Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Інститут цифровізації освіти НАПН України
Національний технічний університет України
«Київський політехнічний інститут» ім. І. Сікорського
Вінницький національний технічний університет
Житомирський військовий інститут імені С.П. Корольова
Тернопільський національний технічний університет імені Івана Пулюя
Харківський національний університет радіоелектроніки
Уманський державний педагогічний університет імені Павла Тичини
Національний університет біоресурсів і природокористування України
Інститут геохімії навколишнього середовища НАН України
Черкаський державний технологічний університет
Державний університет «Київський авіаційний інститут»

Комп'ютерні технології: інновації, проблеми, рішення

Тези доповідей VIII Всеукраїнської науково-технічної конференції

м. Житомир, 02-03 грудня 2025 р.

2025

УДК 327.56:004.056.5

Зеленчук А.Р., здобувач,
Ткачук Р.Л., д.т.н., професор,
Федина Б.І., к.т.н., доцент
Львівський державний університет безпеки життєдіяльності

ІНФОРМАЦІЙНА БЕЗПЕКА В СИСТЕМІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ДЕРЖАВИ

Інформація у сучасному суспільстві є ключовим ресурсом розвитку економіки, науки та технологій, використовується для управління процесами та міжособистісної взаємодії, а її цінність визначається достовірністю, корисністю та доступністю. На макрорівні вона забезпечує державну потугу, ефективне управління економікою та оборонними системами, на мікрорівні – ефективність діяльності підприємств і органів влади.

Інформаційна безпека як складова національної безпеки забезпечує захист даних та інфраструктури, охоплюючи доступність, цілісність і конфіденційність інформації, і стосується захисту інтересів держави, особистості та суспільства, запобігаючи маніпуляціям, дезінформації та інформаційно-психологічним впливам.

Основні загрози інформаційній безпеці виникають як внутрішні (недосконаліть правової системи, низька інформаційна культура, внутрішні комп'ютерні злочини), так і зовнішні (політичний та економічний тиск, діяльність іноземних спецслужб, міжнародний кібертероризм). Вони включають неякісну або фальшиву інформацію, несанкціонований доступ, відмови технічних засобів і порушення прав на інформацію. Особливе значення має кібертероризм, що швидко адаптується до нових технологій, а його транснаціональний характер ускладнює контроль.

Для підвищення рівня інформаційної безпеки (ІБ) держави, суспільства та окремих організацій рекомендується комплексний підхід, який включає наступні напрямки:

Технічні заходи – передбачають впровадження систем виявлення і запобігання вторгнень (IDS/IPS), багатофакторної автентифікації (MFA), розширеного шифрування даних, систем контролю мобільних пристроїв та захисту електронної пошти. Ці засоби дозволяють запобігти несанкціонованому доступу, зберегти цілісність інформації та забезпечити надійність функціонування інформаційної інфраструктури.

Інноваційні підходи – включають застосування штучного інтелекту (ШІ) та методів машинного навчання для прогнозування загроз, виявлення аномалій у великих масивах даних та автоматичного

реагування на інциденти. Використання таких технологій підвищує швидкість і ефективність захисту інформаційних систем у динамічному кіберпросторі.

Організаційні заходи – полягають у підготовці та навчанні персоналу, розмежуванні доступу за принципом мінімальних привілеїв, регулярних тренуваннях із кібербезпеки, а також розробці внутрішніх політик і процедур реагування на інциденти. Ці заходи забезпечують підвищення культури інформаційної безпеки і мінімізацію людського фактору як джерела ризиків.

Криптографічний захист та блокчейн – включає використання сучасних криптографічних алгоритмів і технології блокчейн для забезпечення цілісності, достовірності та незмінності даних. Технологія блокчейн підвищує надійність фінансових транзакцій та зберігання інформаційних ресурсів, запобігає маніпуляціям і несанкціонованим змінам, забезпечуючи прозорість та контроль за потоками даних.

Міжнародна співпраця – передбачає інтеграцію у глобальні системи забезпечення інформаційної безпеки, обмін інформацією про загрози та інциденти, координацію спільних заходів із запобігання кібератакам і протидії транснаціональним інформаційним загрозам. Це дозволяє країні не лише захистити власні ресурси, а й підвищити ефективність міжнародних механізмів реагування на глобальні виклики.

Таким чином, інформаційна безпека є багатогранним процесом управління загрозами, що включає технічні, організаційні, правові та інноваційні складові. Забезпечення ІБ вимагає системного підходу, де поєднуються сучасні технології, нормативно-правова база, організаційні заходи та міжнародна кооперація, що гарантує стабільність, надійність і розвиток інформаційного простору держави.

Список використаних джерел:

1. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про Стратегію забезпечення державної безпеки» : Указ Президента України. від 16.02.2022 року № 56/2022. URL: https://zakon.rada.gov.ua/laws/show/56/2022#Text

2. Івануса А. І., Ткачук Р. Л., Брич Т. Б. Удосконалення методів управління процесами інформаційної безпеки. Сектор безпеки і оборони України на захисті національних інтересів: актуальні проблеми та завдання в умовах воєнного стану : матеріали ІІІ Міжнародної науково-практичної конференції (Хмельницьк, 21 листопада 2024 р.). Хмельницький: НАДПСУ, 2024. С. 1136–1138.