

Проблеми забезпечення інформаційної безпеки суб'єктами освітньої діяльності в цифровому освітньо-науковому середовищі закладів освіти

Ігор Козубцов¹, Наталія Зінченко², Андрій Котенко³, Ігор Аверічев⁴

¹Київський національний університет будівництва і архітектури
пр-т Повітряних Сил, 31, м.Київ, Україна, 03037

²Військовий інститут телекомунікацій та інформатизації імені Героїв Крут
вул. Князів Острозьких 45/1, Київ, Україна, 01011

^{3,4}Державний університет інформаційно-комунікаційних технологій
вул. Солом'янська, 7, м.Київ, Україна, 03037

¹kozubtsov@gmail.com, orcid.org/0000-0002-7309-4365

²zinchenko.natasha@gmail.com, orcid.org/0009-0004-1837-2838

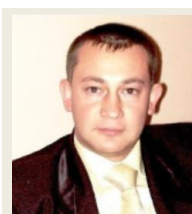
³dutkotenko@gmail.com, orcid.org/0000-0002-0483-6353

⁴laverichev19@gmail.com, orcid.org/0009-0008-9766-0115

Received 17.09.2024, accepted 27.11.2024

<https://doi.org/10.32347/uwt.2024.15.1204>

Анотація. У науковій статті розглядаються сучасні проблеми забезпечення інформаційної безпеки суб'єктами освітньої діяльності в цифровому освітньо-науковому середовищі закладів освіти. В умовах війни (надзвичайних подій, пандемій) освітня діяльність суб'єктів переміщується у цифрове освітньо-наукове середовище закладів освіти, де себе ефективно зарекомендувало. Оскільки всі освітні процеси закладів освіти є інформаційними, а їх спотворення може призвести до негативних наслідків, то виникає потреба у забезпеченні інформаційної безпеки. На підставі цього виокремлено стратегічну ціль забезпечення інформаційної безпеки в цифровому освітньо-науковому просторі закладу освіти - формування у суб'єктів культури особистої інформаційної та кібернетичної безпеки. Тому необхідно ще під час навчання формувати у здобувачів освіти інформаційну компетентність та особисту культуру інформаційної безпеки, особливо потребують здобувачі освіти гуманітарного профілю підготовки. Отже, метою статті є огляд проблем забезпечення інформаційної безпеки суб'єктами освітньої діяльності в цифровому освітньо-науковому середовищі закладів освіти. За результатом дослідження виокремлено та розглянуто багатоаспектність інформаційної безпеки в системі освіти, інформаційний захист суб'єкта навчальної (освітньої) діяльності, проблема відбору викладачем навчальної інформації та проблему захисту цифрового освітньо-наукового простору закладу освіти від внутрішніх та зовнішніх загроз. Підтверджено, що, формування інформаційної культури в



Ігор Козубцов

Професор кафедри кібербезпеки та комп'ютерної інженерії КНУБА



Наталія Зінченко

Старший помічник начальника відділу забезпечення якості освітньої діяльності



Андрій Котенко

к.т.н., доц., доцент кафедри Технічних систем кіберзахисту ДУІКТ



Ігор Аверічев

к.е.н., доцент кафедри Технічних систем кіберзахисту ДУІКТ

освітньому процесі є багатоплановим поетапним процесом безперервної інформаційної підготовки здобувачів освіти. Саме рівень інформаційної культури є показником готовності суб'єкта до навчання і самоосвіти, розвитку і саморозвитку та характеризує ефективність використання

інформації і інформаційних ресурсів в освітній та професійній діяльності в інформаційному просторі при обов'язковому забезпеченні вимог інформаційної безпеки.

Ключові слова: інформаційна безпека, компетентність, інформаційна культура, цифрове освітньо-наукове середовище, заклад вищої освіти.

ВСТУП

Передача надбання суспільства наступним поколінням реалізується через інформаційну діяльність суб'єктів освітнього процесу.

Всі процеси за своєю природою є інформаційними, а їх спотворення можуть призвести до негативних наслідків. Тому поряд із збереженням надбання суспільства є не менш важливим завданням забезпечення *інформаційної безпеки* – безпеки процесів, відносин, об'єктів і суб'єктів.

