УДК 621.391
DOI https://doi.org/10.32782/2663-5941/2024.3.2/08

Маруняк С.Т.
Національний університет «Львівська політехніка»

ЗАСТОСУВАННЯ СУЧАСНИХ ПІДХОДІВ ДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖАХ

Сучасне цифрове середовище зумовлює ряд специфічних викликів, поміж яких забезпечення інформаційної безпеки є одним з пріоритетних. Додаткової нагальності даному напрямку надають сучасні технології, що ґрунтуються на інноваційних рішеннях штучного інтелекту, машинного навчання, квантової криптографії. Метою статті є комплексний аналіз сучасних інноваційних підходів до забезпечення інформаційної безпеки в інфокомунікаційних мережах в світлі змін в загально-організаційному контексті (постановка системи захисту, навчання персоналу, імплементація в інші системи організації, оцінка економічної ефективності). Основна увага зосереджена на аналізі поточних викликів та загроз, з якими стикаються інфокомунікаційні системи, і визначенні ефективних стратегій захисту. Описуються найновіші технології та методології, такі як штучний інтелект, машинне навчання, квантова криптографія, які можуть бути інтегровані в системи захисту інфокомунікаційних мереж. Стаття включає детальний огляд новітніх розробок у сфері аналізу безпеки та ідентифікації загроз, з акцентом на адаптивність та прогнозування. Окрема увага приділяється комплексному підходу до захисту інформації, що включає не тільки технологічні засоби, але й організаційні заходи, політики безпеки та освітні ініціативи. Особлива увага приділяється аналізу ефективності, масштабованості та можливості інтеграції в існуючу інфраструктуру. Стаття доповнює існуючий науковий доробок з розвитку інформаційної безпеки, підкреслюючи важливість інноваційного підходу в контексті його імплементації в загально-організаційний контекст і прийняття стейкхолдерами. Запропонована стаття може бути корисною для фахівців у сфері кібербезпеки, розробників мережевих систем, фахових дослідників науковців, організацій, органів державної та місцевої влади. Подальші перспективи дослідження полягають в постановці системи ключових показників ефективності для оцифрування процесу імплементації сучасної системи інформаційної безпеки на загально-організаційному рівні.

Ключові слова: *інформаційна безпека, інфокомунікаційні мережі, штучний інтелект, машинне навчання, криптографія.*

Постановка проблеми. У сучасному цифровізованому середовищі, де обсяги генерованих і оброблюваних даних зростають надто швидко, інформаційна безпека стає ключовим елементом стійкості інфокомунікаційних мереж. Виклики кіберзагрозам, які стрімко змінюються і стають все більш складними, вимагає постійного розвитку інноваційних підходів і технологій в полі інформаційної безпеки в інфокомунікаційних мережах. Відповідно постає нагальне завдання зосередитися на вивченні сучасних інноваційних стратегій та технологій в сфері інформаційної безпеки, які можуть бути застосовані в інфокомунікаційних мережах. Цей комплекс технологій охоплює штучний інтелект, машинне навчання, квантову криптографію, що дозволяє не тільки реагувати на поточні загрози, а й прогнозувати та запобігати майбутнім викликам. Особлива увага має приділятися аналізу того, як ці технології можуть бути інтегровані в існуючі системи інформаційної безпеки, та їх впливу на загальну структуру та ефективність інфокомунікаційних мереж. В даному ключі важливо проаналізувати організаційні аспекти, включаючи політику безпеки та необхідність постійної освіти і тренінгів у галузі кібербезпеки. Все це зумовлює високу актуальність дослідження в даному напрямку.

Аналіз останніх досліджень і публікацій. У науково-практичній сфері інформаційної безпеки в комунікаційних мережах українські та зарубіжні дослідники запропонували різноманітні інноваційні методи та стратегії. Барта Дж. [1] і Шефер [2] підкреслюють вирішальну роль, яку відіграють нові технології та теоретичні основи для захисту комунікаційних мереж. Дані роботи свідчить про те, що швидкий розвиток цифрових загроз вимагає відповідної еволюції технологій і моделей, які ми використовуємо для протидії цим загрозам. Завдяки інтеграції останніх досягнень у технології з надійними теоретичними моделями

