Тільки в цьому разі підприємства зможуть повною мірою скористатися перевагами ШІ для забезпечення стійкої та надійної інформаційної та фінансової безпеки в умовах цифрового середовища, що динамічно розвивається.

1. Microsoft Security. Що таке інформаційна безпека? URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-information-security-infosec.

2. Горник В. Г., Кравченко С. О. Механізми забезпечення інформаційної безпеки підприємницької діяльності як складника інформаційної безпеки держави. *Вчені записки ТНУ імені В. І. Вернадського.* 2020. № 2. С. 206–212. DOI: https://doi.org/10.32838/2663-6468/2020.2/34.

3. Шевчук М. О. Основні аспекти механізму забезпечення інформаційної безпеки підприємницької діяльності. *Науковий вісник Ужгородського національного університету.* Серія : Право. 2024. Вип. 85. Ч. 3. С. 181–186. DOI: https://doi.org/10.24144/2307-3322.2024.85.3.28.

4. Кицюк В. М., Пупинін О. С. Інформаційна безпека підприємства: теоретичний аспект. *Сучасний захист інформації: науково-технічний журнал*. 2024. № 2. С. 103–108. DOI: https://doi.org/10.31673/2409-7292.2024.020012.

5. Шульга В. І. Сучасні підходи до трактування поняття інформаційна безпека. *Ефективна економіка.* 2015. № 4. URL: http://www.economy.nayka.com.ua/?op=1&z=5514

6. Зубок М. І. Інформаційна безпека в підприємницькій діяльності. Київ : ГНОЗІС, 2015. 216 с.

7. Вудвуд В. В., Батієвська О. В. Фінансова безпека підприємства: сутність, цілі, принципи та шляхи забезпечення. *Entrepreneurship and Trade*. 2019. № 25. С. 89–93. DOI: https://doi.org/10.36477/2522-1256-2019-25-12.

8. Барановський О. І. Фінансова безпека. Ін-т екон. прогнозування. Київ : Фенікс, 2015. 338 с.

9. Бланк І. А. Управління фінансовою безпекою підприємства. Київ : Ніка-Центр, 2014. 784 с.

10. Бердар М. Забезпечення фінансової безпеки суб'єктів підприємництва. *Вісник Київського національного університету ім. Т. Шевченка. Економіка.* 2016. № 125. С. 73.

11. Клочко Т. Фінансова безпека як умова фінансової стійкості підприємства. *Економіка та суспільство.* 2021. № 23. DOI: https://doi.org/10.32782/2524-0072/2021-23-17.

12. Мельник В. В., Жук Т. В. Інформаційне забезпечення як складова фінансової безпеки підприємства. *Ефективна економіка.* 2021. № 6. DOI: https://doi.org/10.32702/2307-2105-2021.6.80.

13. Онищенко С. В., Глушко А. Д. Інформаційно-аналітичне забезпечення фінансової безпеки підприємств у сучасних умовах. *Науковий вісник Одеського національного економічного університету*. 2023. № 7–8 (308–309). С. 145–154. DOI: https://doi.org/10.32680/2409-9260-2023-7-8-308-309-145-154.

14. Galushko O., Ciobanu G. Information systems in finance: challenges and perspectives. *Scientific Bulletin of Dnipropetrovsk State University of Internal Affairs.* 2023. Special Is. № 1. S. 259–265. DOI: https://doi.org/10.31733/2078-3566-2023-5-259-265.

15. Метеленко Н., Сіліна Ф., Попова А., Афонов Р. Оптимізація фінансової безпеки промислового підприємства в епоху цифровізації за допомогою інформаційно-аналітичних технологій. *Humanities Studies*. 2024. № 18 (95). С. 163–175. DOI: https://doi.org/10.32782/hst-2024-18-95-17.

16. Левченко В. Ф., Галушко О. І., Скрипова М. М. Актуальні проблеми визначення та мінімізації ризиків українських підприємств. *Економічний простір.* 2008. № 20/2. С. 200–206.

17. Галушко О., Селівьорстова Т. Кібербезпека в управлінні ланцюгами постачань (SCM). *Науковий вісник Дніпропетровського державного університету внутрішніх справ.* 2022. Спец. вип. № 2 (121). С. 537–542. DOI: https://doi.org/10.31733/2078-3566-2022-6-537-542.

