https://www.proconference.org/index.php/usc/article/view/usc27-00-008
DOI: 10.30888/2709-2267.2024-27-00-008

УДК 371.135:81

INFORMATION SECURITY: FEATURES OF CHANGES IN TODAY'S DIGITAL WORLD

ІНФОРМАЦІЙНА БЕЗПЕКА: ОСОБЛИВОСТІ ЗМІН У СУЧАСНОМУ ЦИФРОВОМУ СВІТІ

Prygodiuk O.M./ Пригодюк О.М.
PhD, Associate professor/ к.е.н., доцент
ORCID: 0000-0002-4706-391X
Parnikov I. Ye./ Парніков І.Є.
Postgraduate student/ аспірант
ORCID: 0009-0001-4598-0108
Cherkasy State Technological University, Cherkasy, Shevchenko 460, 18006
Черкаський державний технологічний університет, Черкаси, Шевченко 460, 18006

Анотація. *В роботі розглядаються актуальні аспекти інформаційної безпеки в умовах цифровізації суспільства. З розвитком інформаційних технологій та глобалізацією кіберпростору зростають ризики, зокрема кіберзагрози, інформаційні війни, витоки конфіденційних даних та атаки на критичну інфраструктуру. Особливу увагу приділено аналізу еволюції загроз та сучасним підходам до їх запобігання, зокрема концепції «нульової довіри», автоматизації захисту, використанню штучного інтелекту й поширенню культури кібергігієни. Наголошено на необхідності розвитку міжнародної співпраці та вдосконалення законодавчої бази для протидії міждержавним кібератакам, розширення управлінського забезпечення та протидії ризикам. Також розглянуто роль соціальних мереж у поширенні дезінформації та інструменти штучного інтелекту, які можуть ефективно боротися з кіберзагрозами. У висновках акцентується увага на важливості інтеграції новітніх технологій, адаптації управлінських підходів і розробки глобальних ініціатив для забезпечення надійного захисту даних у цифровому світі.*

Ключові слова: *інформаційна безпека, цифровізація, кіберзагроза, захист даних, інформаційна війна.*

Abstract. *The work examines current aspects of information security in the conditions of digitalization of society. With the development of information technology and the globalization of cyberspace, risks are increasing, including cyber threats, information wars, leaks of confidential data and attacks on critical infrastructure. Special attention is paid to the analysis of the evolution of threats and modern approaches to their prevention, in particular the concept of «zero trust», automation of protection, the use of artificial intelligence and the spread of cyber hygiene culture. The need to develop international cooperation and improve the legislative framework for countering interstate cyber attacks, expanding management support and countering risks was emphasized. The role of social networks in spreading misinformation and artificial intelligence tools that can effectively combat cyber threats are also discussed. The conclusions emphasize the importance of integrating the latest technologies, adapting management approaches and developing global initiatives to ensure reliable data protection in the digital world.*

Key words: *information security, digitalization, cyber threat, data protection, information war.*

Вступ. Інформаційна безпека насьогодні є одним з ключових аспектів техніко-технологічного, управлінського захисту діяльності підприємств, будь-якої організації та держави, оскільки інформація має стратегічне значення. З

розвитком цифрових технологій, відповідно зростають і ризики, зокрема кібератаки, відбуваються втрати конфіденційних даних, пошкодження соціальної та критичної інфраструктури. Проблема забезпечення інформаційної безпеки стає актуальною не лише на рівні технічного захисту, формування цільової політики підприємств, але й на рівні державної регуляторної політики.

Мета дослідження: проаналізувати особливості змін інформаційної безпеки та визначити основні виклики й перспективи для захисту даних у сучасному цифровому світі.

Основний текст.

В умовах цифровізації та глобального поширення інформаційних технологій ризики для інформаційної безпеки набувають нових різноманітних форм та значних масштабів. Традиційні загрози, проблеми менеджменту, такі як несанкціонований доступ і шкідливе програмне забезпечення, еволюціонують разом із сучасними технологіями, створюючи нові виклики, з якими зіштовхуються державні установи, бізнес спільноти, менеджмент та звичайні користувачі. Основні виклики сучасної інформаційної безпеки пов’язані з кіберзагрозами, інформаційними війнами та зростанням вимог до конфіденційності даних. З розвитком інноваційних технологій кіберзагрози стають дедалі більш складними, витонченими й масштабними (рисунок 1).

