МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАДИМА ГЕТЬМАНА

Факультет економіки та управління

Кафедра національної економіки та публічного управління

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

Цифрове врядування

Галузь знань 28 Публічне управління та адміністрування

Спеціальність 281 Публічне управління та адміністрування

Форма навчання: заочна

КВАЛІФІКАЦІЙНА МАГІСТЕРСЬКА РОБОТА

на тему **«Цифрові інструменти кіберзахисту у сфері публічного управління»**

здобувача Тодорюка Олександра Дмитровича

(підпис)

Науковий керівник: **кандидат технічних наук**
Шпига Петро Семенович

(підпис)

Робота допущена до захисту перед екзаменаційною комісією з атестації здобувачів вищої освіти (ЕК)

Завідувач кафедри:
доктор наук з державного управління, професор, Карпенко О.В.

(підпис)

Київ 2023

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАДИМА ГЕТЬМАНА

Факультет економіки та управління

Кафедра національної економіки та публічного управління

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

Цифрове врядування

Галузь знань 28 Публічне управління та адміністрування

Спеціальність 281 Публічне управління та адміністрування

ПОГОДЖЕНО
Керівник проєктної групи (гарант)
освітньо-професійної програми

О. В. Карпенко
(підпис)

_____2023 р.

ЗАТВЕРДЖУЮ
Завідувач кафедри

О. В. Карпенко
(підпис)

_____2023 р.

ІНДИВІДУАЛЬНЕ ЗАВДАННЯ

здобувачу вищої освіти Тодорюку Олександру Дмитровичу
заочної форми навчання

на підготовку кваліфікаційної магістерської роботи

на тему **«Цифрові інструменти кіберзахисту у сфері публічного управління»**

Тему затверджено наказом ректора Університету від «23» жовтня 2023р .№ 1960ст

Кваліфікаційна магістерська робота виконується на матеріалах Міністерства цифрової трансформації України, Служби безпеки України.

План кваліфікаційної магістерської роботи

Розділ 1	Інформаційна безпека як компонент національної безпеки України.
Розділ 2	Побудова процесу підготовки фахівців у сфері захисту інформації.
Розділ 3	Аналіз стану цифрових систем кіберзахисту та підготовки кадрів з цифрової безпеки в Україні.
Об'єкт дослідження:	Особливості та ефективність застосування цифрових інструментів кіберзахисту в системах публічного управління.
Предмет дослідження:	Цифрові інструменти кіберзахисту у сфері публічного управління.
Мета кваліфікаційної магістерської роботи:	Аналіз ефективності використання цифрових інструментів кіберзахисту у сфері публічного управління, визначення вимог до фахівців у цій галузі та виокремлення ключових аспектів цифрових інструментів захисту інформації для вироблення пропозицій щодо їх удосконалення.

Конкретні завдання, які здобувач повинен виконати для досягнення поставленої мети:

1. Визначити організаційно-правові засади формування державної політики у сфері інформаційної безпеки та кіберзахисту.
2. Провести аналіз цифрових інструментів, що використовуються для протидії кіберзагрозам та забезпечення нормальної функціонування систем управління.
3. Розглянути актуальні вимоги до фахівців у сфері кіберзахисту з урахуванням специфіки публічного управління та сучасних викликів у кіберпросторі.
4. Виокремити важливі аспекти стратегії і тактики використання цифрових інструментів кіберзахисту у сфері публічного управління.
5. Запропонувати шляхи вдосконалення цифрових інструментів кіберзахисту у сфері публічного управління.

Завдання підготував науковий керівник _____ П. С. Шпига
(підпис)

«_____»_____2023р.

Завдання одержав здобувач _____ О.Д. Тодорюк
(підпис)

«_____»_____2023р.

Реферат

Кваліфікаційна магістерська робота містить 74 сторінок, 1 таблицю, список використаних джерел із 86 найменувань.

«Цифрові інструменти кіберзахисту у сфері публічного управління»

Об'єктом дослідження кваліфікаційної магістерської роботи є особливості та ефективність застосування цифрових інструментів кіберзахисту в системах публічного управління.

Предметом дослідження є цифрові інструменти кіберзахисту у сфері публічного управління.

Мета і завдання дослідження. Метою дослідження є аналіз ефективності використання цифрових інструментів кіберзахисту у сфері публічного управління, визначення вимог до фахівців у цій галузі та виокремлення ключових аспектів цифрових інструментів захисту інформації для вироблення пропозицій щодо їх удосконалення.

Відповідно до поставленої мети визначені такі *завдання*:

1. Визначити організаційно-правові засади формування державної політики у сфері інформаційної безпеки та кіберзахисту.
2. Провести аналіз цифрових інструментів, що використовуються для протидії кіберзагрозам та забезпечення нормальної функціонування систем управління.
3. Розглянути актуальні вимоги до фахівців у сфері кіберзахисту з урахуванням специфіки публічного управління та сучасних викликів у кіберпросторі.
4. Виокремити важливі аспекти стратегії і тактики використання цифрових інструментів кіберзахисту у сфері публічного управління.
5. Запропонувати шляхи вдосконалення цифрових інструментів кіберзахисту у сфері публічного управління.

Теоретична, методична та практична значущість отриманих результатів. Під час дослідження було проведено глибокий аналіз організаційно-правових та технічних аспектів формування державної політики з інформаційної безпеки та кіберзахисту, а також ґрунтовно вивчено питання підготовки фахівців у цій галузі.

