

## ІНФОРМАЦІЙНА ТА КІБЕРБЕЗПЕКА: ВИКЛИКИ ТА ПРОБЛЕМИ В УМОВАХ СЬОГОДЕННЯ

**Полотай Орест**

к.т.н., доцент, доцент кафедри управління інформаційною безпекою \ Львівський державний університет безпеки життєдіяльності, м. Львів, Україна  
ORCID: <https://orcid.org/0000-0003-4593-8601>

У сучасному світі інформація відіграє надзвичайно важливу роль. Володіння певною інформацією означає володіння певною цінністю суспільного характеру. З нею тісно пов'язані численні права і свободи громадян, життєві інтереси суспільства та держави. Саме тому прогресивний розвиток України як суверенної, демократичної, правової та економічностабільної держави можливий тільки за умови якнайповнішого забезпечення належного рівня інформаційної безпеки.

І з поміж численних проблем забезпечення інформаційної безпеки України вони виділяють наступні:

- засилля іноземної теле-, радіо-, друкованої продукції;
- зниження наукового потенціалу у галузі інформатизації, телекомунікацій та зв'язку;
- ще більш гострою є мовна проблема ( так з усіх українських періодичних видань лише 20% зареєстровані як україномовні);
- у зовнішньополітичній сфері однією з найвагомійших загроз інформаційної безпеки є поширення у світовому інформаційному просторі викривленої, недостовірної та упередженої інформації, що завдає шкоди національним інтересам України відставання вітчизняних наукоємних і високотехнологічних виробництв, особливо в галузі комп'ютерно-телекомунікаційних засобів і технологій [6];
- відставання України від розвинутих країн за рівнем інформатизації соціогуманітарної сфери, насамперед системи освіти, охорони здоров'я соціального забезпечення, послуг культури [6];
- розголошення інформації, яка становить
- державну та іншу таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави [7, с.154].

В Україні є документи, котрі регламентують питання інформаційної безпеки: Концепція Національної безпеки України та Концепція технічного захисту інформації в Україні. Дані документи стали підставою для визначення основних принципів та напрямків державної політики у сфері інформаційної безпеки [5, с.126].

Останніми роками інформаційна безпека все більше трансформується, або, якщо так можна сказати, підпадає під вплив, у кібербезпеку.

Реалії сьогодення свідчать про те, що кіберзагрози еволюціонують в прискореному темпі, кіберзлочини стають досконалішими, краще організованими і транснаціональними. Це зумовлено тим, що мережа Інтернет, цифрові послуги, інформаційно-комунікаційні технології (ІКТ) стали невід'ємною частиною економіки в усьому світі: від електронного документообігу, інтернет-магазинів та онлайн-банкінгу до систем інтернету речей та інтелектуальних систем управління підприємствами. Зі зростанням залежності від використання ІКТ у бізнесі і підприємстві відповідно зростають кіберризиків і кіберзагрози, що потребує завчасного реагування щодо їх запобігання або вирішення та обізнаності з факторами ризику всіх зацікавлених сторін. Система кібербезпеки має працювати в інтересах громадськості як для постачальників послуг, так і для користувачів послуг [8, с.150].

Все це потребує професійних кадрів, що у свою чергу передбачає відповідну систему підготовки фахівців у даній галузі.

Через відсутність в державі чіткої стратегії, підготовка кадрів для галузі інформаційної безпеки практично не має попиту. В даній ситуації має місце лише створення окремих елементів, котрі не завжди є правильними. Враховуючи базу різноманітних технічних закладів вищої освіти (ЗВО), навчання спрямоване на технічні й технологічні аспекти захисту інформації. Якщо ж брати до уваги юридичні ЗВО, там навчання проходить лише з посиленням вивченням організаційно-правових аспектів інформаційної безпеки.