стає можливим створювати більш стійкі та безпечні системи. Лі М. [3] та Ель-Кенаві Е. та ін. [4] зміщують акцент на загальну важливість безпеки даних та інформації. Робота Лі М. [3] вивчає різні методології та практики, необхідні для забезпечення конфіденційності, цілісності та доступності даних. Ель-Кенаві Е. та ін. [4] пропонує інтегровану структуру, розроблену для підвищення безпеки в Інтернеті. Ця структура може охоплювати різні аспекти, такі як шифрування, протоколи безпеки мережі та системи виявлення вторгнень, пропонуючи комплексний підхід до захисту інформації в Інтернеті. Фріз та ін. [5] і Алсунбул С. та ін. [6] розглядають більш конкретні проблеми в цій галузі. Фріз С. та ін. [5] зосереджується на ускладненнях безпеки, властивих критично важливій інфраструктурі, які часто стають об'єктами складних кібератак через їх важливість для національної та громадської безпеки. Алсунбул С. та ін. [6], з іншого боку, зосереджується на стратегіях протидії хакерам, що є постійною загрозою цифрового сьогодення. Робота включає аналіз різноманітних методів захисту від злому, таких як розгортання брандмауера, зміцнення системи та проактивне виявлення загроз. Абаваджі та ін. [7] і Ніканфар Г. та ін. [8] підкреслюють необхідність передових технологій безпеки та ефективних рішень у цій галузі, що постійно розвивається. Робота Абаваджі Дж. та ін. [7] визначає ключові тенденцій і технологій, які формуватимуть майбутнє інформаційної безпеки. Ніканфар Г. та ін. [8] пропонує особливе рішення у вигляді криптографічної системи, призначеної для інформаційно-орієнтованої мережі. Ця система зосереджена на захисті даних у своїй основі, підкреслюючи важливість орієнтованих на дані підходів до безпеки в мережі, де інформація є розподіленою та мобільною. Даний масив досліджень підкреслює комплексний характер інформаційної безпеки в мережах зв'язку. Роботи даних зарубіжних вчених охоплюють широку проблематику від розробки нових технологій і теоретичних моделей до впровадження комплексних структур і конкретних рішень, спрямованих на захист цілісності, конфіденційності та доступності інформації.

Становить високу науково-практичну цінність також доробок українських дослідників. Хорошко В., Браіловський М. [9] зосереджується на важливості ефективного управління конфліктами та інцидентами інформаційної безпеки в інтернеті. Автори аналізують сучасні методи та підходи до виявлення, аналізу та вирішення проблем інформаційної безпеки, акцентуючи на важливості адаптивності та гнучкості систем управління інформаційною безпекою. Васильківський М. та ін. [10] вивчають перспективи розвитку телекомунікаційних мереж наступного покоління (6G) і їх впливу на інформаційну безпеку. Автори досліджують нові виклики та можливості, які виникають з розвитком 6G технологій, включаючи питання захисту даних та приватності. Крім того, в іншій роботі Васильківський М. та ін. [11] концентруються на аналізі та оцінці технічних характеристик радіотрактів в системах 5G та 6G. Розглядаються ключові параметри, які впливають на ефективність та надійність інфокомунікаційних систем, а також обговорюють методи їх оптимізації. Робота Конопліцької-Слободенюк О. [12] присвячена одному з найбільш перспективних напрямків в області інформаційної безпеки, а саме квантовій криптографії. Автор розкриває основні принципи та переваги використання квантової криптографії для захисту інформації, включаючи неможливість перехоплення без виявлення та порушення. Особлива увага приділяється технологіям квантового розподілу ключів, які забезпечують високий рівень безпеки в комунікаційних системах.

Ці роботи вносять важливий вклад у розвиток сфери інформаційної безпеки та телекомунікацій, демонструючи різноманітність підходів та технологій, що застосовуються для захисту даних. Від управління інцидентами в інтернет-мережах до передових технологій 6G та квантової криптографії, подані вище попередні дослідження підкреслюють необхідність постійного вдосконалення методів захисту інформації відповідно до зростаючих загроз і викликів. Важливим аспектом, що проходить через всі ці дослідження, є інтеграція новітніх технологічних досягнень у практику інформаційної безпеки. Це включає розвиток інфраструктури телекомунікаційних мереж, оптимізацію параметрів радіотрактів для підвищення ефективності та надійності передачі даних, а також застосування передових криптографічних методів для забезпечення конфіденційності інформації. Розробка та впровадження інноваційних рішень у сфері інформаційної безпеки є ключовим фактором у захисті інформаційних ресурсів в умовах постійно змінюваного цифрового середовища. При цьому, додаткового вивчення потребує питання структурування комплексу заходів в контексті сучасних технологій і їх впливу на зміну загально-організаційного контексту постановки системи інформаційної безпеки.

