МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ ПЕДАГОГІЧНИХ НАУК УКРАЇНИ
Інститут педагогіки Національної академії педагогічних наук України
UNIVERSITÉ CÔTE D'AZUR (FRANCE)
UNIVERSIDAD CARLOS III DE MADRID (SPAIN)
MIEDZYNARODOWA AKADEMIA NAUK STOSOWANYCH W ŁOMZY (POLAND)
UNIWERSYTETU KOMISJI EDUKACJI NARODOWEJ W KRAKOWIE (POLAND)
SECONDARY INDUSTRIAL, TECHNICAL AND AUTOMOTIVE SCHOOL JIHLAVA (CZECH REPUBLIC)
УКРАЇНСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІМЕНІ МИХАЙЛА ДРАГОМАНОВА
Кафедра інформаційних технологій і програмування

МАТЕРІАЛИ

Міжнародної науково-практичної конференції

ЦИФРОВА ТРАНСФОРМАЦІЯ В ОСВІТІ: ВИКЛИКИ ТА ПЕРСПЕКТИВИ

КИЇВ – 2025

УДК 37-044.922:004]:005.745
Ц 75

Рекомендовано до друку Вченою радою
Українського державного університету імені Михайла Драгоманова
(протокол № 12 від 25 квітня 2025 р.)

Ц 75 Цифрова трансформація в освіті: виклики та перспективи: *матеріали Міжнародної науково-практичної конференції (15 – 16 квітня 2025 року, м. Київ)* / Упорядники: Твердохліб І.А., Малюх Є.В. Київ: Вид-во УДУ імені Михайла Драгоманова, 2025. 324 с. електронне видання

ISBN 978-966-931-325-6

Збірник містить матеріали доповідей учасників Міжнародної науково-практичної конференції «Цифрова трансформація в освіті: виклики та перспективи».

Доповіді присвячені цифровій трансормації освіти, методичним аспектам використання сучасних інформаційних технологій в освітньому процесі, проблемам модернізації змісту інформатичної середньої та вищої освіти в умовах цифрової трансформації, особливостям впровадження STEAM в освітній процес. Розглянуто актуальні в даний час питання використання штучного інтелекту в освітньому процесі, досвід і перспективи цифровізації освіти України.

ISBN 978-966-931-325-6

3. Морзе Н. В., Гладун М., Дзюба С. Formation of key and subject competences of students by robotic means of STEM-education. Інформаційні технології і засоби навчання, 2018, Т. 65, № 3, 37–52. URL: https://doi.org/10.33407/itlt.v65i3.2041
4. Федоренко Н., Молоціян В. Впровадження освітніх технологій формування soft skills у студентів вищої школи. Вища освіта України, 2024, № 1(92). URL: https://doi.org/10.32782/NPU-VOU.2024.1(92).13

ПРОФЕСІЙНА СПРЯМОВАНІСТЬ НАВЧАННЯ КІБЕРБЕЗПЕКИ СТУДЕНТІВ ІНЖЕНЕРНИХ СПЕЦІАЛЬНОСТЕЙ: ОСОБЛИВОСТІ ФОРМУВАННЯ ЗНАНЬ ТА ВМІНЬ

Ящик Олександр Богданович
доцент кафедри комп'ютерних технологій, кандидат педагогічних наук, доцент
Тернопільський національний педагогічний університет ім. В. Гнатюка,
м. Тернопіль, Україна
SanyTNPU@gmail.com

Ящик Артем Олександрович
здобувач рівня вищої освіти,
Київський національний університет імені Тараса Шевченка м. Київ, Україна
boxartem555@gmail.com

Розвиток цифрових технологій призвів до зростання загроз у сфері кібербезпеки. Для ефективного захисту інформаційних систем необхідно підготувати висококваліфікованих фахівців, зокрема серед студентів інженерних спеціальностей. Навчання кібербезпеки для таких студентів має свою специфіку, адже воно поєднує технічні знання з практичними навичками аналізу та усунення загроз. Інженерні спеціальності, такі як цифрові технології, комп'ютерна інженерія та автоматизація, передбачають роботу з мережевими та програмними системами. Оскільки ці системи є вразливими до атак, знання основ кібербезпеки є важливим для запобігання загрозам і забезпечення захищеності інформації. Майбутні інженери мають навчитися не лише створювати технології, а й захищати їх від можливих кіберзагроз, що постійно змінюються і ускладнюються.

Формування професійної спрямованості навчання кібербезпеки передбачає комплексний підхід, що включає вивчення основ інформаційної безпеки, сучасних методів криптографічного захисту, а також аналізу вразливостей програмних та апаратних систем. Одним із ключових напрямів є розуміння принципів етичного хакінгу та тестування безпеки, що дозволяє студентам практично оцінювати рівень захищеності інформаційних систем. Крім того, значна увага приділяється навчанню методам виявлення, моніторингу та аналізу кіберзагроз. Студенти знайомляться з основами роботи із сучасними інструментами безпеки, такими як SIEM-системи, IDS/IPS-рішення, а також методами реагування на інциденти. Особливий акцент робиться на розумінні безпечного програмування, що дозволяє запобігати вразливостям ще на етапі розробки програмного забезпечення. Не менш важливим є ознайомлення з нормативно-правовими аспектами кібербезпеки, міжнародними стандартами та регламентами, що визначають вимоги до захисту інформації. Такий підхід гарантує всебічну підготовку студентів, дозволяючи їм не лише засвоїти теоретичні основи, а й отримати практичні навички роботи з реальними загрозами у сфері кібербезпеки [1].

