

ЗНАЧЕННЯ КІБЕРБЕЗПЕКИ В ОСВІТНЬО-ІНФОРМАЦІЙНИХ РЕАЛІЯХ СЬОГОДЕННЯ

Ящик Олександр Богданович

кандидат педагогічних наук,

викладач кафедри комп'ютерних технологій,

Тернопільський національний педагогічний університет імені Володимира Гнатюка

sanytnpu@gmail.com

Поєднання досягнень у сфері новітніх інформаційно-комунікаційних технологій (ІКТ) із надбаннями, що постали на базі стрімкого розвитку інформаційно-телекомунікаційних систем (ІТС), спричинили виникнення принципово нових глобальних субстанцій – інформаційного суспільства, а також інформаційного та кібернетичного просторів, які мають нині практично необмежений потенціал і відіграють провідну роль в економічному та соціальному розвитку кожної країни світу. Проте через небачене досі поширення ІКТ та ІТС світова спільнота отримала не лише численні переваги, а й цілу низку проблем, зумовлених дедалі більшою вразливістю інфо-сфери щодо стороннього кібернетичного впливу. Цілком природним наслідком стала необхідність контролю та подальшого врегулювання відповідних взаємовідносин, а отже, і невідкладного створення надійної системи кібернетичної безпеки. Натомість відсутність такої системи може призвести до втрати політичної незалежності будь-якої держави світу, бо йтиметься про фактичний програш нею змагання невійськовими засобами та підпорядкування її національних інтересів інтересам протиборчої сторони. Оскільки саме ці обставини відіграють останнім часом важливу роль у геополітичній конкуренції більшості країн світу, то забезпечення кібербезпеки та злагоди в кіберпросторі стає головним завданням нашої інформаційної епохи.

Кібербезпека – це сукупність умов, при яких всі інформаційні системи, що входять до складу кіберпростору, захищені від нападів, це забезпечення конфіденційності, цілісності та доступності інформації, яка опрацьовується в цьому просторі, виявлення та протидія атакам і кіберінцидентам [1]. В зв'язку з цим надзвичайно актуальним є питання забезпечення інформаційної та кібернетичної безпеки як країни в цілому так і окремих організацій та підприємств. Головною проблемою при вирішенні цих питань є підготовка високо кваліфікованих кадрів, яких нажалі не вистарчає. І це в сучасному суспільстві, у якому індустрія інформаційної безпеки розвивається в 12 разів скоріше ніж всі інші галузі економіки. Для розв'язання цієї проблеми Міністерство безпеки США планує витратити 25 млн. дол., на грантові програми в наступні п'ять років.

Наша країна інтегрована у світовий кіберпростір і, зазнаючи різних загроз і негативних впливів, змушена вирішувати проблему кібербезпеки на загальнодержавному рівні. Це призводить до необхідності вирішення комплексу проблем, пов'язаних із розбудовою національної моделі кібербезпеки та розробки першочергових напрямків діяльності державного та приватного секторів у сфері кібербезпеки [2].

Одним із таких напрямів діяльності держави повинна стати якісна освітня підготовка фахівців у галузі кібербезпеки, а також забезпечення високого рівня культури поведінки у сучасному кіберпросторі всіх громадян України.

Потрібно вдосконалювати сучасну професійну підготовку вчителів, в сфері інформаційних технологій та кібербезпеки зокрема. Всюди де використовуються інформаційні технології існує кіберзагроза, викладач будь-якої дисципліни в своїй професійній діяльності може стикнутися з вірусами, спамом, зломом комп'ютера та багатьма іншими проблемами, на які потрібно знати не тільки як оперативного відреагувати, а й запобігти їх виникненню, а значить постійно слідкувати за інформаційною кібербезпекою. Вчитель повинен знати можливості використання сучасних ІТ, комунікаційно-навігаційних та мережевих технологій.

В навчальних закладах на державному рівні потрібна підтримка для розширення обсягів вивчення інформаційних технологій. Наприклад розробка та впровадження в навчальний процес навчальної дисципліни «Інформаційна безпека», яка включатиме в свою програму модулі з кібербезпеки, або доповнити вже існуючі дисципліни відповідними модулями. Елементи цієї дисципліни, також, повинні бути передбачені шкільною програмою.

