DOI: 10.32347/2412-9933.2024.60.129-135
УДК 004.056

Шкітов Андрій Анатолійович
Аспірант кафедри комп'ютерної інженерії,
https://orcid.org/0009-0005-4600-8467
Відкритий міжнародний університет розвитку людини «Україна», Київ
Кропивницький Дмитро Романович
Кандидат технічних наук, доцент кафедри комп'ютерних систем та мереж,
https://orcid.org/0000-0003-1896-9322
Івано-Франківський національний технічний університет нафти і газу, Івано-Франківськ

СИНТЕЗ ТИПОВИХ АЛГОРИТМІВ ЗАХИСТУ ІНФОРМАЦІЇ В КОРПОРАТИВНИХ МЕРЕЖАХ

Анотація. *У статті розглянуто сучасні підходи до захисту інформації в корпоративних мережах, що включають синтез типових алгоритмів і технологій, спрямованих на підвищення безпеки даних та забезпечення стійкості до зовнішніх і внутрішніх загроз. Особливу увагу приділено криптографічним методам захисту, що охоплюють шифрування даних, цифрові підписи та управління ключами. Розглянуто також системи виявлення та запобігання вторгнень, які дають змогу ідентифікувати підозрілі активності в мережі та вживати заходів для їх нейтралізації. Крім того, розглянуто технології автентифікації та контролю доступу, які забезпечують ідентифікацію користувачів і захищають корпоративну мережу від несанкціонованого доступу. Під час дослідження детально проаналізовано переваги й недоліки кожного з методів з урахуванням таких критеріїв, як ефективність, продуктивність, витрати на впровадження, а також сумісність із різними корпоративними середовищами. Окрему увагу приділено розгляду факторів, що впливають на вибір того чи іншого алгоритму залежно від специфіки корпоративної інфраструктури, таких як масштаб мережі, чутливість даних та наявність ресурсів. На основі проведеного аналізу сформульовано практичні рекомендації для підприємств щодо вибору оптимальних алгоритмів і засобів захисту інформації, які допомагають досягти високого рівня безпеки при мінімальному впливі на загальну продуктивність мережі. Ці рекомендації включають поради щодо комбінування різних методів захисту для забезпечення комплексного підходу, який відповідає сучасним вимогам кібербезпеки і знижує ризики інформаційних втрат або компрометації.*

Ключові слова: захист інформації; корпоративні мережі; криптографія; виявлення вторгнень; запобігання вторгнень; автентифікація; контроль доступу; інформаційна безпека; алгоритми захисту

Вступ

У сучасному світі інформація є однією з найцінніших активів будь-якої організації. Корпоративні мережі містять величезні обсяги даних, які піддаються різноманітним загрозам, таким як несанкціонований доступ, кібератаки, віруси та інші форми шкідливого програмного забезпечення. Захист інформації в корпоративних мережах є надзвичайно важливим для забезпечення безперервної діяльності організацій, захисту конфіденційності даних та збереження репутації.

Злочинці використовують різноманітні методи для несанкціонованого доступу до конфіденційної інформації, що може призвести до значних фінансових втрат, зниження довіри клієнтів та ділових партнерів, а також правових наслідків для організацій:

1. Кібератаки, які стають все більш складними та різноманітними. Вони можуть включати фішингові атаки, DDoS-атаки, атаки з використанням шкідливого ПЗ, та інші форми вторгнення, які можуть значно порушити роботу корпоративних мереж.
2. Несанкціонований доступ, тобто відсутність належного контролю доступу до інформації може призвести до несанкціонованого використання корпоративних даних. Це може бути результатом як зовнішніх атак, так і внутрішніх загроз, таких як дії незадоволених працівників або людські помилки.
3. Витоки даних конфіденційної інформації можуть мати катастрофічні наслідки для організації. Такі інциденти часто призводять до втрати

конкурентних переваг, погіршення репутації та серйозних фінансових збитків.