Ще одним важливим напрямом є навчання принципам захисту критичної інфраструктури, зокрема в енергетичній, транспортній та фінансовій сферах. Інженери, які працюватимуть у цих галузях, повинні розуміти ризики, пов’язані з потенційними атаками, і вміти запроваджувати заходи щодо їхнього запобігання. Окремо слід зазначити, що студенти отримують знання про методи соціальної інженерії – техніки, які використовуються кіберзлочинцями для маніпуляції людьми з метою отримання конфіденційної інформації. Розуміння цих методів допомагає майбутнім фахівцям розробляти ефективні стратегії захисту, які включають не лише технологічні заходи, а й підвищення рівня обізнаності користувачів про загрози. Сучасний навчальний процес також передбачає інтеграцію кібербезпеки в інші дисципліни. Наприклад, курси з розробки програмного забезпечення включають модулі з безпечного кодування, а дисципліни з комп’ютерних мереж приділяють увагу методам виявлення та запобігання атакам.

Розширення співпраці між закладами освіти та бізнесом відіграє ключову роль у підготовці студентів. Завдяки стажуванням, спільним дослідницьким проєктам та залученню експертів із провідних компаній, студенти отримують доступ до найновіших технологій та реальних кейсів, що допомагає їм краще адаптуватися до викликів сучасного цифрового середовища.

Для того щоб студенти могли ефективно засвоїти матеріал, використовуються різні методи навчання. Лекційні курси доповнюються практичними заняттями, де студенти працюють із реальними кейсами. Лабораторні роботи проводяться у віртуальних середовищах, де вони можуть тестувати атаки та шукати способи їхнього запобігання. Особливо цікавим і корисним методом є змагання у форматі Capture The Flag (CTF), які дозволяють учасникам спробувати свої сили у зламі та захисті систем. Крім того, студенти виконують проєктні завдання, де застосовують отримані знання для вирішення практичних завдань у сфері кібербезпеки. Використання інтерактивних симуляторів загроз дає можливість розвивати навички оперативного реагування на атаки. Під час навчання студенти розвивають вміння аналізувати атаки та реагувати на інциденти, розробляти безпечне програмне забезпечення, виявляти та усувати вразливості систем. Вони також навчаються адмініструванню безпечних мережевих інфраструктур, що є ключовим аспектом забезпечення стійкості інформаційних систем. Практичні навички стають основою для подальшої професійної діяльності, адже сучасні роботодавці очікують від випускників не лише теоретичних знань, а й готовності працювати з реальними загрозами.

Щоб детальніше розкрити значення кібербезпеки для інженерних спеціальностей, можна підкреслити важливість цієї дисципліни в контексті постійно зростаючих кіберзагроз, з якими стикаються сучасні інформаційні системи. Успішний розвиток інженерних спеціальностей, таких як комп'ютерні науки, автоматизація, інформаційні технології та інші, неможливий без відповідного забезпечення безпеки цих технологій. Кібербезпека стає важливою, тому що кожна інженерна система, яка працює з інформацією, може бути вразливою до атак. Це може призвести до серйозних наслідків, таких як витік конфіденційних даних, знищення або модифікація критичної інформації, зупинка діяльності підприємств або навіть національна безпека може бути поставлена під загрозу.

Для студентів інженерних спеціальностей важливо розуміти, що їхня роль не тільки у створенні нових технологій, але й у забезпеченні їх захищеності від кіберзагроз. Тому курси з кібербезпеки включають вивчення методів захисту, системного адміністрування безпеки, тестування на вразливості та створення безпечного програмного забезпечення. Важливість кібербезпеки в інженерних спеціальностях можна також пов'язати з тим, що професіонали, які працюють в таких сферах, мають зобов'язання не тільки за розробку, а й за забезпечення стійкості технологічних рішень у разі кіберзагроз. Цей контекст підкреслює необхідність формування у студентів інженерних спеціальностей навичок, які дозволяють не тільки реагувати на атаки, але й створювати інфраструктури, стійкі до таких загроз.