Кожному відомо, що головною проблемою навчального процесу є правильне та ефективне проведення занять з метою підвищення їх ефективності. Важливу роль в цьому відіграє мотивація слухачів [2]. Згідно з опитуваннями, котрі були проведені у різноманітних вузах за напрямом підготовки фахівців з кібербезпеки було виявлено, що значна більшість студентів, котрі знаходяться на навчанні виявили бажання вступити на дану спеціальність з метою вивчення тонкощів злому різноманітних мереж. Відповідно значно менша частина, прагне навчитись захищати мережу від всіх потенційних загроз.

Всі ці проблеми можна вирішити, адже в наш час є значна кількість ЗВО, що надають «подвійну» освіту. Кожен з випускників має базовий рівень знань в тій чи іншій сфері, володіє іноземною мовою та його подальше життя не можливе без використання комп'ютера. Якщо ж говорити про інформаційну сферу, то прикладом може стати спеціальність 125 Кібербезпека Львівського державного університету безпеки життєдіяльності (ЛДУ БЖД), де по закінченню навчання студентам видаються диплом міжнародного зразка – магістра в галузі кібербезпеки [3].

Навчальний процес в ЛДУ БЖД супроводжується за допомогою системи дистанційного навчання «Віртуальний університет ЛДУ БЖД» [1], яка працює на основі системи Moodle. Особливо позитивно дана система себе проявила під час пандемії та умов воєнного стану в нашій країні [4, с.151]. У віртуальному

університету ЛДУ БЖД є можливість курсантам та студентам здійснювати виконання практичних, лабораторних, самостійних чи розрахунково-графічних робіт (в залежності від специфіки курсу), проходити тестування, як поточного так і підсумкового екзаменаційного чи залікового.

Отже, на даному етапі розвитку комп'ютерних технологій в Україні є значний ряд проблем, проте, не враховуючи всі неблагополучні аспекти розвитку фахівців кібербезпеки, слід зазначити, що також є і позитивні моменти: наявність досить потужних центрів та вищих навчальних закладів, котрі здійснюють спеціалізовану підготовку фахівців, тісні взаємодія з іншими країнами, використання їх досвіду та наявність програм, в основі яких є обмін студентами. Саме ці аспекти та вирішення проблем описаних вище можуть допомогти нашій державі вийти на вищий рівень захисту інформації та підготовки висококваліфікованих фахівців у даній сфері діяльності.

### **Список використаних джерел:**

1. Віртуальне навчальне середовище «Віртуальний університет». [Електронний ресурс]. – Режим доступу з <http://virt.ldubgd.edu.ua/>
2. Закон України “Про Концепцію Національної програми інформатизації”. [Електронний ресурс]. – Режим доступу з <http://zakon2.rada.gov.ua/laws/show/75/98-вр>
3. Офіційний сайт Львівського державного університету безпеки життєдіяльності. [Електронний ресурс]. – Режим доступу з <https://ldubgd.edu.ua/>
4. Полотай О.І., Меньшикова О.В. Використання технологій дистанційного навчання в умовах Covid-19 в ЛДУ БЖД. VI Міжнародна науково-практична конференція «Інформаційно-комунікаційні технології в сучасній освіті: досвід, проблеми, перспективи». Львів: ЛДУ БЖД, 2021
5. Полотай О.І., Старенький М.І. До проблеми підготовки фахівців галузі інформаційної безпеки. Зб. матер. наук.-практ. конф. “Актуальні проблеми управління інформаційною безпекою держави” : (м. Київ, 18 березня 2016 р.). [в 2 ч.]. Ч. 2. Київ : Нац. акад. СБУ, 2016. С. 126–128.
6. Про Концепцію (основи державної політики) національної безпеки України: Постанова Верховної Ради України від 16 січня 1997 р. // Відомості Верховної Ради. – 1997. – № 3.
7. Саврук М.В. Проблеми забезпечення інформаційної безпеки України. Тези доповідей III міжнародної науково-практичної конференції «Інформаційна та економічна безпека (INFESCO-2010)». – Харків, 2010. – Випуск 3 (84). – С. 154-155.
8. Трофименко О., Прокоп Ю., Логінова Н., Задерейко О. Кібербезпека України: аналіз сучасного стану. Захист інформації, ТОМ 21, № 3, Липень-вересень 2019. С. 150-157.