Олексій ЛИТВИНОВ,
доктор юридичних наук, професор, Заслужений працівник освіти України
В.о. ректора Національного аерокосмічного університету
ім. М.Є. Жуковського «Харківський авіаційний інститут», Харків, Україна
e-mail: khai@khai.edu
ORCID: 0000-0003-2952-8258

Наталія ФІЛІПЕНКО,
доктор юридичних наук, професор,
професор кафедри права гуманітарно-правового факультету
Національного аерокосмічного університету ім. М.Є. Жуковського
«Харківський авіаційний інститут», Харків, Україна
e-mail: n.filipenko@khai.edu
ORCID: 0000-0001-9469-3650

Сергій ЛУКАШЕВИЧ,
кандидат юридичних наук, доцент,
професор кафедри права гуманітарно-правового факультету
Національного аерокосмічного університету ім. М.Є. Жуковського
«Харківський авіаційний інститут», Харків, Україна
e-mail: serhilukashevych@gmail.com
ORCID: 0000-0001-8386-6237

Карина ПАЛКОВА (Karina PALKOVA),
кандидат філософських наук, доцент, декан факультету Соціальних наук
Ризького університету імені Страдиня, Латвія
e-mail: karina.palkova@rsu.lv
ORCID: 0000-0002-6909-571X

DOI: https://doi.org/10.32620/pls.2024.5.02

КІБЕРБЕЗПЕКА ЯК ФАКТОР ЕФЕКТИВНОСТІ ЗАКЛАДІВ ВИЩОЇ ОСВІТИ

Анотація. *У статті проаналізовано вплив кіберзлочинності на функціонування закладів вищої освіти та розглянуто можливі шляхи попередження і подолання кібератак. Підкреслено, що поряд із численними перевагами використання комп'ютерних технологій, вони також створюють загрози, пов'язані зі складністю забезпечення безпеки даних. Встановлено, що сучасні світові тенденції протидії кіберзагрозам поступаються перед масштабами та ефективністю дій кіберзлочинців, що спричиняє збільшення кількості агресивних і успішних кібератак. Особливу увагу приділено зростанню атак на освітні мережі в останні роки. У статті запропоновано організаційні заходи, спрямовані на вирішення проблем кібербезпеки. Зроблено висновок, що ключовими факторами ефективного протистояння кіберзагрозам є рівень підготовки, компетентність і відповідальність учасників освітнього процесу. Це, у свою чергу, визначає стабільність і успішність роботи закладів вищої освіти України.*

Ключові слова: *кіберзлочинність, кібербезпека, заклади вищої освіти, зовнішні фактори впливу, внутрішні фактори впливу, попередження правопорушень та злочинів.*

Вступ. В умовах зростання загроз у кіберпросторі та поширення кіберзлочинів, заклади вищої освіти повинні звертати підвищену увагу на кібербезпеку своїх інформаційних ресурсів. Кіберзлочинці використовують методи соціальної інженерії, аби зібрати дані про вподобання, поведінку та звички студентів і співробітників, а це дозволяє їм легше проникати у внутрішні системи університету, маніпулювати

користувачами або обманом отримувати доступ до важливих даних.

Для протидії цим загрозам університети несуть підвищену відповідальність за захист академічної інформації, дослідницьких напрацювань та персональних даних студентів та співробітників. Це означає регулярний перегляд політики безпеки й архітектури комп'ютерних мереж, а також обмеження відкритих доступів, що можуть створити уразливі точки для зовнішніх атак. Як зазначають дослідники[1], важливим аспектом безпеки є також навчання студентів і працівників університету принципам кібергігієни, що допоможе мінімізувати випадки шахрайства й викрадення даних. Крім того, університетам слід розробляти ефективні стратегії кіберзахисту, включаючи двофакторну аутентифікацію, шифрування даних, а також системи моніторингу та реагування на підозрілу активність. Такий підхід дозволяє не лише посилити кіберзахист, але й адаптуватися до нових викликів у сфері кібербезпеки, що стає критично важливим у сучасному світі.

Огляд літератури. Розгляд факторів впливу на кібербезпеку закладів вищої освіти України та світу, були предметом дослідження вітчизняних науковців. Це, наприклад, І. Білоус, І. Гальона, О. Захарова, М. Кириченко, О. Кохановська, О. Литвинов, С. Лукашевич, Н. Муранова, О. Сікора, Н. Філіпенко, З. Шацька, І. Шемелинець та ін.

Закордоні дослідники не були осторонь цих проблем. Серед них M. Carr, E. Kost, K. Palkova, A. Piazza, V. Rakstiņš, A. Sprūds, L. Juļa, N. Schwartz, A. Vasudevan та багато інших.

Проте дослідження проблем кібербезпеки освітнього процесу потребують значних подальших теоретичних напрацювань та їх практичної реалізації. В умовах нестабільності, викликаної військовими діями, безпека інформаційних систем та мереж в закладах вищої освіти стає особливо актуальною проблемою. Технічні засоби захисту від кібератак, що можуть загрожувати як даним студентів і викладачів, так і науковим розробкам та адміністративним системам, потребують постійного вдосконалення та адаптації до нових викликів. Тому особливо важливо забезпечити надійний захист інформації від зовнішніх загроз, адже ворог може використовувати кібератаки як інструмент для дестабілізації системи освіти та науки.

