Науково-дослідна частина
Національного університету
кораблебудування
імені адмірала Макарова

54025, м. Миколаїв,
пр. Героїв України, 9
Тел.: (0512) 70-91-04
http://conference.nuos.edu.ua
e-mail: conference@nuos.edu.ua

Навчально-науковий інститут
автоматики та електротехніки
Національного університету
кораблебудування
імені адмірала Макарова

54021, м. Миколаїв,
пр. Центральний, 3
Тел.: (0512) 47-70-95
http://iae.nuos.edu.ua
e-mail: university@nuos.edu.ua

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ
імені адмірала Макарова

НАУКОВО-ТЕХНІЧНІ КОНФЕРЕНЦІЇ
Національний університет кораблебудування
імені адмірала Макарова

# СУЧАСНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ТРАНСПОРТІ

# МАТЕРІАЛИ

## X ВСЕУКРАЇНСЬКОЇ НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ З МІЖНАРОДНОЮ УЧАСТЮ

13-14 грудня 2022 р.

Миколаїв ■ НУК ■ 2022

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ
імені адмірала Макарова

# СУЧАСНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ТРАНСПОРТІ

## СПІБТ–2022

# МАТЕРІАЛИ

## X Всеукраїнської науково-технічної конференції з міжнародною участю

13–14 грудня 2022 року

*Національний університет кораблебудування*
*імені адмірала Макарова*
*Навчально-науковий інститут автоматики та електротехніки*
*просп. Центральний, 3, м. Миколаїв*


МИКОЛАЇВ • НУК • 2022

УДК 004
У 45

**ОРГАНІЗАТОРИ**:

1. Міністерство освіти і науки України
2. Національний університет кораблебудування імені адмірала Макарова
3. ТОВ «БЕЗПЕКАІНФОСЕРВІС»
4. Науково-технічний центр «Квант»



**Відповідальна за випуск** В. В. Трибулькевич

У–45 **Сучасні** проблеми інформаційної безпеки на транспорті: матеріали X Всеукраїнської науково-технічної конференції з міжнародною участю. – Миколаїв : НУК, 2022. – 209 с.

У збірнику подано матеріали X Всеукраїнської НТК "Сучасні проблеми інформаційної безпеки на транспорті".

Розглянуті питання теорії та практики систем інформаційної безпеки транспортних засобів і систем, захисту інформації в каналах зв'язку та глобальних мережах передачі даних, захисту інформації на об'єктах інформаційної діяльності та в інформаційно-телекомунікаційних системах, моделювання об'єктів і процесів технічного захисту інформації, а також питання підготовки кадрів у галузі знань «Інформаційна безпека».

Збірник може бути корисним для наукових співробітників, викладачів, інженерів та студентів.

**УДК 004**

4. Війна в соцмережах: як працюють ботоферми на мільйон акаунтів та який вплив мають. URL: https://www.google.com/amp/s/tsn.ua/amp/exclusive/viyna-v-socmerezhah-yak-pracyuyut-botofermi-na-milyon-akauntiv-ta-yakiy-vpliv-mayut-2147434.html
5. Білий список: 10 медіа, що стали найякіснішими URL : https://imi.org.ua/monitorings/bilyj-spysok-10-media-shho-staly-najyakisnishymy-i41541
6. Що таке ІПСО, чому важливо це знати і які операції зараз проводить Росія проти України. URL : https://tyzhden.ua/News/254439
7. Як рашистські ІПСО ховаються за українською символікою в українському Facebook. URL:https://armyinform.com.ua/2022/08/03/yak-rashystski-ipso-hovayutsya-za-ukrayinskoyu-symvolikoyu-v-ukrayinskomu-facebook/
8. Що таке інформаційно-психологічні операції і як їх розпізнати URL : https://ms.detector.media/manipulyatsii/post/29009/2022-02-23-shcho-take-informatsiyno-psykhologichni-operatsii-i-yak-ikh-rozpiznaty/

**УДК 004.056.5;057.2**

## ПРОБЛЕМИ ПІДГОТОВКИ ФАХІВЦІВ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ВОЄННОГО СТАНУ

***Автори:*** *Турти М.В., к.т.н., доцент; Баронова О.А., ст. викладач, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

План реалізації Стратегії кібербезпеки України [1], затверджений в лютому 2022 року до початку воєнних дій на території України, передбачає досягнення в найближчі роки ряда цілей, частина з яких безпосередньо пов’язана із підготовкою фахівців з інформаційної безпеки (ІБ). В умовах військової агресії підготовка захисників кіберпростору набуває особливого значення.

