УДК 004.77
DOI https://doi.org/10.32689/maup.it.2024.2.2

Микола ВАСИЛЕНКО
доктор фізико-математичних наук, доктор юридичних наук,
професор, професор кафедри кібербезпеки,
Національний університет «Одеська юридична академія», vasylenko.it@journals.maup.kiev.ua
***ORCID:** 0000-0002-8555-5712*

Валерія СЛАТВІНСЬКА
доктор філософії, асистент кафедри кібербезпеки,
Національний університет «Одеська юридична академія», slatvinskaya_valeriya@ukr.net
***ORCID:** 0000-0002-6082-981X*

Валерій РАЧУК
асистент кафедри кібербезпеки,
Національний університет «Одеська юридична академія», rachuk960@gmail.com
***ORCID:** 0000-0003-1793-016X*

АНАЛІЗ НЕСАНКЦІОНОВАНОГО ДОСТУПУ В КОМП'ЮТЕРНІ МЕРЕЖІ В КОНТЕКСТІ ЗАХОДІВ ЩОДО ЇХ БЕЗПЕКИ

Анотація. *У статті проаналізовано можливості та методи несанкціонованого доступу в комп'ютерні мережі в контексті заходів щодо їх безпеки.*

Мета роботи *полягає в аналізі методів та інструментів несанкціонованого доступу до комп'ютерних мереж, а також розробці комплексу заходів щодо запобігання несанкціонованому доступу та захисту комп'ютерних мереж.*

Методологія. *Аналіз наукової літератури з питань інформаційної безпеки комп'ютерних мереж. Вивчення нормативних документів щодо захисту інформації. Розгляд системи ЛОЗА-1 як прикладу програмно-апаратної системи захисту інформації.*

Наукова новизна. *Розроблено комплексний підхід до захисту комп'ютерних мереж від несанкціонованого доступу, який включає в себе як технічні, так і організаційні заходи. Доведено що для забезпечення ефективності асиметричних криптосистем є дві важливі вимоги. По-перше, процес шифрування повинен бути незворотнім і повністю виключати можливість відновлення вихідного тексту з «відкритого ключа». По-друге, секретний ключ, який є похідним від «відкритого ключа», має бути неможливо визначити на сучасному технологічному рівні. Запропоновано використовувати систему захисту інформації «ЛОЗА-1» як приклад комплексного підходу до захисту комп'ютерних мереж.*

Висновки. *Безпека і надійність криптографічних перетворень, а також ступінь захисту, який вони забезпечують, в кінцевому підсумку визначаються алгоритмом, що використовується для шифрування, розміром ключа, методом генерації ключів, суворим дотриманням технології і процедур, а також правильним використанням апаратних засобів і системи управління ключами. Забезпечення інформаційної безпеки комп'ютерних мереж є важливим завданням для будь-якої організації або окремого користувача. Використання комплексного підходу до захисту, який включає в себе як технічні, так і організаційні заходи, може допомогти захистити комп'ютерні системи від кібератак.*

Захист інформації в комп'ютерних мережах найкраще досягається за допомогою комплексного підходу, який поєднує в собі як технічні, так і організаційні заходи. Використання криптографії, як одного з ключових компонентів такого підходу, може допомогти захистити інформацію від несанкціонованого доступу. Однак кінцевий успіх таких зусиль залежить від одночасного і безумовного застосування всіх необхідних заходів, методів та інструментів.

Ключові слова: *комп'ютерні мережі, несанкціонований доступ, інформаційна безпека, методи та інструменти злому, захист мереж, захист інформації, методи та технології захисту.*

Nikolai VASILENKO, Valeriia SLATVINSKA, Valeriy RACHUK. ANALYSIS OF UNAUTHORIZED ACCESS TO COMPUTER NETWORKS IN THE CONTEXT OF THEIR SECURITY MEASURES

Abstract. *The article analyzes the possibilities and methods of unauthorized access to computer networks in the context of their security measures.*

The purpose of the work *is to analyze the methods and tools of unauthorized access to computer networks and to develop a set of measures to prevent unauthorized access and protect computer networks.*

Methodology. *Analysis of scientific literature on information security of computer networks. Study of regulatory documents on information security. Consideration of the LOZA-1 system as an example of a software and hardware information security system.*