Крім того, необхідно розробити механізми адаптації освітнього процесу до змінюваних умов, зокрема з огляду на перехід до дистанційного навчання або використання онлайн-ресурсів, що також створює нові виклики для кібербезпеки. В умовах війни велике значення має навчання студентів та викладачів безпечному використанню інформаційних технологій, а також створення систем, що забезпечують надійний моніторинг і контроль за інформаційними потоками.

Викладення основних результатів. Зі зростанням загроз у кіберпросторі, кіберзлочинці використовують дедалі більш витончені методи соціальної інженерії, щоб отримати доступ до особистих даних працівників та студентів університетів, зокрема інформації про їхню поведінку та інтереси в Інтернеті. Це змушує університети брати на себе підвищену відповідальність за захист академічних цифрових даних. Для цього вони змушені постійно посилювати свою кібербезпеку, забезпечувати регулярний моніторинг комп'ютерних мереж і контролювати доступ до інформаційних ресурсів.

Одночасно існують і проблеми, що супроводжують упровадження та використання інформаційно-комунікаційних технологій (далі – ІКТ) у закладах вищої освіти (далі – ЗВО), зокрема: недостатнє фінансування для закупівлі сучасного обладнання та впровадження ІКТ; відсутність стратегічного бачення з боку керівництва ЗВО щодо інтеграції ІКТ; низький рівень обізнаності серед викладачів і студентів щодо можливостей і використання ІКТ в освітньому процесі; нестача кваліфікованих спеціалістів, здатних забезпечити ефективну роботу та кібербезпеку ІКТ у закладі вищої освіти тощо.

Відповідно до перших трьох пунктів, у багатьох ЗВО помітні зусилля керівників, спрямовані на вирішення цих проблем. Проте четверта проблема – брак спеціалістів у сфері кібербезпеки – є найбільш критичною й актуальною не лише для окремих закладів, а й на державному рівні.

Аналіз досліджень свідчить[2], що однією з найпоширеніших кібератак на освітні ресурси навчальних закладів є атаки типу DDoS. Вони створюють труднощі з доступом до ресурсів і порушують навчальний процес. Це підтверджує, що кіберзагрози є реальною та пріоритетною проблемою для сучасного суспільства, зокрема для освітньо-наукової діяльності ЗВО. Кібербезпека стає особливо актуальною для університетів, які щоденно готують висококваліфіковані кадри й відіграють системотворчу роль у зміцненні обороноздатності нашої держави.

Сучасне впровадження інформаційно-комунікаційних технологій набуло широкого поширення та є глобальною тенденцією, яка проникає у всі сфери життя, особливо у сферу інтерактивного навчання. Інформатизація призводить до зростання

[1] Білявська Ю., Шестак Я. Кібербезпека та кібергігієна: нова ера цифрових технологій. Товари і ринки. 2022. № 3. С. 47–59.

[2] Див. докладніше: Татомир І. (2020) Кібербезпека університетів як спосіб протидії фішинговому шахрайству. Економічний дискурс. 2020. Випуск 1. С. 59-67. DOI: https://doi.org/10.36742/2410-0919-2020-1-7.; Vitālijs Rakstiņš, Karina Palkova, Lidija Juļa and Natalia Filipenko (2024) Improving cybersecurity measures in academic institutions to reduce the risk of foreign influence. Socrates. Rīga Stradiņš University Faculty of Law Electronic Scientific Journal of Law. Volume 2024 (2024): Issue 1-29 (September 2024). P. 75-79. https://doi.org/10.25143/socr.29.2024.2.75-79; Савченко В., Маклюк О. (2024). Кібербезпека як фактор ефективності функціонування закладів вищої освіти. Економіка та суспільство, (60). https://doi.org/10.32782/2524-0072/2024-60-24; Лісовська Ю. Кібербезпека: ризики та заходи : навч. посіб. Київ : Кондор, 2019. 272 с. та ін.

залежності від ІКТ у науково-освітній діяльності, де інформаційні технології стають важливими як інструментами, так і чинниками функціонування та розвитку освіти[3].

Слід зазначити, що більшість закладі вищої освіти пройшли шлях від традиційно-консервативного навчально-наукового процесу до сучасної інформаційної (освітньо-наукової) діяльності. Перехід до нового формату супроводжувався створенням власного інформаційного простору, що включав такі основні кроки:

Оновлення та модернізація ІКТ-обладнання – впровадження сучасної техніки й програмного забезпечення для підтримки освітніх та наукових процесів.

Розробка офіційного сайту ЗВО та його структурних підрозділів – забезпечення доступу до інформації про заклад, його діяльність, освітні програми та інші важливі ресурси.

Підключення закладу вищої освіти до Інтернету та створення внутрішньої мережі – мережа забезпечує обмін інформацією та комунікацію між працівниками, студентами та структурними підрозділами університету.

Впровадження електронного документообігу – перехід від паперової до цифрової форми документів для зручності зберігання, обробки та передачі.

Впровадження системи дистанційного навчання – можливість проводити навчання онлайн, що стає особливо актуальним для сучасних військових українських реалій, коли майже половина студентів та викладачів можуть перебувати в різних регіонах України, навіть за кордоном.

Розробка електронних освітніх ресурсів – створення матеріалів та посібників у цифровому форматі, доступних студентам для самостійного навчання.

Створення електронної бібліотеки – надання студентам і професорсько-викладацькому складу університету доступу до електронних книг, наукових статей та інших інформаційних ресурсів.

Впровадження системи електронних журналів для публікації наукових результатів – забезпечення зручного інструменту для наукової діяльності та публікації наукових досліджень.

