ПЕРСПЕКТИВНІ НАПРЯМИ РОЗРОБКИ ОБЛАДНАННЯ ТА РОЗВИТКУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

УДК 004.056.5

Досенко С. Д.,
Doctor12@i.ua, ORCID ID: 0000-0001-6707-2840,
с.н.с.,
Український науково-дослідний інститут спеціальної техніки та судових експертиз
Служби безпеки України, м. Київ

ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ. ОСНОВНІ ПРОБЛЕМИ ТА СПОСОБИ ЇХ ВИРІШЕННЯ

Анотація. *У статті досліджуються проблеми технічного захисту інформації та способи їх вирішення, особливу увагу приділено механізмам реалізації грифу обмеження доступу. Обґрунтовано, що сучасна інформаційна безпека вимагає постійного вдосконалення системи відповідно до збільшення ризику витоку інформації. Описано процес витоку й наголошено, що він є безперервним і полягає в реалізації сучасних методів і способів поліпшення системи захисту інформації, постійного моніторингу, виявлення його слабких місць і потенційних каналів витоку інформації. Запропоновано перелік методів, які лежать в основі дієвого технічного захисту інформаційного простору сьогодення. Зазначено, що рішення проблем захисту електронної інформації засноване в основному на використанні криптографічних методів, при цьому сучасні методи криптографічних перетворень зберігають вихідну продуктивність автоматизованої системи, що є важливим в умовах постійного впливу. Підкреслено, що основною властивістю забезпечення конфіденційності повідомлень є конфіденційність інформації, це дає змогу абстрагуватися від інших властивостей. Детально описано технічний комплекс «Гриф», який призначено для захисту секретної інформації. Зазначено функціональні можливості, які складаються із забезпечення неможливості неконтрольованого й несанкціонованого ознайомлення, копіювання й відновлення інформації, модифікації й видалення інформації; надання доступу до інформації тільки за умови достовірного розпізнавання користувачів і з урахуванням повноважень, наданих згідно зі службовою необхідністю; облік дій користувачів і реєстрацію спроб порушення встановленого порядку доступу до інформації, включаючи блокування доступу до інформації в разі виявлення таких спроб, а також можливість здійснення контролю за доступом до інформації з боку уповноважених осіб. Сформовано схему взаємодії модулів технічного комплексу з відокремленням інформаційних потоків.*

Ключові слова: технічний захист, інформація, проблеми, вирішення, гриф обмеження доступу, реформування, простір, проникнення.

Dosenko S. D.,
Doctor12@i.ua, ORCID ID: 0000-0001-6707-2840,
Senior Research Fellow,
Ukrainian Scientific and Research Institute of Special Equipment and Forensic Expertise
of the Security Service of Ukraine, Kyiv

TECHNICAL PROTECTION OF INFORMATION. THE MAIN PROBLEMS AND WAYS TO SOLVE THEM

Abstract. *The article examines the problems of technical protection of information and ways to solve them, special attention is paid to the mechanisms of implementation of the stamp of restriction of access. It is substantiated that modern information security requires constant improvement of the system in accordance with the increased risk of information leakage. The process of leakage is described and it is emphasized*

that it is continuous and consists in the implementation of modern methods and ways to improve the system of information protection, constant monitoring, identification of its weaknesses and potential channels of information leakage. The list of methods which underlie effective technical protection of information space of today is offered. It is noted that the solution of electronic information protection problems is based mainly on the use of cryptographic methods, while modern methods of cryptographic transformations preserve the initial performance of the automated system, which is important in the face of constant influence. It is emphasized that the main property of ensuring the confidentiality of messages is the confidentiality of information, it allows to abstract from other properties. The technical complex "Griff", which is designed to protect classified information, is described in detail. Functionalities are indicated, which consist of ensuring the impossibility of uncontrolled and unauthorized access, copying and restoring information, modifying and deleting information; providing access to information only under the condition of reliable identification of users and taking into account the powers granted in accordance with official necessity; registration of user actions and registration of attempts to violate the established procedure for access to information, including blocking access to information in case of detection of such attempts, as well as the possibility of control over access to information by authorized persons. The scheme of interaction of modules of a technical complex with separation of information streams is formed.

Key words: technical protection, information, problems, solutions, stamp restriction of access, reforming, space, penetration.

