Інформаційна і національна безпека

УДК / UDC: 004.056:004
DOI: https://doi.org/10.37750/2616-6798.2026.2(57).364408

Ігор Федорович Корж
Державна наукова установа "Інститут інформації, безпеки і права Національної академії правових наук України"
Київ, Україна
ORCID: https://orcid.org/0000-0003-0446-5975
Володимир Миколайович Фурашев
Державна наукова установа "Інститут інформації, безпеки і права Національної академії правових наук України"
Київ, Україна
ORCID: https://orcid.org/0000-0001-7205-724X

ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ЦИФРОВІЗАЦІЇ

Анотація. *В статті проаналізовано проблемні питання, пов'язані із забезпеченням інформаційної безпеки та кібербезпеки в умовах здійснюваної в Україні цифровізації, яка, у свою чергу, здійснюється в умовах збройної агресії Російської Федерації проти України.*

Зазначено, що проблема захисту даних від втрати, викрадення, спотворення або пошкодження у сучасному суспільстві, особливо у зв'язку із зростаючою роллю інформаційно-комунікаційних технологій, потребує посиленої уваги, а її вирішення сприяє забезпеченню інформаційної безпеки як окремої особистості, організації, так і всієї держави.

У зв'язку із проведенням російським агресором проти України сучасної гібридної війни, акцентовано увагу на необхідності з боку Української держави більш гострого, ширшого, глибшого і динамічнішого реагування на здійснювані сучасні ворожі інформаційні спецоперації, в процесі яких застосовуються динамічно змінювані і постійно вдосконалювані засоби і механізми інформаційного впливу на громадян України. Тому вивчення існуючих та потенційних загроз в інформаційній сфері дає змогу прогнозувати наративи противника, нейтралізувати їх і підтримувати консолідацію суспільства. А системи моніторингу, аналізу та раннього попередження дозволяють швидко виявляти дезінформаційні кампанії та кібератаки й зменшувати їхній ефект (швидше реагувати, блокувати, виправляти інформацію). Так само й інтеграція інформаційної та кібербезпеки підвищує стійкість сил оборони, захищає критичну інфраструктуру, комунікації та системи управління.

Здійснюваний аналіз механік маніпуляцій дозволяє розробляти ефективні освітні програми – громадяни краще розпізнають фейки й менше піддаються впливу. А розуміння загроз допомагає формувати єдині наративи держави, координувати комунікацію між органами влади й вести проактивну інформкампанію на міжнародній арені. У свою чергу, дослідження тактик противника й виявлені докази дають підстави для міжнародної координації, санкцій і спільних протидій, а також для посилення кіберзахисту критичної інфраструктури, держсервісів, ЗСУ, так само і покращення координації між державними органами і з громадянським сектором.

Розкрито важливість здійснюваної в Україні цифровізації, оскільки повсюдне впровадження цифрових технологій у повсякденний побут, державні послуги та взаємодію людей формує більш інклюзивне суспільство, забезпечує швидкий доступ до електронного урядування, онлайн-освіти, медицини та фінансових послуг, підвищуючи якість життя та

ефективність управління. При цьому ключовими аспектами цифровізації соціальної сфери є соціальний захист і доступність послуг.

Водночас, цифровізація несе в собі і відповідні виклики, як то в частині інформаційної безпеки, кібербезпеки, цифрової нерівності, здоров'я для громадян. Виділено наступні основні проблеми інформаційної безпеки :

– недостатній рівень захисту персональних даних, який полягає в низькому рівні технічного захисту;

– проблеми кібергігієни серед користувачів і організацій;

– відсутність або застарілість політик безпеки в організаціях;

– проблеми управління доступом і автентифікації;

– загрози внутрішніх користувачів (інсайдерські загрози);

– технічні проблеми: уразливості програмного забезпечення, апаратні загрози;

– проблеми реагування на інциденти та відновлення після атак.

Зазначено, що в умовах цифровізації, яка охоплює всі сфери життя, бізнесу та державного управління, виникають нові можливості, але водночас і значні виклики для кібербезпеки, з яких доцільно виділити наступні :

– зростання кількості та складності кіберзагроз;

– недостатній рівень кіберграмотності та підготовки персоналу;

– складність захисту розподілених і хмарних систем;

– проблеми з управлінням даними та конфіденційністю;

– недосконалість технологій захисту та їх інтеграції;

– відсутність ефективної стратегії реагування на інциденти.

Підкреслено, що інформаційна безпека та кібербезпека – це два тісно пов'язані, але не тотожні поняття, які разом формують комплексний підхід до захисту інформації в сучасному цифровому світі. Розуміння їх системності допомагає краще організувати заходи захисту, оцінити ризики та побудувати ефективні стратегії безпеки. Кібербезпека є підгалуззю інформаційної безпеки, яка зосереджена на захисті комп'ютерних систем, мереж, програмного забезпечення та даних у цифровому просторі від кіберзагроз, таких як хакерські атаки, шкідливе програмне забезпечення, фішинг, DDoS-атаки тощо.

Акцентовано увагу на тому, що інформаційна безпека – ширше поняття, яке охоплює всі аспекти захисту інформації, включно з фізичними, адміністративними та технічними заходами. У свою чергу, кібербезпека – частина інформаційної безпеки, що фокусується на цифровому середовищі. Системність, щодо такого підходу, означає, що інформаційна безпека і кібербезпека розглядаються як частини єдиної системи захисту інформації, де кожен елемент (технології, люди, процеси) взаємодіє для досягнення загальної мети – забезпечення безпеки інформації.

Тим самим, інформаційна безпека і кібербезпека – це взаємодоповнюючі поняття, які разом формують цілісну систему захисту інформації. Системний підхід дозволяє ефективно координувати технічні, організаційні та людські ресурси для мінімізації ризиків. Розуміння системності цих понять є ключовим для побудови надійної стратегії безпеки в будь-якій організації.

***Ключові слова**: інформаційна безпека; кібербезпека; кібергігієна; кібернапад; персональні дані; технічні проблеми; цифровізація*

Ihor F. Korzh
State Scientific Institution "Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine"
Kyiv, Ukraine
ORCID: https://orcid.org/0000-0003-0446-5975
Volodymyr M. Furashev
State Scientific Institution "Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine"
Kyiv, Ukraine
ORCID: https://orcid.org/0000-0001-7205-724X

INFORMATION SECURITY PROBLEMS IN THE CONDITIONS OF DIGITALIZATION

Summary. *The article analyzes problematic issues related to ensuring information security and cybersecurity in the context of digitalization being carried out in Ukraine, which, in turn, is being carried out in the context of armed aggression by the Russian Federation against Ukraine.*

It is noted that the problem of data protection from loss, theft, distortion or damage in modern society, especially in connection with the growing role of information and communication technologies, requires increased attention, and its solution contributes to ensuring the information security of an individual, an organization, and the entire state.