Постановка завдання. Мета статті – ідентифікувати основні напрямки інноваційних розробок на основі аналізу найновіших розробок у сфері інформаційної безпеки, які зможуть забезпечити більш безпечне та надійне інформаційне середовище в умовах швидко змінюваних кіберзагроз.

Виклад основного матеріалу. Станом на 2024 р. сучасний контекст кібербезпеки визначався комплексом тенденцій, значною мірою сформованим зміною природи кіберзагроз і впровадженням нових технологій. Однією з головних сфер уваги є, зокрема, хмарна безпека. У міру того, як організації все частіше переходять на хмарні сервіси, стає все більш зрозумілою недостатність стандартних заходів безпеки в хмарних сервісах. Ця прогалина створила сприятливий ґрунт для кіберзагроз, що потребує більш надійних протоколів безпеки для захисту конфіденційних даних, що зберігаються в хмарі. Помітною тенденцією у сфері кібербезпеки є зростаюча залежність від технологій штучного інтелекту та машинного навчання. Ці інноваційні інструменти розгортаються для більш ефективного виявлення та протидії кіберзагрозам, що є значним кроком у боротьбі з кіберзлочинністю. На ринку інформаційної безпеки відбулися значні зміни, спричинені підвищенням обізнаності організацій про кіберризики. Опитування Hiscox [13] показало, що 64 % компаній з 8 країн світу застосовують такий інструмент як страхування від кіберзагроз, що відображає все більше визнання кіберзагроз як критичного фактора ризику. Індекс глобального страхового ринку Marsh & McLennan [14] показав стрімке зростання цін на кіберстрахування в США на 79 % у 2022 р., що підкреслює різкий ріст витрат, пов'язаних з кіберінцидентами. Перехід до гібридних робочих середовищ спричинив появу нових викликів кібербезпеки. Дані Microsoft [15] показали, що 81 % корпоративних організацій переходять до гібридної моделі робочого місця, що призвело до розширення поверхні атаки для кіберзагроз. Цей зсув вимагає комплексної переоцінки протоколів безпеки, щоб захистити активи організації в більш складному робочому середовищі. Все це зумовлює сучасний контекст інформаційної безпеки та потребу в інноваційних рішеннях в даному полі.

Інноваційні підходи до забезпечення інформаційної безпеки в інфокомунікаційних мережах включають різноманітні технології та стратегії, спрямовані на захист даних та інформаційних систем від несанкціонованого доступу, зловмисного втручання або інших загроз. Виділимо ключові

Рис. 1. Ключові напрямки інноваційних підходів до забезпечення інформаційної безпеки в інфокомунікаційних мережах

Джерело: власний аналіз

напрямки інноваційних підходів до забезпечення інформаційної безпеки в інфокомунікаційних мережах (рис. 1).

Розглянемо дані напрямки в більших деталях:

– *Квантова криптографія*: дана технологія, перебуваючи на ранніх стадіях розвитку, має потенціал створити надвисокий рівень шифрування за рахунок використання підходів спряженого кодування, що робить практично неможливим перехоплення або втручання в передачу даних без виявлення.

– *Рішення на основі штучного інтелекту (ШІ) та машинного навчання*: Розвиток ШІ і машинного навчання дозволяє створювати системи, здатні аналізувати поведінку мережі в реальному часі, виявляти аномалії, що можуть вказувати на кібератаки, та автоматично адаптуватися до нових загроз. В даному контексті, наприклад, застосування технології блокчейн може забезпечити високий рівень безпеки через децентралізацію, неможливість зміни записів без відома всієї мережі та прозорість транзакцій, що робить дані стійкими до фальсифікацій та несанкціонованого доступу.

– *Розширене виявлення та реагування (Endpoint Detection and Response, EDR)*: Системи EDR надають засоби для моніторингу та аналізу даних про події на кінцевих точках у мережі в реальному часі, що дозволяє швидко виявляти та реагувати на потенційні загрози.