Оскільки всі освітні процеси закладів освіти (ЗВО) є інформаційними, тому:

вони також повинні розглядатися в контексті інформаційної безпеки інформаційного освітнього середовища, в якому взаємодіють всі суб'єкти освітньої діяльності ЗВО;

зміст та проблеми інформаційної безпеки, методи і засоби її забезпечення повинні бути невід'ємною частиною змісту освіти, навчання в рамках будь-якого навчального предмета і, впершу чергу, починаючи зі школи учням в рамках уроків інформатики.

При цьому всі суб'єкти освітньої діяльності ЗВО потребують в набутті інформаційної компетентності, що включає необхідні знання і вміння, з наступним перетворенням у особисту культуру інформаційної безпеки як системно-інтелектуального компонента його особистої культури та світогляду як розвивається особистісної системи інформаційного суспільства. Якщо в технічних ЗВО формування інформаційної компетентності є змістом їх фахової

підготовки [1], то із впровадженням цифрових технологій в закладах гуманітарної освіти – це лишається актуальною проблемою. У зв'язку з цим перед ЗВО, що здійснюють підготовку майбутніх педагогів, постало наукове завдання у розробці системної підготовки майбутніх науково-педагогічних кадрів до нових умов професійної науково-педагогічної діяльності в цифровому освітньому середовищі, які володіють цифровими компетентностями до склу яких увійшла інформаційна [2].

Рішення цієї проблеми започатковане окремими дослідниками в контексті виконання науково-дослідної роботи «Теорія і практика підготовки майбутнього викладача закладу вищої педагогічної освіти до професійної діяльності в умовах цифровізації суспільства», що виконується в Інституті педагогічної освіти і освіти дорослих імені Івана Зязюна НАПН України, в напрямку «цифровізації» освіти, що дозволило виокремити потребу у окремому науковому пошуку та вирішенні часткового завдання:

у осучасненому перегляді проблеми забезпечення інформаційної безпеки в цифровому освітньо-науковому середовищі ЗВО [3];

систематизації підходів до навчання здобувачів вищої освіти в «цифровому освітньо-науковому середовищі» [4].

Під «цифровим освітньо-науковим середовищем» будемо розуміти відкриту та закрити сукупність інформаційних систем, призначених для забезпечення завдань освітнього процесу та наукової діяльності у ЗВО. Необхідно враховувати можливий вплив небезпеку на «цифрове освітньо-наукове середовище» з боку кіберпростору та вживати превентивних заходів для підтримання в актуальності систему захисту від кіберзагроз. Загальне уявлення про структурні складові «цифрового освітньо-наукового середовища» ЗВО зображено на рис. 1, які постійно доповнюються. Заявляють відповідно до них нові загрози.