З розвитком інформаційних технологій виникли нові загрози, серед яких особливе місце посідають інформаційні війни, що є новим викликом сучасності. Ці війни спрямовані на маніпулювання інформацією з метою досягнення політичних, економічних, управлінських або соціальних переваг, що робить їх одним із найсерйозніших викликів для держав, організацій, бізнесу та громадян. У сучасному світі інформаційні війни стають невід’ємною частиною гібридних конфліктів та маніпуляцій даних. Інформаційна зброя націлена на деморалізацію, дезінформацію та маніпуляцію громадською думкою. Основними аспектами інформаційних війн є: поширення дезінформації, маніпуляція суспільної думки, знищення глобальних інформаційних мереж та ін [1].

Рисунок 1 – Групування кіберзагроз в сучасному цифровому світі, що мають найбільшу впливовість на управлінські системи

Авторська розробка

У часи політичної нестабільності чи криз поширення фейкових новин або дезінформації є основним інструментом для маніпулювання масовою свідомістю. Такі підходи можуть використовувати соціальні мережі для поширення недостовірної інформації, завдаючи шкоди репутації компаній, іміджу лідерів іт-сектору, організацій або навіть державі. Використовуючи аналітику великих даних та алгоритми штучного інтелекту створюють точні й таргетовані повідомлення, які впливають на конкретні групи людей, маніпулюючи їхніми поглядами та емоціями. Використання сучасних ботів призводить до масового поширення інформації. Бот видає себе за реальних користувачів у соціальних мережах, що створює ілюзію громадської думки та залучає до обговорень широкі верстви населення, маніпулюючи настроями та

прийняттям рішень [2].

Розвиток технологій і зростання кіберзагроз змушує фахівців з інформаційної безпеки постійно вдосконалювати підходи до захисту даних. Класичні методи, зосереджені на захисті периметра мережі та статичних паролях, поступово замінюються новітніми концепціями, що передбачають гнучкішу та більш адаптивну безпеку. Основні зміни в підходах до інформаційної безпеки включають концепцію «нульової довіри», автоматизацію засобів захисту, персоналізацію та інтеграцію багаторівневих стратегій протидії сучасним загрозам.

Концепція «нульової довіри» відображає новий підхід до безпеки, що відкидає припущення про «безпечний внутрішній периметр» і підходить до кожної дії як до потенційної загрози. Основні аспекти якої є: аутентифікація на кожному етапі доступу, незалежно від місцезнаходження користувача або пристрою; контроль доступу на основі найменшої необхідності, що обмежує доступ лише до тих ресурсів, які користувачеві або системі дійсно необхідні, а, в подальшому це мінімізує ризики потенційного зловживання правами доступу в разі компрометації облікового запису; відстеження поведінки користувачів і мережевих пристроїв, виявляючи аномальні дії, що можуть свідчити про несанкціоновану діяльність, дозволяючи в подальшому виявляти загрози навіть після того, як зловмисник отримав доступ до системи [3].

З огляду на величезний обсяг даних, що потребують захисту, та швидкість, з якою з’являються нові загрози, важливим елементом сучасної інформаційної безпеки є автоматизація. Основні напрямки якої є автоматизовані системи виявлення загроз, автоматизація реагування на інциденти, оркестрація безпеки.

Автоматизовані системи виявлення загроз пришвидшують момент виявлення загрози. Використання штучного інтелекту та машинно-автоматизованого навчання дозволяють автоматизувати виявлення аномальної поведінки, яка може свідчити про наявність загрози. Системи, що аналізують події в реальному часі, здатні ідентифікувати зловмисні дії та негайно реагувати на них, блокуючи підозрілу активність або сповіщаючи фахівців.