Scientific novelty. *An integrated approach to protecting computer networks from unauthorized access, including technical and organizational measures, has been developed. It is proved that there are two important requirements to ensure the effectiveness of asymmetric cryptosystems. Firstly, the encryption process must be irreversible and completely exclude the possibility of recovering the plaintext from the «public key». Secondly, the secret key derived from the «public key» should be impossible to determine at the current technological level. The author proposes using the LOZA-1 information security system as an example of an integrated approach to protecting computer networks.*

Conclusions. *The security and reliability of cryptographic transformations, as well as the degree of protection they provide, are ultimately determined by the algorithm used for encryption, key size, key generation method, strict adherence to technology and procedures, as well as the proper use of hardware and key management systems. Ensuring the information security of computer networks is an important task for any organization or individual user. Using a comprehensive approach to protection, which includes both technical and organizational measures, can help protect computer systems from cyberattacks.*

Protecting information on computer networks is best achieved through a comprehensive approach that combines both technical and organizational measures. The use of cryptography as one of the key components of such an approach can help protect information from unauthorized access. However, the ultimate success of such efforts depends on the simultaneous and unconditional application of all necessary measures, methods, and tools.

Key words: *computer networks, unauthorized access, information security, hacking methods and tools, network protection, information security, protection methods and technologies.*

Вступ. Постановка проблеми. Постійно важливим завданням залишається питання незаконного доступу до комп'ютерних мереж і розробки заходів для їх захисту, оскільки методи нападу і захисту продовжують вдосконалюватися. При цьому практика експлуатації та розширення комп’ютерних систем ведеться за принципом послідовного приєднання з забезпеченням інформаційної прозорості, коли наявний парк комп’ютерів поєднується мережею, а робочі станції включаються безпосередньо в мережу через комутатори або за допомогою віддаленого доступу. Слід пам’ятати, що усі інформаційні ресурси швидко удосконалюються, залишаючись достатньо вразливою категорією, і при цікавості, що виникає до них з боку несанкціонованого втручання в мережу вони стають ще актуальнішими для дослідників. Більшість сучасних систем обробки інформації є розподіленими, побудованими на стандартних мережевих архітектурних конструкціях, які використовують типові набори мережевих сервісів і прикладного програмного забезпечення. Корпоративні мережі використовують всі традиційні методи несанкціонованого доступу, які властиві локальним обчислювальним системам. Вони також мають свої унікальні шляхи проникнення і таємний доступ до інформації через використання мережевих технологій. Для успішного вирішення проблеми потрібно розглянути різні методи і заходи від несанкціонованого доступу до інформації в комп'ютерних системах, аби вчасно запобігти можливим загрозам. Проблема залишається однією з ключових для безпеки комп’ютерних мереж і кібербезпеки взагалі, і вона є досі актуальною.

Аналіз останніх досліджень і публікацій. З кожним днем зростає кількість інформації, яка обробляється, передається та зберігається в сучасних інформаційно-комунікаційних системах та мережах. Авторами [1] виділено основні недоліки при проєктуванні системи захисту інформації, а саме від несанкціонованих дій користувачів і програм; втрати інформації й порушення працездатності комп'ютерної системи (КС) та адміністративного управління мережею. У роботі [2] розглянуто деякі можливі методи проведення тестування безпеки корпоративної мережі організації на несанкціоноване проникнення, проведено моделювання тестування на несанкціонований доступ до вибраних інформаційних ресурсів та охарактеризовано можливі атаки після здобуття такого доступу. У результаті проведеного тестування виявлено значну кількість вразливостей інформаційних ресурсів. Інформація про вразливості допоможе компаніям визначити поточний рівень захисту їхньої інформаційної системи.

Метою статті є аналіз методів та інструментів несанкціонованого доступу, а також розробка пропозиції комплексу заходів щодо запобігання таким атакам та захисту комп'ютерних мереж.