Практичні результати дослідження полягають у конкретних рекомендаціях щодо вдосконалення цифрового інструментарію кіберзахисту в Україні та підвищення ефективності підготовки кадрів у цій сфері. Зокрема, робота виявила проблеми у відсутності необхідної інфраструктури, невиваженості державної політики та використанні іноземних засобів обчислювальної техніки, що призводить до втрат потенціалу для розвитку національних галузей.

Рік виконання кваліфікаційної магістерської роботи – 2023. Рік захисту роботи – 2023.

Ключові слова: «технічний захист інформації», «інформаційна безпека», «підготовка кадрів», «нормативно-правова база», «комп'ютер»

В і д г у к

про кваліфікаційну магістерську роботу
здобувача факультету економіки та управління
освітньо-професійної програми
«Цифрове врядування»
Тодорюка О.Д
на тему **«Цифрові інструменти кіберзахисту у сфері публічного управління»**

1. **Актуальність теми:** Актуальність дослідження обумовлена проблемами в галузі кіберзахисту інформації у сфері публічного управління. Дослідження спрямоване на вирішення конкретних викликів, таких як невиваженість державної політики та відсутність необхідної інфраструктури, що призводить до недостатньо обґрунтованих заходів у плануванні ініціатив з інформатизації та кіберзахисту. Актуальність дослідження підкреслюється необхідністю вдосконалення процесів підготовки фахівців та використання національних ресурсів для забезпечення інформаційної безпеки в умовах зростаючих викликів кіберзагроз.
2. **Позитивні риси кваліфікаційної магістерської роботи:** Проведено глибокий аналіз організаційно-правових аспектів сфери кіберзахисту, ґрунтовно досліджено освітні практики у сфері безпеки інформації в розвинених країнах, а також надано конкретні рекомендації для поліпшення кадрової політики у цій сфері.
3. **Наявність самостійних розробок автора:** Автор вдало розкриває актуальні проблеми інформаційної безпеки, вказує на ризики та пропонує конкретні заходи для їх вирішення. Глибокий аналіз цифрових систем кіберзахисту в Україні та практичні рекомендації виходять за межі теоретичних викладок. Авторський погляд на проблематику та самостійні дослідження відзначаються високою науковою цінністю.
4. **Цінність теоретичних висновків та практичних рекомендацій:** Здійснено якісне наукове обґрунтування теоретичних засад інформаційної безпеки та кіберзахисту, враховано організаційно-правові аспекти державної політики. Розроблено конкретні рекомендації щодо вдосконалення цифрових систем кіберзахисту в Україні. Практичний внесок у розвиток галузі підтверджено об'єктивним аналізом сучасних викликів та необхідності прискорення реформ в інформаційній сфері.
5. **Наявність недоліків:** робота містить деякі стилістичні неточності, окрім того певного бібліографічного доопрацювання потребує й список використаних джерел.
6. **Загальна оцінка кваліфікаційної магістерської роботи та її допущення до захисту перед ЕК:** Дослідження виконано самостійно, якісно та вчасно, з дотриманням установлених вимог. Зміст роботи відповідає індивідуальному плану. Широкий діапазон актуальних питань, елементи наукової новизни і практична цінність дослідження дозволяють зробити висновок, що магістерська робота Тодорюка Олександра Дмитровича на тему «Цифрові інструменти кіберзахисту у сфері публічного управління» виконана на достатньому науково-теоретичному рівні та відповідає кваліфікації «Магістр» за спеціальністю 281 «Публічне управління та адміністрування», а її автор заслуговує на високу оцінку.

Науковий керівник: кандидат технічних наук

«____» _____ 2023 р. **_____ Петро Шпига**
(підпис)

Рецензія

на кваліфікаційну магістерську роботу здобувача вищої освіти
Тодорюка Олександра Дмитровича
на тему *«Цифрові інструменти кіберзахисту у сфері публічного управління»*

Актуальність теми кваліфікаційної магістерської роботи і доцільність її розроблення обумовлені проблематикою захисту від кіберзагроз у сфері публічного управління. Основне завдання, яке ставить перед собою автор, полягає в розв'язанні конкретних викликів, таких як невиваженість стратегій державної політики та відсутність належної інфраструктури, що призводить до непослідовних заходів у плануванні і впровадженні ініціатив з інформатизації та кіберзахисту. Важливість цього дослідження підкреслюється необхідністю виведення на новий рівень процесу навчання фахівців та використання національних ресурсів для забезпечення інформаційної безпеки в умовах зростаючих кіберзагроз.

Якість проведеного дослідження. Дослідження, виконане автором, відповідає основним напрямам наукових досліджень кафедри національної економіки та публічного управління. Автор застосував здобуті під час навчання теоретичні й практичні знання, вміння та навички в галузі публічного управління та адміністрування для вирішення конкретних практичних завдань.

Позитивні риси кваліфікаційної магістерської роботи виявлені у використанні різноманітних підходів та методів наукового дослідження для вирішення поставлених завдань. Автор використав системний комплекс загальнонаукових і спеціальних підходів та методів, враховуючи сучасні теоретичні підходи, що базуються на філософії діалектичного розвитку національних цінностей. Вивчення стану досліджуваної проблеми здійснено за допомогою методів, що використовують принципи наукового мислення, такі як індукція й дедукція, аналіз і синтез, порівняння та спостереження.