Метою даної роботи є визначеня пріоритетних напрямів і форм підготовки фахівців з інформаційної безпеки в умовах воєнного стану. Для досягнення поставленої мети необхідно провести аналіз актуальної нормативно-правової бази і визначити актуальні напрямки підго-

товки фахівців з ІБ за нормативними вимогами, визначити методики викладання, доцільні для застосування в умовах воєнного стану.

Ціль С.1 «Дієва кібероборона» згідно [1] передбачає, що «Україна створить та забезпечить розвиток (у тому числі кадрово та технологічно) підрозділів із повноваженнями ведення збройного протиборства в кіберпросторі, …забезпечить ефективну взаємодію основних суб'єктів національної системи кібербезпеки та сил оборони під час проведення заходів з кібероборони, належне навчання та фінансове забезпечення таких структур, систематичне проведення кібернавчань, оцінку спроможностей та ефективності підрозділів, розроблення та імплементацію індикаторів оцінки їх діяльності». Зокрема передбачається:

1) проведення навчань у сфері кібербезпеки у системі військово-патріотичного виховання та системі територіальної оборони, проведення спільних навчань з підрозділами держав-членів НАТО;

2) запровадження практичних навчань;

3) розробка і впровадження механізмів комунікації між державою та суспільством щодо стримування деструктивної діяльності в кіберпросторі:

– збирання кіберстатистики і щорічне її оприлюднення на офіційних сайтах;

– проведення щорічних соціологічних досліджень спектру загроз у кіберпросторі України та ефективності протидії цим загрозам державних органів;

– проведення «загальнонаціональної інформаційної роз'яснювальної кампанії щодо дій громадян у випадку, коли вони стикаються із кібершахрайством та іншими кіберзлочинами, а також роз'яснення процедур звернення до правоохоронних органів» [1];

– залучення приватного сектору, громадських організацій, наукової спільноти до здійснення заходів протидії загрозам у кіберпросторі;

4) поліпшення матеріально-технічного забезпечення галузі;

5) інтенсифікація наукових досліджень і розробок у галузі кібербезпеки з урахуванням тенденцій розвитку інформаційно-комунікаційних технологій на основі довгострокових програм та програми державної підтримки стратегічно важливих наукових установ та організацій;

6) «створення вітчизняних систем, платформ і продуктів у сфері кібербезпеки» [1];

7) забезпечення в державному секторі матеріального стимулювання фахівців з кібербезпеки «з урахуванням рівнів оплати праці таких фахівців у приватному секторі» [1];

8) підвищення рівня знань з кібербезпеки:

– громадськості шляхом розробки і впровадження Загальнонаціональної програми кіберграмотності,

– здобувачів освіти шляхом включення питань щодо кіберграмотності і кібергігієни до навчальних програм загальної середньої, професійно-технічної та вищої освіти.

– фахівців у сфері кібербезпеки у формі періодичного підвищення кваліфікації, в тому числі залучення «суб'єктів національної системи кібербезпеки до міжнародних програм навчання і підвищення кваліфікації персоналу» [1];

– фахівців, які займаються дослідженнями електронних доказів та безпечності апаратних і програмних засобів;

9) розвиток мережі центрів, що виконуватимуть наступні функції:

– реагування на кібератаки та кіберінциденти;

– акумуляція і оперативне розповсюдження вітчизняних і міжнародних нормативно-правових документів в галузі кібербезпеки, зокрема, регламентів і директив Європейського парламенту та Ради ЄС, галузевих нормативних документів, законів і підзаконних актів України, нормативних документів з технічного захисту інформації;

– узагальнення та обмін досвідом у сфері кібербезпеки;

– підтримка інновацій та вітчизняних розробок у сфері кібербезпеки.

– організація періодичного підвищення кваліфікації фахівців у сфері кібербезпеки;

10) створення національної системи управління інцидентами.

