МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська юридична академія»

ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ: НАУКОВО-ПРАКТИЧНИЙ ВИМІР В УМОВАХ ВОЄННИХ ВИКЛИКІВ

МАТЕРІАЛИ
Міжнародної науково-практичної конференції

Одеса, 26 квітня 2024 року

Одеса
«Фенікс»
2024

УДК 005.332.2(4):316.42(477)“364”“20”(062.552)
Є 24

Рекомендовано до друку вченою радою
Національного університету «Одеська юридична академія»
(протокол № 8 від 15.05.2024 р.)

За загальною редакцією ***С. В. Ківалова***

Відповідальний за випуск ***М. Р. Аракелян***

Є 24 **Європейські орієнтири розвитку України: науково-практичний вимір в умовах воєнних викликів** : матеріали Міжнар.наук.-практ. конф. (Одеса, 26 квітня 2024 р.) / за заг. ред. С. В. Ківалова. – Одеса : Фенікс, 2024. – 1000 с.
ISBN 978-617-8430-05-4

У збірнику відображено наукові напрацювання вчених, практиків, військовослужбовців у теоретичній та емпіричній площині у сферах філософських основ, загальної теорії та історичних досліджень держави і права, актуальних проблем світових соціально-політичних процесів, соціології та психології в умовах повномасштабного військового вторгнення. Висвітлено питання загроз національній безпеці в їх конституційному вимірі у рамках міжнародного та європейського права, трудового права та права соціального забезпечення, земельного, аграрного та екологічного права, пов’язані з функціонуванням економіки та підприємництва в умовах європейського вибору України. Розглянуто проблеми інформатизації та цифровізації суспільства, захисту інформації та кібербезпеки в умовах військового вторгнення, питання методики викладання іноземних мов, теорії та практики перекладу, проблеми лінгвістики та журналістики. Відображено наукові напрацювання у сферах адміністративного права та процесу, фінансового, морського та митного права, організації та вдосконалення судоустрою, прокуратури, інших правоохоронних органів, адвокатури. Висвітлено питання кримінального права, кримінально-процесуальних аспектів кримінального провадження та кримінологічних особливостей протидії злочинності в умовах воєнного стану, криміналістики, судової експертизи, психології та медицини у забезпеченні судочинства, цивільного та сімейного права, інтелектуальної власності та патентної юстиції, цивільного судочинства, господарського права та процесу. Розглянуто актуальні питання діяльності сучасних бібліотек у закладах вищої освіти, фізичної підготовки здобувачів вищої освіти.

Збірник розраховано на наукових і науково-педагогічних працівників, здобувачів вищої освіти, практичних працівників у сферах юридичної, економічної, соціологічної, політологічної, психологічної, філологічної наук, журналістики та кібербезпеки тощо.

УДК 005.332.2(4):316.42(477)»364»»20»(062.552)

Матеріали видано в авторській редакції

ISBN 978-617-8430-05-4

СЕКЦІЯ 24. КІБЕРБЕЗПЕКА ОСОБИ, СУСПІЛЬСТВА ТА ДЕРЖАВИ ЯК ФУНДАМЕНТАЛЬНИЙ ЕЛЕМЕНТ ЗАБЕЗПЕЧЕННЯ ОБОРОНОЗДАТНОСТІ УКРАЇНИ

СЕКЦІЯ 25. ПИТАННЯ МЕТОДИКИ ВИКЛАДАННЯ ІНОЗЕМНИХ МОВ, ТЕОРІЇ ТА ПРАКТИКИ ПЕРЕКЛАДУ ЯК ЗАСОБУ НАЛАГОДЖЕННЯ КОМУНІКАЦІЇ

Савpацький Олександр Олександрович
Національний університет «Одеська юридична академія»,
аспірант кафедри кібербезпеки

ОСОБЛИВОСТІ ПІДГОТОВКИ ФАХІВЦІВ З КІБЕРБЕЗПЕКИ В УМОВАХ ВІЙНИ

Підготовка фахівців з кібербезпеки в умовах війни набуває особливої актуальності та викликів, адже сучасні конфлікти не обмежуються лише традиційним бойовим протистоянням, а все частіше включають в себе і кіберпростір. Це вимагає глибокого переосмислення та адаптації програм підготовки спеціалістів, які займаються захистом інформаційного простору.