In connection with the Russian aggressor conducting a modern hybrid war against Ukraine, attention is focused on the need for the Ukrainian state to respond more sharply, broadly, deeply and dynamically to the ongoing modern hostile information special operations, in the process of which dynamically changing and constantly improving means and mechanisms of information influence on the citizens of Ukraine are used. Therefore, the study of existing and potential threats in the information sphere makes it possible to predict the enemy's narratives, neutralize them and support the consolidation of society. And monitoring, analysis and early warning systems allow you to quickly detect disinformation campaigns and cyberattacks and reduce their effect (faster responding, blocking, correcting information). Similarly, the integration of information and cybersecurity increases the resilience of defense forces, protects critical infrastructure, communications and control systems.

The analysis of manipulation mechanics allows developing effective educational programs - citizens are better able to recognize fakes and are less susceptible to influence. And understanding threats helps to form unified narratives of the state, coordinate communication between government agencies, and conduct a proactive information campaign in the international arena. In turn, research into enemy tactics and the evidence found provide grounds for international coordination, sanctions, and joint countermeasures, as well as for strengthening cyber defense of critical infrastructure, state services, and the Armed Forces of Ukraine, as well as improving coordination between government agencies and the civil sector.

The importance of digitalization in Ukraine is revealed, as the widespread introduction of digital technologies into everyday life, public services, and human interaction forms a more inclusive society, provides quick access to e-government, online education, medicine, and financial services, improving the quality of life and efficiency of management. At the same time, the key aspects of digitalization of the social sphere are social protection and accessibility of services.

At the same time, digitalization also brings with it corresponding challenges, such as in terms of information security, cybersecurity, digital inequality, and health for citizens. The following main information security problems have been identified:

– insufficient level of personal data protection, which consists in a low level of technical protection;

– cyber hygiene problems among users and organizations;

– absence or obsolescence of security policies in organizations;

– access management and authentication problems;
– threats from internal users (insider threats);
– technical problems: software vulnerabilities, hardware threats;
– problems of incident response and recovery from attacks.

It is noted that in the context of digitalization, which covers all spheres of life, business and public administration, which creates new opportunities, but at the same time significant challenges for cybersecurity, of which it is advisable to highlight the following:
– the growth in the number and complexity of cyber threats;
– insufficient level of cyber literacy and personnel training;
– the complexity of protecting distributed and cloud systems;
– problems with data management and confidentiality;
– imperfection of protection technologies and their integration;
– lack of an effective incident response strategy.

It is emphasized that information security and cybersecurity are two closely related, but not identical, concepts that together form a comprehensive approach to protecting information in the modern digital world. Understanding their systemic nature helps to better organize protection measures, assess risks, and build effective security strategies. Cybersecurity is a subfield of information security that focuses on protecting computer systems, networks, software, and data in the digital space from cyberthreats, such as hacker attacks, malware, phishing, DDoS attacks, etc.

It is emphasized that information security is a broader concept that covers all aspects of information protection, including physical, administrative and technical measures. In turn, cybersecurity is a part of information security that focuses on the digital environment. Systematic means that information security and cybersecurity are considered as parts of a single information protection system, where each element (technology, people, processes) interacts to achieve the common goal of ensuring information security.

Thus, information security and cybersecurity are complementary concepts that together form a holistic information protection system. A systemic approach allows for effective coordination of technical, organizational, and human resources to minimize risks. Understanding the systemic nature of these concepts is key to building a reliable security strategy in any organization.

Keywords: *information security; cybersecurity; cyber hygiene; cyber attack; personal data; technical problems; digitalization*

Постановка проблеми. У зв'язку зі зростаючою роллю інформаційно-комунікаційних технологій у сучасному суспільстві проблема захисту даних від втрати, викрадення, спотворення або пошкодження потребує посиленої уваги. Вирішення цієї проблеми сприяє забезпеченню інформаційної безпеки як окремої особистості, організації, так і всієї держави.

Останнім часом до питань інформаційної безпеки включено питання інформаційного впливу на особистість і суспільство, як це здійснюється нині ворогом в контексті інформаційної війни. У лютому 2017 року Указом Президента України була затверджена Доктрина інформаційної безпеки України [1], яка визначала національні інтереси України в інформаційній сфері, загрози їх реалізації, напрями і пріоритети державної політики в інформаційній сфері. Життєво важливими інтересами суспільства та держави було визнано такі:

– захист українського суспільства від агресивного впливу деструктивної пропаганди;

– захист українського суспільства від агресивного інформаційного впливу, спрямованого на пропаганду війни, розпалювання національної і релігійної ворожнечі, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України;

– всебічне задоволення потреб громадян, підприємств, установ і організацій усіх форм власності у доступі до достовірних та об'єктивних відомостей та ін.

Однак, реалії життя показали, що Українська держава має більш гостро, ширше, глибше і динамічніше реагувати на сучасні ворожі інформаційні спецоперації, в процесі яких застосовуються динамічно змінювані і постійно вдосконалювані засоби і механізми інформаційного впливу на громадян. Тому на заміну згаданої Доктрини була напрацьована і прийнята Стратегія національної безпеки [2], оскільки інформаційні спецоперації російських спецслужб у своїй більшості були спрямовані на підрив національної безпеки України, її національних інтересів, ліквідацію української державності та знищення української ідентичності, провокування проявів екстремізму, панічних настроїв у суспільстві, загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації в Україні. А гаряча фаза збройної агресії Російської Федерації проти України підтвердила актуальність забезпечення для України даного виду безпеки.

Російською Федерацією використовувалися нові активні заходи, у тому числі міжнародного характеру, щодо легітимізації спроби анексії Автономної Республіки Крим та міста Севастополя, заперечення своєї участі у війні на території Донецької та Луганської областей та посилення адвокаційної кампанії за зняття санкцій, запроваджених у зв'язку з порушенням Російською Федерацією суверенітету і територіальної цілісності України. Задіяння у цьому процесі Російською Федерацією всіх її спроможностей (політичних, інформаційних, економічних, розвідувальних та інших) залишається і понині особливо небезпечним викликом для України.

Тому вивчення існуючих та потенційних загроз в інформаційній сфері дає змогу прогнозувати наративи противника, нейтралізувати їх і підтримувати консолідацію суспільства. А системи моніторингу, аналізу та раннього попередження дозволяють швидко виявляти дезінформаційні кампанії та кібератаки й зменшувати їхній ефект (швидше реагувати, блокувати, виправляти інформацію). Так само й інтеграція інформаційної та кібербезпеки підвищує стійкість сил оборони, захищає критичну інфраструктуру, комунікації та системи управління.

Дослідження загроз допомагає збалансувати заходи з безпеки та гарантії свободи слова, приватності й захисту персональних даних (вчасне вдосконалення законодавства та процедур). У свою чергу аналіз механік маніпуляцій дозволяє розробляти ефективні освітні програми – громадяни краще розпізнають фейки й менше піддаються впливу. А розуміння загроз допомагає формувати єдині наративи держави, координувати комунікацію між органами влади й вести проактивну інформкампанію на міжнародній арені.