Виклад основного матеріалу дослідження. Наявні вимоги до документації щодо несанкціонованого доступу в комп’ютерні мережі залишаються загальними для всіх рівнів гарантій [3]. В описі функцій безпеки мають бути викладені основні, необхідні для правильного використання послуг безпеки, принципи політики безпеки, що реалізується комплекс засобів захисту (КЗЗ) оцінюваної комп'ютерної системи (КС), а також самі послуги. Настанови адміністратору щодо послуг безпеки мають містити опис засобів інсталяції, генерації та запуску КС, опис всіх можливих параметрів конфігурації, які можуть використовуватися в процесі інсталяції, генерації і запуску КС, опис властивостей КС, які можуть бути використані для періодичної оцінки правильності функціонування КЗЗ, а також інструкції щодо використання адміністратором послуг безпеки для підтримки політики безпеки, прийнятої в організації, що експлуатує КС. Настанови користувачу щодо послуг безпеки мають містити інструкції щодо використання функцій безпеки звичайним користувачем (не адміністратором). Назва документів (розділів) не регламентується. Опис послуг безпеки може відрізнятися для користувача і адміністратора. Настанови адміністратору і настанови користувачу можуть бути об'єднані в настанови з установлення і експлуатації. В цілому методологічні основи вирішення завдань захисту інформації в комп'ютерних системах і створення нормативних і методологічних документів визначає нормативний документ технічного захисту інформації (НД ТЗІ), який залишається чинним донині [4]. В ньому влучно було зауважено, що істотна частина проблем забезпечення захисту інформації в КС може бути вирішена організаційними заходами. Проте з поширенням інформаційних технологій спостерігається збільшення

необхідності використання технічних засобів і заходів для захисту. Однак, існує одна ключова особливість для відображення суті заходів і методів несанкціонованого доступу в комп'ютерні мережі. Якщо ми припустимо, що комп'ютерна мережа – це просто комп'ютери зі зв'язком між ними так званий інформаційно-технічний комплекс [5], то можна вважати наступне. Існує дві категорії методів захисту інформації у каналі зв'язку.

Перша група являє собою методи, які ґрунтуються на обмежені фізичного доступу до мережі комп'ютерного зв'язку та до апаратури, яка безпосередньо створює цю мережу. Другу групу відтворюють методи, які ґрунтуються на перетворюванні сигналів у мережі до форми, котра унеможливлює для зловмисника сприйняття чи спотворення змісту сигналу, який передається цією комп'ютерною мережею.

Практичний аналіз методів побудови систем захисту інформації вимагає побудови (використання) таких заходів та засобів, щоб гарантовано убезпечити діючу комп'ютерну мережу від будь-якого доступу сторонніх осіб.

Саме такими заходами та засобами по гарантійному розпізнаванню, ідентифікації та автентифікації користувачів, дозволить підвищити ефективність та автоматизацію для гарантованого забезпечення усіх гарантій безпеки та конфіденційності для самої інформації, яка буде циркулювати та зберігатися на комп'ютерах (в автоматизованих системах) [6].

Самі первинні ознаки, що використовуються під час побудови структури комп'ютерних систем, з практичної точки зору, доцільно розглядати та втілювати, при реалізації безпекових систем відповідного рівня необхідних гарантій, починаючи з алгоритмів реалізації розпізнавання автентифікації та ідентифікації користувачів.

До таких задач алгоритмів необхідно включити як механізми так званого «почерку» кожного індивідуального користувача, так і алгоритми гарантованої індикації оновлення (змін) зафіксованих «почерків» користувачів. При цьому бажано звернути увагу на умови зменшення часових затрат під час створення самого зразка «почерку».

Така система захисту інформації від несанкціонованого доступу матиме таку перевагу, котра не буде створювати додаткових незручностей під час роботи за комп'ютером, оскілки не потребуватиме додаткових витрат часу під час проведення ідентифікації.

В реальності методи першої групи мають досить обмежене застосування, тому що на переважній протяжності так звана лінія зв'язку перебуває поза віданням суб'єкта, котрий організує захист. Водночас стосовно апаратури термінала та окремих дільниць мережі, вживання необхідних заходів є необхідним. Обмеження стороннього фізичного доступу припускає винятки та утруднення.

Обов'язково необхідно врахувати не тільки місце, де знаходиться ймовірний зловмисник (тобто де є можливість несанкціонованого втручання та перехоплення), а також і можливість застосовувати інші види втручань (несанкціоновані підключення та перехоплення інформації), спостерігання візуально за безпосередньо самим процесом роботи користувача за комп'ютером (в автоматизованій системі), дії з упередження по виявленню зловмисником наявних та захищених каналів зв'язку у мережі.