JEL Classification: O 32
DOI 10.36477/2522-1221-2021-27-04

Постановка проблеми. В умовах сучасного динамічного розвитку суспільства, постійної модернізації технічної та соціальної інфраструктури інформація постає стратегічним об'єктом забезпечення дієвого обміну між усіма ланками сучасного світу. Інноваційні інформаційні технології, які дають змогу створювати, зберігати, передавати інформацію та забезпечувати ефективний захист, стали важливим фактором життя суспільства сьогодення й засобом підвищення ефективності управління всіма сферами суспільної діяльності. При цьому постає беззаперечна умова формування дієвого механізму захисту як персональної, конфіденційної, загальної, так і секретної інформації, що циркулює в умовах інформаційного простору.

Сучасна інформаційна безпека вимагає постійного вдосконалення системи відповідно до збільшення ризику витоку інформації. Цей процес є безперервним і полягає в реалізації сучасних методів і способів поліпшення системи захисту інформації, постійного моніторингу, виявлення його слабких місць і потенційних каналів витоку інформації, постійному вдосконаленні систем за рахунок появи нових способів доступу до інформації ззовні.

Роль інформаційної безпеки в організаційній системі заходів безпеки визначається своєчасністю й точністю управлінських рішень керівництва з урахуванням наявних ресурсів, прийомів і методів забезпечення інформаційної безпеки, а також на підставі чинних нормативно-методичних документів [1].

Аналіз останніх досліджень і публікацій. Науковому осмисленню питання технічного захисту інформації сприяли праці сучасних науковців дослідників.

На території України наукове обґрунтування цього питання розпочалося в 90-х роках XX століття. Д.В. Коц [2] визначив і проаналізував етапи становлення й розвитку системи захисту інформації з обмеженим доступом, зокрема її нормативно-правового регулювання, у період відновлення Україною своєї незалежності. Автором статті описано власний підхід до формування поняття «система захисту інформації з обмеженим доступом», ураховано законодавчі визначення суміжних понять і включено об'єкти, щодо яких суб'єктами правовідносин здійснюються заходи захисту.

М.М. Мандрона, А.В. Панасюк [3] розкрили питання розроблення системи захисту інформації з обмеженим доступом, що озвучується.

У статті [4] наведено перспективи реформування системи охорони державної таємниці та службової інформації. Задекларована в роботі проблематика сформувала принципи впровадження певних новацій із застосуванням виваженого підходу та ретельного вивчення практики інших держав.

В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко й С.В. Толюпа [4] висвітлили головні принципи забезпечення інформаційної та кібернетичної безпеки, розкрили їх сутність, основний зміст і складники. Науковцями значну увагу приді-

лено типовим інцидентам у сфері високих технологій, а також методам і засобам соціального інжинірингу. Докладно розглянуто систему заходів із захисту від соціотехнічних атак. Наведено порядок здійснення процедур із тестування систем захисту інформації в інформаційно-комунікаційних системах на предмет проникнення, а також порядок оцінювання їх параметрів на різних рівнях.

Із зарубіжних авторів варто відзначити такі роботи таких авторів, як J. Bernstein Daniel, Heninger Nadia, Lou Paul, Valenta Luke [5], J. William, I. Lynn [6], J. Daemen, V. Rijmen [7], W.L. Tafoya [8], W. Millan, A. Clark, E. Dawson [9], C. Strider [10], O.V. Manzhai [11] та інші.

Однак сьогодні питання структурного аналізу проблем технічного захисту інформації та головне шляхів їх вирішення залишається відкритим і потребує детального опрацювання.

Постановка завдання. Мета статті – дослідити проблеми технічного захисту інформації та способи їх вирішення, особливу увагу приділити механізмам реалізації грифу обмеження доступу.

Виклад основного матеріалу дослідження. Світовий досвід створення систем захисту дає змогу відокремити три головні елементи, які потребують застосувань систем захисту: фізичних осіб, матеріальні цінності й інформацію. З урахуванням наведеного факту відокремлюють три основні групи засобів захисту: організаційно-правові, технічні та інформаційно-технологічні. Останні застосовуються для забезпечення безпеки інформації в процесі збору, передачі, обробки та приймання інформації.

Технічні засоби захисту базуються на фізичних, апаратних і програмних засобах захисту. Організаційно технічні заходи передбачають блокування можливих каналів витоку інформації.