Важливим також є дослідження тактик противника й виявлені докази дають підстави для міжнародної координації, санкцій і спільних протидій, а також для посилення кіберзахисту критичної інфраструктури, держсервісів, ЗСУ, так само і покращення координації між державними органами (РНБО, Кабмін, МО, СБУ, Нацрада, Центр протидії дезінформації) і з громадянським сектором.

Результати аналізу наукових публікацій (досліджень). Питанням здійснення цифровізації в Україні, як пріоритетній державній трансформації, питанням забезпечення інформаційної та кібербезпеки присвячено ряд публікацій, як наукового, так публіцістичного характеру, в яких проглядається першочергове завдання – сприяти належному забезпеченню інформаційної безпеки разом з кібербезпекою як невід'ємних складових національної безпеки. Так, різні аспекти здійснюваного в Україні дослідження здійснювали О. Баранов, О. Барановський, К. Бєляков, П. Богуцький,

К. Буравченко, Н. Гончаренко, О. Довгань, І. Доронін, М. Дубняк, О. Золотар, М. Ільїн, Ю. Ірха, І. Корж, О. Костенко, Д. Ланде, О. Левенець, А. Марущак, Т. Смірнова, І. Петренко, В. Пилипчук, О. Радзієвська, П. Усік, В. Фурашев, та інші.

Важливість таких досліджень підтверджується тим, що поряд із зазначеними науковцями значну увагу згаданим проблемам приділяли наступні державні практичні центри та наукові установи: Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язку) та Державний центр кіберзахисту та реагування (CERT-UA) у її складі; Державна наукова установа "Інститут інформації, безпеки і права Національної академії правових наук України"; КПІ ім. І. Сікорського; Львівська політехніка; Харківський університет та ін., де ведуться фундаментальні й прикладні дослідження, а також різні лабораторії приватного сектору. Основними темами наукових досліджень є :

– аналіз і протидія шкідливому ПЗ (віруси, трояни, ботнети, рекламні модулі);

– захист мереж і сервісів (DDoS-захист, захист інфраструктури електронних послуг);

– кіберзагрози для мобільних пристроїв і IoT;

– соціальна інженерія, фішинг і інформаційні операції;

– захист критичної інфраструктури та кіберстійкість;

– правові, політичні та нормативні аспекти (політика інформаційної безпеки, національні доктрини) тощо.

Водночас, зростання залежності від цифрових технологій супроводжується збільшенням ризиків кіберзагроз, що породжує новий тип конфліктів — кібервійну. Ці обставини роблять інформаційну та кібербезпеку критично важливими сферами для наукових досліджень. Причинами для зазначеного є: зростання кіберзагроз і складність кіберпростору; необхідність захисту критичної інфраструктури; розвиток технологій штучного інтелекту та автоматизації тощо.

Тим самим, наукові дослідження в галузі інформаційної та кібербезпеки є надзвичайно доцільними та необхідними в умовах стрімкої цифровізації та зростання загроз ведення кібервійни. Вони забезпечують фундамент для розробки ефективних технологій, стратегій та політик, які гарантують безпеку інформаційного простору, захист національних інтересів та стабільний розвиток суспільства в цифрову епоху.

Метою статті є аналіз стану інформаційної безпеки в контексті здійснюваної в Україні цифровізації, а також існуючих її проблем, як і проблем у процесі забезпечення кібербезпеки в умовах ведення Російської Федерації проти України гібридної війни; з'ясування причин загроз та напрацювання пропозицій щодо їх мінімізації.

Виклад основного матеріалу. Незважаючи на збройну агресію Російської Федерації проти України, яка продовжується вже п'ятий рік, в Україні одночасно набирає обертів процес впровадження та використання цифрових технологій і методів у різні аспекти життя та діяльності, включаючи воєнну сферу, бізнес, управління, освіту та повсякденний побут. Таким чином цифровізація є важливою тенденцією, яка трансформує насамперед соціальну сферу, роблячи її більш доступною та ефективною, одночасно вимагаючи захисту користувачів та розширення їхніх цифрових навичок**.**

Як заявив екс-міністр цифрової трансформації України М. Федоров, цифровізація – це поступове перетворення усіх державних послуг на зручні онлайн-сервіси. Цифрова трансформація – це те, що сьогодні виділяє нас у світі. Ми будуємо цифрову державу. Державу, яка стає сервісом. Без бюрократії, черг та корупції [3].

В наукових дослідженнях зазначено [4, с. 67], що ключовим цивілізаційним трендом в сучасних умовах залишається лавиноподібне зростання обсягів даних та

інформації, адже з появою та розвитком потужних суперкомп'ютерів і мережі Інтернет процес цифровізації перейшов у нову фазу. Головними факторами сучасного прискорення стали поява і глобальне розповсюдження персональних, бездротових засобів зв'язку, які технологічно досягли рівня засобів продукування інформації, а також глобальне використання цифрового формату суб'єктами економічної діяльності, адже тут цифрові технології розкрили власні системні можливості та змінили усі попередні правила та уявлення про віртуальні товари, право власності, додану вартість, прибутки тощо.

Зазначимо, що ключовою нормативно-правовою базою для впровадження в Україні цифровізації, слугують наступні нормативно-правові акти:

– Закон України "Про національну програму інформатизації" [5], який визначає основи державної політики у сфері інформатизації, цифрового розвитку та цифровізації; встановлює цілі, завдання та механізми реалізації національної програми інформатизації;

– Закон України "Про цифровий контент та цифрові послуги" [6], положеннями якого забезпечується гармонізація національного законодавства з європейськими стандартами; регулюються відносини, пов'язані з цифровим контентом, цифровими правами та послугами, визначається правовий статус цифрових активів, цифрових речей, цифрових прав;

– Стратегія здійснення цифрового розвитку, цифрових трансформацій і цифровізації системи управління державними фінансами на період до 2030 року та затверджений план заходів щодо її реалізації [7], яка визначає пріоритети та заходи для цифрової трансформації державного управління фінансами. З метою підвищення прозорості в частині планування та використання бюджетних коштів на місцевому рівні у 2023 році в інтегрованій інформаційно-аналітичній системі "Прозорий бюджет" з'явилася можливість оприлюднення та завантаження з інформаційно-аналітичної системи управління плануванням та виконанням місцевих бюджетів "LOGICA" різних фінансових документів.

До даної бази можна також віднести комплексні теоретико-правові аналізи державної політики у сфері цифровізації та штучного інтелекту, а також законодавчі ініціативи, що регулюють цифрові права, цифрові активи, електронні послуги, кібербезпеку тощо.