Саме тому розроблення та впровадження ефективних алгоритмів захисту інформації є ключовими завданнями для забезпечення інформаційної безпеки в корпоративних мережах. Існує безліч підходів та методів захисту, кожен з яких має свої переваги та недоліки. Вибір оптимального набору алгоритмів захисту є складним завданням, яке потребує ретельного аналізу та врахування специфіки конкретного корпоративного середовища.

Ця стаття спрямована на синтез типових алгоритмів захисту інформації, які використовуються в корпоративних мережах, з метою визначення їхньої ефективності та розроблення рекомендацій щодо вибору найкращих підходів для забезпечення максимального рівня захисту інформації при мінімальному впливі на продуктивність мережі.

Аналіз останніх досліджень і публікацій

Останні дослідження у сфері захисту інформації надають цінні знання та рекомендації для покращення кібербезпеки і виявлення вторгнень, що є важливим для подальших наукових досліджень та практичного застосування [1–3].

У роботі " Кібербезпека, керована штучним інтелектом: огляд, моделювання аналізу безпеки та напрямки досліджень " автори А. Могімі, Дж. Віхельманн, Т. Айзенбарт, Б. Сунар оглядають використання штучного інтелекту, зокрема машинного навчання та глибокого навчання, для вирішення сучасних проблем кібербезпеки. Основна увага приділяється моделюванню безпеки та дослідницьким напрямам, що є важливими для створення ефективних систем кіберзахисту.

Наступна робота "Алгоритми класифікації додатків для захисту інформації в Інтернеті: огляд" зосереджується на алгоритмах класифікації додатків, які використовуються для забезпечення інформаційної безпеки. У дослідженні розглядаються різні методи та підходи, що уможливлюють ефективно ідентифікувати та класифікувати додатки для виявлення потенційних загроз.

"Звіт про кібербезпеку 2023" від Check Point Software аналізує основні кіберзагрози та тренди в галузі кібербезпеки за 2022 р. У доповіді розглядаються атаки на хмарні сервіси, хактивізм та використання легітимних інструментів для здійснення атак. Це дослідження дає уявлення про сучасний ландшафт кіберзагроз і допомагає розробити стратегії для захисту від нових типів атак.

Авторами роботи "Опитування систем виявлення вторгнень: методи, набори даних і виклики" є L. A. Дханабал та С. П. Шантараджа, яка надає комплексний аналіз методів та підходів, що використовуються для виявлення вторгнень. Автори розглядають різні набори даних і виклики, з якими стикаються дослідники під час створення ефективних систем виявлення вторгнень.

Представлені дослідження надають сучасні підходи й алгоритми для захисту інформації в корпоративних мережах, що може бути корисним для подальших досліджень та розробок у галузі кібербезпеки. Використання штучного інтелекту, машинного навчання та глибокого навчання дає змогу значно підвищити ефективність систем кіберзахисту та протидіяти сучасним кіберзагрозам.

Мета дослідження

Метою пропонованої статті є дослідження та синтез типових алгоритмів захисту інформації в корпоративних мережах. Вивчення сучасних підходів і методів, що використовуються для забезпечення кібербезпеки, аналізує ефективність різних алгоритмів класифікації додатків та систем виявлення вторгнень, а також основні кіберзагрози і тренди у сфері кібербезпеки в корпоративних мережах за останні роки.

Виклад основного матеріалу

У сучасному світі корпоративні мережі є важливим елементом інфраструктури будь-якої організації [4–6]. З розвитком інформаційних технологій збільшується ризик несанкціонованого доступу до конфіденційної інформації, що підвищує актуальність розроблення та впровадження ефективних алгоритмів захисту даних [7].

Світова статистика засвідчує мільйонну кількість кібератак у корпоративних мережах за останні три роки та мільярдні витрати на боротьбу з ними (табл. 1).