Таким чином, ще в мирний час була визначена необхідність модернізації системи управління інформаційною безпекою України і розроблена відповідна система заходів, до яких входить проведення докорінної реформи системи підготовки та підвищення кваліфікації фахівців у сфері кібербезпеки. Перші кроки у напрямі реалізації цієї реформи були зроблені протягом 2021-2022 року з метою забезпечення відповідності стандартам ЄС і США, впровадження в освітній процес

найкращих світових практик, досвіду Стратегічної освітньої ініціативи у сфері кібербезпеки США та досвіду розробки і впровадження Європейської рамки кваліфікації.

Тривалий час у Класифікаторі професій були лише дві професії, що безпосередньо стосувалися кібербезпеки і відповідали освітньо-кваліфікаційним рівням «бакалавр» і «магістр» - фахівець та професіонал із організації захисту інформації. 25 жовтня 2021 року у Класифікатор професій за поданням Держспецзвязку було внесено 17 нових професій, серед яких «Фахівець з технічного захисту інформації», «Аналітик загроз безпеки», «Дізнавач сфери кібербезпеки та захисту інформації» та ін. [2]. Для кожної професії мали бути сформульовані кваліфікаційні вимоги і розроблені стандарти. За цими стандартами в кваліфікаційних центрах випускники закладів вищої освіти повинні складати професійні іспити щоб здобути кваліфікацію за конкретним напрямом.

У 2022 році були розроблені, пройшли публічне обговорення та експертизу перші шість професійних стандартів для професій «Адміністратор мереж і систем», «Аналітик з безпеки інформаційно-телекомунікаційних систем», «Інструктор-методист з інформаційної безпеки та кібербезпеки», «Розробник систем захисту інформації», «Фахівець з питань безпеки» та «Фахівець сфери захисту інформації» [3].

Планується [3], що у 2023 році будуть розроблені стандарти для 14 професій, кількість професій у сфері кібер- та інформаційної безпеки буде збільшена до 20, і відкриються перші незалежні кваліфікаційні центри.

В рамках реформи підготовки фахівців у сфері кібербезпеки і в умовах воєнного стану можна вважати дцільною трансформацію освітнього процесу за спеціальністю 125 «Кібербезпека» на наступних засадах:

1. Розширення спектру освітньо-професійних програм у вищих навчальних закладах з метою підготовки вузькоспеціалізованих фахівців згідно новим професіям у Класифікаторі професій.

2. Використання регіональних центрів як баз практик студентів вищих навчальних закладів.

3. Динамічна модифікація робочих програм дисциплін і (за необхідності) навчальних планів) за результатами оприлюднених результатів моніторингу стану кіберпростору України.

4. Підсилення практичної складової освітнього процесу:

– використання на практичних і лабораторних заняттях реальних прикладів застосування новітніх практик рішення задач кіберзахисту за матеріалами регіональних центрів;

– залучення здобувачів освіти за спеціальністю 125 «Кібербезпека» до вирішення практичних завдань Плану реалізації Стратегії кібербезпеки України: збирання кіберстатистики, проведення соціологічних досліджень, участь у заходах протидії загрозам у кіберпросторі, участь у загальнонаціональній інформаційній роз'яснювальній кампанії та створенні апаратних і програмних засобів захисту в рамках студентської наукової роботи, курсових і дипломних проектів, виробничої практики та наукового стажування;

– залучення здобувачів освіти за спеціальністю 125 «Кібербезпека» до наукових досліджень і розробок у галузі кібербезпеки, що проводяться випусковою кафедрою або іншими організаціями (з відома кафедри), відповідно до наявних у студентів форм допуску.

5. Раціональне використання наукового потенціалу вищих навчальних закладів:

– формування переліків пріоритетних напрямів наукових досліджень в галузі кібербезпеки, які фінансуються Держбюджетом і приватним сектором;

– формування переліків пропозицій щодо напрямів наукових досліджень від науковців;

– розробка механізму створення тимчасових творчих колективів з вітчизняних та закордонних науковців і практиків, що є співробітниками організацій різного підпорядкування;

– скорочення витрат часу науковців навчальних закладів на документаційне забезпечення навчального процесу за рахунок використання електронних бібліотечних фондів регіональних центрів, до яких пропонується включити без порушення авторського права електронні конспекти лекцій, методичні вказівки до лабораторних і практичних робіт тощо.