Цифровізація соціального життя – це повсюдне впровадження цифрових технологій (Інтернет, ШІ, хмарні сервіси) у повсякденний побут, державні послуги та взаємодію людей, що формує більш інклюзивне суспільство. Вона забезпечує швидкий доступ до електронного урядування (наприклад, Дія), онлайн-освіти, медицини та фінансових послуг, підвищуючи якість життя та ефективність управління.

Ключовими аспектами цифровізації соціальної сфери є :

– ***соціальний захист***: автоматичне продовження виплат, онлайн-оформлення допомоги та впровадження Єдиної інформаційної системи соціальної сфери (ЄІССС);

– ***доступність послуг***: швидкий доступ до державних послуг, зниження бюрократичного навантаження, розвиток онлайн-освіти та медицини;

– комунікація та побут: поширення соціальних мереж, месенджерів та електронної комерції.

Основними перевагами здійснюваної в Україні цифровізації є :

– ефективність, тобто зменшення витрат, підвищення продуктивності та швидкості прийняття рішень;

– зручність, тобто можливість отримати послуги 24/7 у будь-якому місці;

– персоналізація, тобто створення продуктів, адаптованих до уподобань клієнта.

Поряд з цим, як зазначають дослідники, виникають різні загрози, ризики і виклики, з'являються нові цифрові технології, що потребує більш детального дослідження та виокремлення проблем розвитку цифровізації соціальної сфери та її функціонування у рамках забезпечення інформаційної безпеки України [8, с.254].

Сучасними викликами цифровізації є:

– інформаційна безпека: належне зберігання інформації;

– кібербезпека: потреба у технічному захисті особистих даних;

– цифрова нерівність: необхідність розвитку цифрових навичок у всіх верств населення;

– здоров'я: ризики, пов'язані з малорухливим способом життя, стресом, порушенням сну та соціальною ізоляцією.

Інформаційна безпека нині є вкрай важливою складовою національної безпеки, так само як і важливою складовою сучасного життя. Основна мета інформаційної безпеки в контексті цифрової трансформації – це забезпечити захищеність як інформації, так і IT-інфраструктури від випадкових чи навмисних впливів (атак тощо), які можуть завдати неприйнятної шкоди власникам інформаційних активів.

Зазначимо, які впливи цифровізації можуть бути на інформаційну безпеку в умовах цифровізації:

– характеристика цифровізації: тенденції, технології (хмарні сервіси, IoT (інтернет речей), Big Data, AI);

– нові виклики та загрози, пов'язані з цифровізацією;

– зміни в ландшафті кіберзагроз (кіберзлочинність, кібершпигунство, кібертероризи);

– вразливість цифрових систем і мереж.

З огляду на зазначене можна виділити наступні основні проблеми інформаційної безпеки:

1. ***Недостатній рівень захисту персональних даних, який полягає в низькому рівні технічного захисту.*** Багато організацій і сервісів не впроваджують сучасні технології шифрування, багатофакторну аутентифікацію, системи виявлення вторгнень та інші засоби кіберзахисту. Це робить персональні дані вразливими до несанкціонованого доступу, витоків і кібератак.

Крім того, відсутнє або недостатнє нормативно-правове регулювання. У багатьох організаціях відсутні чіткі правила та стандарти щодо обробки, зберігання і захисту персональних даних. Це призводить до хаотичного підходу, коли персональні дані можуть бути використані або передані без згоди власника.

Також проявляється низька обізнаність користувачів і працівників. Часто користувачі не знають, як правильно захищати свої дані, не використовують складні паролі, не оновлюють програмне забезпечення, що створює додаткові ризики. Аналогічно, працівники організацій можуть не дотримуватися політик безпеки.

Багатьма власниками інформації використовуються застарілі або вразливі системи. Системи, які не отримують регулярних оновлень безпеки, стають легкою ціллю для зловмисників, що призводить до компрометації персональних даних.

Відповідним викликом слугує масштабність і складність цифрових систем. Зі збільшенням обсягів даних і кількості цифрових сервісів зростає складність їх захисту. Відсутність централізованого контролю і моніторингу ускладнює виявлення і реагування на загрози.

Наступним видом проблеми є соціальна інженерія та фішинг. Зловмисники часто використовують психологічні методи для отримання доступу до персональних даних, що ускладнює технічний захист. Таким чином це комплексна проблема, що включає технічні, організаційні, правові та освітні аспекти. Для її подолання необхідно впроваджувати сучасні технології безпеки, розробляти і дотримуватися нормативних актів, підвищувати обізнаність користувачів і персоналу, а також постійно оновлювати і контролювати інформаційні системи.

2. ***Проблеми кібергігієни серед користувачів і організацій***. Серед користувачів можна виділити наступні основні проблеми. Насамперед мова може йти про недостатню обізнаність і освіту. Багато користувачів не мають достатніх знань про кіберзагрози, методи захисту, правила безпечної поведінки в інтернеті. Це призводить до необережного поводження з паролями, відкриття підозрілих листів, завантаження шкідливого ПЗ.

Наступним є використання слабких паролів і повторне їх застосування. Часто користувачі обирають прості паролі або використовують один і той самий пароль для багатьох сервісів, що значно підвищує ризик компрометації облікових записів.

Поширеним є ігнорування оновлень програмного забезпечення. Відсутність регулярного оновлення систем і додатків залишає уразливості відкритими для атак. Таким же є вразливість до соціальної інженерії. Користувачі можуть стати жертвами фішингових атак, шахрайських повідомлень, що змушує їх розкривати конфіденційну інформацію.

Для організацій притаманна відсутність або недостатність політик кібергігієни. Багато організацій не мають чітко прописаних правил і процедур, які регламентують безпечну роботу з інформацією, що призводить до хаотичного підходу до безпеки.

Крім того недостатнім є навчання персоналу. Працівники часто не проходять регулярних тренінгів з кібербезпеки, що підвищує ризик людської помилки.

В організаціях відсутній багаторівневий захист. Організації можуть не впроваджувати комплексні системи захисту, такі як багатофакторна аутентифікація, системи моніторингу, резервне копіювання.

Наступним є інфраструктурна вразливість, тобто використання застарілих або незахищених систем, недостатній контроль доступу до інформації. А недооцінка кіберзагроз і ризиків призводить до відсутності інвестицій у захист і реагування на інциденти.

Таким чином проблеми кібергігієни серед користувачів і організацій – це комплекс викликів, пов’язаних з недостатньою обізнаністю, відсутністю належних політик і процедур, а також технічними недоліками. Тому для підвищення рівня кібергігієни необхідно:

– проводити регулярне навчання і підвищення обізнаності;

– впроваджувати сучасні технології захисту;

– розробляти і дотримуватися чітких політик безпеки;

– забезпечувати регулярне оновлення і моніторинг систем.

3. ***Відсутність або застарілість політик безпеки в організаціях,*** що мають застарілі, або в них відсутні формалізовані документи, які визначають правила, стандарти та процедури захисту інформації в організації. Відсутність або застарілість таких політик створює низку серйозних проблем, що негативно впливають на інформаційну безпеку. Ними можуть бути наступні проблеми.

