ГЕРАСИМЕНКО *Ігор Олександрович*
Київський інститут Національної гвардії України

ОСНОВНІ ЗАГРОЗИ ТА ВИКЛИКИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ В ДЕРЖАВНОМУ СЕКТОРІ

В сучасному світі, де інформаційні технології відіграють дедалі вагомішу роль, загрози інформаційній безпеці неухильно зростають. Розглянемо основні загрози, які стоять перед інформаційною безпекою в державному секторі.

1. Кіберзлочинність.

Кіберзлочинність є однією з найсерйозніших загроз інформаційній безпеці. У державному секторі, де обробляються чутливі дані, фішинг може мати катастрофічні наслідки.

2. Інформаційна війна.

Використання ЗМІ для поширення неправдивих відомостей з метою керування суспільною думкою особливо важливо в умовах війни. Напади на репутацію державних органів можуть здійснюватися через активні дії в соціальних мережах.

3. Внутрішні загрози.

Це можуть бути як недобросовісні службовці, так і низька кваліфікація кадрів. Працівники, які мають доступ до конфіденційної інформації, можуть свідомо або випадково сприяти її витоку [1, с. 201].

4. Недосконала правова база.

Правовий фундамент інформаційної безпеки в Україні вимагає поліпшення. Існування пропусків у законах може статися так, що певні загрози залишаться поза увагою правоохоронців.

5. Технологічне відставання.

Більшість державних організацій використовують застаріле обладнання та методи, що не спроможне ефективно гарантувати захист інформації. Недолік

сучасних систем шифрування та захисту даних збільшує ризик витоку конфіденційної інформації.

6. Недостатня обізнаність.

Значна кількість співробітників не проходять навчання з базових правил кібербезпеки, що збільшує ймовірність помилок під час роботи з конфіденційними даними.

Забезпечення інформаційної безпеки вимагає комплексного підходу, який охоплює юридичні, організаційні, технічні та освітні аспекти [2]. Механізми реагування на загрози інформаційній безпеці мають бути спрямовані на захист державного сектору від різних кібер-нападів, дезінформаційних кампаній, витоків даних та інших загроз, які можуть порушити стабільність та суверенітет країни [3].

Інституційний механізм передбачає низку державних органів та організацій, які відповідають за гарантування інформаційної безпеки. Ці органи мають злагоджено працювати для дієвого реагування на виклики [4, с. 136]. Основними дійовими особами цього механізму є:

- Кабінет Міністрів України.
- Рада національної безпеки і оборони України (РНБО).
- Служба безпеки України (СБУ).
- Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ).

Чинне законодавство України охоплює низку нормативно-правових актів, що визначають принципи та процедуру забезпечення кібербезпеки:

1. Закон України «Про національну безпеку України» окреслює ключові підвалини державної політики у сфері національної безпеки, зокрема, інформаційної [5].

2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» регулює взаємини, пов'язані із захистом інформації в інформаційно-телекомунікаційних системах, конкретизує права та

обов’язки власників інформації, операторів інформаційних систем і споживачів [6].

3. Закон України «Про електронні комунікації» закладає правові основи діяльності у сфері електронних комунікацій, встановлює права та обов'язки операторів та провайдерів електронних комунікацій, а також користувачів їхніх послуг [7].

Слід підкреслити наявність певних прогалин у законодавстві, що вимагають усунення для результативної адаптації до теперішніх викликів. Зокрема, постала нагальна потреба прийняття правок до закону про кібербезпеку, який би брав до уваги міжнародний досвід та окреслював стратегічні вектори розвитку кібербезпеки в Україні.

Для підвищення результативності системи реагування на інформаційні виклики в Україні, критично важливо вжити комплекс заходів, що охоплюють правове поле, технічне оснащення, освітню сферу та взаємодію на міжнародному рівні:

1. Розробка нормативно-правової бази, що регулює діяльність у соціальних медіа.

2. Запровадження технологій штучного інтелекту для автоматизації процесів виявлення та аналізу кіберзагроз.

3. Впровадження курсів з кібербезпеки в навчальні плани шкіл, професійних училищ та вишів.

4. Залучення ІТ-компаній до розробки рішень для захисту інформації.

5. Обмін набутим досвідом з країнами, які мають позитивні практики протистояння кібернетичним загрозам, може допомогти Україні у розбудові дієвої системи кібербезпеки [8].

Механізми реагування на загрози інформаційній безпеці мусять бути комплексними, адаптивними та постійно вдосконалюватися. Лише за умови системного підходу та безперервного розвитку можна забезпечити надійний захист інформаційного простору України від сучасних викликів та загроз.

СПИСОК ВИКОРИСТОВУВАНИХ ДЖЕРЕЛ

1. Гаврильців М.Т. Інформаційна безпека держави в системі національної безпеки України. Юридичний науковий журнал. 2020. № 2. С. 200–203.

2. Указ Президента України № 449/2014 Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» URL: http://www.president.gov.ua/documents/17588.html?PrintVersion (дата доступу 02.04.2025)

3. Державна служба спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua/ua (дата доступу 02.04.2025)

4. Нестерович В. Забезпечення інформаційної безпеки як функція держав в умовах сучасних викликів і загроз. Fìlosofsʹkì ta metodologìčnì problemi prava. 2020. № 1 (19). С. 136–137.

5. Закон України «Про національну безпеку України». Документ 2469-VIII, поточна редакція від 09.08.2024.

6. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах». Документ 80/94-ВР, поточна редакція від 28.06.2024.

7. Закон України «Про електронні комунікації». Документ 1089-IX, поточна редакція від 01.04.2025.

8. Закон України «Про основні принципи забезпечення кібербезпеки України». Документ № 2163-VIII, набув чинності 9 травня 2018 року.