Дієвий технічний захист інформаційного простору сьогодення характеризується такими методами:

– структуризація інформації за ступенем конфіденційності й забезпечення криптографічного захисту кожного ступеня при передачі інформації;

– розподіл інформаційних потоків з урахуванням відстані передачі інформації за напрямками трасування (локальна мережа, канали передачі повідомлень тощо);

– формування журналів атак із застосуванням сучасних механізмів обліку в разі спроб доступу сторонніх об’єктів в інформаційній системі та друкованих документах;

– забезпечення цілісності програмного забезпечення й інформації;

– застосування інноваційних засобів відновлення інформаційної безпеки на всіх рівнях впливу;

– обслуговування обладнання, систем і магнітних носіїв, формування ефективного фізичного захисту;

– створення, підтримка й удосконалення спеціальних служб захисту інформації.

Рішення проблем захисту електронної інформації засноване в основному на використанні криптографічних методів. При цьому сучасні методи криптографічних перетворень зберігають вихідну продуктивність автоматизованої системи, що важливо. Це найбільш ефективний спосіб забезпечення конфіденційності, цілісності й автентичності даних. Використання криптографічних методів в поєднанні з технічними й організаційними заходами забезпечує захист від широкого спектру загроз.

В українському державному стандарті ДСТУ ISO/IEC 27000:2019 (ISO/IEC 27000:2018, IDT) [12] інформаційна безпека відноситься до стану системи, яка гарантує конфіденційність, доступність і цілісність інформації та забезпечує її автентичність, достовірність, надійність, не відмову й відповідальність.

Основною властивістю забезпечення конфіденційності повідомлень є конфіденційність інформації, це дає змогу абстрагуватися від інших властивостей. Властивість конфіденційності інформації досягається за допомогою механізмів шифрування за допомогою ключа, що перетворює інформацію в нечитабельну форму для неавторизованих користувачів. З метою захисту конфіденційної інформації, що передається по відкритих каналах зв’язку, використовуються системи шифрування відкритого ключа, в яких відкритий ключ використовується для шифрування інформації, а секретний ключ – для її дешифрування. Принцип роботи таких систем заснований на обчислювальній складності зворотного перетворення інформації без використання секретного ключа.

Сьогодні найпоширенішим алгоритмом шифрування з відкритим ключем є алгоритм RSA, який використовує обчислювальну складність великого цілого числа, вирішуючи проблему факторизації. Незважаючи на поширеність і важливість алгоритму RSA, існують проблеми, які

можуть призвести до розкриття зашифрованої інформації.

Однією із цих проблем є проблема змінюваності розміру ключа RSA. Зростання обчислювальної потужності дає можливість більш ефективно вирішувати проблему факторизації великих цілих чисел, що шкодить алгоритму RSA. Ще однією найважливішою проблемою є поява якісно нових обчислювальних засобів, фундаментальною основою яких є квантові комп'ютери, які використовують явища квантової механіки для обробки та передачі даних. У квантовому комп'ютері стан інформації визначається кубітом, який через явище суперпозиції може одночасно мати стан 0 і 1, що допускає паралельність у розрахунках. Маючи ефективний квантовий комп'ютер, можна використовувати алгоритм Шора [13], за допомогою якого можна буде ефективно розкласти великі ключі алгоритму RSA за мінімальний час.