Відсутність чітких правил і стандартів безпеки. Без політик безпеки співробітники не мають чітких інструкцій щодо того, як поводитися з інформацією, які заходи захисту

застосовувати, як реагувати на інциденти. Зазначене призводить до хаотичного підходу, коли кожен діє на свій розсуд, що підвищує ризик помилок і витоків даних.

Застарілі політики не відповідають сучасним загрозам. Кіберзагрози постійно еволюціонують, з'являються нові вразливості та методи атак. Якщо політики безпеки не оновлюються, вони не враховують сучасні ризики, технології та нормативні вимоги. Це робить організацію вразливою до нових типів атак і порушень.

Наступним недоліком є недостатній контроль і відповідальність. Відсутність або застарілі політики ускладнюють визначення відповідальних за безпеку осіб і процесів. Без чітких ролей і обов'язків складно контролювати дотримання заходів безпеки, що призводить до неефективного управління ризиками.

Великим негативом є порушення нормативних вимог і штрафи. Багато галузей мають законодавчі вимоги щодо захисту інформації (наприклад, Закон України "Про захист персональних даних"). Відсутність актуальних політик безпеки може призвести до невідповідності цим вимогам, що загрожує штрафами, судовими позовами та репутаційними втратами.

Зниження довіри клієнтів і партнерів – організації з неактуальними або відсутніми політиками безпеки викликають сумніви у клієнтів і партнерів щодо надійності захисту їхніх даних. Це може призвести до втрати бізнесу і конкурентних переваг.

І, насамперед, ускладнення реагування на інциденти, тобто без актуальних політик безпеки неможливо ефективно організувати процеси виявлення, реагування та відновлення після кіберінцидентів. Це збільшує час і збитки від атак.

Тим самим, відсутність або застарілість політик безпеки в організаціях створює серйозні ризики для інформаційної безпеки, бізнес-процесів і репутації. Тому для мінімізації цих ризиків необхідно:

– регулярно оновлювати політики безпеки з урахуванням нових загроз і нормативних вимог;

– забезпечувати чітке визначення ролей і відповідальностей;

– проводити навчання персоналу щодо дотримання політик;

– впроваджувати механізми контролю і аудиту дотримання політик.

4. ***Проблеми управління доступом і автентифікації.*** Вони є ключовими елементами інформаційної безпеки, що забезпечують контроль над тим, хто і як може отримати доступ до інформаційних ресурсів організації. Проблеми в цих сферах можуть призводити до серйозних порушень безпеки. Таким проблемами є наступні.

Недостатня складність і надійність автентифікації, тобто використання простих або легко вгадуваних паролів. Крім того, відсутність багатофакторної автентифікації (MFA) значно підвищує ризик компрометації облікових записів, як і застосування однакових паролів для різних систем.

Неефективне управління права доступу, тобто надання користувачам надмірних прав, які не відповідають їхнім функціональним обов'язкам (принцип мінімальних привілеїв порушується). Водночас, відсутність регулярного перегляду і оновлення прав доступу призводить до накопичення зайвих або застарілих дозволів. Так само відсутність централізованого контролю за доступом ускладнює моніторинг і аудит.

Відсутність або слабка політика управління обліковими записами викликані відсутністю процедур створення, зміни і видалення облікових записів, а також залишення активних облікових записів колишніх співробітників або тимчасових користувачів. Так само відсутність контролю за використанням спільних облікових записів.

Технічні вразливості систем автентифікації викликані використанням застарілих або вразливих протоколів автентифікації, як і відсутність шифрування при передачі облікових даних. Також потрібно враховувати недостатній захист від атак типу “brute force” (грубий перебір) або “credential stuffing” (підстановка облікових даних), тобто це методи кібератак для несанкціонованого доступу до акаунтів. “Brute force” автоматично перебирає всі паролі, а “credential stuffing” використовує бази вкрадених логінів/паролів з інших сайтів, розраховуючи на повторне використання користувачами однакових даних.

Недостатній моніторинг і аудит доступу викликаний відсутністю або неповним журналом доступу до систем і ресурсів, так само як і неефективне виявлення і реагування на спроби несанкціонованого доступу, а також відсутністю аналітики для виявлення аномальної поведінки користувачів.

Таким чином проблеми управління доступом і автентифікації створюють значні ризики для безпеки інформації в організаціях. Для їх подолання необхідно:

– впроваджувати багатофакторну автентифікацію;

– дотримуватися принципу мінімальних привілеїв і регулярно переглядати права доступу;

– розробляти і підтримувати чіткі політики управління обліковими записами;

– використовувати сучасні, захищені протоколи автентифікації;

– забезпечувати постійний моніторинг і аудит доступу.

5. ***Загрози внутрішніх користувачів (інсайдерські загрози),*** під якими доцільно розуміти ризики, які виникають через дії або бездіяльність співробітників, підрядників або інших осіб, які мають легальний доступ до інформаційних систем організації. Вони є однією з найнебезпечніших категорій загроз, оскільки інсайдери мають знання про внутрішню структуру, процеси та слабкі місця систем. Основними їх видами є наступні.

Зловмисні дії інсайдерів, тобто: навмисне викрадення, пошкодження або розголошення конфіденційної інформації; саботаж інформаційних систем або бізнес-процесів; використання доступу для особистої вигоди або на шкоду організації.

Наступним є ненавмисні помилки або недбалість, тобто: помилки при роботі з даними, які призводять до витоків або втрати інформації; відкриття шкідливих файлів або посилань через необережність; недотримання політик безпеки через недостатню обізнаність.

Знаковим недоліком є зловживання правами доступу, тобто використання доступу до інформації поза межами службових обов’язків, що може призвести до несанкціонованого копіювання або передачі даних.

Викрадення облікових даних, тобто інсайдер може передати свої облікові дані третім особам або використовувати їх для несанкціонованого доступу.

Причинами виникнення інсайдерських загроз можуть бути:

– незадоволеність роботою або конфлікти в колективі;

– фінансові або особисті проблеми співробітників;

– недостатній контроль і моніторинг дій користувачів;

– відсутність або слабка політика управління доступом;

– недостатнє навчання і підвищення обізнаності персоналу.

Наслідками таких загроз можуть стати:

– витік конфіденційної інформації (персональні дані, комерційна таємниця);

– фінансові збитки через шахрайство або зупинку бізнес-процесів;

– репутаційні втрати і втрата довіри клієнтів;

– юридичні наслідки через порушення законодавства про захист даних.

Таким чином, інсайдерські загрози є складною і багатогранною проблемою, що вимагає комплексного підходу до управління безпекою, а саме:

– впровадження систем моніторингу і аудиту дій користувачів;

– чітке управління правами доступу за принципом мінімальних привілеїв;

– регулярне навчання і підвищення обізнаності персоналу;

– розробка політик і процедур реагування на інциденти;

– психологічна підтримка і робота з персоналом для зниження ризиків.