18. Марценюк Л. Вплив штучного інтелекту на розвиток туристичної індустрії. The 3th International scientific and practical conference "Theoretical aspects of education development" (January 24–27, 2023). Warsaw, Poland. International Science Group. 2023. P. 561.

Юлія КОСЕНКО
заступник директора
ННІ права та інноваційної освіти
Дніпровського державного
університету внутрішніх справ
(м. Дніпро, Україна)

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК АСПЕКТ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Більшість сучасних авторів, які досліджують окремі аспекти національної безпеки – економічну безпеку, соціальну безпеку, політичну стабільність тощо, – розглядають ці аспекти як частину загальнолюдської діяльності, в якій породжуються ризики та загрози національній безпеці [2]. Одним із таких аспектів є інформаційна безпека, аналізу якої присвячено цю роботу.

З точки зору загального поняття безпеки термін «національна безпека» позначає стан нації, громадянина та держави, в якому ризикам та загрозам їхньому існуванню та розвитку протистоїть надійна система (система національної безпеки) [1].

Примітно також, що більшість сучасних авторів, які досліджують окремі аспекти національної безпеки, розглядають їх як частину загальнолюдської діяльності, в якій генеруються ризики та загрози безпеці й національній безпеці зокрема [4].

Те, що сьогодні визначається як національна безпека, протягом століть розумілося як здатність – відбивати агресію. Закрите суспільство очікує і знаходить причини своєї нестабільності ззовні. Війна є кінцевою еманацією цього зовнішнього конфлікту.

Нове розуміння безпеки – це також питання зміни менталітету, чого досягти надзвичайно важко [3].

Наприклад, нерідко дослідники, які поділяють так зване широке розуміння безпеки, використовують фразу «безпека та оборона», зважаючи на те, що це поняття, які відображають різний ступінь узагальнення. Без сумніву, воєнний аспект безпеки є надзвичайно важливим, але це один із аспектів національної безпеки. Також часто зустрічаємо вислів «внутрішній порядок і безпека», який знову ж таки представляє ці два поняття рівноправними в плані узагальнення, а в умовах глобалізації «внутрішнє» і «зовнішнє» мають цілком умовний характер і навряд чи є продуктивними для проведення аналізу [3].

Це дає нам можливість визначити поняття «середовище безпеки». Загалом це сукупність процесів у суспільстві, у контексті яких у певній публічній сфері генеруються ризики та загрози.

Система національної безпеки – це фактично все суспільство, організоване для протидії ризикам і загрозам безпеки. Його можна трактувати через призму основних органів влади та їхньої ролі в процесі управління, а також розглядати як взаємодію інститутів парламенту, президента, уряду, підкреслюючи їхні повноваження у визначенні та проведенні політики безпеки. Очевидно, що держава має місце в такій визначеній системі, але вона не є єдиним суб'єктом політики безпеки.

Держава в системі безпеки реалізує численні галузеві політики –досягнення економічної безпеки, соціальної безпеки, духовної цілісності, екологічної безпеки, інформаційної безпеки тощо.

Що дає підстави визначати інформаційну безпеку як один із найважливіших аспектів національної безпеки?

Ключовою характеристикою сучасного суспільства є якісно нове ставлення до інформації як наслідок великих технічних досягнень у створенні та розвитку комунікаційних і комп'ютерних технологій.

В результаті масового надходження інформації та використання технологій, які полегшують доступ до інформації, люди опинилися в «інформаційному потопі». Людські здібності та навички поводження й корисного використання такого величезного ресурсу виявилися обмеженими. Доступ до занадто великої кількості інформації, яку люди не можуть зрозуміти і з якої вони не можуть отримати корисні знання протягом розумного періоду часу, має той самий ефект, що й брак інформації.

На початку XXI ст. стало зрозуміло, що чим більш інноваційним, що швидко змінюється шляхом генерування безперервного потоку нових і нових знань, стає суспільство, і в цьому сенсі чим більше воно рефлексивне, тим більше воно завантажене небезпеками, ризиками, конфліктами та невизначеністю. Це призводить до епістемологічних збоїв у процесі рефлексії, які порушують функціонування соціальних систем [3].

Людський вимір змін не менш важливий, ніж технологічний, економічний чи політичний. Соціальна дезінтеграція окремої людини або певної соціальної групи може призвести до серйозних наслідків для всієї соціальної системи.