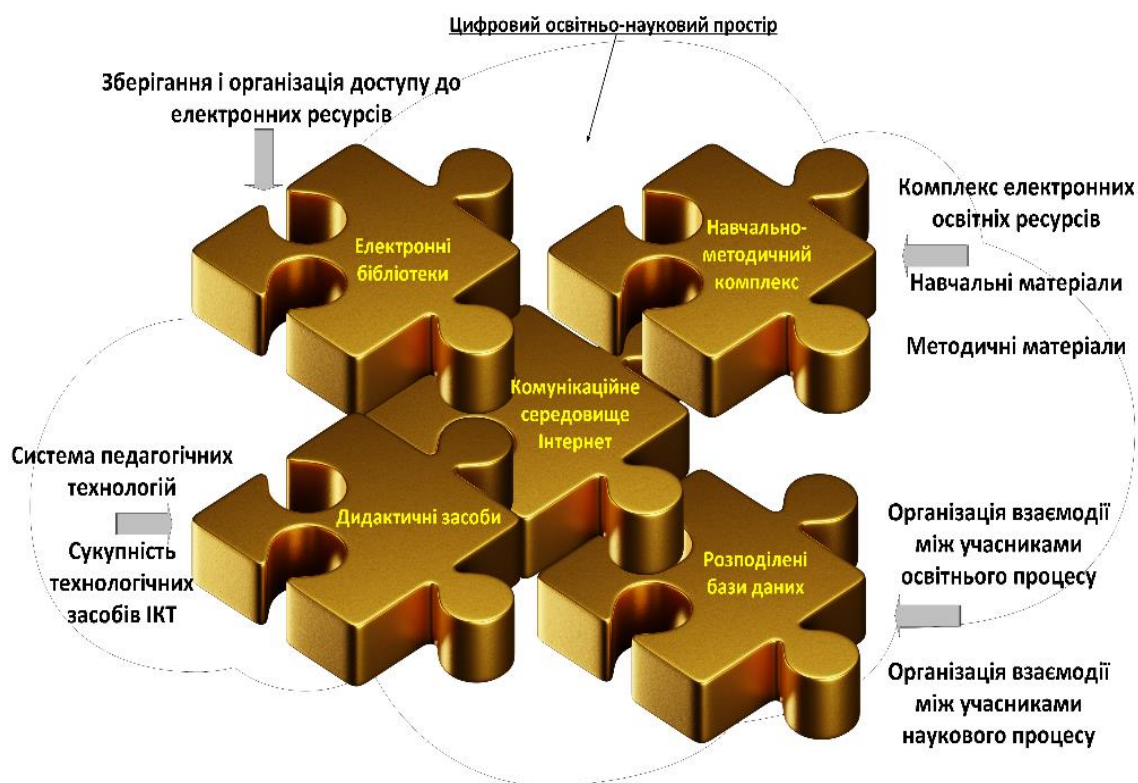


Рис. 1. Структурні складові «цифрового освітньо-наукового середовища» ЗВО

Fig. 1. Structural components of the “digital educational and scientific environment” of higher education institutions

Таким чином, однією із стратегічних цілей забезпечення інформаційної безпеки в цифровому освітньо-науковому просторі ЗВО є формування у громадян культури особистої інформаційної та кібернетичної безпеки.

ЗВ’ЯЗОК ПРОБЛЕМИ З ВАЖЛИВИМИ НАУКОВИМИ ЗАВДАННЯМИ

На потребу у формування культури інформаційної безпеки зазначається в рекомендації Організації економічного співробітництва та розвитку «OECD Guidelines for the security of information systems and networks: Towards a culture of security» [5], прийняті в далекому ще 2002 р. та з наступним оновленням в 2015 р. на рекомендацію щодо управління ризиками цифрової безпеки для економічного та соціального процвітання [6].

Слід зазначити, що окремі рекомендації з документа [5] знайшли відображення у

резольції Генеральної Асамблеї ООН «Створення глобальної культури кібербезпеки» [7] («Елементи для створення глобальної культури кібербезпеки»).

Таким чином, можна вважати, що проблема забезпечення інформаційної безпеки в цифровому освітньо-науковому середовищі ЗВО отримала світову визнання тож і потребує адекватних заходів щодо її вирішення.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Проблема забезпечення інформаційної безпеки в цифровому освітньо-науковому середовищі закладах освіти не є порівняно новою. Над їх вирішенням згуртувалися небагато дослідники у всьому світі.

Взаємодія з кіберпростором, на думку автора дослідження [8], розвиває знання і культуру людини, культуру інформаційної безпеки, у той час як культура і знання

людини, його знання з інформаційної безпеки і культура інформаційної безпеки оптимізують це взаємодія.

На проблему технологізації віртуального світу, кіберпростору, а разом з цим і технологізації мислення людини звертають все більшу увагу. Так група вчених в своїх дослідженнях незалежно один від одного [9 – 12] прийшли до висновку, що інформаційне поле інтернету та активна присутність користувачів в соціальних мережах, в інших віртуальних форумах або формах спільнот істотно впливають на ціннісно-смыслову сферу особистості.

Автор монографії [13] зазначає на необхідність супроводу «кіберсоціалізації» особистості та формування в її кіберкультури. Крім того, вона повинна включати в себе і особисту кіберкультуру інформаційної безпеки.

В роботі [14] обґрунтовано необхідність вбудовування системи забезпечення інформаційної безпеки в діяльність освітніх установ, оскільки одним з найбільш активних споживачів і генераторів інформації є сфера освіти, де формується інтелектуальний і моральний потенціал майбутніх поколінь. А оскільки науково-педагогічна діяльність викладача ЗВО унеможливилась без засобів автоматизації, які вразливі до кібервпливу, то очевидно і назріла потреба в обов'язковому забезпеченні її кібербезпеки [15].

Неминуча і тому необхідна технологізація діяльності і пізнання суб'єкта освіти не повинна вести до технологізації його мислення. Небезпека технізації суспільства помітив Н. Бердяєв [16], який писав про відрив людини від природи, про технізації світу людини, що виявляється в його дегуманізації, втрати морального і духовного в створюваній ним технічної цивілізації. Зараз, на жаль, цей «відрив» пішов далеко вперед завдяки світовій кризи, спровокованої пандемією коронавірусу, що не має аналогів у сучасній історії. З цього приводу є слушна думка К. Schwab [17, с. 7] «Ніщо ніколи не повернеться у «вихідне положення» світ, яким ми його знали в перші місяці 2020 року, більше не існує, світ перетнув точку біфуркації епох «до

коронавірусу» та «після коронавірусу». Тому на разі спостерігається інтенсивний процес технологізації суб'єктів освітньої діяльності без обґрунтованої теорії цифрового навчання носить сумнівний характер [3].