Реалізація запланованих заходів з реформування освіти в галузі кібербезпеки під час воєнного стану ускладнюється ресурсними об-

меженнями. Крім того, дистанційне навчання під час відсутності гарантованого електроживлення і зв'язку вимагає застосування гнучких методів навчання і оцінювання знань студентів:

– відсутність можливості проведення занять в спеціалізованих лабораторіях частково може бути скомпенсована застосуванням файлів зображень і відеороликів, які знаходяться у вільному доступі або можуть бути створені викладачем;

– джерела інформації з дисциплін мають бути надані студентам у формі електронних документів, що дозволяє скоротити час пошуку, наприклад нормативних документів, за посиланнями в мережі і зменшити залежність студента від наявності Інтернет-зв'язку;

– завдання до лабораторних і практичних робіт, модульні контрольні роботи доцільно формувати за варіантами, кількість яких дорівнює кількості студентів, що дозволяє оцінити работу без процедури захисту;

– усі методичні матеріали, підручники, нормативні документи мають бути сформовані у вигляді кейсу, який розташовується наприклад на Google-диску і протягом семестру в ідеалі не коригується;

– втрачається значимість присутності студента на заняттях, активності студентів на заняттях і дотримання термінів виконання робіт протягом семестру внаслідок унеможливлення об'єктивної оцінки умов, в яких знаходяться студенти, особливо здобувачі освіти, що перебувають на тимчасово окупованих територіях;

– студенти повинні отримувати протягом семестру інформацію про набрані ними бали за всіма формами контролю і причини зниження балів за окремі види робіт, наприклад у вигляді таблиць на Google-диску, що, по-перше, стимулює конкурентну діяльність студентів, а по-друге – дозволяє оперативно виявити загублені при передачі чи не зараховані з якоїсь причини роботи;

– змінюються вимоги щодо форматів представлення робіт: в разі відсутності у студента можливостей створювати документи в текстовому редакторі робота може бути представлена як набір фотографій рукописного тексту (за виключенням кваліфікаційних робіт);

– зростає значення індивідуального підходу до студентів, створення атмосфери дружньої підтримки і взаєморозуміння;

– навчальний процес виходить за стандартні рамки відповідальності викладача за вчасність і якість проведення занять, а стає резуль-

татом спільної роботи колективу кафедра-викладач-студенти, який (в разі необхідності) призначає і узгоджує час проведення додаткових занять у формі консультацій, їх тематику;

– зростає значимість планування навчання на наступних курсах, на наступних освітніх рівнях, участі в науковій роботі, що настроює студентів на отримання невеликих але позитивних результатів у недалекому майбутньому, тобто сприяє створенню психологічного комфорту.

**Висновки**

В даній роботі проведено аналіз нормативно-правової бази, визначені актуальні напрямки підготовки фахівців з ІБ та методики викладання, доцільні для застосування в умовах воєнного стану.

**Список літератури:**

1. План реалізації Стратегії кібербезпеки України. URL: https://zakon.rada.gov.ua/laws/show/n0087525-21#Text

2. Олександр Потій: до класифікатора внесено 17 додаткових професій у галузі безпеки інформації та кіберзахисту. URL: https://cip.gov.ua/ua/news/oleksandr-potii-do-klasifikatora-vneseno-17-dodatkovikh-profesii-u-galuzi-bezpeki-informaciyi-ta-kiberzakhistu

3. Реформування системи підготовки професійних кадрів у сфері кібербезпеки в Україні: затверджені перші шість професійних стандартів. URL: https://cip.gov.ua/ua/news/reformuvannya-sistemi-pidgotovki-profesiinikh-kadriv-u-sferi-kiberbezpeki-v-ukrayini-zatverdzheni-pershi-shist-profesiinikh-standartiv

## ЗМІСТ

*Наукове видання*

# СУЧАСНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ТРАНСПОРТІ

## СПІБТ–2022

X Всеукраїнська науково-технічна конференція
з міжнародною участю

**13–14 грудня 2022 року**

*Національний університет кораблебудування*
*імені адмірала Макарова*
*Навчально-науковий інститут автоматики та електротехніки*
*просп. Центральний, 3, м. Миколаїв*

## МАТЕРІАЛИ КОНФЕРЕНЦІЇ

(*українською мовою*)

Відповідальна за випуск В. В. Трибулькевич