Зауваження. робота містить деякі стилістичні неточності, окрім того певного бібліографічного доопрацювання потребує й список використаних джерел.

Магістерська робота *Тодорюка Олександра Дмитровича* на тему *«Цифрові інструменти кіберзахисту у сфері публічного управління»* відповідає вимогам, які висуваються до дипломних робіт на здобуття кваліфікації магістра за спеціальністю 281 «Публічне управління та адміністрування», може бути допущена до захисту перед ЕК та заслуговує на оцінку «відмінно».

Рецензент:
державний експерт експертної групи
формування Національної програми
інформатизації директорату розвитку
Національної програми інформатизації
Міністерства цифрової трансформації України
кандидат наук з державного управління Сергій ГОРБЛЮК

підпис Горблюка С. засвідчую
Начальник управління О. Маленко

ЗМІСТ

ВСТУП

Актуальність теми. Впродовж всієї своєї історії людство прагнуло оволодіти матерією, енергією й інформацією. Цілі епохи в розвитку людства одержували назву на ім'я найбільш передової технології цієї епохи. Так “кам'яний вік” – це епоха технології обробки каменя для отримання знарядь праці, “бронзовий ” – епоха оволодіння технологією обробки металу, – епоха оволодіння новими методами інформації. Ще 30-50 років тому говорили, що наступило “атомне століття”, зараз все частіше можна чути про “століття інформації”. Більш того, вважається, що сьогодні світ переживає інформаційний бум. Інформація найважливішим чинником стійкого розвитку будь-якого об'єкту. З іншого боку, на рубежі XX століття людство зіткнулося з проблемою виживання, продиктованою деформацією навколишнього середовища, людської свідомості і суспільних відносин. Усе це з особливою гостротою вимагає забезпечення безпеки виробничо-технічних і соціально-економічних систем, що формуються людиною.

Актуальність даної теми визначається важливістю завдання яке стоїть перед державою у сфері захисту інформації як компоненту національної системи безпеки.

Водночас слід відзначити, що не виваженість державної політики та відсутність необхідної інфраструктури в інформаційній сфері іноді призводять до недостатньо обґрунтованих заходів у плануванні та реалізації ініціатив з інформатизації, створення та управління автоматизованими інформаційними системами. Значущі зміни, які відбулися в політичному та економічному житті країни після набуття суверенітету, вимагають переосмислення ролі та функцій держави в інформаційній сфері. Практика обмежень кордонів та жорсткої цензури вже належить минулому, і держава, що декларує свою орієнтацію на ринкові відносини та свідомо уникає використання адміністративного

впливу на процеси формування інформаційного простору, виявляється не готовою до конкуренції з різноманітністю вітчизняних та закордонних суб'єктів інформаційної діяльності.

Нерозвиненість інфраструктури інформаційної сфери змушує Україну створювати та реалізовувати національні концепції та програми інформатизації, спираючись на досягнення розвинених країн. Використання широкої кількості відносно доступних та якісних засобів обчислювальної техніки іноземного виробництва призводить до втрати можливостей країни для розвитку відповідних національних галузей науки та виробництва. Це, в свою чергу, може призвести до стратегічної залежності ключових сфер суспільної діяльності від іноземних технологій, які не контролюються державою.

Недоліки в інфраструктурі інформаційної діяльності найяскравіше виявляються у недостатній інформаційній підтримці процесів державного управління та координації. Майже не використовуються можливості створення міжвідомчих довідково-інформаційних систем, а роботи зі створення національних реєстрів, державної паспортної системи та інших проектів рухаються повільно. Існуючі технології обробки інформації не відповідають потребам сучасності за характеристиками та рівнем технічного забезпечення. У період економічної кризи наукова діяльність у галузі інформатизації фактично припинена, і науковий та інженерно-технічний потенціал країни розподіляється на інші галузі та за кордон.

Розвиток телекомунікаційних систем та їх використання для забезпечення мережевих інформаційних технологій породив нові явища та закономірності в інформаційній сфері. Змога отримувати дистанційний доступ до глобальних ресурсів комп'ютерних мереж, вражаюче збільшення швидкості та обсягів обробки інформації, впровадження телекомунікацій в особисті потреби людей формують нові соціальні відносини. Існування інформаційних ресурсів і широкі можливості їх використання, а також обмеженість трудових, сировинних та

енергетичних ресурсів розвинених країн призводять до того, що інформація стає стратегічним ресурсом. У цих умовах систему захисту інформації можна вважати основною складовою частиною забезпечення інформаційної безпеки суспільства, без якої неможлива реалізація будь-якої форми інформаційної діяльності. Отже, не вирішивши проблеми захисту інформації на рівні, відповідному економічно розвиненим країнам, Україна не зможе стати повноправним учасником світової спільноти.

Аналіз останніх досліджень і публікацій. При викладенні матеріалу використовувались праці зарубіжних та вітчизняних вчених таких як: Маслянко П.П., Ліссов П.М., Марутян Р.Р., Кунанець Н., Липак Г., Биков В.Ю., Пунченко О.П., Лазаревич А.А., Кравченко М.С, Кєтриш О.С., Гладиш С.В., Росс А., Палаева Л.В., Хафизов А.М., Гилязетдинова А.М., Вахитова А.Р., Давыдова К.Н., Сиротина Е.Р.

Мета і завдання дослідження. Метою цієї роботи є аналіз ефективності використання цифрових інструментів кіберзахисту у сфері публічного управління, визначення вимог до фахівців у цій галузі та виокремлення ключових аспектів цифрових інструментів захисту інформації для вироблення пропозицій щодо їх удосконалення.