Педагогічний супровід крім вивчення предметів природничо-наукового і професійного циклу (математики, інформатики, інформаційних технологій) вже не в стані системно вирішити проблему, тут необхідна методична система навчання, що забезпечує формування рівня інформаційної культури у здобувачів вищої освіти з обов'язковою складовою – компетентністю в області захисту інформації та забезпечення інформаційної безпеки в освіті [18].

Дана проблема має міждисциплінарний характер і потребує педагогічного осмислення у розвитку особистості здобувачів вищої освіти в аспекті забезпечення інформаційної безпеки в сучасному цифровому суспільстві. Слід зазначити, що поняття «цифрове суспільства» в Україні з'явилося за результатами ухвали Урядом держави «Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки» [19].

На жаль, у педагогічній науці не в повній мірі приділяють увагу різним питань з підготовки випускника ЗВО до забезпечення інформаційної безпеки у повсякденній діяльності про що зазначається у схваленій стратегії розвитку вищої освіти в Україні на 2022-2032 роки [20].

Виходячи з вище розглянутого, в дослідженні під проблемами інформаційної безпеки, будемо розглядати:

- захист інформаційного цифрового освітньо-наукового середовища суб'єкта освіти від негативної інформації, дезінформації та інформаційного впливу на нього;
- формуванні особистісних якостей здобувачів освіти в якості «активів» його особистої інформаційної безпеки.

Тоді під проблемами інформаційної безпеки освіти будуть:

- адекватне відображення тем і проблем інформаційної безпеки в змісті освіти і предметного навчання;
- розвиток у педагогічних дослідженнях теми інформаційної безпеки та її реалізації у сфері освіти;
- формування особистої інформаційної культури та критичного мислення суб'єктів освітньої діяльності.

Метою статті є огляд проблем забезпечення інформаційної безпеки суб'єктами освітньої діяльності в цифровому освітньо-науковому середовищі ЗВО.

МЕТОДИ ДОСЛІДЖЕННЯ

Основні інструменти дослідження: методи теоретичного аналізу й узагальнення наукової літератури, за темою дослідження;

узагальнення – для формулювання висновків і рекомендацій щодо результативності.

РЕЗУЛЬТАТ ДОСЛІДЖЕННЯ

Інформаційна безпека виражається в захищеності, гарантії збереження стану людини, суспільства, їхніх ресурсів, надбання, знань, умов, середовища, в яких вони живуть, діють і розвиваються, що відповідають їх рівню і цілям розвитку [18]. Забезпечення інформаційної безпеки суб'єктам освітньої діяльності в цифровому освітньо-науковому середовищі ЗВО – це створення необхідних і достатніх умов для стану захищеності, гарантованості і збереження навчальної та фундаментальної інформації та даних. В першу чергу викладачами необхідно знати проблеми інформаційної безпеки і вміти їх усувати.

Інформаційна безпека передбачає наступне:

- безпека інформаційного цифрового освітньо-наукового середовища, інформаційно-пізнавальної сфери;
- безпека особистої інформаційно-пізнавальної сфери людини, породжуваної її процесами, засобами і результатами, процесами

- інформатизації та використання інформації;
- безпека багатовимірного інформаційного простору, реального і віртуального, кіберпростору.

1. Багатоаспектність інформаційної безпеки в системі освіти

1.1 Інформаційна безпека має до системи освіти багатоаспектне відношення.

Зовнішніми чинниками є потреби у розвитку освіти. Він представлений у змісті навчання інформатики, комп'ютерних наук та інших суміжних навчальних дисциплінах.

Внутрішніми чинниками освітньої системи є забезпечення викладачами якісного і навчально-методичного супроводу здобувачів освіти. Оскільки освітній процес – це система інтерсуб'єктивних інформаційних процесів, процесів інформатизації та інформаційного взаємодії. Виходячи з цього представлення інформаційну безпеку в системі освіти можна виділити в наступному:

- в гарантії безперервності процесів пізнання, навчання, навчальної та навчально-пізнавальної діяльності здобувачів освіти;
- в безпеці суб'єктів освіти при взаємодії через інформаційне цифрове освітньо-наукове середовище системи дистанційної освіти;
- в безпеці відносин між суб'єктами освітньої діяльності в умовах застосування технологій дистанційного навчання.