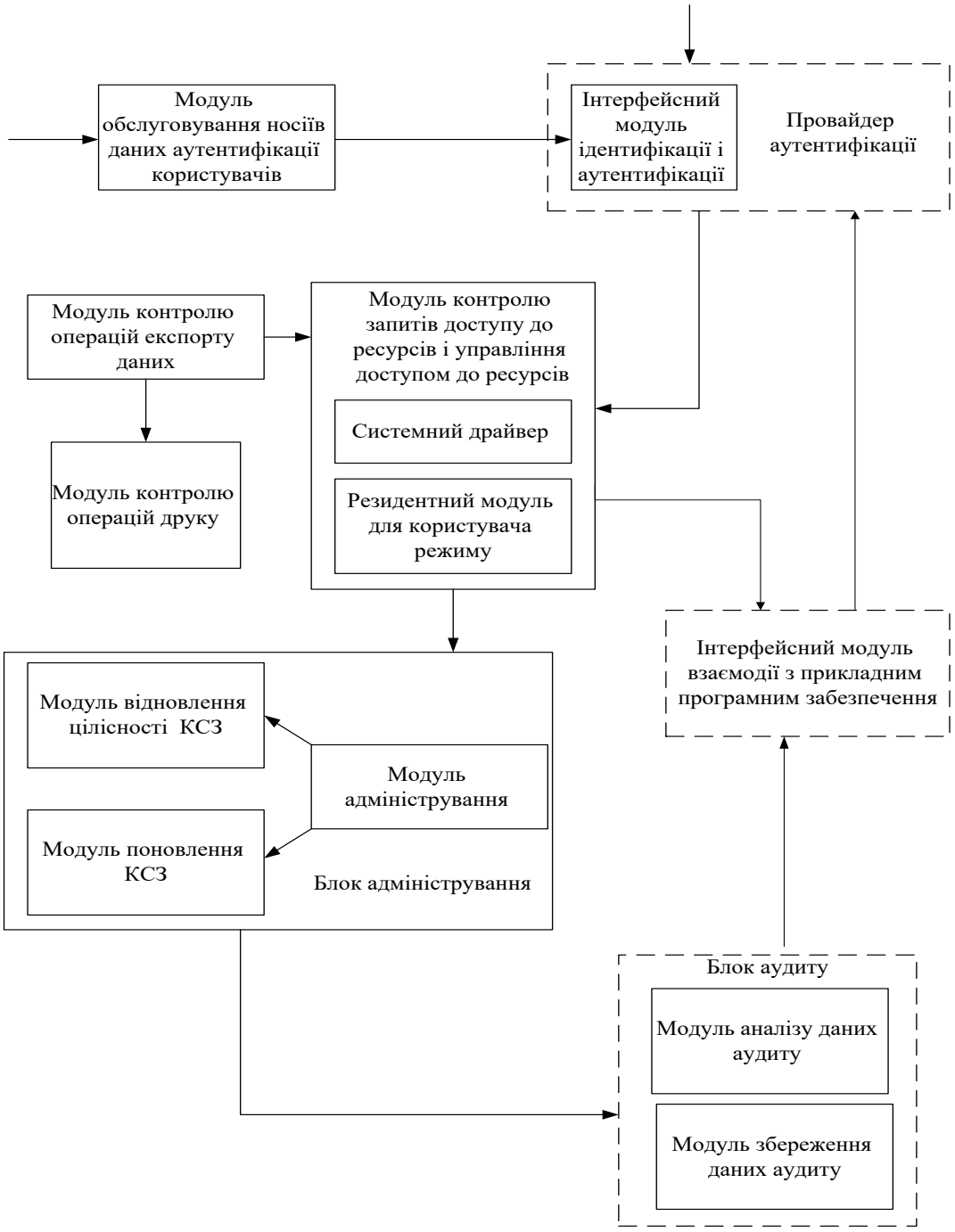

Рис. 1. Схема взаємодії модулів технічного комплексу захисту інформації

Джерело: власна розробка автора на основі [15]

Можливість реалізації інформаційної загрози створює багато соціальних і гуманітарних проблем. Щодо людини, то основною проблемою є захист персональних повідомлень і розмов, що є наслідком захисту її прав і свобод. Труднощі із забезпеченням конфіденційності повідомлень пояснюються використанням соціальних мереж і відкритих каналів зв'язку для їх передачі [14]. Для цього використовуються технічні засоби захисту інформації.

Один із найбільш ефективних сьогодні є технічний комплекс «Гриф», який призначено для захисту секретної інформації. Його функціональні можливості складаються із забезпечення неможливості неконтрольованого й несанкціонованого ознайомлення, копіювання й відновлення інформації; неможливості неконтрольованої й несанкціонованої модифікації та видалення інформації; надання доступу до інформації тільки за умови достовірного розпізнавання користувачів і з урахуванням повноважень, наданих згідно зі службовою необхідністю; обліку дій користувачів і реєстрації спроб порушення встановленого порядку доступу до інформації, включаючи блокування доступу до інформації в разі виявлення таких спроб, а також можливості здійснення контролю за доступом до інформації з боку уповноважених осіб [15]. Схема взаємодії модулів технічного комплексу наведена на рис. 1.

З огляду на описані методи та механізми захисту інформації, сьогодні постає головною проблемою захист прав власності на результати інтелектуальної діяльності, конфіденційної інформації та секретної. Необхідно комерційній тайні придати статус повноцінного об'єкта захисту, що виведе на новий рівень підхід до вирішення проблеми захисту одного з видів інтелектуальної власності й сформує основу захисту, що відповідає світовим стандартам.