Для досягнення цієї мети були поставлені такі *завдання*:

– визначити організаційно-правові засади формування державної політики у сфері інформаційної безпеки та кіберзахисту;

– провести аналіз цифрових інструментів, що використовуються для протидії кіберзагрозам та забезпечення нормальної функціонування систем управління;

– розглянути актуальні вимоги до фахівців у сфері кіберзахисту з урахуванням специфіки публічного управління та сучасних викликів у кіберпросторі;

– виокремити важливі аспекти стратегії і тактики використання цифрових інструментів кіберзахисту у сфері публічного управління;

– запропонувати шляхи вдосконалення цифрових інструментів кіберзахисту у сфері публічного управління.

Об'єктом дослідження є особливості та ефективність застосування цифрових інструментів кіберзахисту в системах публічного управління.

Предметом дослідження є цифрові інструменти кіберзахисту у сфері публічного управління.

Методи дослідження. У процесі виконання мігістерського дослідження були використані різні методи дослідження такі як аналіз наукової літератури, кількісного та якісного порівняння при аналізі статистичних даних, вивчення міжнародного досвіду підготовки кадрів в області інформаційної безпеки.

Інформаційною базою дослідження стали Конституція України, Закони України «Про інформацію», «Про захист інформації в автоматизованих системах», «Про державну таємницю», «Про науково-технічну інформацію», інші нормативно-правові акти, а також міжнародні угоди України, що стосуються сфери інформаційних відносин аналітичні та статистичні матеріали Центральних органів виконавчої влади, наукові статті та дослідження спеціалістів із цієї сфери діяльності.

В роботі зроблена спроба виявлення принципів удосконалення сучасної підготовки та перепідготовки спеціалістів на стадіях вивчення та відбору на навчання, а також удосконалення учбового процесу, яке позначається у застосуванні нових дисциплін, а також вироблення рекомендацій щодо вимог до спеціалістів даної категорії.

Теоретична, методична та практична значущість отриманих результатів. Під час дослідження було проведено глибокий аналіз організаційно-правових та технічних аспектів формування державної політики з інформаційної безпеки та кіберзахисту, а також ґрунтовно вивчено питання підготовки фахівців у цій галузі.

Практичне значення одержаних результатів. Практичні результати дослідження полягають у конкретних рекомендаціях щодо вдосконалення

цифрового інструментарію кіберзахисту в Україні та підвищення ефективності підготовки кадрів у цій сфері. Зокрема, робота виявила проблеми у відсутності необхідної інфраструктури, не виваженості державної політики та використанні іноземних засобів обчислювальної техніки, що призводить до втрат потенціалу для розвитку національних галузей.

Структура роботи. Робота складається зі вступу, трьох розділів, висновків, списку використаних джерел та додатків.

Апробація дослідження. Результати дослідження представлені автором на науково-комунікативному заході, зокрема на Міжнародній науково-практичній конференції:

Тодорюк О.Д. Особливості підготовки фахівців з кіберзахисту у сфері публічного управління. «Кібербезпека державних інституцій та подолання кризових станів» в 2 т. Том 2. Особливості діяльності органів державної влади в умовах кризи зб. тез наук. доп. (Київ – Вроцлав. Травень 2023). [Електронне видання]. – Київ: «ОФІС ЦИФРОВОГО ВРЯДУВАННЯ», 2023. Т.2. С. 109–110

РОЗДІЛ 1
ІНФОРМАЦІЙНА БЕЗПЕКА ЯК КОМПОНЕНТ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

1.1. Організаційно-правові засади формування державної політики у сфері інформаційної безпеки та кіберзахисту

Інформаційна безпека в рамках загальної системи національної безпеки України відзначається особливим статусом. З урахуванням стрімкого розвитку інформаційних технологій та їх широкого застосування у виробництві, обороні, правовому захисті, науці, освіті тощо, інформаційна діяльність стає необхідним і часто вирішальним компонентом у всіх сферах суспільства. Отже, питання інформаційної безпеки стає невід'ємною складовою національної безпеки країни. У сучасних умовах проблематика інформаційної безпеки набуває все більшого самостійного значення в суспільному контексті.

Водночас система зовнішніх та внутрішніх загроз інформаційній безпеці має складний характер, а її реалізація спрямована на завдання збитків у політичній, економічній, соціальній, військовій, екологічній, науково-технічній сферах і т.д. Як показав аналіз стану новизни й великої соціальної ролі інформаційних процесів, а також особливостей існуючої системи права, в Україні регулювання названих відносин відбувається в рамках різних галузей права – конституційного (право на інформацію), цивільного (договору про надання послуг доступу в мережу Інтернет, електронні угоди й розрахунки), адміністративного (законодавство про зв'язок). «Множинність» регулювання породжує наявність незбалансованої системи юридичних дефініцій, різні підходи до визначення суб'єктів, що беруть участь в інформаційних процесах при використанні інформаційних технологій і відповідно, співіснування різних способів визначення прав і обов'язків суб'єктів цих відносин.