Таблиця 1 – ***Статистика кібератак у корпоративних мережах за останні роки***

Рік	Загальна кількість кібератак	Найпоши-реніші типи атак	Середній викуп за вимагання	Значні інциденти витіку даних
2021	Збільшен-ня на 38%	Фішинг, зловмисне ПЗ, вимагання	$812,380	Marriott-Starwood, витік даних MGM
2022	Збільшен-ня на 38%	Фішинг, соціальна інженерія, DDoS	$1,542,33	ICMR, витік даних Redcliffe Labs
2023	Витік даних 8.2 млрд записів	Вимагання, фішинг, компроме-тація електронної пошти	$1,542,33	23andMe, витік MOVEit Transfer

За останні роки кібератаки на корпоративні мережі значно зросли як за кількістю, так і за складністю. Середня виплата за вимагання зросла з $812,380 у 2022 р. до $1,542,333 у 2023 р. Відновлення після вимагання в середньому коштує близько $2 мільйонів, причому лише 8% компаній, що платять викуп, повертають всі свої дані. На основі цих даних можна зробити висновок, що кібератаки продовжують становити серйозну загрозу для корпоративних мереж, вимагаючи від організацій впровадження комплексних заходів безпеки для захисту своїх систем та даних.

У табл. 2 наведено кількість несанкціонованих доступів у світі в корпоративних мережах за останні роки і понесені витрати на боротьбу з ними.

Таблиця 2 – ***Статистика несанкціонованих доступів в корпоративних мережах за останні п'ять років***

Рік	Кількість несанкціонованих доступів	Середня вартість одного інциденту (USD)	Загальні витрати (USD)
2020	2,000 скарг на день до ФБР	$3.86 млн	$6 трлн
2021	Зростання на 102% атак використанням ransomware порівнянні з 2020 р.	$4.24 млн	$6 трлн
2022	130 порушень безпеки на організацію на рік	$4.35 млн	$7.2 трлн
2023	553 організації, досліджені IBM, зазнали порушень	$4.45 млн	$9.5 трлн
2024	Прогноз на 2024 р.	$4.72 млн	$10.5 трлн

За останні роки кількість несанкціонованих доступів у корпоративних мережах значно зросла. У 2020 р. ФБР отримувало 2000 скарг на день, що свідчить про високу активність кіберзлочинців. Зі збільшенням використання цифрових технологій і віддаленої роботи ця тенденція продовжувала зростати. У 2021 р. відбулося зростання атак з використанням ransomware на 102% порівняно з попереднім роком. Середня вартість одного інциденту постійно зростає. У 2020 р. вона становила $3.86 млн, а до 2023 р. збільшилася до $4.45 млн. Це пояснюється як збільшенням складності атак, так і зростанням витрат на виявлення й усунення наслідків інцидентів. Загальні витрати на боротьбу з кіберзлочинністю також значно зросли, досягнувши $9.5 трлн у 2023 р. і прогнозуються до $10.5 трлн у 2024 р. Це включає витрати на інциденти, інвестиції в безпеку, виплати клієнтам і втрати від репутаційних збитків. Ці дані вказують на необхідність підвищення інвестицій у кібербезпеку і впровадження передових технологій для зменшення ризиків і витрат, пов'язаних з кіберзлочинністю.

Також статистика фіксує витоки даних інформації за останнє п'ятиріччя (табл. 3).

Вся статистика останніх років засвідчує зростаючу тенденцію до різноманітних загроз щодо збереження конфіденційності інформації в корпоративних мережах [8]. Помітно, що витоки даних інформації в корпоративних мережах в останні 2022 та 2023 рр. мають тенденцію до зменшення кількісно та відповідно фінансово, що пов'язано із розвитком і впровадженням різних алгоритмів захисту інформації.

Таблиця 3 – ***Витоки даних інформації в корпоративних мережах останні роки***

Рік	Кількість витоків даних	Кількість записів, що були скомпрометовані (млн)	Фінансові збитки (млрд дол. США)
2019	300	100	3.5
2020	450	150	4.8
2021	620	200	6.0
2022	580	175	5.5
2023	490	0160	4.9

У цій статті розглянуто типові алгоритми захисту інформації, які застосовуються в корпоративних мережах, їхні переваги, недоліки та рекомендації щодо їх використання.