1.2 Безпека освітнього процесу в цифровому освітньо-науковому середовищі досягається насиченістю навчальними засобами, розвитком інфраструктури, методичними розробками, інформаційним управлінням та програмними (апаратними) засобами кібербезпеки.

1.3 Безпека суб'єктних відносин в системі освіти визначається їх відповідністю та закономірностям як соціально-інформаційної системи, культурою цих відносин, сприятливими умовами середовища.

1.4 Фізичне вираження інформаційної безпеки суб'єкта – це дотримання норм роботи з інформаційно-комунікаційними

технологіями в цифровому освітньо-науковому просторі.

Пізнання різноманіття світу, культури, знань передбачає наявність такого ж різноманіття засобів сприйняття, джерел інформації, учасників інформаційного діалогу. Обмеженість діяльнісно-пізнавального середовища спричиняє обмеженість здобувачів освіти, так як «будь-яка віртуалізація, яка підміняє органічні, культурно обґрунтовані детермінанти мікро – і самосприйняття, в результаті вириває людину з контексту реальності» [21, с. 16].

Занурення у віртуальний світ відображеної (абстрактної) інформації також тягне замикання людини в обмеженому просторі ілюзій і уявлень. Тому дане «занурення» є вкрай небезпечним для людини [16].

2. Інформаційний захист суб'єкта навчальної (освітньої) діяльності

Інформаційний захист суб'єктів навчання досягається за рахунок:

- ефективною та раціональною передачею і сприйняття навчальної інформації у відповідності з цілями освіти;
- захисту здобувачів освіти від недоброякісної, недостовірної та негативної інформації;
- в усвідомленні способів якісного розпізнавання шкідливої інформації і диференціації інформації;
- формування здатності пізнавати й захищати свій внутрішній світ, зберігати його цілісність, вміти правильно оцінювати інформацію, що надходить із зовнішнього середовища, на предмет її достовірності та об'єктивності, несуперечності та адекватності, значущості та цінності, вміти давати їй правову оцінку;
- облік особливостей і пізнавальних інтересів кожного суб'єкта у відповідності з його природними здібностями і психологічним типом.

Забезпечення інформаційної безпеки має отримати відповідне відображення в змісті освіти, у змісті предмета «Інформатика». Суб'єкт освіти повинен навчитися розуміти проблеми інформаційної безпеки, зберігати суб'єктну та об'єктну сфери суспільства,

вміти жити в єдності з природою і навколишнім світом. Стан інформаційної безпеки має стати частиною загальної інформаційної культури людства, а знання основ забезпечення інформаційної безпеки – частиною особистої інформаційної культури кожного громадянина. Слід погодитися з думкою авторів [22, с. 42], що суб'єкт освітньої діяльності повинен володіти не тільки зростаючою за обсягом і якістю інформаційно-комунікативною компетентністю, але й соціальною, інформаційно-правовою, яка передбачає знання і дотримання відповідних соціальних та інформаційно-правових норм.

Інформаційна культура здобувача освіти повинна включати в себе і культуру особистої безпеки. Інакше людина, яка вміє будувати конструктивні і продуктивні відносини з середовищем, медіа середовищем, може так захопитися ними, що стане «бранцем» кіберпростору, «сама структура віртуального простору веде людину зовсім в іншому напрямку, відмінному від його первісної інтенції».

3. Проблема відбору викладачем навчальної інформації

Особливо гостро ставиться проблема інформаційної безпеки у сфері освіти у зв'язку з її інформатизацією. Все більше з'являється в мережі Інтернет різних освітніх ресурсів. На відміну від друкованої навчально-методичної літератури, яка проходить експертизу, в Інтернеті навчальний матеріал може розмістити будь-який бажаючий. Експертиза інформаційних освітніх ресурсів неможлива. Адже величезний обсяг інформації та комерційні умови доступу не завжди дозволяють оцінити якість таких ресурсів, грамотність, наукову достовірність [23].

Необхідні цілеспрямованість і критерії відбору інформації з цифрового освітньо-наукового простору, ознаки її суттєвості і достовірності, а також уміння суб'єктів навчання критично оцінювати інформацію при самостійному пошуку в інтернеті та в інших доступних їм джерел [24].