6. ***Технічні проблеми: уразливості програмного забезпечення, апаратні загрози.*** У сучасних інформаційних системах технічні проблеми безпеки поділяються на дві основні категорії: уразливості програмного забезпечення та апаратні загрози. Обидві категорії мають суттєвий вплив на загальний рівень інформаційної безпеки організацій.

Уразливості програмного забезпечення – це слабкі місця або помилки в коді програм, які можуть бути використані зловмисниками для отримання несанкціонованого доступу, викрадення даних або порушення роботи систем.

Типи вразливостей:

– помилки кодування, тобто неправильна обробка вхідних даних, що призводить до SQL-ін’єкцій, XSS (міжсайтового скриптингу) (тип кібератаки, при якій зловмисник впроваджує шкідливий JavaScript-код у веб-сторінки, що переглядаються іншими користувачами. Скрипт виконується в браузері жертви, дозволяючи викрасти сесійні cookie, паролі, отримати доступ до особистих даних або змінити вміст сайту), буферних переповнень. Це одна з найпоширеніших технік злому програм та веб-сайтів, що працюють з різними базами даних. Атака, як правило, проводиться на основі впровадження в різні типи запитів некоректних SQL операторів (це зарезервовані слова або символи, що використовуються в запитах до баз даних для виконання арифметичних операцій, порівняння значень, об’єднання умов або маніпуляції даними), що дозволяє зловмиснику отримати практично повний несанкціонований доступ до відповідної бази даних, локальних файлів, а також можливість віддаленого виконання довільних операцій на сервері. Крім того, SQL-атаки часто є результатом неекранованого введення, що передається сайту і використовується як частина запиту до бази даних;

– недостатня аутентифікація та авторизація: помилки в перевірці прав користувачів, що дозволяють отримати доступ до ресурсів без відповідних прав;

– відсутність або слабке шифрування**:** дані передаються або зберігаються у відкритому вигляді, що робить їх вразливими до перехоплення;

– вразливості в бібліотеках і компонентах: використання застарілих або небезпечних сторонніх компонентів;

– неправильне налаштування систем: відкриті порти, слабкі паролі, відсутність оновлень.

Наслідками таких вразливостей може стати:

– несанкціонований доступ до систем;

– витік конфіденційної інформації;

– порушення цілісності і доступності даних;

– використання системи для подальших атак.

Причиною появи зазначених вразливостей може бути :

– недостатня увага до безпеки при розробці;

– відсутність регулярного тестування і аудиту коду;

– затримки з оновленнями і патчами (невелике оновлення програмного забезпечення, призначене для автоматичного внесення змін у файли програми:

виправлення помилок (“багів”), підвищення продуктивності, оновлення графіки чи зміни функціоналу).

Апаратні загрози пов’язані з фізичними пристроями, які використовуються для зберігання, обробки і передачі інформації. Типи апаратних загроз:

– фізичне пошкодження або крадіжка обладнання: серверів, комп’ютерів, мобільних пристроїв, що призводить до втрати або викрадення даних;

– вразливості в апаратних компонентах: наприклад, уразливості в мікропроцесорах (Spectre, Meltdown), які дозволяють отримати доступ до захищеної пам’яті;

– атаки через апаратні інтерфейси: USB-атаки, підключення шкідливих пристроїв;

– відсутність фізичного контролю доступу: що дозволяє несанкціонованим особам отримати доступ до серверних кімнат або робочих місць;

– зловмисне апаратне забезпечення: наприклад, вбудовані шпигунські пристрої або модифіковані компоненти.

Наслідками таких загроз можуть бути:

– втрата або компрометація даних;

– порушення роботи інформаційних систем;

– можливість подальших кібератак через апаратні уразливості.

Причиною появи зазначених загроз можуть бути:

– недостатній фізичний захист обладнання;

– використання несертифікованих або підозрілих пристроїв;

– відсутність контролю за апаратними оновленнями і замінами.

Таким чином технічні проблеми у вигляді вразливостей програмного забезпечення та апаратних загроз є критичними для безпеки інформаційних систем. Для їх мінімізації необхідно:

– впроваджувати регулярне тестування безпеки (пентести, аудит коду) (тестування на проникнення) – процес тестування системи шляхом спроб її злому виявлення вразливостей. Фахівець із безпеки після узгодження сторін намагається зламати чи обійти захисні заходи інформаційної системи, щоб знайти слабкі місця; аудит - незалежна, систематична перевірка та аналіз вихідного коду ПЗ експертами для виявлення вразливостей, помилок, оцінки якості, відповідності стандартам та безпеки. Він допомагає оптимізувати продуктивність, покращити сумісність, зменшити ризики та витрати на підтримку, часто завершуючись звітом із рекомендаціями;

– своєчасно оновлювати програмне забезпечення і застосовувати патчі (невелике оновлення програмного забезпечення, призначене для автоматичного внесення змін у файли програми: виправлення помилок (“багів”), підвищення продуктивності, оновлення графіки чи зміни функціоналу;

– забезпечувати фізичний захист обладнання і контроль доступу;

– використовувати сертифіковані апаратні компоненти;

– проводити навчання персоналу щодо безпечного використання техніки.

7. ***Проблеми реагування на інциденти та відновлення після атак***.

а) Проблеми реагування на інциденти: реагування на інциденти – це процес виявлення, аналізу та реагування на кіберінциденти або інші загрози інформаційній безпеці. Основними проблемами, що виникають у цій сфері, є:

– недостатня швидкість виявлення інцидентів. Часто організації не мають належних систем моніторингу або аналітики, що призводить до затримок у виявленні атак. Це дає зловмисникам більше часу для завдання шкоди;

– відсутність чітких процедур реагування. Без заздалегідь розроблених і протестованих планів реагування персонал може діяти хаотично або неефективно, що збільшує шкоду від інциденту;

– обмежені ресурси та кваліфікація персоналу. Недостатня кількість фахівців з кібербезпеки або їх низька кваліфікація ускладнює швидке і правильне реагування на інциденти;

– проблеми з комунікацією. Відсутність ефективної внутрішньої та зовнішньої комунікації під час інциденту може призвести до плутанини, неправильного розподілу завдань і втрати важливої інформації;

– відсутність автоматизації. Ручне реагування на інциденти часто повільне і схильне до помилок. Відсутність автоматизованих систем реагування знижує ефективність;

– недостатня інтеграція систем безпеки. Розрізнені інструменти безпеки без централізованого управління ускладнюють аналіз інцидентів і координацію дій.