Шифрування даних є одним з найефективніших способів захисту інформації. Воно забезпечує конфіденційність даних, перетворюючи їх у вигляд, що не може бути прочитаним без наявності спеціального ключа. Нижче описано види шифрування даних (рис. 1).

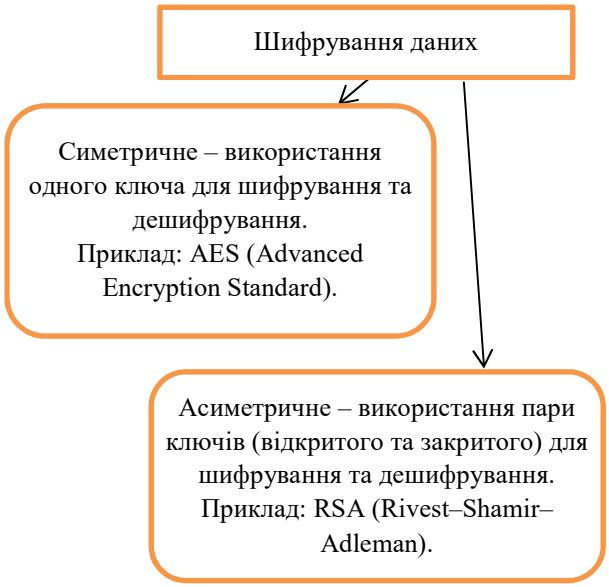

Рисунок 1 – Види шифрування даних

Ці дані допомагають зрозуміти переваги та недоліки кожного алгоритму і зробити обґрунтований вибір залежно від конкретних вимог до безпеки та продуктивності системи. Тож, як бачимо, AES є найбільш універсальним алгоритмом, забезпечуючи високу швидкість шифрування і високу стійкість до атак при використанні ключів різної довжини (128, 192, 256 біт). Він підходить для широкого спектру застосувань, включаючи захист даних у реальному часі (рис.2).

Проведемо порівняння деяких алгоритмів шифрування та їх швидкісних характеристик (табл. 4 та рис. 5).

Таблиця 4 – ***Порівняння алгоритмів шифрування***

Алго-ритм	Тип шифруван-ня	Ключ (біт)	Швид-кість шифру-вання	Стій-кість до атак
AES	Симетрич-ний	128/192/256	Висока	Висока
DES	Симетрич-ний	56	Середня	Низька
RSA	Асиметрич-ний	1024/2048	Низька	Висока
ECC	Асиметрич-ний	256	Висока	Висока
Blow fish	Симетрич-ний	32-448	Висока	Висока

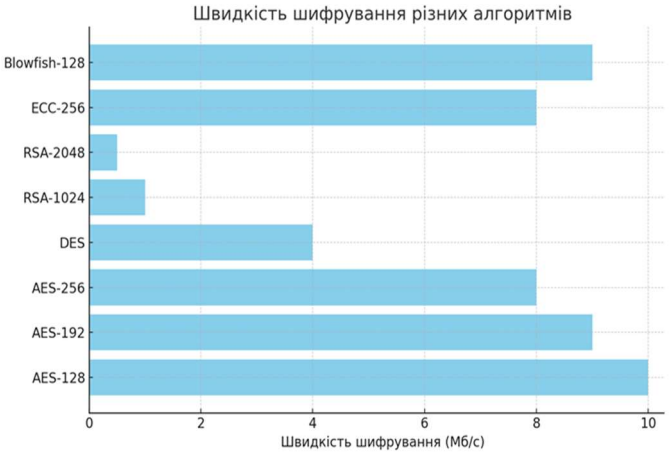

Рисунок 2 – Швидкісні характеристики алгоритмів шифрування

Згідно з даними ефективність шифрування підтверджується тривалим часом його використання та широким застосуванням у різних сферах. Наприклад, компанія ESET пропонує рішення для шифрування даних, яке забезпечує надійний захист файлів, папок, електронної пошти та змінних медіаносіїв. Такі рішення допомагають запобігти витокам даних і забезпечити віддалене управління системами шифрування з будь-якої точки світу.