Для «фізичних» користувачів, які працюють в так званому «блукаючому» режимі, надзвичайно важко створити режими обмеження доступу, а саме через це необхідно вжити додаткові заходи, з метою безумовного виконання усіх гарантій безпеки.

Для прикладу згадаємо ліцензовану та сертифіковану програмно – апаратну систему захисту інформації «ЛОЗА-1» [7].

Система ЛОЗА-1 виконує такі функції щодо захисту інформації:

– ідентифікація та автентифікація користувачів;

– захист даних на знімних носіях;

– захист даних на рівні папок жорсткого диска;

– захист текстових документів та електронних таблиць;

– контроль цілісності програмного середовища (перевіряється цілісність файлів та папок, розділів та параметрів реєстру, завантажувальних секторів, а також облікових записів Windows);

– реєстрація важливих подій та аудит журналів Windows.

Система ЛОЗА-1 підтримує:

– різні рівні повноважень користувачів та різні рівні конфіденційності інформації (цілком таємно, таємно, для службового користування, відкрита інформація);

– різні ролі користувачів: роль звичайного користувача та декілька адміністративних ролей (адміністратор безпеки, системний адміністратор, адміністратор документів);

– зберігання документів на жорсткому диску та на знімних носіях.

Користувачі системи працюють з текстовими документами та електронними таблицями з використанням звичних засобів Microsoft Word та Microsoft Excel відповідно.

Система надає адміністратору зручні засоби керування та дозволяє формувати довільні протоколи роботи системи.

Згідно з нормативним документом «НД ТЗІ 2.5–004–99. Критерії оцінки захищеності інформації у комп'ютерних системах від несанкціонованого доступу», процес розробки системи відповідає вимогам до рівня гарантій Г-3.

Відповідні дії за напрямом методики другої групи мають намір змінити форму інформації у зворотному напрямку. З тим, що інформація з конфігураціями безпеки («Стандартна безпека» та «Підвищена безпека»), мають змогу також бути переданими по мережі) [8].

Отже, стандартні механізми захисту інформації (цілісність, спостережність, доступність та конфіденційність), з урахуванням шифрування інформації (даних), будуть підкріплені безпосередньо самою технологією криптології.

Сама по собі криптологія об'єднує два напрямки: крипто аналіз та криптографію.

Криптографічне перетворення самої інформації у форму, котра незрозуміла для сторонніх, фактично є надійним та універсальним способом захисту цієї інформації.

Фактично, два основних типи математичних перетворень (перестановка та зміна), котрі лежать в основі криптографічних алгоритмів, дозволяють добитися високої практичної стійкості в захисті інформації.

Тобто класифікувати методи захисту інформації можна наступним чином (рис. 1):

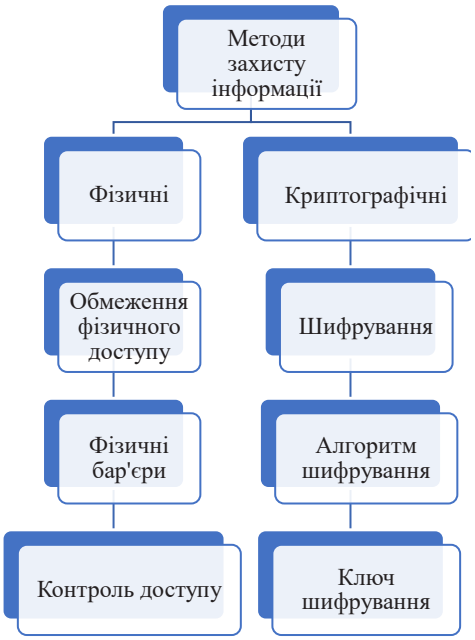

Рис. 1. Класифікація методів захисту інформації (розроблено авторами)

Для гарантування надійного захисту інформації (в асиметричних системах), необхідно дотримуватися двох важливих та очевидних вимог:

1. Перетворення початкового тексту має бути незворотнім і повністю виключати його відновлення на основі «відкритого ключа».

2. Визначення «секретного» ключа, який створено на основі «відкритого ключа», також повинен бути унеможливленим на сучасному технологічному рівні.