З розвитком інформаційних і комунікаційних технологій змінюється структура й динаміка суспільного розвитку, виникають нові галузі економіки й збільшується їхня інтеграція, визначаються нові схеми державного управління, змінюються соціальні зв'язки і соціально-психологічний вигляд людини. Всі названі процеси неоднорідні, тому що протікають на фоні нерівності і є залежним від науково-технічного прогресу. У зв'язку із цим регулювання сучасних суспільних відносин в інформаційній сфері, серед яких найпоширенішими є доступ до інформаційних ресурсів і використання інформаційних послуг, стає однією з найбільш актуальних завдань сучасного законодавства.

1.2.Технічний захист інформації як складова частина забезпечення національної безпеки України

Технічний захист інформації має забезпечити єдність принципів формування й проведення такої політики в усіх сферах життєдіяльності особистості, суспільства та держави (соціальної, політичної, економічної, військової, екологічної, науково-технологічної, інформаційної тощо) і служити підставою для створення програм розвитку сфери ТЗІ.

ТЗІ – це діяльність, спрямована на забезпечення інженерно-технічними заходами порядку доступу, цілісності та доступності (унеможливлення блокування) інформації, яка становить державну та іншу передбачену законом таємницю, конфіденційної інформації, а також цілісності та доступності відкритої інформації, важливої для людини, суспільства і держави.

Ця діяльність спрямована на виконання наступних завдань:

– захист від загроз конфіденційності (несанкціонованого відбору) інформації за всіма каналами її витоку (мовному, видовому, електромагнітному, оптичному, віброакустичному), особливо, за рахунок

ПЕОМ і таємних каналів зв’язку (закладних пристроїв, радіомікрофонів і ін.);

– захист від загроз цілісності (несанкціонованої зміни інформації);

– захист від загроз досяжності інформації (несанкціонованого чи випадкового обмеження інформації і ресурсів самої системи);

– захист від загроз аудиту системи (наприклад, загрози несанкціонованого вторгнення в систему, маніпуляції з протоколами обміну і аудиту, загальносистемним програмним забезпеченням і ін.).

Зростання загроз для інформації, спричинене лібералізацією суспільних та міждержавних відносин, кризовим станом економіки, застосуванням технічних засобів оброблення інформації та засобів зв'язку іноземного виробництва, поширенням засобів несанкціонованого доступу до інформації та впливу на неї, визначає необхідність розвитку ТЗІ.

Напрями розвитку ТЗІ обумовлюються необхідністю своєчасного вжиття заходів, адекватних масштабів загроз для інформації, і ґрунтуються на засадах правової демократичної держави відповідно до прав суб'єктів інформаційних відносин, на доступ до інформації та приведення інформаційних відносин у сфері ТЗІ у відповідність із міжнародними стандартами, сприятиме становленню України у світі як демократичної правової держави.

Технічне забезпечення комп'ютерної безпеки розглядається як один з елементів її комплексного захисту й, відповідно, елемент попередження комп'ютерних злочинів. Під інженерно-технічним захистом розуміють сукупність спеціальних органів, технічних засобів і заходів щодо їхнього використання в інтересах забезпечення безпеки суб'єкта господарювання. Технічні засоби забезпечення комп'ютерної безпеки містять у собі засоби протидії технічним засобам ведення розвідки (ТЗВР), фізичні, апаратні, програмні, апаратно-програмні засоби й криптографічні методи захисту.

У наш час важливою складовою формування інформаційних ресурсів є впровадження систем електронного обігу та зберігання

документів. Розробка таких систем вимагає чіткого визначення поняття "електронний документ", регламентації процедур щодо їх створення, зберігання та утилізації, а також розробки ефективних заходів захисту інформаційних ресурсів у форматі електронних документів.

В Україні впровадження електронного документообігу в органах влади спрямоване на підвищення ефективності, швидкості та прозорості роботи державних установ. У цьому контексті використовуються спеціальні електронні платформи та системи, які сприяють створенню, обробці, передачі і збереженню документів у цифровому форматі. Це сприяє зменшенню використання паперу, спрощенню обробки документів і забезпеченню їхньої безпеки.

Електронний документообіг також сприяє забезпеченню громадян доступом до публічної інформації та активною участі в процесах прийняття рішень органами влади. Цей підхід визначає новий рівень взаємодії з інформацією, сприяючи сучасним технологіям та покращенню комунікації між учасниками державного управління та громадськістю.

В системі електронного документообігу, проблема захисту інформаційних ресурсів отримує новий акцентований контекст. Традиційне уявлення про документ як фізичний носій інформації, такий як аркуш паперу чи фотографія, потребує переосмислення на рівні свідомості. Технології створення та обробки електронних документів спрямовані на полегшення процесів відтворення, передачі та поширення інформації, що створює конфлікт із традиційним уявленням про збереження основних характеристик інформації – цілісності, доступності та конфіденційності.

Проблеми, пов'язані із захистом інформації у формі електронних документів, визнаються новими як з точки зору об'єкта діяльності, так і з технологічного аспекту здійснення такої діяльності. Це породжує необхідність розробки постійно діючої системи безперервного навчання для фахівців відповідного профілю та підвищення їх кваліфікації. Такий підхід враховує різноманіття викликів, пов'язаних із захистом електронної

інформації, і визначає важливість постійного удосконалення навичок та знань фахівців у цій області.

Концептуальні завдання захисту інформації визначають зміст навчальних планів підготовки спеціалістів цього профілю, зміст програм спеціальних дисциплін, а також необхідну тематику лабораторних робіт за основними навчальними дисциплінами.