Світ вступає в нову еру якісних змін у конфліктах. Невелике локальне насильство може легко набути глобальних масштабів, невеликі загрози – призвести до глобальних наслідків. У сучасному світі насильство реалізується через різні типи мереж із різними акторами.

Базове уявлення про інформаційну цивілізацію пов'язане з розумінням того, що це черговий якісний еволюційний етап у розвитку суспільних відносин і суспільних практик. Він характеризується не тільки тотальним домінуванням інформації, але насамперед авангардними технологіями її використання в глобальній соціальній практиці. Трансформації та радикальні зміни, які відбуваються на сучасному етапі розвитку суспільства, охоплюють

усі сфери життя і впливають як на людину, так і на всю цивілізацію.

Розвиток Інтернету найкраще демонструє синергетичний ефект реалізації переходу, за якого економічні та соціальні функції переміщуються від капіталу до інформації (будь-який матеріальний ресурс зрештою може бути перетворений в інформацію); рівень знань поступово, але назавжди витісняє власність як чинник соціальної диференціації, і виникає симбіоз між соціальними організаціями та інформаційними технологіями. Кожна подія являє собою ланцюжок трансакцій, а не простий причинно-наслідковий зв'язок. У суспільстві вже не існує класичного поділу сфер людської діяльності в чистому вигляді. Інформаційна сфера, безсумнівно, стає однією з головних складових соціальної системи, а інформація – найважливішим стратегічним ресурсом [3].

Інформація, у всьому розмаїтті, в якому вона проявляється, є цінним ресурсом, як і фінансові, матеріальні та людські ресурси. Тобто слід визначити інформаційну безпеку як аспект національної безпеки, як стан нації, її громадян і держави.

Інформаційна безпека – це здатність держави, суспільства, соціальної групи, особистості забезпечити необхідний інформаційний ресурс, оптимальну соціальну ентропію та інформаційне середовище для підтримки життєдіяльності та сталого розвитку суспільства, а також протистояти інформаційним загрозам та негативним інформаційним впливам на індивідуальну та суспільну свідомість, а також на критичну інформаційну інфраструктуру [2].

Можна визначити інформаційну безпеку і як стійкий стан інформаційної сфери, який забезпечує її цілісність і гарантує захист об'єктів від несприятливих внутрішніх і зовнішніх впливів, що базується на цінностях, потребах і цілях розвитку соціальних суб'єктів [4].

З точки зору визначення національної безпеки, де незмінно присутня держава, додаткові аргументи для розгляду інформаційної безпеки як аспекту національної безпеки знаходимо у такому визначенні: «Інформаційна безпека – це захист держави на стратегічному, оперативному та тактичному рівнях».

Надзвичайно важливо при визначенні інформаційної безпеки звернути увагу на ризики та загрози, а також систему захисту інформації. У сучасному світі інформаційна безпека піддається різноманітним загрозам, включаючи кібератаки, соціальну інженерію, віруси та шкідливі програми. Ці загрози не знають кордонів і можуть стосуватися як державних установ, так і приватних компаній і громадян. Тому для забезпечення ефективної інформаційної безпеки країни повинні розробити комплексні стратегії та політику, які охоплювали б усі аспекти цієї проблеми.

Важливо підкреслити відмінність змісту поняття «інформаційна безпека» від таких категорій, як «захист інформації», «таємна інформація», «захист секретної інформації». Побудова системи захисту інформації базується на домінуванні технологічної складової. Наприклад, побудова державної системи захисту секретної інформації, сертифікація її засобів і формування дієвих механізмів її захисту є невід'ємною частиною досягнення інформаційної безпеки країни.

На початку XXI ст. сформувалися два конкуруючі сек'юритизаційні дискурси у сфері інформаційної безпеки. У межах цих дискурсів виділяються два основні типи інформаційної безпеки: інформаційно-технічна та інформаційно-психологічна (також використовується термін «політична та ідеологічна безпека») [3].

Забезпечення інформаційно-технічної безпеки включає захист, контроль, дотримання закону, застосування правового порядку та дотримання правил у сфері телекомунікацій (захист від несанкціонованого доступу, злому комп'ютерних мереж і сайтів, логічних бомб, комп'ютерних вірусів і шкідливого програмного забезпечення, несанкціонованого використання частот, електронних атак тощо).