Практично криптографічні перетворювання, ступінь захищеності, визначаються лише застосуванням алгоритму шифрування, розмірністю та методом формування ключа, безумовним виконанням технології та правил користування апаратурою та ключовою системою [9, 10].

Будь яка безпека, а також безпека інформації, буде гарантованою тільки при умові одночасного, безперечного, комплексного застосування усіх необхідних заходів, методів та засобів.

Висновки даного дослідження і перспективи подальших розвідок у даному напрямку. Безпека і надійність криптографічних перетворень, а також ступінь захисту, який вони забезпечують, в кінцевому підсумку визначаються алгоритмом, що використовується для шифрування, розміром ключа, методом генерації ключів, суворим дотриманням технології і процедур, а також правильним використанням апаратних засобів і системи управління ключами. Забезпечення інформаційної безпеки

комп'ютерних мереж є важливим завданням для будь-якої організації або окремого користувача. Використання комплексного підходу до захисту, який включає в себе як технічні, так і організаційні заходи, може допомогти захистити комп'ютерні системи від кібератак.

Захист інформації в комп'ютерних мережах найкраще досягається за допомогою комплексного підходу, який поєднує в собі як технічні, так і організаційні заходи. Використання криптографії, як одного з ключових компонентів такого підходу, може допомогти захистити інформацію від несанкціонованого доступу. Однак кінцевий успіх таких зусиль залежить від одночасного і безумовного застосування всіх необхідних заходів, методів та інструментів.

Список використаних джерел:

1. Андрощук О., Коваленко О., Тітова В., Чешун В., Поляков А. Удосконалення систем захисту інформації в комп'ютерних мережах Державної прикордонної служби України. *Військові науки*. 2021. № 2, 3(8). С. 5–21. DOI: https://doi.org/10.32453/3.v85i2-3.828 URL: https://periodica.nadpsu.edu.ua/index.php/military_tech/article/view/828

2. Бойко В., Василенко М., Золотоверх Д. Безпека комп'ютерних систем у контексті законодавства та запобігання кіберзагрозам. *Юридичний вісник*. 2019. № 2. С. 70–76. URL: http://yurvisnyk.in.ua/v2_2019/14.pdf

3. Бурячок В. Л. Технології забезпечення безпеки мережевої інфраструктури. [Підручник] / В.Л. Бурячок, А.О. Аносов, В.В. Семко, В.Ю. Соколов, П.М. Складанний. Київ: КУБГ, 2019. 218 с. URL: https://elibrary.kubg.edu.ua/id/eprint/27191/1/VL_Buriachok_TZBMI.pdf

4. Бутенко Т. А. Сирий В. М. Інформаційні системи та технології : навчальний посібник. Харків: ХНАУ ім. В.В. Докучаєва, 2020. 207 с. URL: https://repo.btu.kharkov.ua/bitstream/123456789/4849/1/INFO_SYSTEMS_20.pdf

5. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. ДСТСЗІ СБ України. Київ. 1999. 21 с. URL: https://tzi.com.ua/downloads/1.1-002-99.pdf

6. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. ДСТСЗІ СБ України. Київ. 1999. 60 с. URL: https://tzi.com.ua/downloads/2.5-004-99.pdf

7. Система захисту інформації ЛОЗА™-1 версія 3.6.0 а. URL: http://avtoprom.kiev.ua/avtoprom/sites/default/files/loza-1_passport.pdf

8. Технології захисту локальних мереж на основі обладнання CISCO: навч. посіб. Т.І. Коробейнікова, С.М. Захарченко. Львів: Видавництво Львівська політехніка, 2021. 232 с. URL: https://ami.lnu.edu.ua/wp-content/uploads/2024/02/Computer-Network-Security.pdf

9. Тишик І. Я. Тестування корпоративної мережі організації на несанкціонований доступ. *Кібербезпека: освіта, наука, техніка*. 2022. № 2 (18), С. 39–46. DOI: https://doi.org/10.28925/2663-4023.2022.18.3948

10. Храпкін О. М. Захист інформаційно-комунікаційної мережі установи від несанкціонованого доступу. *Системи озброєння і військова техніка*. 2020. № 3(63). С. 45–53. DOI: 10.30748/soivt.2020.63.07 URL: https://journal-hnups.com.ua/index.php/soivt/article/view/390