На наростаючу проблему забезпечення інформаційної безпеки у сучасній динамічній науковій картині світу молодих

вчених та студентів, свого часу В. Куцаєв та інші привертали наукове суспільство [24]. Зазначена категоріє здобувачів вищої освіти часто без вагань і перевірки копіюють інформацію з Wikipedia та інших їм подібних не перевірених ресурсів до рефератів, дисертацій. В результаті відбувається спотворення передачі надбання суспільства наступним поколінням.

Будь-яка інформація здатна чинити певний вплив на людину, в тому числі на суб'єкта освіти, – інформаційно-пізнавальне, соціокультурне, психологічний. Це інформаційно-психологічний вплив може бути як позитивним (достовірною, якісною інформацією), так і негативним (недостовірною, неякісною інформацією – дезінформацією). Необхідно навчити здобувачів освіти оцінки та диференціації інформації, стійкості до можливих негативних інформаційно-психологічних впливів, активного протистояння і конструктивної протидії їм. Необхідно формування критичного ставлення до інформації та критичного мислення суб'єкта освіти, які передбачають створення базового ставлення до себе і світу, передбачає варіативну, самостійну, осмислену позицію. Ця позиція значно підвищує надійність освіти – тому що воно стає усвідомленим і рефлексивним і підвищує комунікативний потенціал особистості».

Критичне ставлення здобувача освіти до інформації можна ідентифікувати як:

- здатності до осмислення і диференціювання сприйманої інформації;
- здатності до системного аналізу інформації на основі застосування до неї критеріїв пошуку і інших ознак;
- здібності до визначення синтетичних властивостей досліджуваної (аналізованої) інформації;
- здібності до створення похідної інформації на підставі ефективного використання інформаційних ресурсів середовища;
- здатності до систематизації інформації на підставі її інваріантних відносин і закономірних взаємозв'язків.

Отже, критичне ставлення до інформації – це компонент системи оцінки інформації у всіх її аспектах: змістовних і формальних, експертних і технологічних, методичних та алгоритмічних. Критичне ставлення особистості до інформації тягне за собою формування її критичного мислення як якісної характеристики, що виражається в інваріантній стійкості до негативних інформаційно-психологічних впливів та протидії їм.

4. Проблема захисту цифрового освітньо-наукового простору закладу освіти від внутрішніх та зовнішніх загроз безпеки інформації

Проблеми інформаційної безпеки мереж ЗВО набагато ширші, різноманітніші і гостріші, ніж в інших системах. Це пов'язано з такими особливостями:

- мережа закладу вищої освіти будується, як правило, на основі мізерного фінансування (обладнання, кадри, неліцензійне програмне забезпечення);
- зазвичай мережі не мають стратегічних цілей розвитку, а саме топологія мереж, їх технічне та програмне забезпечення розглядаються з позицій поточних завдань;
- в одній корпоративній мережі ЗВО вирішуються дві основні задачі: забезпечення освітньої та наукової діяльності і вирішення завдання управління освітнім та науковим процесами;
- корпоративні мережі гетерогенні як за обладнанням, так і за програмним забезпеченням у зв'язку з тим, що створювалися протягом тривалого періоду часу для різних завдань;
- плани інформаційної безпеки, як правило, або відсутні, або не відповідають сучасним вимогам.

У закладі освіти можлива низка як внутрішніх, так і зовнішніх загроз безпеки інформації [25]:

- спроби несанкціонованого адміністрування баз даних;
- дослідження мереж, несанкціонований запуск програм з аудиту мереж;
- видалення інформації, у тому числі бібліотек;

- запуск на виконання ігрових програм;
- установка вірусних програм і троянських коней;
- сканування мереж, у тому числі інших організацій через Інтернет;
- несанкціоноване скачування з Інтернету неліцензійного програмного забезпечення та інсталяція його на робочі станції;
- пошук — дірок у операційній системі, міжмережевих екранах;
- спроби несанкціонованого віддаленого адміністрування операційних систем;
- сканування портів тощо.

Проаналізувавши загрози інформаційної безпеки ЗВО можна запропонувати систему захисту, яка включає в себе чотири етапи:

- 1 етап – визначення та аналіз загроз інформаційної безпеки ЗВО;
- 2 етап – розроблення системи захисту інформації в ЗВО;
- 3 етап – реалізація плану захисту інформації;
- 4 етап – керування та контроль за функціонуванням системи захисту інформації.