В деяких випадках для досягнення необхідної високої ефективності технічних засобів захисту інформації виникає потреба в унікальній апаратній підтримці, що не завжди може бути реалізована серійними промисловими електронними приладами і, навіть, потребує відповідної апаратної науково-дослідної розробки. Використання в навчальному лабораторному практикумі дослідних взірців апаратури, розробленої за індивідуальними технічними завданнями в науково-дослідних установах галузі технічного захисту інформації, є дуже бажаним як засіб забезпечення найбільш ефективного навчального процесу.

Одним з першочергових завдань у створенні системи підготовки спеціалістів з інформаційної безпеки на сучасному етапі є необхідність враховувати такі особливості:

– інформаційна безпека – специфічна предметна галузь, підготовка спеціалістів для якої передбачає необхідність викладання специфічних розділів фундаментальних та загально інженерних дисциплін на міждисциплінарній основі: спеціальні розділи математики, електроніка, радіотехніка, радіоелектроніка, акустика, оптика, кібернетика та ін.;

– система освіти у галузі інформаційної безпеки має забезпечувати відповідність рівня підготовки спеціалістів рівню наукових знань, що у реальному вимірі часу (без запізнення на декілька років) реалізується через центри підготовки та підвищення кваліфікації, а також шляхом підготовки висококваліфікованих науково-педагогічних кадрів у магістратурі, аспірантурі, докторантурі;

– підготовка спеціалістів з інформаційної безпеки усіх категорій має бути на єдиній науково-методичній та правовій основі,

Високими технологіями почав активно цікавитися злочинний світ. Професійна майстерність деяких його представників, особливо в економічній та фінансовій сфері, викликає подив. Експерти в усьому світі визнають, що міжнародний характер сучасних комп'ютерних і телекомунікаційних технологій приводить до появи нових форм транснаціональної злочинності. Це призвело до появи такого феномену, як "комп'ютерна злочинність" (або "кіберзлочинність" від англ. cyber crime). Таким чином одним з найважливіших завдань сучасності є боротьба з комп'ютерною злочинністю і кібертероризмом. Спектр злочинів у сфері інформаційних технологій по зведеннях системи обліку злочинів дуже широкий, він варіюється від Інтернет-шахрайства до дитячої порнографії, і включає такі потенційно небезпечні діяння як електронне шпигунство й підготовка до терористичних актів [11].

Відповідно до досліджень [19] недостатня захищеність даних і неуважність можуть мати серйозні фінансові наслідки. У 2020 році втрата даних в середньому коштувала 3,86 мільйонів доларів. Вчені роблять прогноз, що до 2025 року кіберзлочинність витягне з світу 10,5 трильйона доларів на рік. Істотну протидію росту злочинів у сфері інформаційних технологій може зробити грамотна політика підготовки національних кадрів у сфері інформаційної безпеки.

Невід'ємною складовою державної політики України, спрямованої на захист інформаційних ресурсів держави і захист інформації з обмеженим доступом, є підготовка фахівців у сфері захисту інформації і інформаційної безпеки. Завдання підготовки фахівців є особливо актуальною ще й тому, що в даний час достатньо вільно поширюються друковані та електронні видання, де описуються технології здійснення комп'ютерних злочинів, що одержали особливу популярність серед молоді. У даний час будь-який підліток може купити за невеликі гроші книгу, що навчає його

елементарним прийомам атаки на інформаційні системи. За допомогою викладених у книзі знань такий підліток стає реальною погрозою безпеки комп'ютерних систем. В Інтернеті представлено більш 30 тисяч сайтів, що навчають комп'ютерному злочину. У мережі Інтернет проводяться форуми, віртуальні конференції й семінари по обміну досвідом здійснення комп'ютерних злочинів [33]. Таким чином, комп'ютерні злочинці активно працюють над підвищенням своєї кваліфікації, втягують у своє середовище підростаюче покоління й активно його навчають, причому легально. Все це підкреслює важливість рішення ще однієї задачі – активної протидії залученню молоді в злочинне середовище й розробки ефективних методів проведення виховної роботи серед молоді.

Насущною задачею сучасної освіти стає розробка таких методів навчально-виховної роботи, де б гармонійно поєднувалось навчання сучасним інформаційним технологіям із формуванням високих моральних якостей для вироблення імунітету до здійснення комп'ютерних злочинів.

З метою протидії зазначеним загрозам в Україні функціонує система технічного захисту інформації, яка є сукупністю організаційних структур, поєднаних цілями і завданнями захисту інформації, нормативно-правової та матеріально-технічної бази й спрямована на забезпечення інженерно-технічними засобами конфіденційності, цілісності та доступності інформації, охорона якої забезпечується державою відповідно до законодавства.

На сьогодні в Україні створено необхідну нормативно-правову базу з питань технічного захисту інформації (ТЗІ, яка визначає правові та організаційні засади ТЗІ, норми та вимоги із ТЗІ, порядок здійснення та контролю його ефективності. Нормативні документи з питань ТЗІ в Україні розроблено з урахуванням існуючих підходів до захисту інформації в країнах ЄС, Канади, США, та ін.

Організаційна структура системи технічного захисту інформації має ієрархічну структуру. Функції органу державного управління в сфері ТЗІ

виконує Державна служба спеціального зв’язку та захисту інформації України, яка є суб'єктом сектору оборони і безпеки, основним суб'єктом національної системи кібербезпеки, що здійснює координацію діяльності суб'єктів забезпечення кібербезпеки в галузі кіберзахисту та адміністратором зв'язку, а також державний контроль за функціонуванням системи ТЗІ (КСЗІ).

