KHARKIV IT CLUSTER

Громадська спілка "Харківський кластер інформаційних технологій"
вул.Громадянська 11/13,
м.Харків, 61057 Україна
+38 (050) 658-88-46
olga.shapoval@it-kharkiv.com
www.it-kharkiv.com

РЕЦЕНЗІЯ
на освітньо-професійну програму «Кібербезпека»
підготовки здобувачів першого (бакалаврського) рівня вищої освіти
за спеціальністю 125 Кібербезпека
галузі знань 12 Інформаційні технології
у Державному біотехнологічному університеті

У сучасних умовах постійного зростання кіберзагроз та масштабної цифровізації державних сервісів в Україні підготовка фахівців за спеціальністю 125 «Кібербезпека» набуває критичного значення. Рецензована освітня програма повною мірою відповідає актуальним потребам ринку, зокрема у частині захисту критичної інформаційної інфраструктури.

Освітня програма «Кібербезпека» є важливим напрямом підготовки кадрів, що корелює з чинною нормативно-правовою базою України у сфері кібербезпеки. Програма сформована з урахуванням стрімкого розвитку технологій і зростання складності кіберзагроз, що визначає її високу практичну цінність для підготовки конкурентоспроможних фахівців.

Структура навчального плану відзначається логічністю, цілісністю та методичною збалансованістю. Фундамент підготовки забезпечується такими компонентами, як адміністрування операційних систем, хмарні сервіси та віртуалізація, безпека баз даних і систем управління ними, алгоритмізація та об’єктно-орієнтоване програмування. Зазначені дисципліни формують стійкий технологічний базис, необхідний для глибокого розуміння процесів обробки та захисту даних.

Окрему цінність для стейкхолдерів становлять спеціалізовані модулі, спрямовані на вивчення стеганографічних методів приховування даних, протоколів безпечної передачі інформації та проєктування комплексних систем захисту інформації (КСЗІ). Важливо, що ці компоненти розглядаються у контексті відповідності державним нормативним вимогам (НД ТЗІ), що забезпечує готовність випускників до роботи з об’єктами критичної інфраструктури.

Ключовою перевагою програми є потужний лабораторний складник. Організація навчання у спеціалізованих симуляційних середовищах дозволяє студентам набути практичних навичок у сфері виявлення аномалій мережевого трафіку, проведення криптографічного аналізу та розробки політик доступу. Проходження виробничої практики на базі провідних компаній галузі забезпечує інтеграцію теоретичних знань із реальними бізнес-кейсами та сприяє швидкій професійній адаптації випускників.

Освітня програма узгоджується з європейськими стандартами у сфері кібербезпеки та рекомендаціями SANS Institute. Вона орієнтована на підготовку фахівців, здатних не лише впроваджувати рішення, але й здійснювати комплексний аудит систем, оцінювати ризики та забезпечувати безперервність бізнес-процесів.

Аналіз навчально-методичного забезпечення (силабусів і робочих програм) підтверджує відповідність змісту дисциплін сучасним вимогам ринку. Лабораторно-практична складова побудована таким чином, щоб трансформувати теоретичні знання у прикладні компетентності.

Важливу роль відіграють дисципліни «Системний аналіз» та «Теорія ризиків», які формують сучасне бачення управління кіберзагрозами. Актуальним є перехід від статичних моделей оцінки до безперервного моніторингу та використання інструментів кіберрозвідки і прогнозування атак на основі аналізу великих даних.

У межах курсу «Безпека безпровідних, мобільних та хмарних технологій» доцільним є впровадження підходів DevSecOps, що передбачає інтеграцію безпеки у процеси розробки. Практичні навички мають включати налаштування контейнеризованих середовищ, використання автоматизованих інструментів аналізу безпеки та захист API.

Дисципліна «Аналіз і моніторинг кібернетичної безпеки» виконує інтегруючу функцію, поєднуючи технічні рішення з нормативною базою. Особливу увагу приділено повному циклу функціонування SOC (Security Operations Center), включаючи налаштування систем збору логів і розробку процедур реагування на інциденти. Важливим є також формування вміння обґрунтовувати вибір засобів захисту, що мають відповідні експертні висновки.

Розгляд процесу створення КСЗІ подається як комплексна інженерно-управлінська задача — від формування технічного завдання до впровадження сертифікованих рішень і проходження державної експертизи.

Для подальшого посилення конкурентоспроможності випускників доцільно поглибити вивчення методів та засобів збереження, маскування та відновлення даних в сфері інформаційних технологій (зокрема стратегії резервного копіювання, правило 3-2-1, налаштування програмного RAID-масиву в Linux, специфіка відновлення даних з SSD та NVMe).

У цілому рецензована освітня програма за спеціальністю 125 «Кібербезпека» є цілісною, науково обґрунтованою та актуальною. Вона забезпечує формування ключових професійних компетентностей, необхідних для успішної кар’єри у сфері безпеки інформаційно-комунікаційних технологій, та має високий потенціал для підготовки кваліфікованих фахівців.

Рецензент,
виконавча директорка
Громадської спілки
«Харківський кластер
інформаційних
технологій»

Ольга ШАПОВАЛ