Використання системи відеоконференцій – відкриває можливість для проведення лекцій, семінарів та нарад дистанційно, що набуває особливого значення для закладів вищої освіти в умовах війни. Завдяки таким технологіям навчальні процеси можуть тривати без фізичної присутності в аудиторіях, що є критичним заходом для безпеки як студентів, так і викладачів, оскільки дозволяє уникнути ризиків ушкоджень у зонах можливих небезпек. Це також сприяє збереженню стабільності освітніх процесів, мінімізуючи перерви в навчанні та підтримуючи якість освітніх програм навіть у складних обставинах.

Впровадження системи відеоспостереження на території закладу вищої освіти – важливий крок для забезпечення контролю та підвищення рівня безпеки. Така система дозволяє оперативно відстежувати ситуацію, фіксувати потенційно небезпечні події, контролювати доступ до навчальних приміщень та попереджати випадки несанкціонованого проникнення. Крім того, відеоспостереження сприяє забезпеченню правопорядку на території закладу, зменшуючи ризики правопорушень та покращуючи реакцію на надзвичайні ситуації. Це особливо актуально в сучасних умовах збройної агресії, коли безпека студентів і працівників навчального закладу потребує додаткової уваги [4].

Автоматизація фінансово-економічної діяльності – використання автоматизованих систем для управління фінансами.

Автоматизація господарської діяльності – підвищення ефективності за рахунок автоматизації адміністративних процесів.

Автоматизація кадрової діяльності – це перехід до електронної системи ведення обліку співробітників, що включає управління всіма аспектами кадрових процесів. Це рішення забезпечує централізований облік даних про персонал, спрощує процедуру підбору та адаптації працівників, моніторинг їхньої продуктивності та ведення електронних особових справ. Автоматизація також сприяє оперативному обміну інформацією між різними підрозділами закладу та полегшує дотримання нормативних вимог щодо кадрової звітності. Використання електронної системи обліку дозволяє більш ефективно управляти кадровими процесами, автоматизувати рутинні завдання, покращувати точність даних і забезпечувати захищеність персональної інформації. Такий підхід не лише зменшує обсяг паперової роботи, але й значно підвищує ефективність кадрового управління, дозволяючи керівникам оперативно отримувати актуальні дані про співробітників.

Встановлення системи контролю доступу – забезпечення безпеки на території закладу вищої освіти та обмеження доступу до окремих зон.

Інформатизація у закладі вищої освіти з одного боку, підвищує якість і ефективність освітньо-наукової діяльності, але з іншого боку, створює багаторівневу інформаційну систему, яка стає критичною для їхньої надійної роботи та кібербезпеки.

[3] Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О. Довгань; упоряд. О. Довгань, Л. Литвинова, С. Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І. Вернадського. К., 2023. №7 (липень). 270 с.

[4] Nataliia Filipenko, Hanna Spitsyna, Olena Agapova, Karina Palkova (2024) The Concept of Comprehensive Security for Higher Educational Institutions: Ukrainian and European Experience: Integrated Computer Technologies in Mechanical Engineering - 2023 Synergetic Engineering. Synergetic Engineering. Presents the proceedings of the ICTM´23 Conference held in Kharkov, Ukraine. URL https://doi.org/10.1007/978-3-031-60549-9_23.

Саме тому під поняттям **«інформаційний простір закладу вищої освіти»** ми розуміємо інтегроване цифрове середовище, що складається з різних інформаційно-комунікаційних технологій (ІКТ) і надає можливість для комплексної взаємодії між викладачами, студентами та адміністрацією. Воно служить платформою для спільного обміну знаннями, навчальними матеріалами та комунікації, забезпечуючи різноманітність освітніх процесів і ресурсів.

Кібербезпека в цьому контексті означає комплекс заходів, спрямованих на захист інформаційного простору від несанкціонованого доступу, зловмисного втручання та порушень цілісності даних. Це передбачає досягнення високого рівня конфіденційності інформації, підтримку її цілісності та доступності для учасників освітнього процесу, що є запорукою стабільності функціонування всіх складових освітньої діяльності та ефективної взаємодії в академічній спільноті..

Критичність інформаційного простору ЗВО зумовлена тим, що в ньому накопичується велика кількість конфіденційної інформації, зокрема: персональні дані (інформація про студентів, співробітників і зміни в складі); службові дані (директиви, накази, розпорядження та інші документи з обмеженим доступом); фінансова інформація (звіти та ресурси); юридична інформація (судові справи, розслідування); освітньо-наукові матеріали (інтелектуальна власність, патенти, наукові дослідження, програми навчання, електронні журнали, навчальні курси та ресурси) тощо.

Через це інформаційний простір закладу вищої освіти є потенційною ціллю для різних видів кіберзагроз, а успішна атака може призвести до таких наслідків: технічні збитки (пошкодження обладнання, блокування доступу до ресурсів, знищення інтелектуальної власності); матеріальні втрати (фінансові витрати на відновлення, проведення аудиту кібербезпеки); репутаційні ризики (втрата довіри партнерів і студентів, зниження авторитету); моральні втрати (шантаж, психологічний стрес співробітників і студентів, особливо у разі витоку даних) тощо.

Виходячи з цього, забезпечення кібербезпеки закладу вищої освіти стає важливим завданням, що включає:

1. Аналіз факторів, які впливають на кібербезпеку ЗВО.

2. Розробку та впровадження моделі кіберзахисту для закладу вищої освіти.

3. Оцінку ефективності цієї моделі кіберзахисту закладу вищої освіти.

4. Підготовку рекомендацій для підвищення ефективності роботи моделі кіберзахисту.