На відомчому рівні в центральних органах виконавчої влади, інших державних органах, підпорядкованих їм підприємствах, установах та організаціях створюються або визначаються підрозділи (підрозділи ТЗІ, служби захисту інформації в інформаційно-телекомунікаційних системах), на які покладаються завдання забезпечення ТЗІ (КСЗІ).

Функціонування системи ТЗІ здійснюється з урахуванням необхідності забезпечення гарантії відповідності рівня захищеності інформації вимогам нормативних документів. При цьому необхідну якість робіт із ТЗІ можна забезпечити за умови залучення висококваліфікованих спеціалістів, які мають відповідну фахову підготовку та досвід роботи, при відповідному технічному оснащенні.

Висновки до розділу 1

Таким чином, одним із факторів забезпечення надійного функціонування й розвитку захищених інформаційних систем є вирішення проблеми створення та розвитку системи кадрового забезпечення в галузі інформаційної безпеки, причому під інформаційною безпекою розуміється галузь науки і техніки, що охоплює сукупність програмних, апаратних і організаційно-правових методів і засобів забезпечення безпеки інформації при обробці, зберіганні і передачі з використанням сучасних інформаційних технологій. Ефективний розвиток будь-якого регіону, та й усієї країни в цілому, неможливий без створення в державних або інших структурах для належного захисту інформації спеціальних служб захисту, укомплектованих висококваліфікованими кадрами.

РОЗДІЛ 2
ПОБУДОВА ПРОЦЕСУ ПІДГОТОВКИ ФАХІВЦІВ У СФЕРІ ЗАХИСТУ ІНФОРМАЦІЇ

2.1. Особливості підготовки кадрів в області інформаційної безпеки в США

Попередній аналіз існуючих підходів до побудови процесу підготовки фахівців в області захисту інформації в США дозволив виділити домінуючі напрямки й сконцентрувати увагу на розгляді існуючих підходів до процесу навчання.

США визнають значення інформаційної безпеки як одного з найважливіших компонентів національної безпеки. Тому підготовка кадрів в даній галузі в країні відбувається з великою увагою та врахуванням специфіки цього сегмента. Маючи потужну інформаційну інфраструктуру та багато цінних даних, США активно працюють над забезпеченням відповідного рівня захисту цієї інформації.

Важливо відзначити, що в США дуже багато уваги приділяється залученню суспільної уваги до проблеми інформаційної безпеки. В 1998 році був створений Національний центр захисту інфраструктури (NIPC) [23], що поєднує представників органів влади, військових і приватного сектору, для захисту національних інфраструктур. Міжнародна асоціація фахівців з комп'ютерних досліджень (IACIS), забезпечує навчання в області комп'ютерних технологій. Успішно функціонує Національний союз кібербезпеки, створений спільно урядом і промисловцями США [24]. Ціль союзу – розробка підходів до проблеми безпеки в кіберпросторі, підвищення рівня утворення в сфері інформаційної безпеки, залучення суспільної уваги до проблеми кібертероризму.

Сполучені Штати Америки володіють широким спектром університетів, коледжів, технічних шкіл та інших навчальних закладів, які пропонують програми з інформаційної безпеки. Це дозволяє студентам мати великий вибір освітніх установ для отримання необхідних знань і навиків. Більшість з цих навчальних закладів також підтримують академічні програми, спрямовані на практичне навчання та дослідження в області інформаційної безпеки. Серед найвідоміших можна відзначити Check Point Software Technologies, Cisco Systems, IBM Tivoli Systems Global Security Laboratory, Internet Security Systems, Microsoft, Network Associates, Prosoft Training. Com, Sun Microsystems, Symantec. Серед навчальних центрів, що спеціалізуються на підготовці фахівців із захисту інформації можна відзначити: CERT, GIAC, CSI, Cisco Systems .

Крім комерційних компаній, підготовку фахівців в області інформаційної безпеки здійснює ряд державних структур: аспірантура NAVAL пропонує 12 різних курсів, агентство по захисту інформаційних систем (Defense Information Systems Agency, DISA) – 8 курсів, коледж управління інформаційними ресурсами (Information Resource Management College) – 1 курс [35].

Для вдосконалення методів навчання в Міністерстві оборони створений спеціальний підрозділ - «Управління програм по інформаційній безпеці (Information Assurance Program Office)». Агентство національної безпеки (NSA) сформувало ще в 1999 році ряд центрів післядипломної освіти, а в 2000 році підключило до них 14 ведучих університетів США. Одночасно Білий Дім приступив до навчання урядових чиновників (до 10 тис. чоловік) у рамках федеральної програми забезпечення безпеки інформаційних технологій з бюджетом 25 млн. доларів у рік [36].

Перш за все, підготовка кадрів в області інформаційної безпеки в США базується на комплексному підході. Це означає, що навички та знання, необхідні для ефективної роботи в даній галузі, формуються з

різних напрямків, щоб професіонали могли краще розуміти всі аспекти інформаційної безпеки.

Початковий етап підготовки включає отримання відповідних освітніх ступенів, таких як бакалавр або магістр в галузі комп'ютерних наук, інформаційних систем, кібербезпеки та інших суміжних спеціальностей. Важливим елементом такої підготовки є освоєння фундаментальних знань про комп'ютерні мережі, програмування, системи зберігання даних, криптографію та інші аспекти, пов'язані з інформаційними технологіями.