– *Захищені протоколи інтернету (IPv6, DNSSEC)*: Впровадження нових версій протоколів інтернету з підвищеною безпекою, таких як IPv6 та DNSSEC, забезпечує кращий захист від різноманітних атак, включаючи атаки на DNS.

– *Автоматизація безпеки в рамках єдиної платформи*: Інтеграція різних інструментів безпеки в єдину платформу для автоматизації рутинних задач і координації відповідей на інциденти забезпечує швидше виявлення та мінімізацію наслідків атак.

– *Інтелектуальне розпізнавання загроз*: Розвиток систем інтелектуального розпізнавання загроз, які можуть аналізувати великі обсяги даних для ідентифікації складних і непомітних атак, забезпечуючи більш ефективний захист.

Ці інноваційні підходи є частиною безперервного процесу вдосконалення інформаційної безпеки, який має пристосовуватися до постійно змінюваного ландшафту кіберзагроз. Важливо зазначити, що ефективна стратегія інформаційної безпеки зазвичай включає комбінацію кількох підходів і технологій, щоб забезпечити всебічний захист.

Аналіз сучасних методів забезпечення інформаційної безпеки вимагає розгляду широкого спектру технологій, стратегій та практик, які застосовуються для захисту інформаційних систем і даних від несанкціонованого доступу, втрати або пошкодження. Сучасні методи можна класифікувати на кілька основних категорій, що подано в Табл. 1.

Оцінка успішності технологій та стратегій в контексті інформаційної безпеки є ключовим аспектом для забезпечення ефективного захисту інформаційних активів організації. Для цього використовуються різні критерії, які дозволяють оцінити ефективність заходів безпеки, їх відповідність бізнес-вимогам та здатність протистояти актуальним та потенційним загрозам. Виділимо ряд ключових критеріїв для оцінки:

1. Зменшення кількості інцидентів безпеки:

– *Кількість виявлених вразливостей*: Зменшення кількості вразливостей, виявлених під час регулярних аудитів та сканувань безпеки.

– *Кількість успішних атак*: Зниження кількості успішних кібератак або інцидентів безпеки, що свідчить про ефективність захисних механізмів.

2. Відповідність нормативним вимогам:

– *Аудит та сертифікація*: Успішне проходження зовнішніх аудитів та отримання сертифікацій (наприклад, ISO 27001), що підтверджують відповідність організації встановленим стандартам безпеки.

– *Дотримання законодавчих вимог*: Виконання законодавчих та регуляторних вимог, наприклад GDPR, HIPAA, що знижує ризик правових санкцій та штрафів.

3. Час виявлення та реагування на інциденти:

– *Час до виявлення (Time to Detect, TTD)*: Зменшення часу, необхідного для ідентифікації безпекового інциденту або вразливості. Швидке виявлення є критичним для мінімізації потенційної шкоди.

– *Час до реагування (Time to Respond, TTR)*: Зменшення часу, необхідного для реагування на інцидент безпеки або загрозу. Ефективне реагування обмежує вплив інцидентів та допомагає у відновленні операцій.

Таблиця 1

Сучасні методи забезпечення інформаційної безпеки в інфокомунікаційних мережах

Методи	Коментарі
Технологічні засоби	– Шифрування: Використання алгоритмів шифрування для захисту даних під час їх зберігання та передачі. Це включає шифрування даних на диску та шифрування каналів зв'язку. – Мережева безпека: Застосування брандмауерів, систем виявлення та запобігання вторгненням (IDS/IPS), віртуальних приватних мереж (VPN) та інших інструментів для захисту мережевого трафіку. – Аутентифікація та контроль доступу: Використання багатофакторної аутентифікації, розподілених систем управління ідентифікаційними даними, політик мінімальних прав та інших методів для забезпечення доступу тільки авторизованим користувачам.
Аналітичні інструменти	– Моніторинг та аналіз: Використання сучасних інструментів для постійного моніторингу інформаційних систем і аналізу подій безпеки, щоб виявляти та реагувати на потенційні загрози в реальному часі. – Прогнозування загроз: Застосування штучного інтелекту та машинного навчання для аналізу даних та прогнозування потенційних атак або вразливостей.
Організаційні заходи	– Політики безпеки: Розробка та впровадження комплексних політик інформаційної безпеки, які визначають правила та процедури для захисту даних. – Освітні заходи: Проведення тренінгів з безпеки для співробітників для підвищення обізнаності про потенційні загрози та методи їх запобігання. – Управління інцидентами: Розробка процесів для ефективного реагування на інциденти безпеки, мінімізації шкоди та відновлення послуг.