Перше і, мабуть, найважливіше – зростає потреба у фахівцях, здатних оперативно реагувати на кіберзагрози, які еволюціонують з надзвичайною швидкістю. У відповідь на це освітні програми мають акцентувати на розвитку практичних навичок у реальних умовах, що включає не тільки теоретичне навчання, але й регулярні практичні заняття з використанням симуляторів кібератак та захисту, а також стажування в організаціях пов'язаних з кібербезпекою [1].

Іншим критичним аспектом є включення до програми вивчення психології ворога та методів психологічної війни в кіберпросторі. Розуміння мотивів та методів противника дозволяє ефективніше протидіяти кібератакам. Окрім технічних аспектів, важливу роль відіграє підготовка фахівців до роботи під тиском та в умовах обмежених часових ресурсів, що є характерним для воєнного стану.

Змінюються і методи навчання. Все більшу роль відіграють онлайн-курси та дистанційне навчання, яке дозволяє спеціалістам продовжувати освіту незалежно від їхнього місцезнаходження. Це особливо важливо в умовах війни, коли доступ до традиційних освітніх закладів може бути обмеженим. Однак, незважаючи на переваги дистанційного навчання, важливо забезпечити високий рівень інтерактивності та можливість для студентів здобувати практичний досвід.

Важливу роль у підготовці фахівців з кібербезпеки в умовах війни відіграє міжнародне співробітництво [2].

Обмін знаннями, досвідом та навичками між країнами та організаціями дозволяє формувати глобальну систему кібербезпеки, здатну ефективно протистояти масштабним кіберзагрозам. Це також сприяє стандартизації підходів до кібербезпеки та розвитку єдиних навчальних програм, які будуть актуальні на міжнародному рівні.

Підготовка фахівців з кібербезпеки в умовах війни вимагає комплексного підходу, який включає розвиток технічних навичок, психологічну стійкість, здатність працювати в команді під тиском, а також глобальну співпрацю та обмін знаннями. Це дозволить створити нове покоління фахівців, здатних ефективно захищати кіберпростір в найскладніших умовах.

Особливу увагу слід звернути на важливість інновацій та технологічного прогресу у сфері кібербезпеки. Військові конфлікти акцентують необхідність впровадження передових технологій для захисту інформаційних систем та мереж. Це означає, що програми підготовки мають інтегрувати найновіші розробки у галузі штучного інтелекту, машинного навчання та квантових технологій, щоб підготувати фахівців, які можуть ефективно протистояти не лише сучасним, але й майбутнім кіберзагрозам. Інноваційний підхід передбачає не лише засвоєння новітніх технологій, але й розвиток критичного мислення, здатності до швидкого аналізу та адаптації стратегій захисту в змінних умовах.

Також важливим аспектом є психологічна підготовка фахівців, що передбачає формування вмінь ефективно працювати під високим рівнем стресу, розвиток лідерських якостей та вміння приймати швидкі та обґрунтовані рішення. В умовах війни, коли на кону стоять людські життя та безпека держави, ці навички стануть вирішальними.

Заохочення до неперервного самовдосконалення та навчання є ще однією критичною складовою. Сфера кібербезпеки швидко розвивається, і фахівці повинні бути готові до постійного оновлення своїх знань та навичок, щоб відповідати зростаючим викликам. Це вимагає від освітніх програм включення модулів з самоосвіти та методик ефективного навчання, які допоможуть спеціалістам з кібербезпеки залишатися на передовій боротьби з кіберзлочинністю.

На міжнародному рівні, співпраця у сфері кібербезпеки має включати не лише обмін інформацією про загрози та вразливості, але й спільну розробку стандартів та практик захисту. Така співпраця сприяє створенню єдиної глобальної системи кіберзахисту, здатної ефективно протистояти міжнародному кібертероризму та еспіонажу.