Системи виявлення вторгнень (IDS) є ключовим компонентом кібербезпеки, які допомагають виявляти та реагувати на підозрілі дії в мережі або на хості. На рис. 3 наведено основні типи виявлення вторгнень [8].

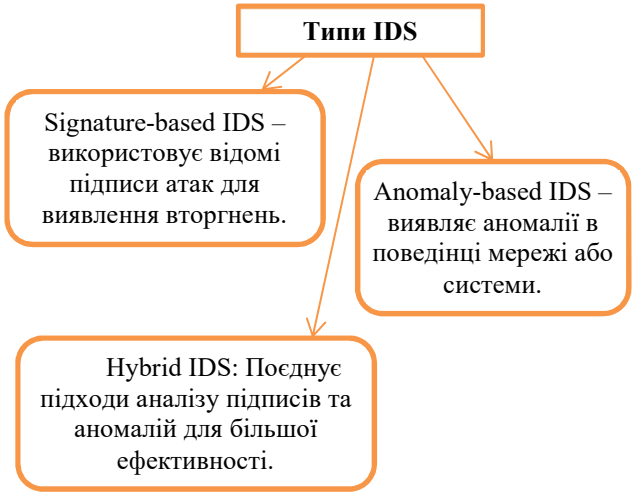

Рисунок 3 – Основні типи виявлення вторгнень

Таблиця 5 – ***Порівняльна характеристика різних алгоритмів IDS***

Параметр	Signature-based IDS	Anomaly-based IDS	Hybrid IDS
Метод виявлення	Аналіз підписів	Виявлення аномалій	Комбінований підхід
Переваги	Висока точність	Виявлення нових атак	Поєднує переваги обох методів
Недоліки	Висока кількість помилкових спрацьовувань	Високий рівень помилкових спрацьовувань	Складність у реалізації та налаштуванні
Приклади використання	Антивірусні програми	Виявлення аномалій у трафіку	Корпоративні мережі

На рис. 4 наведено графік, який порівнює ефективність різних типів IDS за точністю та кількістю помилкових спрацьовувань.

Згідно з аналізом табл.5 та графіка, Signature-based IDS є найкращим вибором захисту інформації від відомих атак через високу точність та низьку кількість помилкових спрацьовувань. Anomaly-based IDS ефективніші для виявлення нових атак, але мають більше помилкових спрацьовувань. Hybrid IDS поєднує обидва підходи, пропонуючи збалансовану ефективність, але складний у реалізації.

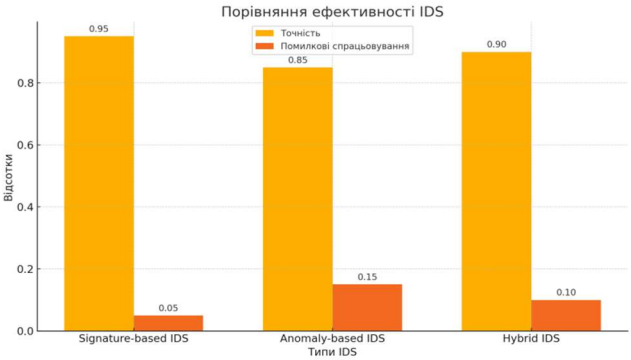

Рисунок 4 – Порівняльна характеристика типів IDS

Контроль доступу, як алгоритм захисту інформації в корпоративних мережах, забезпечує, щоб тільки авторизовані користувачі мали доступ до певних ресурсів [9]. У вигляді табл. 6 зображено основні методи контролю доступу до інформації та характеристику кожного з них.

Таблиця 6 – ***Основні методи контролю доступу до інформації***

№	Метод контролю	Характеристика
1	Мандатний контроль доступу (MAC)	Доступ до ресурсів визначається центральною політикою безпеки
2	Дискреційний контроль доступу (DAC)	Власник ресурсу визначає, хто має доступ до нього
3	Рольовий контроль доступу (RBAC)	Користувачам призначаються ролі, які визначають їхні права доступу

Якщо порівнювати наведені методи контролю доступу, то бачимо, що кожен метод контролю доступу має свої унікальні переваги і недоліки, що робить їх придатними для різних сценаріїв використання (табл. 7).