З огляду на мету статті, основну увагу зосередимо на першому завданні — аналізі факторів, що впливають на кібербезпеку закладу вищої освіти. Кібербезпека навчального закладу тісно інтегрована з системою кіберзахисту, яка представляє собою комплекс взаємозалежних заходів, спрямованих на всебічний захист інформаційних ресурсів від численних загроз. Такі загрози можуть бути як зовнішніми, так і внутрішніми, впливаючи на інформаційні системи по-різному – від позитивного зміцнення до негативного зниження їх стійкості.

Комплекс заходів з кіберзахисту включає технологічні, адміністративні та організаційні методи, що разом формують стійку систему безпеки, здатну швидко адаптуватися до нових кіберзагроз. Внутрішні чинники, такі як людський фактор, політики управління доступом, та дотримання стандартів безпеки, можуть суттєво посилити кіберзахист, тоді як слабка внутрішня інфраструктура чи недостатня обізнаність користувачів – послабити. Зовнішні фактори, такі як нові види кіберзагроз і оновлення законодавства в галузі захисту даних, також потребують постійного моніторингу та оперативного реагування, щоб знизити їх негативний вплив на освітню установу.

Внутрішні та зовнішні фактори впливу

Внутрішні фактори, на які заклад може впливати безпосередньо, залежать від дій керівництва та працівників закладу. Вони можуть позитивно вплинути на рівень кібербезпеки, але також мають потенціал для зниження її рівня через помилкові або недбалі дії.

Зовнішні фактори не контролюються безпосередньо закладом вищої освіти і зумовлені зовнішніми умовами, однак їхній вплив можна послабити завдяки вдосконаленню внутрішніх заходів захисту.

Вплив цих факторів обумовлює необхідність проведення постійного моніторингу стану кіберзахищеності закладу. Стан кібербезпеки залежить від того, наскільки ефективно розроблена та реалізована модель кіберзахисту, яка має враховувати результати аналізу впливу обох груп факторів.

Аналіз зазначених факторів допомагає ухвалювати обґрунтовані управлінські рішення, спрямовані на забезпечення ефективної взаємодії університету із зовнішнім інформаційним простором як у коротко-, так і у довгостроковій перспективі. Постійний моніторинг та прогнозування дають змогу керівництву закладу розробляти ефективні стратегії реагування на можливі загрози.

Основні зовнішні фактори, що впливають на кібербезпеку закладу вищої освіти:

Надзвичайні ситуації — можуть призвести до фізичного пошкодження інформаційної інфраструктури.

Розробка та виробництво апаратно-програмного забезпечення — впливає на якість та надійність систем, що використовуються для захисту.

Кібератаки — створюють ризики витоку даних та порушення роботи критично важливих систем.

Вербування або шантаж персоналу — посилює загрозу внутрішніх витоків інформації.

Розгляньмо детальніше зовнішні фактори, які впливають на кібербезпеку університету.

1. Надзвичайні ситуації

Заклади вищої освіти розташовані на певній території, яка може бути вразливою до природних або техногенних небезпек, що часто виникають одночасно, підсилюючи загальний вплив на об’єкт.

Одне небезпечне явище може спричинити низку інших, посилюючи шкоду.

Природні небезпеки: Будь-яка діяльність чи функціонування об'єктів ЗВО здійснюється у взаємодії з природним середовищем, як-от повітря, вода чи ґрунт. Інформаційне середовище закладу вищої освіти також контактує з природними елементами через свої компоненти, такі як інформаційно-телекомунікаційні системи, лінії зв'язку, супутникові та Wi-Fi антени. Ці компоненти можуть зазнавати впливу природних катастроф, зокрема:

- геологічні загрози: землетруси, зсуви ґрунту, обвали, карстові провали та абразія;
- гідрологічні загрози: повені, паводки, підтоплення, снігові лавини, сильні дощі.

Техногенні небезпеки: у закладі вищої освіти використовується енергія, горючі матеріали та інші потенційно небезпечні речовини, що може спричинити аварії. Аналіз показує, що пожежа або вибух можуть завдати значної шкоди як інфраструктурі, так і особовому складу закладу. Важливо запобігати подібним небезпекам шляхом усунення умов їх виникнення та підтримання техногенної безпеки на належному рівні.

Воєнні дії поступово набувають статусу специфічного зовнішнього фактору небезпеки для закладів вищої освіти, оскільки вони можуть істотно впливати на безпеку та стабільність навчального процесу, змінюючи звичний хід освітнього та наукового життя. Як зазначають фахівці[5], крім безпосередніх загроз життю та здоров'ю студентів, викладачів і працівників університетів, війна може призводити до серйозних руйнувань інфраструктури навчальних закладів. Це включає пошкодження чи знищення будівель, лабораторій, аудиторій, бібліотек та іншого обладнання, що використовується для наукових та освітніх цілей. Наслідки таких руйнувань можуть бути надзвичайно складними, оскільки не лише порушується нормальний навчальний процес, а й ускладнюється проведення важливих досліджень та реалізація освітніх ініціатив, які потребують доступу до спеціалізованого обладнання та ресурсів.

Крім того, війна може мати катастрофічні наслідки для організації навчальних планів та програм, призводячи до зупинки або значних змін у графіках занять, викладання та здачі іспитів. Це особливо стосується спеціальностей, які вимагають практичного навчання чи роботи з сучасними технологіями, де навіть тимчасове припинення освітнього процесу може вплинути на кваліфікацію студентів та їхню здатність працювати у високотехнологічних сферах.

