД) та витоку інформації на об'єктах інформаційної діяльності (ОІД) є ідентифікація та/або аутентифікація користувачів [1, с. 2]. Тому науково-практичне завдання щодо удосконалення механізмів охорони державної таємниці та захисту інформації на основі біометричної ідентифікації та/або аутентифікації користувачів є своєчасним та актуальним.

Виникнення цього важливого науково-практичного завдання обумовлено існуючим об'єктивним протиріччям між вимогами до зменшення потенційних збитків від внутрішніх загроз та принциповою неможливістю їх уникнення за рахунок існуючої системи ідентифікації та/або аутентифікації користувачів, що й визначає своєчасність та актуальність досліджень.

Аналіз останніх досліджень та публікацій. На сьогодні вже розроблено та реалізовано ряд методів ідентифікації на основі біометричних особливостей людини. Авторами у [3] наведено результати аналізу методів розпізнавання обличчя та алгоритмів порівняння шаблонів образів, а також тенденцій розвитку систем біометричної ідентифікації та аутентифікації осіб за геометрією обличчя; у [4] проведено аналіз методів біометричної ідентифікації, наведено переваги та недоліки технологій їх реалізації; у [5] розглянуто сучасні методи біометричної ідентифікації користувачів комп'ютерних систем, призначені для забезпечення захисту конфіденційної інформації; у [6] описуються загальні методи та програми

біометричної ідентифікації; у [7] розглядається класифікація моделей і методів біометричного контролю відвідуваності, наведено результати аналізу аутентифікації людини; у [8] запропоновано структуру біометричного шаблона аутентифікації користувача мобільного банкінгу; у [9] розв'язано актуальну науково-технічну задачу розробки інформаційної технології для ідентифікації персоналу на основі комплексу біометричних параметрів з використанням поєднання статично-динамічних методів розпізнавання та удосконаленням методів створення еталонних зразків.

Отже, результати аналізу науково-практичних джерел свідчать про те, що для вирішення завдань біометричної ідентифікації/аутентифікації розроблено достатню кількість методів. Проте дослідженням процесів та методів блокування доступу до ІТС користувачами у науковій літературі не присвячено належної уваги.

Тому, **мета статті** полягає в удосконаленні методу біометричної ідентифікації/аутентифікації та його застосуванні при вирішенні завдань блокування доступу до ІТС користувачами.

Постановка завдання. *Нехай* для деякої множини $\{O\}$, в якій зберігається опис об'єктів та $\{K\}$ – кінцевої множини номерів класів, *необхідно* класифікувати об'єкти (зображення) за визначеними ознаками, а саме, за номером (класом), до якого належить цей (конкретний) об'єкт.

Обмеження. Для заданих множин встановлюється залежність $K^* : O \Rightarrow K$.

Навчальна вибірка визначається:

$$O_i = \{(o_i, \kappa_i)\},\ i \in [1; n],\ n \in N, \tag{1}$$

де N – кінцева кількість даних.

У результаті для $\{O\}$ описується деяка функція, яка для будь-якого можливого значення цієї множини класифікує об'єкт, тобто $o_i \in O$. Результат класифікації об'єктів забезпечить надійність ідентифікації користувачів, зокрема блокування доступу користувачами до ІТС.

Викладення основного матеріалу дослідження. На цей момент розвитку ІТ парольні, які базуються на унікальній персональній інформації, та атрибутні методи ідентифікації втрачають свою актуальність, проте користуються великим попитом серед користувачів. Ці методи забезпечення доступу мають суттєві технологічні недоліки, які стають все більш вираженими. Однією з проблем є неточність ідентифікації користувача у системі та велика ймовірність порушення її безпеки в результаті НСД до інформації, витоку інформації, імітації певного атрибута або зламу паролю тощо. Також важливою проблемою цих методів є відсутність функціонала для виявлення підміни авторизованого «легітимного» користувача. Тобто порушник режиму доступу до інформації може незаконно увійти до системи чи/або ОІД у той момент, коли «легітимний» користувач залишає її без контролю після етапу проходження авторизації. Однак неперервний прихований моніторинг дає можливість своєчасно виявити відсутність такого користувача та унеможливити доступ до системи або об'єкта з обмеженим доступом для порушників [3, с. 106].

Порівняно з попередніми методами, біометричні характеристики користувача як спосіб аутентифікації можуть гарантувати підвищений рівень безпеки, враховуючи невід'ємність біометричних даних конкретної особи. Біометрична ідентифікація – це технології розпізнавання за окремими специфічними біометричними ознаками (ідентифікаторами), які властиві конкретній особі або користувачу [10, с. 206].