б) Проблеми відновлення після атак: відновлення після кібернападу – це процес повернення систем, даних і бізнес-процесів до нормального функціонування. Основними проблемами можуть бути:

– відсутність або недостатність резервного копіювання. Якщо резервні копії не створюються регулярно або зберігаються ненадійно, відновлення даних після атаки може бути неможливим або дуже тривалим;

– недостатня готовність планів відновлення. Відсутність чітких, протестованих планів відновлення призводить до хаотичних дій, затримок і додаткових втрат;

– технічні складнощі відновлення. Відновлення складних систем, особливо після атак типу ransomware (небезпечне шкідливе програмне забезпечення, яке шифрує файли або блокує доступ до пристрою, вимагаючи викуп (часто в криптовалюті) за відновлення доступу), може вимагати спеціалізованих знань і часу;

– втрата довіри користувачів і клієнтів. Тривале відновлення або повторні інциденти можуть негативно вплинути на репутацію організації;

– фінансові втрати. Відновлення систем і компенсація збитків часто вимагає значних витрат, які можуть бути непередбаченими;

– проблеми з відповідністю нормативам. Після інциденту організація може зіткнутися з юридичними або регуляторними санкціями, якщо відновлення не відповідає вимогам безпеки та захисту даних.

Таким чином проблеми реагування на інциденти та відновлення після атак тісно пов’язані між собою і вимагають комплексного підходу, що може включати в себе :

– розробку і тестування планів реагування та відновлення;

– впровадження сучасних технологій моніторингу та автоматизації;

– підвищення кваліфікації персоналу;

– забезпечення регулярного і надійного резервного копіювання;

– ефективну комунікацію і координацію дій.

Зазначене дозволить мінімізувати шкоду від кіберінцидентів і швидко повернутися до нормальної роботи.

Цифровізація охоплює всі сфери життя, бізнесу та державного управління, що створює нові можливості, але водночас і значні виклики для кібербезпеки. В нинішніх умовах цифровізації можна виділити наступні основні проблеми кібербезпеки.

1. ***Зростання кількості та складності кіберзагроз.*** Розвиток кіберзлочинності – зловмисники використовують все більш складні методи атак, такі як фішинг, ransomware, атаки на ланцюги постачання, DDoS-атаки;

– автоматизація атак – використання штучного інтелекту та автоматизованих інструментів дозволяє масштабувати атаки, роблячи їх більш ефективними;

– цільові атаки – зростає ***кількість*** атак, спрямованих на конкретні організації або інфраструктуру, що ускладнює захист.

2. ***Недостатній рівень кіберграмотності та підготовки персоналу:***

– людський фактор – більшість інцидентів пов'язані з помилками користувачів – слабкі паролі, відкриття шкідливих посилань, недотримання політик безпеки;

– відсутність кваліфікованих кадрів – попит на фахівців з кібербезпеки перевищує пропозицію, що призводить до дефіциту експертів.

3. ***Складність захисту розподілених і хмарних систем:***

– хмарні сервіси – перехід до хмарних технологій створює нові вектори атак, пов'язані з неправильним налаштуванням, доступом та контролем;

– інтернет речей (IoT) – велика кількість підключених пристроїв з обмеженими можливостями безпеки створює додаткові ризики;

– розподілені мережі – захист складних мереж і систем, що працюють у різних географічних локаціях, ускладнюється.

4. ***Проблеми з управлінням даними та конфіденційністю*:**

– великі обсяги даних – збір і обробка великих масивів даних підвищує ризик витоків і зловживань;

– регуляторні вимоги – необхідність дотримання законодавства (GDPR, локальні закони) ускладнює процеси обробки та зберігання інформації;

– відсутність прозорості – недостатня прозорість у використанні даних користувачів підриває довіру.

5. ***Недосконалість технологій захисту та їх інтеграції:***

– застарілі системи – багато організацій використовують застарілі програмні та апаратні рішення, які вразливі до сучасних атак;

– інтеграція рішень – відсутність єдиної стратегії безпеки і проблеми сумісності між різними системами ускладнюють ефективний захист;

– відсутність автоматизації – ручне управління безпекою не встигає за швидкістю розвитку загроз.

6. ***Відсутність ефективної стратегії реагування на інциденти:***

– повільне виявлення атак – недостатній моніторинг і аналіз подій безпеки призводить до затримок у реагуванні;

– відсутність планів реагування – багато організацій не мають чітких процедур для швидкого відновлення після кіберінцидентів;

– недостатня співпраця – відсутність координації між різними підрозділами та зовнішніми партнерами послаблює захист.

Враховуючи зазначене вище, необхідно підкреслити, що інформаційна безпека та кібербезпека – це два тісно пов'язані, але не тотожні поняття, які разом формують комплексний підхід до захисту інформації в сучасному цифровому світі. Розуміння їх системності допомагає краще організувати заходи захисту, оцінити ризики та побудувати ефективні стратегії безпеки.

Кібербезпека є підгалуззю інформаційної безпеки, яка зосереджена на захисті комп'ютерних систем, мереж, програмного забезпечення та даних у цифровому просторі від кіберзагроз, таких як хакерські атаки, шкідливе програмне забезпечення, фішинг, DDoS-атаки тощо. Її особливістю є наступне :

– вона орієнтована на цифрові технології та інтернет-середовище;

– включає захист мереж, пристроїв, додатків і даних;

– акцент робиться на протидії кіберзлочинам і кібертероризму.

Таким чином, інформаційна безпека – ширше поняття, яке охоплює всі аспекти захисту інформації, включно з фізичними, адміністративними та технічними заходами. У свою чергу, кібербезпека – частина інформаційної безпеки, що фокусується на цифровому середовищі. Системністьозначає, що інформаційна безпека і кібербезпека розглядаються як частини єдиної системи захисту інформації, де кожен елемент (технології, люди, процеси) взаємодіє для досягнення загальної мети – забезпечення безпеки інформації.

Основними компонентами цієї системи є :

– технічні засоби (антивіруси, фаєрволи (програмні або апаратні засоби безпеки, які фільтрують мережевий трафік, аналізуючи вхідні та вихідні дані на основі встановлених правил. Вони діють як “щит”, захищаючи пристрої від несанкціонованого доступу, кібератак та шкідливого контенту), системи виявлення вторгнень);

– організаційні заходи (політики безпеки, навчання персоналу);

– процеси управління ризиками (оцінка загроз, планування реагування);

– людський фактор (усвідомлення, відповідальність, поведінка користувачів).

Прикладами зазначеної взаємодії є :

– захист корпоративної мережі: кібербезпека забезпечує захист від зовнішніх атак, а інформаційна безпека – контроль доступу до інформації всередині організації;

– політика безпеки: встановлює правила для користувачів, які охоплюють як фізичний захист документів, так і цифровий захист паролів і доступу;

– інцидент-менеджмент: включає виявлення кіберінцидентів, їх аналіз і реагування, а також заходи для запобігання повторним випадкам на рівні всієї інформаційної системи.