Таблиця 7 – ***Переваги та недоліки методів контролю доступу***

Метод контролю доступу	Опис	Переваги	Недоліки
ACL	Списки контролю доступу	Проста реалізація	Складно управля-ти
RBAC	Рольова модель контролю доступу	Гнучкість і масштабо-ваність	Склад-ність налашту-вання
ABAC	Атрибутив-ний контроль доступу	Висока гнучкість і точність	Високі вимоги до ресурсів

Отже, ACL підходить для менших або менш складних систем завдяки своїй простоті, RBAC є ефективним у великих організаціях з чітко визначеними ролями, тоді як ABAC пропонує найбільшу гнучкість і точність, але вимагає більше ресурсів і складніше в налаштуванні. Вибір методу контролю доступу має базуватися на конкретних потребах організації, її розмірах, динаміці змін та доступних ресурсах.

1. Аутентифікація й авторизація – це процес перевірки особи користувача, авторизація – процес надання прав доступу до ресурсів [10]. Розрізняють одноразові паролі (OTP), тобто паролі, що дійсні тільки для однієї сесії або транзакції, та двофакторну аутентифікацію (2FA) – комбінує два різних фактори для підвищення безпеки (наприклад, пароль + SMS-код). На рис. 5 наведено графік, який порівнює ці методи за рівнем безпеки, зручністю для користувача та вартістю впровадження.

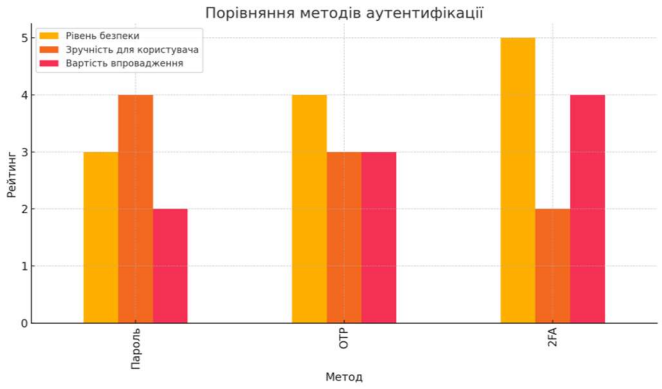

Рисунок 5 – Порівняльна характеристика двох методів аутентифікації

2. На основі аналізу графіка бачимо, що двофакторна аутентифікація (2FA) забезпечує найвищий рівень безпеки, але є менш зручною для користувачів і вимагає більше витрат на впровадження. Одноразові паролі (OTP) мають середній рівень безпеки та зручності, а також середню вартість впровадження. Паролі забезпечують найменшу безпеку, але є найбільш зручними для користувачів і мають низькі витрати на впровадження. Вибір методу аутентифікації залежить від балансу між безпекою, зручністю та витратами, які найбільше відповідають потребам організації.

Висновки

Захист інформації в корпоративних мережах є критично важливим завданням для сучасних організацій. Використання типових алгоритмів, таких як шифрування, системи виявлення вторгнень, контроль доступу й аутентифікація, уможливлює значно підвищити рівень безпеки і захистити

конфіденційні дані від несанкціонованого доступу. Захист інформації в корпоративних мережах є багатогранним завданням, що вимагає комплексного підходу і застосування різноманітних алгоритмів і технологій в поєднанні з додатковими заходами, такими як: резервне копіювання, антивірусний захист, регулярне оновлення програмного забезпечення та навчання співробітників.

Всі ці підходи дають змогу значно підвищити рівень безпеки і захистити конфіденційні дані від несанкціонованого доступу. Дотримання цих принципів є критично важливим для збереження цілісності та конфіденційності інформації, що циркулює в корпоративних мережах.