Метод блокування доступу користувачами до ІТС, що розробляється, містить такі кроки:

Крок 1. Виявлення та локалізація геометрії обличчя користувача на зображенні відеопотоку. На підставі аналізу [3–9] у цій роботі для пошуку форми (геометрії) обличчя на зображенні систем відеоспостереження використано алгоритм Віоли-Джонса. Як правило, цей пошук відбувається швидко, проте інтелектуальне вивчення ознак класифікатором проводиться тривалий час. Відповідно, обраний метод є кращим рішенням, порівняно з іншими алгоритмами, за критеріями ефективності та оперативності розпізнавання обличчя [8, с. 120].

Під час використання такого методу відеозображення подається в інтегральному вигляді (матриця значень сумарної яскравості) для підвищення оперативності аналітичних обчислень та розрахунків. У кожному елементі цієї матриці зберігається значення суми інтенсивності пікселів, які геометрично окреслюють об'єкт зліва та зверху [6, с. 85].

Елементи інтегрального подання розраховуються за формулою:

$$L(x,y) = \sum_{i=0}^{i \le x} \sum_{j=0}^{j \le y} I(i,j), \tag{2}$$

де $I(i,j)$ – значення яскравості пікселя на зображенні.

Кожен елемент $L(x,y)$ відповідає сумі пікселів, які знаходяться у певному прямокутнику.

У загальному вигляді алгоритм здійснює пошук обличчя та його контури (геометрію) за допомогою сканування вікна. Відеозображення, на якому здійснюється пошук об'єкта, подається у вигляді

двовимірної матриці розмірністю (x, y), кожен піксель якої приймає значення для однотонного зображення $[0;255]$ та для кольорового зображення формату RGB – $[0;255^3]$. Пошук здійснюється в активній області зображення прямокутними ознаками (опис користувача та його геометрія обличчя):

$$RECT = \{(x,y),(w,h),\alpha\}, \quad (3)$$

де (x,y) – координати центра i-го прямокутника;

w, h – ширина та висота прямокутника відповідно;

α – кут нахилу прямокутника відносно вертикальної осі зображення.

Крок 2. Нормалізація зображення за масштабом, яскравістю тощо.

Крок 3. Обчислення набору базових ознак (характеристик) зображення. Основними принципами, на яких базується метод Віоли-Джонса, є використання базових понять теорії розпізнавання об'єктів, зокрема ознак (примітивів) Хаара, застосування каскаду ознак/примітивів для аналізу результату ідентифікації. Усі ознаки надходять на вхід класифікатора та обробляються з деяким підсиленням, так званим бустингом (*від англ.* boost – вдосконалення, посилення);

Ознаки (примітиви) Хаара – це відображення f :

$$\chi \Rightarrow D_f, \quad (4)$$

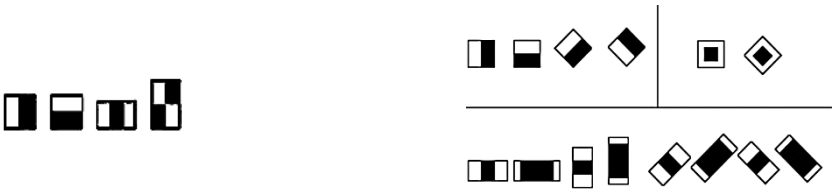
де D_f – множина допустимих значень ознаки.

За умови, що ознака $f_1,...,f_n$ визначена, вираз (4) прийме вигляд:

$$\chi \Rightarrow \{f_1,...,f_n\}, \quad (5)$$

який називається ознакою опису об'єкта.

У стандартному методі Віола-Джонса використовуються прямокутні ознаки (примітиви Хаара), а у розширеному – додаткові, які входять до складу типізованої бібліотеки OpenCV (*від англ.* Open Source Computer Vision Library – бібліотека комп'ютерного зору з відкритим вихідним кодом) (рис. 1).



а) *б)*

Рис. 1. Базові ознаки (характеристики) Хаара: а) примітиви; б) додаткові

У процесі пошуку обчислення всіх ознак Хаара є практично не можливим, відповідно класифікатор має враховувати лише певну підмножину важливих ознак. Таким чином, для досягнення ефективності функціонування алгоритму та надійної роботи необхідно проводити інтелектуальне навчання класифікатора, наприклад з використанням нейронних мереж. Цей процес є складовою концепції та технології Data Mining (дослідження та інтелектуальний аналіз даних). Машинне навчання в методі Віоли-Джонса вирішує завдання класифікації об'єктів за ознаками.