ВИСНОВКИ

Отже, суб'єкту освітньої діяльності необхідна особиста культура інформаційної безпеки як складової інформаційної культури. Цей умовивід впливає з наступних міркувань:

1) впровадження інформаційних технологій в освітню діяльність, інтеграція педагогічних та комп'ютерних технологій в навчання без прив'язки до забезпечення інформаційної безпеки істотно підвищують ризик прояву інформаційних загроз, захисту даних, інформації тощо;

2) надмірне захоплення спілкуванням з віртуальним світом так само шкідливе, як і через недостатню увагу до них. При відсутності «живого» спілкування з світом у людини притуплюються природні почуття, збіднюється духовний світ, він стає добровільним «бранцем» віртуального світу. Віртуальні цінності можуть стати для нього більш важливими, ніж реальні.

Важливим компонентом інформаційної культури є культура інформаційної безпеки, розглянута в двох аспектах:

- 1) безпека інформаційного цифрового освітньо-наукового середовища і її компонентів, засобів, ресурсів, технологій;
- 2) безпека суб'єктів середовища – як фізична, так інтелектуальна – в разі можливого негативного впливу середовища.

Таким чином, формування інформаційної культури в освітньому процесі є багатоплановим поетапним процесом безперервної інформаційної підготовки здобувачів освіти. Саме рівень інформаційної культури є показником готовності суб'єкта до навчання і самоосвіти, розвитку і саморозвитку і характеризує ефективність використання інформації і інформаційних ресурсів в освітній та професійній діяльності в інформаційному просторі при обов'язковому забезпеченні вимог інформаційної безпеки.

REFERENCES

1. **Kozubtsov I.M., Khlaponyn Yu.I., Protsiuk Yu.O.** (2022). Metodolohichni osnovy pidhotovky fakhivtsiv informatsiinoi bezpeky v tekhnichnykh VNZ: filosofsko-tekhnichni aspekt. Informatsiina bezpeka. Naukovyi zhurnal. Skhidnoukrainskyi natsionalnyi universytet im. Volodymyra Dalia, 35-41.
2. Pro skhvalennia Stratehii rozvytku vyshchoi osvity v Ukraini na 2022-2032 roky. Rozporiadzhennia Kabinetu Ministriv Ukrainy №286-r (2022). <https://zakon.rada.gov.ua/laws/show/286-2022-h>
3. **Kozubtsov I.M., Beskrovnyi O.I., Kozubtsova L.M., Palahuta A.M., Myronenko O.V.** (2022). Tendentsii u osvitno-naukovomu prostori: problemy ta ryzyky. Visnyk Kremenchutskoho natsionalnoho universytetu imeni Mykhaila Ostrohradskoho, 1(132), 40–48.
4. **Kozubtsov I.M., Kozubtsova L.M., Palahuta A.M., Snovyda V.Ie., Sukhomlynova O.V.** (2023). Systematyzatsiia pidkhodiv do navchannia zdobuvachiv vyshchoi osvity v «tsyfrovomu osvitn-naukovomu seredovyschi». Naukovi innovatsii ta peredovi tekhnologii, 1(15), 373-383.
5. OECD (2002). Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security.

