СУЧАСНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ У НАВЧАЛЬНОМУ СЕРЕДОВИЩІ ЗАКЛАДУ ВІЙСЬКОВОЇ ОСВІТИ

Ольга Павлівна Пінчук,
старша наукова співробітниця,
заступниця директора з науково-експериментальної роботи
Інституту інформаційних технологій і засобів навчання НАПН України,
кандидатка педагогічних наук,
м. Київ
opinchuk1001@gmail.com

Алла Анатоліївна Прокопенко,
молодша наукова співробітниця
наукового центру дистанційного навчання
Національного університету оборони України
ім. Івана Черняховського,
м. Київ
allicka7@gmail.com

Кіберборотьба та протидія кіберзагрозам в інформаційній сфері розглядається сучасним суспільством будь-якої країни як один із найважливіших пріоритетів безпеки, вагомий чинник у розвитку військового, соціального, економічного та інших секторів. Концептуально розроблення ефективних засобів кібербезпеки Української держави та, зокрема, Збройних сил України, передбачено в низці законодавчих документів, що націлені на розвиток спроможностей сил оборони України. А саме, щодо стратегічних комунікацій у сфері оборони, упровадження сучасних інформаційних та космічних технологій, автоматизації управлінських процесів та їх цифровізації, а також діяльності в силах оборони України з відповідним рівнем захищеності інформації, що опрацьовується.

Подальша інтеграція в європейські структури безпеки та міжнародне оборонне співробітництво передбачають: державну підтримку оснащення Збройних сил України та інших складових сил оборони новим високотехнологічним озброєнням, військовою та спеціальною технікою; розвиток спроможностей щодо забезпечення кібербезпеки, кіберзахисту й кібероборони під час підготовки та ведення всеохопної оборони України; набуття повноправного членства України в НАТО [1]. Також важливим аспектом є формування

й організація виконання завдань оборонної реформи в частині, що стосується питань цифрової трансформації, інформаційних технологій, автоматизації, інформатизації та інформаційної безпеки (в тому числі й кібербезпеки) [2]. Фактично ж ідеться про досягнення повноцінного кібернетичного суверенітету держави.

Аналіз зарубіжних джерел та міжнародної співпраці між ЄС та НАТО, зокрема стосовно вимог про взаємодію в галузі кіберзахисту, дає підстави стверджувати, що негайного вирішення потребує проблема підвищення кваліфікації робочої сили в галузі кібербезпеки та інвестування в дослідження й інновації захисту від кіберзагроз. Завданням цифрової освіти є підвищення рівня обізнаності щодо кібербезпеки.

Освіта, зокрема професійна, повинна сприяти розвитку навичок критичного мислення, цифрової грамотності і навичок кіберзахисту. Нині дедалі більшої значущості набуває створення безпечного інформаційно-освітнього середовища закладів освіти різного рівня та профілю, що здійснюють підготовку фахівців і підвищення їхньої кваліфікації за різними спеціальностями [3].

Законом України «Про основні засади забезпечення кібербезпеки України» визначено поняття кіберпростору. Уразливість у кіберпросторі є реальною, серйозною, і вона швидко збільшується. Об'єкти критичної інфраструктури повністю залежать від ІТ-систем, об'єднаних у мережі. Порушення кібербезпеки мають руйнівні наслідки — від крадіжки особистої інформації до державних таємниць [4]. Підтримуючи думку дослідників [3], розглядаємо кіберпростір як тріаду: 1) інформація у своєму цифровому представленні; 2) технічна інфраструктура; 3) інформаційна взаємодія суб'єктів із використанням отриманої (переданої) інформації та обробки через технічну інфраструктуру.

Важливим завданням сьогодення є необхідність створення надійної системи кібернетичної безпеки. Тобто напряму, який пов'язаний із захистом цифрової інформації, операційних систем, комп'ютерних мереж, серверів, баз даних тощо від несанкціонованого втручання сторонніх осіб. Отже, ми виокремили основні кіберзагрози у сфері освіти: порушення конфіденційності, цілісності, доступності інформаційних ресурсів, що обробляються (передаються, зберігаються) у закладах освіти, злам баз даних працівників освіти, знищення вірусами баз даних, порушення безпеки режиму функціонування документообігу, порушення безпеки, сталого,

надійного та штатного режиму функціонування комунікаційних і технологічних систем.

Проблемою є використання недостовірної, ненаукової інформації або дезінформації з мережі Інтернет під час підготовки та/або проведення навчальних занять, відсутність захисту відомостей з електронної пошти, використання інтернет-ресурсів з відкритих джерел і засобів електронних комунікацій.

Отже, для України залишається актуальною низка проблемних питань, вирішення яких потребуватиме часу та зусиль як з боку держави, так і сектору безпеки й оборони. Від ефективності їх вирішення залежить, якою мірою українське суспільство зможе відповісти на сучасні кібербезпекові виклики.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про Стратегію воєнної безпеки України : Указ Президента України від 25 березня 2021 р. № 121. URL: https://www.president.gov.ua/documents/1212021–37661 (дата звернення: 09.06.2021).

2. Положення про Директорат політики цифрової трансформації та інформаційної безпеки у сфері оборони Міністерства оборони України : затверджено наказом Міністерства оборони України від 25 листопада 2020 р. № 440. URL: https://www.mil.gov.ua/content/mou_orders/mou_2020/440_nm.pdf (дата звернення: 09.06.2021).

3. Пінчук О. П., Литвинова С. Г., Буров О. Ю. Синтетичне навчальне середовище — крок до нової освіти. *Інформаційні технології і засоби навчання*. 2017. № 60 (4). С. 28–45. URL: https://doi.org/10.33407/itlt.v60i4.1831 (дата звернення: 10.06.2021).

4. Биков В. Ю., Буров О. Ю., Дементієвська Н. П. Кібербезпека в цифровому навчальному середовищі. *Інформаційні технології і засоби навчання*. 2019. № 70 (2). С. 313–331. URL: https://doi.org/10.33407/itlt.v70i2.2876 (дата звернення: 09.06.2021).