Потрібно поступово вдосконалювати систему допуску співробітників до інформації та забезпечувати порядок роботи з документами, що мають гриф «КТ», формувати поняття «збереження» та «конфіденційно». Регулювання за допомогою правових засобів цих складних суспільних відносин і встановлення дієвого технічного захисту є складовою частиною побудови захищеного інформаційного простору сьогодення.

Висновки і перспективи подальших досліджень у цьому напрямі. У роботі досліджено проблеми технічного захисту інформації та способи їх вирішення, особливу увагу приділено механізмам реалізації грифу обмеження доступу. Наявні технічні засоби захисту інформації, що забезпечують її конфіденційність, у майбутньому можуть стати недостатньо ефективними для забезпечення інформаційної безпеки. Це пов'язано з нестабільністю наявних алгоритмів шифрування даних із відкритим ключем до квантових обчислень, розробка яких не стоїть на місці.

Неможливість використання правового регулювання як єдиного методу вирішення проблеми загрози конфіденційності інформації вимагає створення нових технічних підходів до захисту конфіденційної інформації, що сприяє формуванню цілі подальших досліджень.

ЛІТЕРАТУРА:

1. Рибальський О.В., Хахановський В.Г., Кудінов В.А. Основи інформаційної безпеки та технічного захисту інформації. Київ : Вид. Національної академії внутріш. справ, 2012. 104 с.

2. Коц Д.В. Становлення й розвиток системи захисту інформації з обмеженим доступом в Україні (1991–2019 рр.). *Вісник НТУУ «КПІ». Серія «Політологія. Соціологія. Право»*. Київ, 2019. № 3 (43). С. 250–254.

3. Мандрона М.М., Панасюк А.В. Розроблення системи захисту інформації з обмеженим доступом, що озвучується. *Проблеми та перспективи розвитку системи безпеки життєдіяльності :* матеріали XI Міжнародної науково-практичної конференції молодих вчених, курсантів та студентів. Львів : Львівський державний університет безпеки життєдіяльності, 2016. С. 240–242.

4. Болдир С.В. Перспективи реформування системи охорони державної таємниці та службової інформації. *Інформація і право*. 2017. № 4. С. 79–85.

5. Інформаційна та кібербезпека: соціотехнічний аспект : підручник / В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа ; за заг. ред. докт. техн. наук, професора В.Б. Толубка. Київ : ДУТ, 2015. 288 с.

6. Bernstein D., Lange, T. Post-quantum cryptography. *Nature*. 2017. Vol. 549 (7671). P. 188–194.

7. Lynn III W.F. Defending a new domain-the Pentagon's cyberstrategy. *Foreign Aff.* 2010. Vol. 89. P. 97.

8. Daemen J., Rijmen V. AES Proposal: Rijndael, AES Algorithm Submission. URL: http://www.docstoc.com/docs/14641406/AES-Implementation-and-Performance-Evaluationon-8-bit-Microcontrollers (Last accessed: 17.03.2021).

9. Tafoya W.L. Cyber Terror. FBI Law Enforcement Bulletin, 2011. URL: http://www.fbi.gov/stats-services/publications/law-enforcement-

bulletin/november- 2011/cyber-terror/ (Last accessed: 17.03.2021).

10. Millan W., Clark A., Dawson E. Boolean function design using hill climbing methods. *Australasian conference on information security and privacy.* Springer, Berlin, Heidelberg. 1999. Num. 1587. P. 1–11.

11. Strider C. Cyberespionage group turns eye of Sauron on targets. 2021. URL: http://www.symantec.com/connect/blogs/strider-cyberespionage-group-turns-eye-sauron- targets (Last accessed: 17.03.2021).

12. Manzhai O.V. Procedure Analysis of the Special Investigative Actions Through Cyberspace in Countries of Common and Continental Law. *Internal Security*. 2012. Vol. 1 (4). P. 141–152.

13. ДСТУ ISO/IEC 27000:2019 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд і словник термінів (ISO/IEC 27000:2018, IDT).

14. Shor P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *Foundations of Computer Science*. 1997. P. 1484–1509.

15. Гільгурт С.Я. Підвищення ефективності реконфігурованих систем виявлення вторгнень. *Безпека інформаційних технологій* : матеріали IX Міжнар. наук.-техн. конф. ITSec-2019 (м. Шармель-Шейх, Єгипет. 22–27 березня 2019). Київ : НАУ, 2019. С. 10–11.