- <https://www.oecd.org/sti/ieconomy/oecdguidelinesforthesecurityofinformationsystemsandnetworkstowardsacultureofsecurity.htm>.
6. OECD (2015). Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, OECD Publishing, Paris. DOI: <http://dx.doi.org/10.1787/9789264245471-en>.
 7. Creation of a global culture of cybersecurity. UN Council Resolution. (2003). <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N02/555/24/PDF/N0255524.pdf?OpenElement>.
 8. **Abdurazakov M., Korotekov Yu., Muhidinov M.** (2016). Educational space representation in cyberspace. International Conference “Education Environment for the Information Age” (EEIA-2016), 29, 01001, DOI: <http://dx.doi.org/10.1051/shsconf/20162901001>.
 9. **Benkler Y.** (2006). *The wealth of networks: How social production transforms markets and freedom*. New Haven, London: Yale University Press.
 10. **Kopecký K., Szotkowski R., Krejčí V.** (2012). The risks of Internet communication. *Procedia – Social and Behavioral Sciences*, 69, 1348-1357.
 11. **Livingstone S., Haddon L.** (2008). Risky experience for children online: Charting European research on children and the Internet. *Children and Society*, 22(4), 314-323.
 12. **Livingstone S., Smith P.** (2014). Annual research review: Harms experienced by child users of online and mobile technologies: the nature, prevalence and management of sexual and aggressive risks in the digital age. *Journal of Child Psychology and Psychiatry*, 55(6), 635-654.
 13. **Pleshakov V.** (2011). Teoriya kybersotsyalyzatsyy. M.: «Homo Cyberus».
 14. **Kozlov O., Guzikova L.** (2017). Information security as requisition of educational organization activity. *Teaching Methodology in Higher Education*, 6(22), 43-50.
 15. **Khloponin Yu., Kozubtsova L., Kozubtsov I.** (2021). On the need to ensure cybersecurity in educational information systems and technologies. *Scientific and Practical Cyber Security Journal (SPCSJ)*, 5(3), 25-29.
 16. **Berdyayev N.** (2022). Man and Machine (Problem of Sociology and Metaphysics of Technology). Courier of Kutafin, (4), 246-256.
 17. **Schwab K., Malleret T.** (2020). COVID-19: *The Great Reset. Edition 1.0*. Switzerland. Cologny/Geneva: Forum publishing World Economic Forum.
 18. **Abdurazakov M., Batygov Z.** (2021). Modern problems of ensuring information security in the educational and pedagogical sphere. *Informatics and Education*, 36(10), 57-64.
 19. Pro skhvalennia Kontseptsii rozvytku tsyfrovoy ekonomiky ta suspilstva Ukrainy na 2018-2020 roky ta zatverdzhennia planu zakhodiv shchodo yii realizatsii. Rozporiadzhennia Kabinetu Ministriv Ukrainy vid 17.01.2018 № 67-r. <https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#Text>.
 20. **Abdurazakov M.** (2018). Teacher-student interaction in information-related educational environment: The culture of knowledge – cognition – informational communication. *Pedagogy*, (9), 39-46.
 21. **Kyrylenko N.M.** (2012). Problemy informatsiinoi bezpeky osvithno seredovyscha vyshchoho navchalnoho zakladu. Informatsiino-telekomunikatsiini tekhnolohii v suchasni osviti: dosvid, problemy, perspektyvy: tretia mizhnarodna naukovo-praktychna konferentsiia. Lviv, 1, 149-151.
 22. **Kozubtsov I.M., Kutsaiev V.V.** (2013). Filosofiia informatsiinoi bezpeky v umovakh yii kibernetichnoho rozpovsiudzhennia v suchasni dynamichni naukovi kartyni svitu na prykladi nadannia znan molodym vchenym ta studentam. Hileia: naukovyi visnyk. Zbirnyk naukovykh prats, 73(6), 291–293.
 23. **Kukharska N.P.** (2015). Otsinka informatsiinoho seredovyscha vyshchokh navchalnykh zakladiv ta analiz zahroz yoho bezpetsi. Informatsiino-komunikatsiini tekhnolohii v suchasni osviti: dosvid, problemy, perspektyvy», 2, 31-35.

Problems of ensuring information security by subjects of educational activity in the digital educational and scientific environment of educational institutions

Ihor Kozubtsov, Nataliia Zinchenko, Andrei Kotenko, Ihor Averichev

Abstract: The article discusses the current problems of ensuring information security by educational entities in the digital educational and scientific environment of educational institutions. In times of war (emergencies, pandemics), the educational activities of subjects are moving to the digital educational and scientific environment of educational institutions, where they have proven themselves effectively. Since all educational processes of educational institutions are

information-based, and their distortion can lead to negative consequences, there is a need to ensure information security. Based on this, the strategic goal of ensuring information security in the digital educational and scientific space of an educational institution is to form personal information and cybersecurity in cultural subjects. Therefore, it is necessary to form information competence and personal culture of information security in students during their studies, especially for students of the humanitarian profile. Thus, the purpose of the article is to review the problems of ensuring information security by educational entities in the digital educational and scientific environment of educational institutions. Based on the results of the study, the author distinguishes and considers the multidimensionality of information security in the education system, information protection of the subject of educational (training) activity, the

problem of selection of educational information by a teacher, and the problem of protecting the digital educational and scientific space of an educational institution from internal and external threats. It is confirmed that the formation of information culture in the educational process is a multifaceted, phased process of continuous information training of students. It is the level of information culture that is an indicator of the subject's readiness for learning and self-education, development and self-development and characterizes the effectiveness of the use of information and information resources in educational and professional activities in the information space with the obligatory provision of information security requirements.

Keywords: information security, competence, information culture, digital educational and scientific environment, higher education institution.