Забезпечення інформаційно-психологічної безпеки також включає захист психологічного стану суспільства та держави від негативного інформаційного впливу.

Що стосується поняття «кібербезпека», то воно міститься в загальному визначенні поняття «інформаційна безпека».

Таким чином, значущість захищених національних інтересів, необхідність адекватного та своєчасного реагування на темпи та динаміку в процесі розвитку суспільних відносин у глобальному масштабі визначають пріоритети діяльності із забезпечення ефективного функціонування та вдосконалення системи захисту інформації як стратегічного ресурсу.

---

1. Кононенко В. П., Здоровко С. С., Корольова А. Є. Інформаційна безпека як стан. *Науковий вісник Ужгородського національного університету.* Серія «Право». 2023. Вип. 76. Ч. 2. С. 244–251.

2. Панченко О. Інформаційна складова національної безпеки. *Вісник Національної академії*

Державної прикордонної служби України. 2021. Вип. 3. С. 8–11.

3. Dobak I. Thoughts on the evolution of national security in cyberspace. *Security and Defence Quarterly.* 2021. № 33 (1). С. 75–85. URL : https://securityanddefence.pl/Thoughts-on-the-evolution-of-national-security-in-cyberspace,133154,0,2.html.

4. Holdsworth J., Kosinski M. What is information security? IBM. URL : https://www.ibm.com/think/topics/information-security.

Наталія ПРОТОПОПОВА
старший викладач кафедри
соціально-економічних дисциплін
Дніпровського державного
університету внутрішніх справ
(м. Дніпро, Україна)
https://orcid.org/0000-0002-0207-9301

ІНФОРМАЦІЙНА БЕЗПЕКА МАЛИХ ПІДПРИЄМСТВ В УМОВАХ ВОЄННОГО СТАНУ В УКРАЇНІ

Інформаційна безпека є важливим аспектом діяльності будь-якого підприємства, особливо в умовах воєнного стану. Малі підприємства стають вразливими до кіберзагроз через обмежені ресурси та недостатню обізнаність у сфері кіберзахисту. В умовах війни в Україні зростає ризик кібератак, витоків конфіденційної інформації, фінансових шахрайств та інших загроз, що можуть паралізувати роботу бізнесу.

Основними загрозами інформаційній безпеці малих підприємств є:

1. Кібератаки – зловмисники можуть використовувати фішинг, віруси, шкідливе програмне забезпечення для доступу до корпоративних даних;
2. Соціальна інженерія – маніпулювання співробітниками для отримання важливої інформації або доступу до внутрішніх систем;
3. Витоки даних – ненавмисне або навмисне розголошення конфіденційної інформації через необережність персоналу чи недоліки в системах захисту;
4. Фізичні загрози – втрата або крадіжка носіїв інформації, руйнування серверів унаслідок бойових дій;
5. Несанкціонований доступ до хмарних сервісів – уразливість облікових записів у разі ненадійних паролів або недостатніх заходів безпеки;
6. Шахрайство та фінансові махінації – кібершахраї можуть створювати фальшиві рахунки та підробляти фінансові документи.

Основними методами забезпечення інформаційної безпеки можна визначити наступні:

1. Захист IT-інфраструктури:
   - використання оновлених антивірусних програм і брандмауерів;
   - регулярне оновлення програмного забезпечення та операційних систем;
   - налаштування багатофакторної автентифікації для всіх критичних систем;
2. Контроль доступу:
   - обмеження доступу співробітників до важливих даних;
   - використання VPN для захисту з'єднання під час віддаленої роботи;
   - створення резервних копій критично важливих даних;
3. Захист від соціальної інженерії:
   - навчання персоналу основам інформаційної безпеки та розпізнавання фішингових атак;
   - перевірка автентичності запитів, що стосуються фінансових операцій;
4. Захист фізичних носіїв інформації:
   - використання шифрування для захисту файлів і носіїв інформації;
   - організація безпечного зберігання паперових документів;
   - контроль над використанням особистих USB-носіїв у корпоративних мережах;
5. План дій у разі кіберінцидентів:
   - розробка алгоритму дій для відновлення роботи у разі кібератаки;
   - регулярне тестування систем безпеки та вразливостей;