Ще однією важливою проблемою є обмеження у проведенні наукових досліджень і реалізації інноваційних проектів. Багато українських університетів активно співпрацюють із закордонними партнерами, але воєнний конфлікт може призвести до розриву таких міжнародних зв'язків, ускладнивши участь у глобальних наукових ініціативах, міжнародних конференціях та обміні досвідом. Це також може позначитися на фінансуванні наукових досліджень, оскільки грантові програми можуть бути скорочені або заморожені.

Зміни в соціально-економічній ситуації також створюють додаткові труднощі для університетів. Зокрема, нестабільність економіки призводить до зменшення бюджетного фінансування, труднощів у залученні інвестицій для розвитку нових наукових напрямів, а також проблем у забезпеченні університетів необхідними матеріальними ресурсами. У таких умовах заклади вищої освіти вимушені оптимізувати свої витрати, що може позначитися на якості освітніх послуг і наукових досліджень.

Усі ці фактори разом підвищують ризики для майбутнього української освіти та науки, тому важливо розробляти стратегії, які дозволяють мінімізувати наслідки воєнних дій, зберігаючи при цьому високий рівень освітнього процесу та наукового розвитку навіть в умовах кризи [6].

2. Інформаційно-комунікаційні технології (ІКТ) нині стали основою для підвищення ефективності в наукових, прикладних і освітніх завданнях в Україні. Однак, як підкреслюють науковці [7], таке впровадження також зумовило значну залежність від ІКТ, зокрема апаратних і програмних складових, які є критично важливими для належного функціонування багатьох освітніх і наукових процесів.

Апаратна частина ІКТ забезпечує технічний базис — це материнська плата, процесори, графічні адаптери, дискові накопичувачі тощо. Програмне забезпечення ж надає можливість ефективної роботи цих апаратних ресурсів, включаючи операційні системи та численну кількість прикладного програмного забезпечення. Ці два компоненти нерозривно пов'язані й утворюють єдину систему. Однак більшість програмних і апаратних засобів, які використовуються в Україні, походять з-за кордону, і це зумовлено цілим рядом факторів, головним серед яких є обмежені ресурси на науково-дослідні роботи в галузі технологій. Відсутність достатнього фінансування та інфраструктури для розвитку власних розробок ускладнює створення конкурентоспроможних українських продуктів. Незважаючи на те, що в

---

[5] Жила Г. Вища освіта в умовах війни: виклики, проблеми, перспективи для студентів та науковців. Молодь і ринок, 2023. №2 (210). С. 141–145. DOI: https://doi.org/10.24919/2308-4634.2023.276118

[6] Nataliia Filipenko (2023) The security for higher educational institutions during military aggression of the Russian federation against Ukraine. Проєктний та логістичний менеджмент: нові знання на базі двох методологій. Том 7 : збірник наукових праць. – Одеса: КУПРІЄНКО СВ, 2023. 198 с.: іл., табл. - (Серія «Проєктний та логістичний менеджмент: нові знання на базі двох методологій», Том 7). ISBN 978-617-7880-38-6. DOI: 10.30888/2616-8936.2023-07. Pp. 52-55.

[7] Биков В. Ю., Буров О. Ю., Дементієвська Н. П. Кібербезпека в цифровому навчальному середовищі. Інформаційні технології і засоби навчання. 2019. Т. 70, № 2. С. 313-331. Режим доступу: http://nbuv.gov.ua/UJRN/ITZN_2019_70_2_25

Україні є численні талановиті спеціалісти в галузі інформаційних технологій, економічні обмеження та низький рівень інвестицій у наукові дослідження значно знижують можливості для масштабних інновацій. Станом на сьогодні, брак фінансування та недостатня державна підтримка вітчизняних розробок програмного та апаратного забезпечення призводять до того, що в Україні зберігається серйозний дефіцит високоякісних національних продуктів, здатних задовольнити внутрішні потреби країни. У той же час, міжнародні корпорації, які мають потужні фінансові можливості, доступ до найсучасніших технологій та висококваліфіковану команду фахівців, можуть створювати і постачати продукцію, яка значно перевищує вітчизняні аналоги за якістю та функціональними можливостями. Це дає їм значну перевагу на глобальному ринку, що ускладнює конкуренцію для українських розробників. Особливо страждає при цьому науковий потенціал вітчизняних закладів вищої освіти, оскільки обмежене фінансування та відсутність достатніх ресурсів для проведення наукових досліджень призводять до спаду якості наукових робіт і зниження конкурентоспроможності українських університетів на міжнародній арені. Через дефіцит коштів багато вищих навчальних закладів змушені скорочувати науково-дослідні програми, обмежувати кількість дослідницьких проєктів і знижувати рівень участі у міжнародних наукових ініціативах. Це також веде до зменшення кількості молодих учених, які не мають можливості реалізувати свої ідеї через відсутність належного фінансування. Крім того, інфраструктура для проведення наукових досліджень часто не відповідає сучасним вимогам, що значно обмежує можливості для розвитку інновацій. Українські науковці, не маючи доступу до новітніх технологій і сучасних лабораторій, змушені працювати в умовах, які істотно ускладнюють досягнення значних наукових результатів. Це також веде до еміграції талановитих науковців, які шукають кращі умови для розвитку своєї кар'єри за кордоном, що ще більше посилює проблему. У таких умовах українські університети все більше зосереджуються на утриманні існуючого наукового потенціалу, а не на його розвитку, що призводить до поступового відставання вітчизняної науки від світових тенденцій.