В умовах постійного збільшення числа інцидентів та обмежених людських ресурсів, автоматизація реагування дозволяє суттєво скоротити час між виявленням загрози та запровадженням заходів. Автоматизація також знижує навантаження та полегшує роботу фахівців з інформаційної безпеки, провідного менеджменту звільняючи їх для вирішення стратегічних, більш важливих та складних питань.

Сучасна теорія інформаційної безпеки швидко змінюється, враховуючи появу нових загроз, регуляторних вимог і технологій цифровізації. Для того щоб залишатися ефективною, ця теорія повинна не тільки адаптуватися до нових викликів практики, але й розробляти нові підходи та інструменти захисту, отже розглянемо основні перспективи розвитку та рекомендації щодо підвищення ефективності інформаційної безпеки.

Однією з перспектив підвищення ефективності інформаційної безпеки є – кібергігієна в системі менеджменту підприємства. Поняття кібергігієни охоплює комплекс практичних навичок і процедур для забезпечення безпеки інформаційного середовища. Підтримка кібергігієни серед співробітників організацій є одним із найважливіших компонентів запобігання кіберзагрозам. До ключових рекомендацій належать: своєчасне оновлення операційних систем та додатків, що знижує ризики атак через відомі вразливості, використання багатофакторної автентифікації та вимога регулярної зміни паролів, проведення тематичних тренінгів із кібергігієни, де працівники навчаються розпізнавати фішингові повідомлення, маніпулятивні посилання та інші методи впливу соціальної інженерії. Розвиток управлінської культури кібергігієни знижує ймовірність проникнення загроз через людський фактор, який є основною причиною багатьох успішних атак [4].

Наступна перспектива, це використання штучного інтелекту, що стрімко захоплює сучасний цифровий світ. Штучний інтелект та машинне навчання відіграють дедалі важливішу роль у підвищенні ефективності систем захисту інформації. Ці технології дозволяють швидко, досить чітко ідентифікувати аномальну шкідливу поведінку в системах і реагувати на потенційні загрози.

Перспективні напрямки використання штучного інтелекту включають: побудову моделей нормальної адекватної поведінки користувачів та пристроїв для виявлення відхилень, які можуть свідчити про злом або несанкціоноване використання, такі системи можуть «навчатися» на нових типах атак і підвищувати точність виявлення невідомих раніше загроз. Штучний інтелект з легкістю автоматизує рутинні процеси, такі як фільтрація спаму, класифікація даних або управління доступом, що зменшує людський фактор і підвищує оперативність реагування на інциденти. Інтеграція штучного інтелекту у систему інформаційної безпеки підвищує загальну стійкість до сучасних загроз та дозволяє реагувати на атаки в реальному часі.

Сучасний цифровий світ потребує тісної міжнародної співпраці для боротьби з кіберзагрозами, оскільки кіберпростір не має чітких державних кордонів. Створення глобальних ініціатив та альянсів є важливим елементом для протидії міждержавним кібератакам і забезпечення інформаційної безпеки. Важливо розробляти загальноприйняті протоколи, які дозволять різним країнам більш ефективно співпрацювати в боротьбі з кіберзлочинністю та підтримувати договори, угоди на рівні ООН, які регулюють поведінку держав в кіберпросторі й сприяють розвитку міжнародного права щодо кібербезпеки.

Міжнародна координація дозволяє більш ефективно реагувати на великомасштабні кібератаки, що можуть завдати шкоди національним економікам і міжнародній стабільності.

Для належного захисту даних, забезпечення відповідності новим викликам необхідно постійно оновлювати та вдосконалювати законодавчу базу, розширювати її компоненти з векторністю на врахування не лише проблем сьогодення, а й майбутніх станів (рисунок 2).

Динамічна та сучасна регуляторна база сприятиме швидкому реагуванню на зміни у сфері кібербезпеки й забезпеченню захисту прав громадян, організацій та держави.