Підготовка фахівців з кібербезпеки в умовах війни вимагає глобального погляду на проблему, інтеграції технічних, психологічних та міжнародних аспектів, а також підтримки інновацій та технологічного прогресу. Тільки такий комплексний підхід забезпечить формування ефективної глобальної системи кібербезпеки, здатної протистояти викликам сучасності та майбутнього.

Основні ключові аспекти підготовки фахівців з кібербезпеки в умовах війни:

1. Розуміння контексту війни – фахівці з кібербезпеки повинні ретельно аналізувати та розуміти контекст військових дій, включаючи мету, стратегії та тактику сторін конфлікту.
2. Постійна підготовка до нових загроз – військові конфлікти швидко змінюються, і фахівці з кібербезпеки повинні бути завжди готові до нових типів кібератак і методів оборони.
3. Спеціальні навички та знання – підготовка фахівців з кібербезпеки включає в себе здобуття спеціалізованих навичок і знань, таких як аналіз шкідливих програм, виявлення інтранет-зловмисників, криптографія тощо.
4. Ефективність реагування на інциденти – фахівці повинні бути готові швидко реагувати на кібератаки та вживати заходів для мінімізації шкоди.
5. Співпраця з іншими військовими відділами – фахівці з кібербезпеки повинні співпрацювати з іншими військовими відділами, включаючи розвідку, зв'язок та військові команди, для ефективного захисту військових мереж та систем.
6. Розвиток симуляцій та тренувань – важливо проводити симуляції кібератак та тренування для підвищення навичок фахівців і вдосконалення захисту військових систем.
7. Забезпечення безпеки інформації – фахівці повинні бути в змозі забезпечувати конфіденційність, цілісність і доступність важливої інформації в умовах активних кібератак [3].

Ці аспекти підкреслюють важливість спеціалізованої підготовки та спроможностей фахівців з кібербезпеки в умовах війни для ефективного захисту військових мереж і систем від кіберзагроз.

Підготовка фахівців з кібербезпеки в умовах війни вимагає глибокого розуміння воєнного контексту, оскільки це дозволяє адаптувати стратегії та тактики оборони до змінюваних загроз. Спеціалізовані навички та знання, як-от аналіз шкідливих програм та криптографія, стають фундаментальними для розробки ефективних методів протидії кібератакам.

Важливу роль відіграє швидке та ефективне реагування на інциденти, що вимагає від фахівців здатності до оперативного аналізу ситуації та прийняття рішень. Співпраця з іншими військовими підрозділами є ключовою для створення об'єднаної системи оборони, де кожен елемент взаємодіє для забезпечення цілісного захисту. Розвиток симуляцій та тренувань допомагає вдосконалити навички фахівців і підвищити готовність до неочікуваних загроз. Окрім того, забезпечення безпеки інформації є критичним аспектом, що включає захист конфіденційності, цілісності та доступності даних. В цілому, підготовка фахівців з кібербезпеки у воєнний час вимагає комплексного підходу, який поєднує технічні знання, оперативну гнучкість та міжвідомчу координацію для забезпечення надійного захисту від кіберзагроз.

Список використаних джерел

1. Гелешко І., Ящук В. Сучасні тенденції використання інформаційних технологій при підготовці фахівців з кібербезпеки. *Інформаційна безпека та інформаційні технології* : матеріали зб. тез доп. IV Міжнар. наук.-практ. конф. (м. Львів, 30 листоп. 2022 р.). Львів, 2022. С. 339–341.

2. Арсенович Л. А. Організація професійної підготовки фахівців із кібербезпеки основними суб'єктами національної системи кібербезпеки: практичний аспект. *Ефективність державного управління*. 2021. Вип. 1, № 62 (1). С. 91–102.

3. Трушкіна Н. В. Трансформація системи підготовки кадрів та підвищення професійної компетентності фахівців у сфері кібербезпеки в умовах війни. *Формування іміджу закладу освіти на основі сучасних комунікаційних технологій* : матеріали всеукр. наук.-пед. підвищ. кваліфікації з екон. наук, 27 берез. – 7 трав. 2023 р. Львів ; Торунь, 2023. С. 197–201.

Ключові слова: кібербезпека, війна, фахівці, інновації, безпека інформації.
Keywords: cybersecurity, war, specialists, innovations, information security.