Проблема відсутності національного ІКТ-обладнання та софту також стає ризиком для кібербезпеки. Іноземне походження техніки та програм часто зумовлює додаткові труднощі з її обслуговуванням та забезпеченням безпеки даних, що циркулюють у внутрішніх системах ЗВО.

З огляду на викладене вище, виникає необхідність визначення ключових аспектів впливу іноземного програмного забезпечення на кібербезпеку ЗВО. Основні чинники можна викласти таким чином:

По-перше, недоліки під час розробки і виробництва апаратно-програмного забезпечення. Відсутність можливості контролювати всі етапи виробництва й тестування такого обладнання може призвести до небажаних наслідків під час його роботи, зокрема до повного чи часткового виходу з ладу. Це потенційно підвищує ризики для функціонування інформаційної інфраструктури ЗВО.

По-друге, відсутність юридичної відповідальності за забезпечення кіберзахисту під час розробки й виробництва. Оскільки відповідальність за можливі кібератаки або зброї часто несе саме користувач, а не розробник чи виробник, ЗВО можуть зазнавати труднощів у забезпеченні кіберзахисту за умов використання іноземного ПЗ.

По-третє, гіпотетична ймовірність існування навмисно вбудованих вразливостей. Ураховуючи сучасні тенденції інформаційного протистояння між державами, можна припустити, що в іноземних апаратно-програмних рішеннях потенційно можуть бути закладені вразливості, що згодом можуть бути використані для реалізації національних інтересів іноземних держав на шкоду інтересам України.

По-четверте, складність створення цілісної системи кіберзахисту у ЗВО відповідно до рішень іноземних виробників. Брак фінансових ресурсів для впровадження ефективної системи кіберзахисту означає, що заклади вищої освіти змушені шукати компроміси між високим рівнем кібербезпеки та витратами на відповідні технології.

Отже, апаратно-програмне забезпечення іноземного походження створює додаткові ризики для кібербезпеки закладу вищої освіти.

3. Кібератаки. Одним з основних факторів, що впливають на кібербезпеку ЗВО, є кібератаки. Під кіберзагрозами слід розуміти цілеспрямовані дії, що впливають на складові інформаційного середовища з використанням різноманітних апаратно-програмних засобів, порушуючи конфіденційність, цілісність і доступність даних. Кібератаки можуть бути як віддаленими (коли зловмисник перебуває за межами операційної зони об'єкта), так і локальними (при фізичному доступі до об'єкта).

Як підкреслюють фахівці [8], до основних видів атак належать:

Шкідливе програмне забезпечення: забезпечує повний доступ до операційної системи, дозволяє контролювати дії користувача, видаляти чи змінювати конфіденційні дані тощо.

Фішинг: атака, спрямована на використання імпульсивності об’єкта, зокрема через електронні листи зі шкідливими посиланнями чи файлами,

[8] Трофименко О. Г. Кібербезпека освітнього сектора. Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття (до 25-річчя Національного університету «Одеська юридична академія» та 175-річчя Одеської школи права) : у 2 т. : матеріали Міжнар. наук.-практ. конф. (м. Одеса, 17 червня 2022 р.) / за загальною редакцією С. В. Ківалова. Одеса : Видавничий дім «Гельветика», 2022. Т. 1. С. 698–700. Режим доступу: https://hdl.handle.net/11300/19765.

SMS-атаки (смішинг) або голосові дзвінки (вішинг), що змушують об'єкт здійснити небезпечні дії [9].

SQL-ін'єкція: використання команд структурованого запиту (SQL) для впливу на базу даних сервера, що може дати доступ до чутливих даних або дозволити виконання шкідливого коду.

XSS-атака (міжсайтовий скриптинг). Цей вид атаки дозволяє використовувати вразливість сайту чи сервера для проведення кібернападу на конкретний об'єкт. Атакуючий може інтегрувати шкідливий код у вебсторінку, яку, ймовірно, відвідає об'єкт атаки. Це забезпечує кіберзлочинцю можливість отримати, наприклад, авторизаційні куки жертви, що дозволяє обійти захист облікового запису, отримати несанкціонований доступ до системи або інформації.

DoS-атака (відмова в обслуговуванні). В основі цього методу атаки лежить перевантаження цільової системи, коли до неї одночасно підключаються численні пристрої-боти. Це призводить до повного вичерпання оперативної пам'яті та ресурсів процесора сервера, внаслідок чого користувачі втрачають доступ до ресурсу. Такі атаки можуть паралізувати роботу вебсайту або іншого інформаційного ресурсу на тривалий час.

Атака нульового дня. Цей тип загрози використовує недоліки апаратно-програмного забезпечення, про які ще не знають розробники або користувачі. Це дає можливість зловмисникам використовувати ці вразливості у своїх цілях до того, як вони будуть виправлені. Результатом таких атак може бути порушення конфіденційності, цілісності або доступності інформаційного ресурсу.