Управлінське та правове забезпечення, інституційне закріплення системного розвитку інформаційної економіки, комплексної цифровізації

суспільного відтворення передбачає формування теоретичних знань, накопичення та опрацювання базових категорій, окреслення принципів та цілісної методології, напрацювання заходів, що прискорює закріплення ефективних технологій, бажаних та стрімких процесів в діяльності влади, бізнесу, населення. Особливої уваги набувають питання інституціоналізації заходів безпекового характеру, як елементу стабільності діяльності, якісного виконання різноманітних завдань, ефективного прийняття рішень (особливо за умов невизначеності в умовах ведення війни) [5].

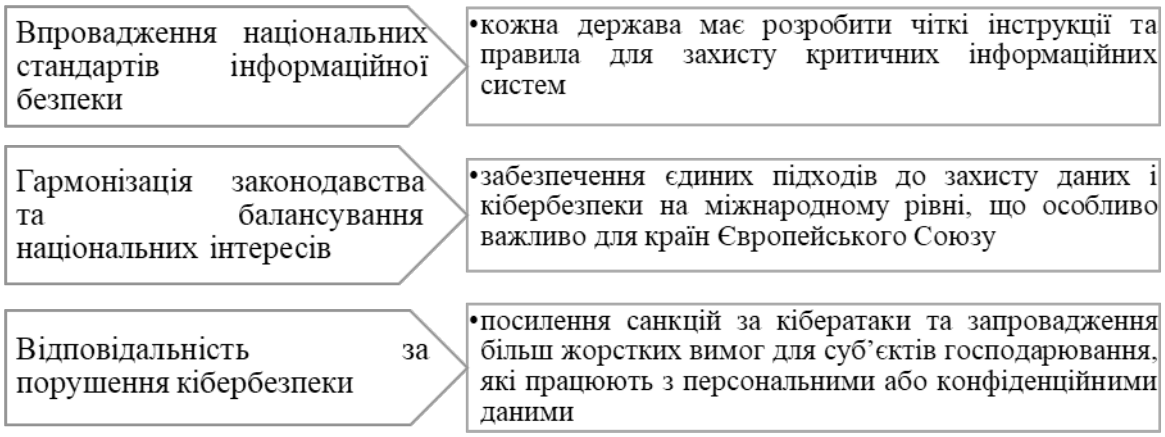

Рисунок 2 – Напрями щодо вдосконалення законодавчої бази для захисту інформаційної безпеки

Авторська розробка

Висновки.

Зміни в теорії та практиці інформаційної безпеки обумовлені як розвитком технологій, так і зростанням кіберзагроз. Майбутнє інформаційної безпеки полягає в інтеграції новітніх технологій із сучасними підходами до управління даними, а також у глобальній координації заходів щодо запобігання загрозам. Сучасна теорія інформаційної безпеки повинна адаптуватися до швидкозмінного середовища і забезпечити належний рівень захисту для різних галузей діяльності, враховуючи державні й комерційні потреби.

Література.

1. Виздрик, В., & Мельник, О. (2023). ІНФОРМАЦІЙНА БЕЗПЕКА В УКРАЇНІ: СУЧАСНИЙ СТАН. *Grail of Science*, (24), 196–202. https://doi.org/10.36074/grail-of-science.17.02.2023.034

2. Грабар, Н. (2022). ІНФОРМАЦІЙНА БЕЗПЕКА В СУЧАСНОМУ ГЛОБАЛІЗОВАНОМУ СВІТІ. Вісник Національного технічного університету «ХПІ». Сер. : Актуальні проблеми розвитку українського суспільства , (2), 43-47. https://doi.org/10.20998/2227-6890.2022.2.08

3. https://www.microsoft.com/uk-ua/security/business/zero-trust

4. https://www.microsoft.com/uk-ua/security/security-insider/practical-cyber-defense/cyber-resilience-hygiene-guide

5. Matvienko, O. (2023). CLOUD TECHNOLOGIES OF THE INFORMATION ECONOMY: ISSUES OF INSTITUTIONALIZATION AND MEASURES OF UKRAINIAN MANAGEMENT IN THE CONDITIONS OF WAR. *Збірник наукових праць Черкаського державного технологічного університету. Серія: Економічні науки*. (70), 78-85. https://doi.org/10.24025/2306-4420.70.2023.297130

Статья отправлена: 17.11.2024 г.