Список літератури

1. Rabei R. Research on Corporate Protection Systems using Advanced Protection Techniques and Information Security / R. Rabei, M. S. Zearah, A. M. Saleem, S. Q. Al-Tahee, M. K. Abbas // International Conference on Emerging Research in Computational Science (ICERCS). 2023. URL: https://doi.org/10.1109/icercs57948.2023.10433954.

2. Asyaev G., Sokolov A., Ruchay A. Intelligent Algorithms for Event Processing and Decision Making on Information Protection Strategies against Cyberattacks. Mathematics. 2023. URL: https://doi.org/10.3390/math11183939.

3. Tyshyk I. Testing the organization's corporate network for unauthorized access. Cyber security: education, science, technology. 2022. URL: https://doi.org/10.28925/2663-4023.2022.18.3948.

4. Goncharov V. V., Goncharov A. V., Shavrin S. S., Shishova N. A. The Cyber Attack on the Corporate Network Models Theoretical Aspects. Systems of Signals Generating and Processing in the Field of on Board Communications. 2021. URL: https://doi.org/10.1109/IEEECONF51389.2021.9416130.

5. Gruzdeva L. M., Kapustina N., Kobiashvili N. A., Lebedev A. I., Bogonosov K. Complexity Assessment Eliminating the Risk of Transmission of Digital Information in Enterprise Networks. Economic Issues of Social Entrepreneurship. 2021. URL: https://doi.org/10.1007/978-3-030-77291-8_5.

6. Lavrov E. A., Zolkin A. L., Aygumov T. G., Chistyakov M. S., Akhmetov I. V. Analysis of information security issues in corporate computer networks. IOP Conference Series: Materials Science and Engineering. 2021. URL: https://doi.org/10.1088/1757-899X/1047/1/012117.

7. Бардіс Н. Розробка підходу і застосування апарату булевих функцій для аналізу і синтезу ефективних криптографічних алгоритмів захисту інформації. Автореф. дис... канд. техн. наук: 05.13.13. Київ: НТУУ "КПІ". 1998. С. 16.

8. Блінцов В. С., Гальчевський Ю. Л. Математичні основи криптології + CD : Навчальний посібник для студ. вищих навч. закл. Миколаїв: НУК. 2006. 232 с.

9. Гапак О. М., Балога С. І. Захист інформації в комп'ютерних системах: підручник для студ. спец. 123 «комп'ютерна інженерія». Ужгород: ПП "АУТДОР-ШАРК". 2021. 184 с.

10. Бабаш А. В., Шанкін Г. П., Шерстюк В. П., Применко Е. А. Криптографія. Москва : Солон-Р. 2002. С. 511. ISBN 5-93455-135-3.

Стаття надійшла до редколегії 22.10.2024

Shkitov Andrii
PhD student of the Department of Computer Engineering,
https://orcid.org/0009-0005-4600-8467
Open International University of Human Development "Ukraine", Kyiv
Kropyvnytskyi Dmytro
Ph.D. Department of Computer Systems and Networks,
https://orcid.org/0000-0003-1896-9322
Ivano-Frankivsk National Technical University of Oil and Gas, Ivano-Frankivsk

SYNTHESIS OF TYPICAL INFORMATION PROTECTION ALGORITHMS IN CORPORATE NETWORKS

Abstract. *The article examines modern approaches to protecting information in corporate networks, which include the synthesis of typical algorithms and technologies aimed at improving data security and ensuring resistance to external and internal threats. Special attention is paid to cryptographic methods of protection, covering data encryption, digital signatures and key management. Intrusion detection and prevention systems, which allow identifying suspicious activities in the network and taking measures to neutralize them, are also considered. In addition, authentication and access control technologies that ensure user identification and protect the corporate network from unauthorized access are discussed. During the study, the advantages and disadvantages of each method were analyzed in detail, taking into account such criteria as efficiency, productivity, implementation costs, as well as compatibility with various corporate environments. Particular attention is paid to the consideration of factors that influence the choice of one or another algorithm depending on the specifics of the corporate infrastructure, such as the scale of*

the network, the sensitivity of the data, and the availability of resources. On the basis of the conducted analysis, practical recommendations were formulated for enterprises regarding the choice of optimal algorithms and means of information protection, which allow to achieve a high level of security with minimal impact on the overall performance of the network. These guidelines include advice on combining different protection methods to provide a comprehensive approach that meets today's cybersecurity requirements and reduces the risks of information loss or compromise.