4. Вербування або шантаж персоналу. Останнім часом в Україні та в інших країнах зростає кількість повідомлень про діяльність іноземних агентів, що викликає широке обговорення в суспільстві, зокрема через випадки затримання високопосадовців, підозрюваних у співпраці з ворожими силами чи іноземними агентами (наприклад, країною - агресором). Такі інциденти стають об'єктами гучних медійних розслідувань і створюють серйозні виклики для національної безпеки. Агентурна діяльність, особливо коли вона спрямована на активне вербування або шантаж громадян, які займають ключові позиції у владі або в стратегічних сферах, може мати далекосяжні наслідки. Загроза, пов'язана з використанням таких методів, розповсюджується не лише на державні органи, але й на інші інституції, серед яких важливу роль займають заклади вищої освіти, особливо ті, що займаються підготовкою висококваліфікованих кадрів у технічних та наукових сферах. Заклади вищої освіти, як основа для розвитку національної інтелектуальної еліти, є важливими елементами формування незалежності та безпеки держави. Вони готують не лише фахівців, які здійснюють безпосередньо технологічні та наукові інновації, але й тих, хто бере участь у розробці та управлінні критичними інфраструктурами, що є основою для функціонування країни. Тому захист цих інститутів від впливу іноземних агентів і забезпечення їхньої кібербезпеки стає однією з пріоритетних задач у контексті загрози національній безпеці.

Запобігання вербуванню співробітників, які займаються управлінням інформаційною інфраструктурою університетів, а також професорсько-викладацького складу, є важливим етапом у протидії такій загрозі. Ці особи можуть бути найбільш уразливими до маніпуляцій або шантажу через своє значення у забезпеченні функціонування навчального процесу та збереження інформаційної безпеки закладів вищої освіти. Під тиском чи обіцянками вигод вони можуть бути змушені здійснювати дії, які поставлять під загрозу не тільки окремі системи, але й всю інформаційну безпеку університету. Це може включати несанкціонований доступ до критичних даних, порушення норм кібербезпеки або навіть створення каналів для передачі конфіденційної інформації іноземним силам. У таких умовах необхідно розробляти цілісні стратегії, які включатимуть не лише технологічні засоби захисту (таких як система моніторингу та виявлення порушень у мережах), але й організаційні заходи, спрямовані на зміцнення внутрішньої безпеки.

Як зазначають спеціалісти [10], до цих заходів можуть належати постійні тренінги для персоналу, розробка етики та процедур перевірки на благонадійність співробітників, а також створення патріотичної, культурної та психологічної підтримки для виявлення та запобігання спробам маніпуляцій. Крім того, важливим є підвищення рівня свідомості серед студентів і викладачів щодо кіберзагроз і їхніх потенційних наслідків для безпеки не лише навчального закладу, але й країни в цілому.

Тільки комплексний підхід до забезпечення безпеки вищих навчальних закладів може дати змогу не лише захистити їх від зовнішніх загроз, а й забезпечити стабільність і незалежність країни в умовах сучасної геополітичної ситуації.

Висновки. Аналіз зовнішніх чинників, які впливають на кібербезпеку закладів вищої освіти, виявляє їх неконтрольований характер із боку самих установ. До таких зовнішніх загроз належать кібернапади (DDoS, фішинг, атаки нульового дня), постійно змінювані законодавчі вимоги, поява нових технологій та інші фактори, що можуть поставити під загрозу інформаційні системи та особисті дані навчальних закладів. Через це виникає нагальна потреба у зміцненні внутрішніх компонентів, які можуть протистояти таким зовнішнім впливам і забезпечувати стійкість кіберзахисту університету.

---

[9] Татомир І. (2020) Кібербезпека університетів як спосіб протидії фішинговому шахрайству. Економічний дискурс. 2020. Випуск 1. С. 59-67. DOI: https://doi.org/10.36742/2410-0919-2020-1-7.

[10] Vitālijs Rakstiņš, Karina Palkova, Lidija Juļa and Natalia Filipenko (2024) Improving cybersecurity measures in academic institutions to reduce the risk of foreign influence. Socrates. Rīga Stradiņš University Faculty of Law Electronic Scientific Journal of Law. Volume 2024 (2024): Issue 1-29 (September 2024). P. 75-79. https://doi.org/10.25143/socr.29.2024.2.75-79

Побудова міцної системи кібербезпеки у ЗВО має ґрунтуватися на комбінації сильних внутрішніх чинників. До них належать інфраструктура кібербезпеки, регулярне навчання та підвищення кваліфікації персоналу, чітко визначені процедури управління ризиками, інформованість про загрози та належний рівень захищеності ІТ-інфраструктури. Програми з кібербезпеки мають враховувати оновлення програмного забезпечення, регулярні аудити безпеки та політики моніторингу інцидентів. Впровадження такої стратегії дозволить значно підвищити загальний рівень кіберзахисту, водночас забезпечуючи швидке реагування на нові загрози.

Крім того, постійний аналіз внутрішніх чинників є важливим елементом побудови ефективної системи безпеки у закладі вищої освіти. Це включає оцінку рівня обізнаності всього персоналу щодо кіберзагроз, аналіз існуючих політик і процедур безпеки та розробку заходів для створення культури безпеки у ЗВО. Важливо, щоб керівництво ЗВО забезпечувало регулярні тренінги для співробітників, впроваджувало оновлені процедури роботи з конфіденційною інформацією та підтримувало сучасні технологічні рішення для запобігання загрозам.

Систематичний підхід до забезпечення безпеки, який враховує як зовнішні, так і внутрішні фактори, дозволяє закладам вищої освіти значно підвищити рівень захисту даних та забезпечити ефективне функціонування в умовах швидко змінюваних кіберризиків. Такий підхід охоплює не лише технічні засоби, як-от антивірусні програми, фаєрволи та системи виявлення вторгнень, але й організаційні стратегії, які включають постійну оцінку та адаптацію до нових загроз. Врахування внутрішніх факторів, таких як рівень обізнаності персоналу, політика доступу до інформації та безпека комунікацій, дозволяє мінімізувати ризики, пов'язані з людським фактором, який часто є найбільш уразливим елементом у системах кібербезпеки.