Джерело: власний аналіз

4. Ефективність процесу відновлення:

– *Час до відновлення (Time to Recover, TTR)*: Зменшення часу, потрібного для відновлення послуг або систем до нормального функціонування після інциденту. Швидке відновлення важливе для забезпечення неперервності бізнесу.

– *Втрати даних*: Мінімізація втрат даних у випадку інцидентів безпеки, що забезпечує збереження цінної інформації та довіри клієнтів.

5. Економічна ефективність заходів:

– *Загальні витрати на інформаційну безпеку (Return on Investment)*: Оцінка витрат на інформаційну безпеку відносно бюджету організації та аналіз повернення інвестицій (ROI) в безпеку: Важливо, щоб витрати були виправдані зниженням ризиків і потенційних втрат від інцидентів.

– *Ефективність інвестицій у безпеку (Security Investment Efficiency)*: Аналіз, наскільки ефективно використовуються інвестиції в інструменти та заходи безпеки для досягнення цілей організації у сфері безпеки.

6. Задоволеність користувачів та бізнесу:

– *Задоволеність бізнес-користувачів*: Оцінка того, наскільки задоволені користувачі та бізнес-відділи впровадженими заходами безпеки, чи не викликають вони незручностей у роботі та чи сприяють вони досягненню бізнес-цілей.

– *Сприйняття безпеки серед співробітників*: Позитивне сприйняття політик та процедур безпеки співробітниками, а також їхня обізнаність і розуміння важливості заходів безпеки для загальної безпеки організації.

7. Гнучкість та масштабованість:

– *Адаптивність до змін у загрозах*: Здатність системи безпеки адаптуватися до нових загроз та змін у ландшафті кіберзагроз без значних додаткових витрат або переробок.

– *Масштабованість*: Можливість безпекових рішень масштабуватися відповідно до зростання організації та змін у її інфраструктурі, без компромісів у рівні безпеки.

Відповідно даний комплекс критеріїв має бути систематизований, пріоритезований та інтегрований в загально-організаційну систему інформаційної безпеки. Критично важливим є інформування стейкхолдерів (співробітники, керівники підрозділів, клієнти, бізнес-партнери, інші) про дані критерії для їх прийняття та дієвого застосування.

Висновки. В підсумку, в запропонованому дослідженні акцентовано на критичній необхідності впровадження інноваційних підходів для зміцнення захисту інформаційних систем. В умовах стрімкого розвитку технологій та розширення кіберзагроз, традиційні методи інформаційної безпеки вже не здатні забезпечити достатній рівень захисту. Відповідно для ефективного протистояння сучасним викликам, важливо не лише використовувати новітні технології, такі як машинне навчання, штучний інтелект та вдосконалювати існуючі моделі інформаційної безпеки. Таке рішення передбачає інтеграцію комплексних рішень, які здатні адаптуватися до змін у кіберпросторі та ефективно реагувати на нові загрози. Ключовим критерієм є здатність інноваційних підходів ефективно протистояти сучасним і потенційним кіберзагрозам. Аналіз показав, що впровадження технологій штучного інтелекту, машинного навчання, квантової криптографії може значно підвищити рівень безпеки за рахунок автоматизації процесів виявлення та нейтралізації атак. Важливим аспектом є здатність системи швидко адаптуватися до змінних умов кіберпростору та розширення загроз. Інноваційні моделі, що базуються на самонавчальних алгоритмах, демонструють високий рівень адаптивності. Інноваційні підходи мають забезпечувати високий рівень прозорості у виявленні та реагуванні на загрози, дозволяючи здійснювати контроль і аудит безпеки на всіх рівнях. Оцінка економічної ефективності впровадження інноваційних підходів є важливим критерієм, оскільки ресурси організацій є обмеженими. Технології, що пропонують оптимальне співвідношення ціни та якості захисту, набувають пріоритету. Майбутні дослідження полягають в розробленні ключових показників ефективності для оцифрування процесу імплементації сучасної системи інформаційної безпеки на загально-організаційному рівні.

Список літератури:

1. Bárta J., Sadovská V., Srník A., Urbánek J. Protection of information and communication systems. *ISESS 2013: Environmental Software Systems. Fostering Information Sharing*. 2013. № 413. P. 302–310.