Враховуючи зростання кількості загроз в інформаційній діяльності та стрімкий розвиток інформаційних технологій необхідно врахувати відповідні вимоги до випускників – знання основ кібербезпеки, вміння дотримуватися вимог кібербезпеки в практичній діяльності та організувати безпеку особистого інформаційного простору.

Необхідно зазначити, що в наш час держстандарт для початкового, середнього і вищого рівня освіти не включає дисциплін з предметної області «Основи кібербезпеки». В рамках скорочення дисципліни «Інформатика» завдання з інформатичної безпеки доцільно розглядати так:

– необхідно сформувати навички та вміння безпечного та ціленаправленого використання комп'ютерних програм та дотримання в Інтернеті норм інформаційної етики та права;

– вміння використовувати засоби інформаційних та комунікаційних технологій для вирішення когнітивних, комунікативних і організаційних завдань з дотриманням вимог ергономіки, техніки безпеки, ресурсозаощадження, гігієни, правових та етичних норм, вимог інформатичної безпеки;

– розуміння правових основ використання комп'ютерних програм та роботи в Інтернеті і т. д.

Базою курсу «Основи кібербезпеки» може стати неперервна інформатична освіта в школі, причому питання кібербезпеки повинні розглядатися як при вивченні інформатики, так і при вивченні інших навчальних дисциплін. Тому одним із завдань дисципліни – підвищення кваліфікації в області кібербезпеки вчителів всіх навчальних дисциплін, в яких так чи інакше використовуються комп'ютерні технології. Найбільш очевидною є можливість доповнення питаннями з кібербезпеки уроків інформатики, якщо навчальний план школи передбачає її вивчення впродовж всього шкільного курсу. Однак можна включити модулі з кібербезпеки в курси «Я у світі», «Основи безпеки життєдіяльності»,

«Технології», тим більше що питання організаційного та правового забезпечення інформаційної безпеки добре узгоджуються з наявними вимогами до рівня підготовки учнів.

Завдання курсу «Основи кібербезпеки» – вдосконалення шкільної освіти і підготовки в сфері інформаційних технологій, а також популяризація професій, пов'язаних з нею. Мета вивчення «Основ кібербезпеки» – дати загальні уявлення про безпеку в інформаційному суспільстві і на цій основі сформувані розуміння технологій інформаційної безпеки і вміння застосовувати правила кібербезпеки в усіх сферах діяльності. Виховна мета курсу – формування на якісно новому рівні культури розумової праці і взаємодії з оточуючими, відповідального ставлення до питань безпеки життєдіяльності.

Таким чином, в умовах глобалізації сучасних міжнародних відносин, а також у зв'язку з дедалі більшою роллю інформаційно-комунікаційних систем в житті сучасного суспільства, швидке вирішення вищезначених проблем, а також адекватну відповідь на загрози міжнародній і національній кібербезпеці є справою надзвичайної важливості, що вимагає своєчасних змін в освітній галузі.

Список використаних джерел:

1. Глобальна програма кібербезпеки МСЕ. Основа для міжнародної співпраці в області кібербезпеки [Електронний ресурс] / Режим доступу: <http://www.ifap.ru/pr/2008/080908aa.pdf>.
2. Діордіца І. В. Поняття та зміст національної системи кібербезпеки. [Електронний ресурс]. / Режим доступу: <http://goal-int.org/ponyattya-ta-zmist-nacionalnoi-sistemi-kiberbezpeki>.
3. Черноног О. О. Напрями підвищення ефективності забезпечення кібербезпеки інформаційних технологій в системі публічного управління [Електронний ресурс]. / Режим доступу: <http://mino.esrae.ru/pdf/2015/Ref/1484.pdf>.
4. Ящик О. Б. Зміцнення глобальної культури кібербезпеки в мережі Інтернет / О. Б. Ящик // Комп'ютерно-орієнтовані системи навчання : зб. наук. праць / відп. ред. М. І. Жалдак. Ю.С. Рамський – К. : НПУ ім. М. П. Драгоманова, 2017. – № 19(26). – С. 136–140.