Особливо важливим є набуття навичок розробки безпечного програмного забезпечення. Студенти вивчають принципи захищеного кодування, що допомагають уникнути основних вразливостей (наприклад, SQL-ін'єкцій, buffer overflow, тощо). Вони також навчаються проводити аудит безпеки програмного забезпечення для виявлення потенційних загроз. Практичні навички адміністрування безпечних мережевих інфраструктур є основою для подальшої професійної діяльності. Студенти отримують досвід у налаштуванні та адмініструванні систем безпеки для захисту інформаційних ресурсів на рівні мереж, серверів та робочих станцій. Вони вивчають методи моніторингу, виявлення аномалій і аналізу подій в реальному часі. Значну роль відіграє також навчання управлінню інцидентами: студентам надаються практичні завдання з реагування на інциденти безпеки, включаючи виявлення атак, блокування загроз та відновлення роботи систем після атаки. Це навчання відбувається в умовах реальних симуляцій, де вони вчаться застосовувати інструменти для виявлення та усунення загроз в умовах, наближених до реальних. Така практична підготовка дає студентам не лише глибоке розуміння теоретичних основ кібербезпеки, але й здатність оперативно діяти в умовах реальних кіберзагроз. Це підготовка фахівців, здатних працювати в умовах постійно змінюваного цифрового середовища.

Формування знань та вмінь з кібербезпеки у студентів інженерних спеціальностей є ключовим аспектом їхньої професійної підготовки. Завдяки поєднанню теоретичних основ і практичного досвіду майбутні фахівці отримують необхідні навички для захисту інформаційних систем. Впровадження практико-орієнтованого підходу дозволяє створити ефективну систему навчання, що відповідає сучасним вимогам ринку праці та сприяє забезпеченню безпеки цифрового середовища. Формування знань та вмінь у сфері кібербезпеки є надзвичайно важливим аспектом професійної підготовки студентів інженерних спеціальностей. В умовах постійно зростаючих кіберзагроз і розвитку цифрових технологій, ефективний захист інформаційних систем стає однією з основних задач майбутніх фахівців.

Успішна підготовка майбутніх інженерів у сфері кібербезпеки потребує інтеграції теоретичних знань із практичними навичками. Студенти повинні не лише вивчати основи інформаційної безпеки, криптографії, методів тестування на вразливості, але й розвивати здатність застосовувати ці знання для забезпечення реального захисту інформаційних систем. Використання сучасних методів навчання, таких як практичні заняття, лабораторні роботи, змагання Capture The Flag (CTF), інтерактивні симулятори загроз, дають можливість студентам набувати

необхідні практичні навички. Моделювання різних ситуацій дає можливість їм відчути реальні умови, з якими вони зіштовхнуться в професійній діяльності, і отримати досвід у виявленні та усуненні кіберзагроз. Використання комплексного підходу до навчання, що включає теоретичну підготовку, практичні завдання, проєкти та взаємодію з реальними кейсами, сприяє формуванню професіоналів, здатних ефективно вирішувати питання кіберзахисту в умовах сучасного цифрового світу.

Перспективи розвитку цього напрямку навчання виглядають обнадійливими. Впровадження нових технологій, співпраця з реальними компаніями та впровадження сучасних інструментів дає можливість підготувати висококваліфікованих спеціалістів, готових до викликів, що стоять перед кібербезпекою на глобальному рівні. Отже, кібербезпека для інженерів є не просто галуззю знань, а обов'язковою складовою професійної підготовки, що дає можливість забезпечити стабільність та безпеку цифрового середовища в умовах постійних технологічних змін.

Список використаних джерел:

1. Oleksandr Yashchyk. Shielding Web Application against Cyber-Attacks using SIEM / Andriy Yushko; Ruslan Shevchuk; Karol Łopaciński; Maja Leszczynska; Tetiana Yurchyshyn // 2023 13th International Conference on Advanced Computer Information Technologies (ACIT) – Proceedings 21-23 September 2023, Wroclaw, Poland. Pages 393-397 DOI: 10.1109/ACIT58437.2023.10275630
2. Ніколіна І. І., Гулівата І. О. Моделювання кіберзлочинності як загрози цифровізації економіки. Комп'ютерно-інтегровані технології: освіта, наука, виробництво. 2020. № 39. С. 190-196.
3. Ящик О. Б., Симонов В. В., Іваненко Р. О. Забезпечення кібербезпеки в еру штучного інтелекту: аналіз технологічних підходів та стратегій для захисту інформації. БІЗНЕСІНФОРМ № 1_2024. С. 81-86. DOI: https://doi.org/10.32983/2222-4459-2024-1-81-86.

Наукове видання

МАТЕРІАЛИ

Міжнародної науково-практичної конференції

ЦИФРОВА ТРАНСФОРМАЦІЯ В ОСВІТІ: ВИКЛИКИ ТА ПЕРСПЕКТИВИ

Упорядники: І.А. Твердохліб, Є.В. Малюх

Матеріали подано мовою оригіналу

Електронне видання

ВИДАВНИЦТВО
УКРАЇНСЬКОГО ДЕРЖАВНОГО УНІВЕРСИТЕТУ
імені Михайла Драгоманова

Підписано до друку 12.05.2025 р.
Гарнітура Times.
Облік.видав.арк. 29,09
Зам. № 038
Віддруковано з оригіналів.

Видавництво Українського державного університету
імені Михайла Драгоманова.
01601, м. Київ-30, вул. Пирогова, 9
Свідоцтво про реєстрацію ДК 7896 від 25.07.2023.
(044) 239-30-26.