REFERENCES:

1. Rybalskyi, O. V., Khakhanovskyi, V. H., Kudinov, V. A. 2012. *Osnovy informatsiinoi bezpeky ta tekhnichnoho zakhystu informatsii* [Fundamentals of information security and technical protection of information]. Kyiv : Vyd. Natsionalnoi akademii vnutrish. sprav.

2. Kots, D. V. 2019. Stanovlennia y rozvytok systemy zakhystu informatsii z obmezhenym dostupom v Ukraini (1991–2019 rr.) [Formation and development of the information protection system with limited access in Ukraine (1991–2019).]. *Visnyk NTUU «KPI». Politolohiia. Sotsiolohiia. Pravo*, no. 3 (43), pp. 250–254.

3. Mandrona, M. M., Panasiuk, A. V. 2016. Rozroblennia systemy zakhystu informatsii z obmezhenym dostupom, shcho ozvuchuietsia [Development of a system of protection of information with limited access to voice]. In: Lvivskyi derzhavnyi universytet bezpeky zhyttiediialnosti*, Problemy ta perspektyvy rozvytku systemy bezpeky zhyttiediialnosti,* Materialy XI Mizhnarodnoi naukovo-praktychnoi konferentsii molodykh vchenykh, kursantiv ta studentiv, pp. 240–242.

4. Boldyr, S. V. 2017. Perspektyvy reformuvannia systemy okhorony derzhavnoi taiemnytsi ta sluzhbovoi informatsii [Prospects for reforming the system of protection of state secrets and official information]. *Informatsiia i pravo*, no.4, pp. 79–85.

5. Buriachok, V. L. Tolubko, V. B., Khoroshko, V. O., Toliupa, S. V. 2015. Informatsiina ta kiberbezpeka: sotsiotekhnichnyi aspekt [Information and cybersecurity: socio-technical aspect]. In : V. B. Tolubka, ed. Kyiv : DUT.

6. Bernstein, D., Lange, T. 2017. Post-quantum cryptography. Nature, no. 549(7671), pp.188–194.

7. Lynn, III W. F. 2010. Defending a new domain-the Pentagon's cyberstrategy. *Foreign Aff*, vol. 89, p. 97.

8. Daemen, J., Rijmen, V. 2021. AES Proposal: Rijndael, AES Algorithm Submission. [online] Available at: http://www.docstoc.com/docs/14641406/AES-Implementation-and-Performance-Evaluationon-8-bit-Microcontrollers [Accessed 17 March 2021].

9. Tafoya, W. L. 2011. Cyber Terror. FBI Law Enforcement Bulletin, [online] Available at: http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/november-2011/cyber-terror/ [Accessed 17 March 2021].

10. Millan, W., Clark, A., Dawson, E. 1999 Boolean function design using hill climbing methods. *Australasian conference on information security and privacy*, no. 1587. pp. 1–11.

11. Strider, C. 2021. Cyberespionage group turns eye of Sauron on targets [online] Available at: http://www.symantec.com/connect/blogs/strider-cyberespionage-group-turns-eye-sauron- targets [Accessed 17 March 2021].

12. Manzhai, O. V. 2012. Procedure Analysis of the Special Investigative Actions Through Cyberspace in Countries of Common and Continental Law. *Internal Security*. vol. 1 (4), pp. 141–152.

13. DSTU ISO/IEC 27000:2019 *Informatsiini tekhnolohii. Metody zakhystu. Systemy keruvannia informatsiinoiu bezpekoiu. Ohliad i slovnyk terminiv (ISO/IEC 27000:2018, IDT).* [Information Technology. Methods of protection. Information security management systems. Overview and glossary (ISO / IEC 27000: 2018, IDT)]. Kyiv: Derzhspozhyvstandart Ukrainy

14. Shor, P. W. 1997. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *Foundations of Computer Science*, pp. 1484–1509.

15. Hilhurt, S. Ia. 2019. Pidvyshchennia efektyvnosti rekonfihurovnykh system vyiavlennia vtorhnen [Improving the efficiency of reconfigured intrusion detection systems]. In: NAU, *Bezpeka informatsiinykh tekhnolohii*, materialy IKh Mizhnar. nauk.-tekhn. konf. ITSec-2019, Sharm-el-Sheikh, Yehypet, 22–27), pp. 10–11.

Стаття надійшла до редакції 30.07.2021