Крок 4. Порівняння обчислених ознак з еталонними, які містяться у базі даних.

Загальний алгоритм методу блокування доступу до ІТС на основі біометричної ідентифікації/аутентифікації інсайдер-користувачів наведено на рисунку 2.

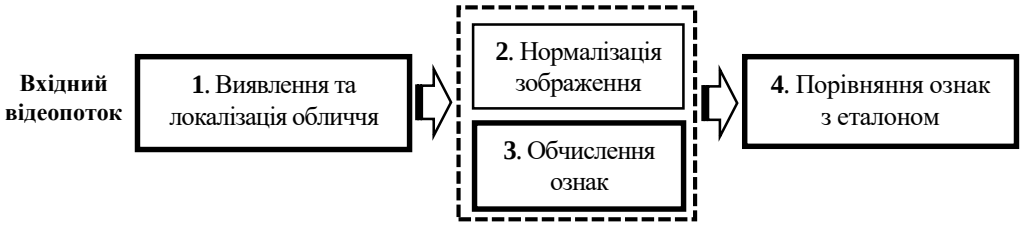


Рис. 2. Алгоритм блокування доступу інсайдер-користувачами до ІТС

Верифікацію запропонованого методу проведено з використанням розробленого авторами спеціалізованого програмного забезпечення [11] на відеозображеннях, отриманих за допомогою відеокамери *Infinity SR-DN530SD* з роздільною здатністю відеопотоку HDTV 720p.

Умови проведення верифікації методу та дослідження працездатності розробленого СПЗ:

– до бази даних занесено 4 записи шаблонних користувачів ІТС (кожен запис містить до 30 зображень, прізвище, ім'я, унікальний номер тощо);

– природня (достатня та недостатня) освітленість приміщення – 100–400 люкс;

– мінімальна відстань між засобом відеоспостереження та об'єктом ідентифікації складає 0,5 м, максимальна – 2,0 м;

– кількість експериментів дослідження – 200;

– тестовими користувачами обрано відеозображення користувачів № 1 (його дані занесені до БД) та двох інших користувачів, один з яких авторизований (користувач № 2);

– одиночна (персональна) та групова ідентифікація.

Результати верифікації наведено у таблиці 1 та програмної реалізації – на рисунках 3–4.

Таблиця 1

Результат ідентифікації/аутентифікації користувачів ІТС

Відстань, (м)	Результат ідентифікації, (%) ([0–20] – *заблоковано*; [21–100] – *доступ надано*)			
	Персональна ідентифікація		Групова ідентифікація	
	недостатня освітленість, 100–200 (лк)	достатня освітленість, 200–400 (лк)	недостатня освітленість, 100–200 (лк)	достатня освітленість, 200–400 (лк)
0,5	30	100	5	100
1,0	20	98	5	95
1,5	20	95	0	60
2,0	10	85	0	20

а) *б)*

Рис. 3. Результат персональної ідентифікації за достатньої освітленості: а) відстань 0,5 м; б) відстань 2 м

а) *б)*

Рис. 4. Групова ідентифікація за достатньої освітленості: а) відстань 0,5 м; б) відстань 2 м

Висновки та перспективи подальших досліджень. У роботі наведено результати вирішення актуального науково-практичного завдання, яке полягало в удосконаленні механізмів охорони державної таємниці та захисту інформації на основі біометричної ідентифікації та/або аутентифікації користувачів.

Розроблений метод інтелектуальної біометричної ідентифікації/аутентифікації користувачів ІТС та його програмна реалізація дозволяють блокувати доступ в умовах недостатньої освітленості на відстані до 0,5 м під час персональної ідентифікації та взагалі блокувати доступ в умовах недостатньої освітленості під час групової ідентифікації. Особливість розробленого методу полягає у можливості його реалізації у мобільних додатках, що особливо актуально в умовах інформатизації сьогодення. Практичне значення одержаних результатів полягає в можливості: впровадження методу в сучасні системи контролю та пропускного режиму ОІД; інтеграції програмного забезпечення в системи аутентифікації засобів обчислювальної техніки, у тому числі ПЕОМ; блокування доступу до інформації та засобів її обробки для неавторизованих користувачів тощо.

У подальшому планується реалізація мультимодальної ідентифікації груп осіб на основі отриманих зображень їх обличь у відкритих серверах мережі Інтернет.