Таким чином інформаційна безпека і кібербезпека – це взаємодоповнюючі поняття, які разом формують цілісну систему захисту інформації. Системний підхід дозволяє ефективно координувати технічні, організаційні та людські ресурси для мінімізації ризиків. Розуміння системності цих понять є ключовим для побудови надійної стратегії безпеки в будь-якій організації.

У рамках цифрової трансформації суспільства жодна із сфер діяльності не обходиться без комп’ютерних технологій збору, обробки та зберігання інформації. Таким чином, інформація має унікальну цінність і є критично важливим ресурсом, який потребує надійних методів захисту. Превентивні заходи щодо усунення загроз та ризиків в умовах цифрової економіки, забезпечення безпеки сучасного інформаційно-технологічного (ІТ) середовища стали сьогодні основою конкурентоспроможності для людини, бізнесу та держави [9, с. 9].

Висновок. Широта, глибина і темпи сучасної цифровізації у глобальному вимірі створюють як нові можливості, так і серйозні виклики для інформаційної безпеки та кібербезпеки. Основні існуючі проблеми пов’язані зі зростанням масштабів та складності загроз, з наявним людським фактором, зі складністю захисту сучасних технологій, з недосконалими механізмами управлінням даними, а також з недосконалістю існуючих механізмів та шляхів прийняття рішень та здійснення їхніх процедур. Для ефективного протистояння цим викликам необхідна комплексна стратегія, що включає суттєве підвищення інформаційної культури та кіберосвіченості на всіх рівнях, впровадження сучасних технологій та механізмів захисту даних, автоматизацію процесів та механізмів забезпечення безпеки.

Нині під інформаційною безпекою слід розуміти комплексну систему захисту даних від несанкціонованого доступу. У свою чергу, кібербезпека – це спеціалізована

частина інформаційної безпеки, що зосереджена на цифрових технологіях, на носіях збереження та обробки даних, на мережах їх передачі. Системність цих двох понять забезпечує ефективність захисту даних, інтегруючи кібербезпеку в загальну стратегію інформаційної безпеки.

ПОДЯКИ: Немає

КОНФЛІКТ ІНТЕРЕСІВ: Немає

Використана література

1. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25.02.2017 р. № 47/2017. URL : https://zakon.rada.gov.ua/laws/show/47/2017#Text (дата звернення: 03.03.2026).

2. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» : Указ Президента України від 28.12.2021 р. № 685/2021. URL : https://zakon.rada.gov.ua/laws/show/685/2021#n7 (дата звернення: 03.03.2026).

3. Цифровізація – це поступове перетворення усіх державних послуг на зручні онлайн-сервіси. URL : https://www.rv.gov.ua/news/cifrovizaciya-ce-postupove-peretvorennya-usih-derzhavnih-poslug-na-zruchni-onlajn-servisi (дата звернення: 03.03.2026).

4. Мех О. А., Бублик С. Б. Глобальна цифровізація як виклик суб'єктам наукової та науково-педагогічної діяльності в Україні : концептуальні проблеми і шляхи їх вирішення. *Наука та наукознавство*. 2023. № 2 (120). С. 59-83. URL : file:///C:/Users/Admin/Downloads/Nauka_ta_Naukoznavstvo_2-2023-59-83%20(1).pdf (дата звернення: 03.03.2026).

5. Про національну програму інформатизації : Закон України від 01.12.2022 р. № 2807-IX. URL : https://zakon.rada.gov.ua/laws/show/2807-20#Text (дата звернення: 03.03.2026).

6. Про цифровий контент та цифрові послуги : Закон України від 10.08.2023 р. № 3321-IX. URL : https://zakon.rada.gov.ua/laws/show/3321-20#Text (дата звернення: 03.03.2026).

7. Про схвалення Стратегії здійснення цифрового розвитку, цифрових трансформацій і цифровізації системи управління державними фінансами на період до 2030 року та затвердження плану заходів щодо її реалізації : Розпорядження Кабінету Міністрів України від 17.11.2021 р. № 1467-р. URL : https://zakon.rada.gov.ua/laws/show/ 1467-2021-р#Text (дата звернення: 04.03.2026).

8. Жаворонок А. В., Лопащук І. А.. Цифровізація соціальної сфери в контексті забезпечення економічної безпеки держави. *Економічний простір.* 2024. № 189. С. 253-258. URL : https://archer.chnu.edu.ua/xmlui/bitstream/handle/123456789/10808/1420-Текст%20статті-1501-2-10-20240311.pdf?sequence=1&isAllowed=y (дата звернення: 03.03.2026).

9. Близнюк М. М. Інформаційна безпека в епоху цифрових трансформацій (с. 9-14). Безпека життя і діяльності людини: теорія та практика : зб. наук. пр. всеукр. наук.-практ. конф., присвяченої Всесвітнім Дням цивільної оборони та охорони праці. (Полтава, 28 квіт. 2022 р.) / під ред.: В. П. Титаренко, О. В. Кудря. Полтава : ПНПУ, 2022. 242 с. URL : http://dspace.pnpu.edu.ua/bitstream/123456789/19230/1/3.pdf (дата звернення: 04.03.2026).

Ігор Федорович Корж
доктор юридичних наук, старший науковий співробітник
заступник керівника наукового центру цифрової трансформації і права Державної наукової установи "Інститут інформації, безпеки і права Національної академії правових наук України"
04053, Україна, м. Київ, пров. Несторівський, 4
email: garry52@ukr.net

Володимир Миколайович Фурашев
кандидат технічних наук, старший науковий співробітник
заступник директора Державної наукової установи “Інститут інформації, безпеки і права Національної академії правових наук України”
04053, Україна, м. Київ, пров. Несторівський, 4
email: vfurashev@gmail.com

Ihor F. Korzh
Doctor of Law, Senior Research Fellow
Deputy Head of the Scientific Center for Digital Transformation and Law
State Scientific Institution "Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine"
4 Nestorivskyi Lane, Kyiv, 04053, Ukraine
email: garry52@ukr.net
Volodymyr M. Furashev
PhD in Technical Sciences, Senior Research Fellow
Deputy Director of the State Scientific Institution "Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine"
4 Nestorivskyi Lane, Kyiv, 04053, Ukraine
email: vfurashev@gmail.com

Рекомендоване цитування: Корж І.Ф., Фурашев В.М. Проблеми інформаційної безпеки в умовах цифровізації. *Інформація і право.* № 2(57)/2026. 2026. С. 112-129. https://doi.org/10.37750/2616-6798.2026.2(57).364408

Suggested Citation: Korzh I., Furashev V. (2026) Information Security Problems in the Conditions of Digitalization. Information and Law. 2(57)/2026. 112-129. https://doi.org/10.37750/2616-6798.2026.2(57).364408

Дата надходження статті до редакції: 11.03.2026 р.
Дата прийняття статті до друку після рецензування: 18.03.2026 р.
Дата публікації (оприлюднення): 31.05.2026 р.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~