Зовнішні фактори, такі як глобальні кіберзагрози, діяльність хакерських груп або вплив іноземних агентів, вимагають постійної моніторингу міжнародних тенденцій та адаптації внутрішніх процедур до нових викликів. У такому середовищі важливо не лише реагувати на поточні загрози, але й здійснювати прогностичну оцінку потенційних ризиків для того, щоб передбачити і запобігти можливим інцидентам.

Завдяки комплексному підходу, що поєднує технічні, організаційні та кадрові заходи, ЗВО можуть не лише зміцнити свою кіберзахищеність, але й забезпечити безперервність навчального процесу, наукових досліджень та інновацій, навіть в умовах змінних і складних кіберзагроз.

Бібліографічні посилання

1. Nataliia Filipenko (2023) The security for higher educational institutions during military aggression of the Russian federation against Ukraine. Проєктний та логістичний менеджмент: нові знання на базі двох методологій. Том 7 : збірник наукових праць. – Одеса: КУПРІЄНКО СВ, 2023. 198 с.: іл., табл. - (Серія «Проєктний та логістичний менеджмент: нові знання на базі двох методологій», Том 7). ISBN 978-617-7880-38-6. DOI: 10.30888/2616-8936.2023-07. Pp. 52-55.

2. Nataliia Filipenko, Hanna Spitsyna, Olena Agapova, Karina Palkova (2024) The Concept of Comprehensive Security for Higher Educational Institutions: Ukrainian and European Experience: Integrated Computer Technologies in Mechanical Engineering - 2023 Synergetic Engineering. Synergetic Engineering. Presents the proceedings of the ICTM´23 Conference held in Kharkov, Ukraine. URL https://doi.org/10.1007/978-3-031-60549-9_23.

3. Vitālijs Rakstiņš, Karina Palkova, Lidija Juļa and Natalia Filipenko (2024) Improving cybersecurity measures in academic institutions to reduce the risk of foreign influence. Socrates. Rīga Stradiņš University Faculty of Law Electronic Scientific Journal of Law. Volume 2024 (2024): Issue 1-29 (September 2024). P. 75-79. https://doi.org/10.25143/socr.29.2024.2.75-79

4. Биков В. Ю., Буров О. Ю., Дементієвська Н. П. Кібербезпека в цифровому навчальному середовищі. Інформаційні технології і засоби навчання. 2019. Т. 70, № 2. С. 313-331. Режим доступу: http://nbuv.gov.ua/UJRN/ITZN_2019_70_2_25

5. Білявська Ю., Шестак Я. Кібербезпека та кібергігієна: нова ера цифрових технологій. Товари і ринки. 2022. № 3. С. 47–59.

6. Жила Г. Вища освіта в умовах війни: виклики, проблеми, перспективи для студентів та науковців. Молодь і ринок, 2023. №2 (210). С. 141–145. DOI: https://doi.org/10.24919/2308-4634.2023.276118

7. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І.Вернадського. К., 2023. №7 (липень). 270 с.

8. Савченко В., Маклюк О. (2024). Кібербезпека як фактор ефективності функціонування закладів вищої освіти. Економіка та суспільство, (60). https://doi.org/10.32782/2524-0072/2024-60-24; Лісовська Ю. Кібербезпека: ризики та заходи : навч. посіб. Київ : Кондор, 2019. 272 с.

9. Татомир І. (2020) Кібербезпека університетів як спосіб протидії фішинговому шахрайству. Економічний дискурс. 2020. Випуск 1. С. 59-67. DOI: https://doi.org/10.36742/2410-0919-2020-1-7.

10. Трофименко О. Г. Кібербезпека освітнього сектора. Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття (до 25-річчя Національного університету «Одеська юридична академія» та 175-річчя Одеської школи права) : у 2 т. : матеріали Міжнар. наук.-практ. конф. (м. Одеса, 17 червня 2022 р.) / за загальною редакцією С. В. Ківалова. Одеса : Видавничий дім «Гельветика», 2022. Т. 1. С. 698–700. Режим доступу: https://hdl.handle.net/11300/19765.

O. Lytvynov, N. Filipenko, S. Lukashevych, K. Palkova

Cyber security as a factor of the efficiency of higher education institutions.

Abstract. The article examines the impact of cybercrime on the functioning of higher education institutions and explores possible methods for preventing and addressing cyberattacks. It emphasizes that, despite the numerous advantages of using computer technologies, these technologies also pose risks related to the complexity of ensuring data security. It has been established that modern global trends in countering cyber threats fall short of the scale and efficiency of cybercriminal activities, resulting in an increase in the number of aggressive and successful cyberattacks. Particular attention is paid to the growing number of attacks on educational networks in recent years. The article proposes organizational measures aimed at addressing cybersecurity challenges. It concludes that the key factors for effectively countering cyber threats include the level of preparedness, competence, and responsibility of participants in the educational process. These factors, in turn, determine the stability and success of higher education institutions in Ukraine.

Keywords: cybercrime, cybersecurity, higher education institutions, external influencing factors, internal influencing factors, prevention of offenses and crimes.

Зразок для цитування:
Литвинов О., Філіпенко Н., Лукашевич С., Палкова К. Кібербезпека як фактор ефективності закладів вищої освіти. Пропілеї права та безпеки: наук. журнал. Національний аерокосмічний університет ім. М.Є. Жуковського «Харківський авіаційний інститут», 2024. № 5. С. 15-23. DOI: https://doi.org/10.32620/pls.2024.5.02.