Список використаної літератури:

1. Концепція створення національної системи ідентифікації громадян України, іноземців та осіб без громадянства : Розпорядження Кабінету Міністрів України № 1428-2015-р від 23.12.2015 [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/main/1428-2015-%D1%80.
2. *Гуменюк І.В.* Методика забезпечення захисту інформації в інформаційно-телекомунікаційних системах / *І.В. Гуменюк, В.Л. Барилюк, М.В. Файдюк* // Забезпечення інформаційної безпеки держави у воєнній сфері: проблеми та шляхи їх вирішення : мат-ли науково-практичної конференції. – Київ : НУОУ ім. І.Черняховського, 2019. – С. 66–67.
3. *Нечипоренко О.В*. Біометрична ідентифікація і автентифікація особи за геометрією обличчя / *О.В. Нечипоренко, Я.В. Корпань* // Вісник Хмельницького національного університету. Серія : Технічні науки. – 2016. – № 4. – С. 133–138.
4. *Коваль Л.Г.* Методи і технології біометричної ідентифікації за результатами літературних джерел / *Л.Г. Коваль, С.М. Злепко, Г.М. Новіцький* // Вчені записки ТНУ ім. В.І. Вернадського. Серія : Технічні науки. – 2019. – Т. 30 (69), Ч. 1, № 2. – С. 104–112.
5. *Бідюк П.* Сучасні методи біометричної ідентифікації / *П.Бідюк, В.Бондарчук* // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2009. – Вип. 1 (18). – С. 137–146.
6. *Divyarajsinh N. Parmar and other* Face Recognition Methods & Applications / *Divyarajsinh N. Parmar and other* // Int. J. Of Computer Technology & Applications. – 2015. – Vol. 4 (1). – P. 84–86.
7. *Александрович Д.В.* Исследование моделей и методов биометрического контроля посещаемости / *Д.В. Александрович, А.Л. Ерохин* // Системи обробки інформації. – 2014. – Вип. 6 (122). – С. 157–162.
8. *Нємкова О.А.* Біометрична ідентифікація у кіберпросторі / *О.А. Нємкова* // Системи обробки інформації. – 2015. – Вип. 7 (132). – С. 118–121.
9. *Кумченко Ю.О.* Інформаційна технологія ідентифікації персоналу на основі комплексу біометричних параметрів : дис. на здобуття наукового ступеня канд. техн. наук / *Ю.О. Кумченко*. – 2017. – 143 с.
10. *Гуменюк І.В.* Біометрична ідентифікація у кіберпросторі на основі розпізнавання обличчя / *І.В. Гуменюк, М.С. Басараба, О.В. Некрилов* // Проблеми теорії та практики інформаційного протиборства в умовах ведення гібридних війн : тези доповідей наук.-практ. конф. 24–25 жовтня 2019 р. – Житомир : ЖВІ, 2019. – С. 205–207.
11. Спеціалізоване програмне забезпечення біометричної ідентифікації/аутентифікації користувачів інформаційно-телекомунікаційних систем на основі геометрії обличчя : заявка про реєстрацію авторського права на твір № АПС 95-19 ; дата затвердження заявки 28.10.2019.
12. *Viola P.* Rapid object detection using a boosted cascade of simple features / *P.Viola, M.Jones* // IEEE Conference on Computer Vision and Pattern Recognition. – 2001. – Vol. 1. – P. 511–518.
13. *Ніколаєв С.С.* Залежність якості детектора облич на ознаках Хаара від варіативності навчальної вибірки / *С.С. Ніколаєв, Ю.О. Тимошенко, К.Ю. Матвіїв* // Наукові вісті НТУУ «КПІ» : міжнародний науково-технічний журнал. – 2017. – № 6 (116). – С. 38–46.

References:

1. Kabinet Ministriv Ukrayiny (2015), *Kontseptsiya sozdanyya natsyonal'noy systemy identifikatsiyi hromadyan Ukrayiny, inozemtsiv ta osib bez hromadyanstvo*, Rozporyadzhennya No. 1428-2015-r vid 23.12.2015, [Online], available at: https://zakon.rada.gov.ua/laws/main/1428-2015-%D1%80
2. Humeniuk, I.V., Barylyuk, V.L. and Faydyuk, M.V. (2019), «Metodyka zabezpechennya zakhystu informatsiyi v informatsiyno-telekomunikatsiynikh systemakh», *Zabezpechennya informatsiynoyi bezpeky derzhavy u voyenniy sferi: problemy ta shlyakhy yikh vyrishennyu*, m-ly naukovo-praktychnoyi konferentsyy, NUOU im. I.Chernyakhovs′koho, Kyyiv, pp. 66–67.
3. Nechyporenko, O.V. and Korpan′, YA.V. (2016), «Biometrichna identyfikatsiya y avtentyfikatsiya osobyny za heometriyeyu lytsa», *Visnyk Khmel'nyts'koho natsional'noho universytetu*, Serija *Tekhnichni nauky*, No. 4, pp. 133–138.
4. Koval′, L.H., Zlepko, S.M. and Novits′kyy, H.M. (2019), «Metody y tekhnolohiyi biometrichnoyi identifikatsiyi za rezul′tatamy literaturnykh dzherel», *Vcheni zapysky TNU im. V.I. Vernads'koho*, Serija *Tekhnichni nauky*, Vol. 30 (69), Part 1, No. 2, pp. 104–112.
5. Bidyuk, P. and Bondarchuk, V. (2009), «Suchasni metody biometrichnoyi identifikatsiyi», *Pravove, normatyvne ta Metrolohichne zabezpechennya systemy zakhystu informatsiyi v Ukrayini*, Issue 1 (18), pp. 137–146.

6. Divyarajsinh N. Parmar and other (2015), «Face Recognition Methods & Applications», *Int. J. of Computer Technology & Applications*, Vol. 4 (1), pp. 84–86.
7. Oleksandrovych, D.V. and Yerokhin, A.L. (2014) «Doslidzhennya modeley i metodiv biometrychnoho kontrolyu vidviduvanosti», *Systemy obrobky informatsiji*, Issue 6 (122), pp. 157–162.
8. Nyemkova, O.A. (2015), «Biometrichna identyfikatsiya u kiberprostori», *Systemy obrobky informatsiji*, Issue 7 (132), pp. 118–121.
9. Kumchenko, Yu.O. (2017), «Informatsiyna tekhnolohiya identifikatsiyi personalu na osnove kompleksu biometrichnikh parametriv», PhD Thesis, 143 p.
10. Humeniuk, I.V., Basaraba, M.S. and Nekrilov, O.V. (2019) «Biometrichna identyfikatsiya u kiberprostori na osnove rozpiznavannya lytsa», *Problemy Teoriyi ta praktyky informatsiynoho protiborstva v uslovyyakh vedennya hibridnikh viyn*, tezy dopovidey nauk.-prakt. konf. 24–25 zhovtnya 2019 r., ZHVI, Zhytomyr, pp. 205–207.
11. *Spetsializovane prohramne zabezpechennya biometrichnoyi identifikatsiyi/autentifikatsiyi Korystuvachiv informatsiyno-telekomunikatsiynikh system na osnove heometriyi oblychchya*, zayavka pro reyestratsiyu avtors′kym pravom na tvir No. APS 95-19, data zatverdzhennya zayavky 28.10.2019.
12. Viola, P. and Jones, M. (2001), «Rapid object detection using a boosted cascade of simple features», *IEEE Conference on Computer Vision and Pattern Recognition*, Vol. 1, pp. 511–518.
13. Nikolayev, S.S., Tymoshenko, YU.O. and Matviyiv, K.YU. (2017), «Zalezhnist′ yakosti detektora oblych na oznakakh Khaara vid variatyvnosti navchal′noyi vybirky», *Naukovi visti NTUU «KPI»*, mizhnarodnyy naukovo-tekhnichnyy zhurnal, No. 6 (116), pp. 38–46.

Бойченко Олег Сергійович – кандидат технічних наук, начальник науково-дослідної лабораторії наукового центру Житомирського військового інституту ім. С.П. Корольова.
http:// orcid.org/ 0000-0003-3048-4184.
E-mail: bos_2006@ukr.net.

Гуменюк Ігор Володимирович – кандидат технічних наук, старший викладач кафедри захисту інформації та кібербезпеки Житомирського військового інституту ім. С.П. Корольова.
http:// orcid.org/ 0000-0001-5853-3238.
E-mail: ig_gum@ukr.net.

Сметанін Кирило Володимирович – кандидат технічних наук, викладач кафедри захисту інформації та кібербезпеки Житомирського військового інституту ім. С.П. Корольова.
http:// orcid.org/ 0000-0002-6062-550X.
E-mail: kiry221982@gmail.com.

Некрилов Олександр Володимирович – курсант навчального курсу Житомирського військового інституту ім. С.П. Корольова.
http:// orcid.org/ 0000-0002-2405-4949.
E-mail: fucklolgopvp@ukr.net.

Стаття надійшла до редакції 07.04.2020.