Keywords: information security; corporate networks; cryptography; intrusion detection; intrusion prevention; authentication; access control; information security; security algorithms

References

1. Raad, R., Zearah, S. A., Saleem, M., Al-Tahee, A. M., Abbas, S. Q. & Kadhim, M. (2023, December). Research on Corporate Protection Systems using Advanced Protection Techniques and Information Security. In *2023 International Conference on Emerging Research in Computational Science (ICERCS)* (pp. 1–6). IEEE. https://doi.org/10.1109/icercs57948.2023.10433954.
2. Asyaev, G., Sokolov, A. & Ruchay, A. (2023). Intelligent Algorithms for Event Processing and Decision Making on Information Protection Strategies against Cyberattacks. *Mathematics*, 11 (18), 3939. https://doi.org/10.3390/math11183939.
3. Tyshyk, I. (2022). Testing the organization's corporate network for unauthorized access. *Cybersecurity: Education, Science, Technique*, 2 (18), 39–48. https://doi.org/10.28925/2663-4023.2022.18.3948.
4. Goncharov, V. V., Goncharov, A. V., Shavrin, S. S. & Shishova, N. A. (2021, March). The Cyber Attack on the Corporate Network Models Theoretical Aspects. In *2021 Systems of Signals Generating and Processing in the Field of on Board Communications* (pp. 1-4). IEEE. https://doi.org/10.1109/IEEECONF51389.2021.9416130.
5. Gruzdeva, L. M., Kapustina, N. V., Kobiashvili, N. A., Lebedev, I. A. & Bogonosov, K. A. (2021). Complexity Assessment Eliminating the Risk of Transmission of Digital Information in Enterprise Networks. *Economic Issues of Social Entrepreneurship*, 47-59. https://doi.org/10.1007/978-3-030-77291-8_5.
6. Lavrov, E. A., Zolkin, A. L., Aygumov, T. G., Chistyakov, M. S. & Akhmetov, I. V. (2021, February). Analysis of information security issues in corporate computer networks. In *IOP Conference Series: Materials Science and Engineering* (Vol. 1047, No. 1, p. 012117). IOP Publishing. https://doi.org/10.1088/1757-899X/1047/1/012117.
7. Bardis, N. (1998). *Development of the approach and application of the Boolean function apparatus for the analysis and synthesis of effective cryptographic algorithms for information protection* [Doctoral dissertation, KPI]. URL: https://uacademic.info/en/document/0499U000361
8. Blintsov, V. & Halchevskyi Yu. L. (2006). *Mathematical foundations of cryptology + CD: Study guide for students higher education closing.* WITH.
9. Hapak, O. M., Baloga, S. I. (2021). *Information protection in computer systems: a textbook for students. special 123* "*computer engineering*. Uzhgorod: PE «OUTDOR-SHARK»".
10. Babash, A., Shankin, H., Sherstyuk V., Primenko E. (2002). Cryptography. URL: http://nbuv.gov.ua/sites/default/files/msd/0710kry.pdf

---

Посилання на публікацію

APA Shkitov, A. & Kropyvnytskyi, D. (2024). Synthesis of typical information protection algorithms in corporate networks. *Management of Development of Complex Systems*, 60, 129–135, dx.doi.org\10.32347/2412-9933.2024.60.129-135.

ДСТУ Шкітов А. А., Кропивницький Д. Р. Синтез типових алгоритмів захисту інформації в корпоративних мережах. *Управління розвитком складних систем.* Київ, 2024. № 60. С. 129 – 135, dx.doi.org\10.32347/2412-9933.2024.60.129-135.