2. Schaefer R.F., Boche H., Khisti A., Poor H.V. Information theoretic security and privacy of information systems. *Cambridge University Press eBooks*. 2017. 558 p.

3. Li M. Data and Information Security Technology in network communication. *Journal of Networking and Telecommunications*. 2020. № 2 (2). P. 38–41.

4. El-Kenawy E., Saber M., Arnous R. An integrated framework to ensure information security over the Internet. *International Journal of Computer Applications*. 2019. № 178 (29). P. 13–15.

5. Fries S., Falk R. Ensuring Secure Communication in Critical Infrastructures. *ENERGY 2016: The Sixth International Conference on Smart Grids, Green Communications and IT Energy-aware Technologies*. 2016. P. 15–20.

6. Alsunbul S., Le P.D., Tan J. A Defense Security Approach for Infrastructures against Hacking. *2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*. 2013. P. 1600–1606.

7. Abawajy J., Islam, R. Applications and techniques in information and network security. *Concurrency and Computation: Practice and Experience*. 2017. № 29 (23). P. 1–4.

8. Nicanfar H., Talebi-Fard P., Zhu C., Leung V.C. Efficient Security Solution for Information-centric Networking. *2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing*. 2013. P. 1290–1295.

9. Хорошко В., Браіловський М. Управління конфліктами та інцидентами інформаційної безпеки в мережі Internet. *Інформатика та математичні методи в моделюванні*. 2021. № 11 (1–2). С. 15–25.

10. Васильківський М., Будаш М., Болдирева О. Забезпечення інформаційного захисту в телекомунікаційних мережах 6G. *Комп'ютерно-інтегровані технології: освіта, наука, виробництво*. 2023. № 50. С. 142–150.

11. Васильківський М., Коломієць А., Будаш М Оцінювання параметрів радіотрактів інфокомунікаційних систем 5G/6G. *Вісник Хмельницького національного університету*. 2022. № 6. С. 53–60.

12. Конопліцька-Слободенюк О. Принципи захисту інформації за допомогою квантової криптографії. *Всеукраїнська науково-практична конференція «Інформаційна безпека держави, суспільства та особистості»*. 16 квітня 2015 року, м. Кіровоград: КНТУ, 2015. С. 58–59.

13. Hiscox Cyber insurance. URL: https://www.hiscox.co.uk/business-insurance/cyber-and-data-insurance (дата доступу: 01.02.2024).

14. Marsh & McLennan Cyber Risk. URL: https://www.marsh.com/pt/en/services/cyber-risk.html (Дата доступу: 01.02.2024).

15. Microsoft. URL: https://www.microsoft.com/en-us/worklab/work-trend-index/hybrid-work-is-just-work (дата доступу: 01.02.2024).

Maruniak S.T. APPLICATION OF MODERN APPROACHES TO INFORMATION SECURITY IN INFOCOMMUNICATION NETWORKS

The modern digital environment poses a number of specific challenges, among which information security is one of the priorities. Modern technologies based on innovative solutions of artificial intelligence, machine learning, and quantum cryptography add additional urgency to this area. The purpose of the article is to provide a comprehensive analysis of modern innovative approaches to ensuring information security in information and communication networks in the light of changes in the overall organizational context (setting up a protection system, training of personnel, implementation in other organizational systems, and assessment of economic efficiency). The main focus is on analyzing current challenges and threats faced by information and communication systems and identifying effective protection strategies. It describes the latest technologies and methodologies, such as artificial intelligence, machine learning, quantum cryptography, which can be integrated into the protection systems of infocommunication networks. The article includes a detailed overview of the latest developments in security analysis and threat identification, with a focus on adaptability and forecasting. Particular attention is paid to an integrated approach to information security, which includes not only technological means, but also organizational measures, security policies and educational initiatives. Particular attention is paid to the analysis of efficiency, scalability, and the possibility of integration into existing infrastructure. The article adds to the existing scientific work on the development of information security, emphasizing the importance of an innovative approach in the context of its implementation in the overall organizational context and acceptance by stakeholders. The proposed article may be useful for cybersecurity specialists, network system developers, professional researchers, scientists, organizations, state and local authorities. Further prospects for research are to set up a system of key performance indicators to digitize the process of implementing a modern information security system at the general organizational level.

Key words: *information security, information and communication networks, artificial intelligence, machine learning, cryptography.*