Окрім академічної підготовки, США дуже цінують практичний досвід у сфері інформаційної безпеки. Для студентів та випускників розроблені спеціальні програми стажування та практики, які надають можливість отримати реальний досвід роботи в цій галузі. Такі програми відбуваються в університетах, дослідницьких лабораторіях, державних органах та приватних компаніях, які спеціалізуються на інформаційній безпеці.

Не менш важливим аспектом підготовки кадрів є постійне професійне підвищення кваліфікації.

Після трагічних подій 11 вересня 2001 року у багатьох містах США почали регулярно проводитися семінари, конференції, симпозіуми з проблем кіберзлочинності і кібертероризму. Практично на кожній із зустрічей звучали заклики поліпшити підготовку й навчання користувачів комп'ютерів з інформаційної безпеки. Так, наприклад, в 2002 році проводився семінар "Комп'ютерні злочини і безпека" міст Тампа й Сарасота (штат Флорида), у роботі якого, поряд з фахівцями з комп'ютерних технологій, взяли участь співробітники правоохоронних органів [57]. Як і у всьому світі, підготовка та навчання є надзвичайно важливими в аспекті комп'ютерів, організації мають бути впевнені, що їх користувачі комп'ютерів розуміють потенційні небезпеки, які можуть

виникнути в Інтернеті. Крім того, користувачі повинні дотримуватися політики та правил організації, в якій вони працюють [37].

На думку С. Вілдера й Б. Віоліно [38], для успішної боротьби з кіберзлочинністю необхідно, щоб, з одному боку, поліцейські академії включали питання розслідування комп'ютерних злочинів в основний курс карного розшуку; з іншого боку – у навчальні плани підготовки фахівців із забезпечення інформаційної безпеки повинні бути включені розділи, що стосуються профілактики комп'ютерних злочинів.

США проголосили необхідність введення нових стандартів безпеки даних та кібербезпеки. Це означає, що країна потребує спеціалізованих фахівців із підготовки та впровадження таких стандартів. Крім того, наявність технологічно розвиненої бізнес-сфери в США дозволяє створювати нові робочі місця та кар'єрні можливості для фахівців інформаційної безпеки.

Разом з тим, Сполучені Штати привертають до себе талановитих фахівців з усього світу, які бажають отримати освіту та розвиватися в галузі інформаційної безпеки. Це створює міжнародну спільноту фахівців, яка сприяє обміну знаннями та досвідом. Багатонаціональні компанії та урядові організації в США також активно залучають іноземних спеціалістів [39].

Ще одним із способів покращення підготовки кадрів в області захисту інформації в США є співпраця з міжнародними консорціумами. Інтернаціональний характер проблеми державного забезпечення захисту інформації вимагає консолідації й координації зусиль усіх країн у плані підготовки фахівців із захисту інформації. США виступили ініціаторами створення мережі міжнародних консорціумів по підготовці кадрів в області захисту інформації. Партнерство з міжнародними консорціумами також може допомогти сприяти обміну найкращими практиками та знаннями у сфері кібербезпеки. Організації такого роду здатні створювати навчальні програми, семінари та конференції, де фахівці з усього світу можуть

обмінюватися досвідом та взаємодіяти для пошуку нових інноваційних рішень. Це сприяє розширенню загального рівня знань у галузі захисту інформації.

Попередній досвід підготовки кадрів в США відображає значення співпраці з міжнародними консорціумами. Наприклад, така організація, як Міжнародна асоціація по безпеці інформації (International Information Systems Security Certification Consortium, ISC) [34], пропонує визнаний у всьому світі сертифікат Certified Information Systems Security Professional (CISSP). Цей сертифікат підтверджує технічні та управлінські знання та навички з управління інформаційною безпекою. Багато кадрів у галузі безпеки інформації в США мають CISSP сертифікат, що підкреслює важливість таких міжнародних стандартів.

До претендентів на одержання сертифіката (CISSP) пред'являються досить високі вимоги. Необхідно мати досвід не менш 4 років роботи як фахівця по інформаційному захисту (чи не менш 3 років і ступінь бакалавра), здати строгий іспит, підписати Кодекс Етики (ISC)2 і постійно підвищувати свою кваліфікацію. Для підтвердження сертифікації CISSP не потрібно повторної здачі іспиту, досить кожні три роки проходити навчання на авторизованих курсах по інформаційній безпеці й брати участь в конференціях по цій темі.

Здача офіційного іспиту вимагає від кандидатів детального й всебічного знання теорії й практики інформаційної безпеки. Питання іспиту охоплюють широкий діапазон проблем безпеки, заснованих на "Загальноприйнятому обсязі знань" (Common Body of Knowledge, «CBK») [35]. CBK охоплює 10 тем: методи керування інформаційною безпекою, архітектура й моделі безпеки, методологія й системи керування доступом, безпека розробки додатків і систем, безпека операцій, фізична безпека, криптографія, безпека телекомунікацій, мереж і Інтернет, планування безперервності бізнесу й планування відновлення після збоїв, законодавство, розслідування й етика.

У ході 6-годинного іспиту учасники повинні були письмово відповісти на 250 індивідуальних питань, що мають чотири варіанти відповідей. Важливо відзначити, що інформація у СВК і відповідно питання іспиту постійно змінюються, не відстаючи від змін в інформаційних технологіях.

З метою налагодження партнерських зв'язків з навчальними заставами Європи, Близького Сходу і Африки співробітники Стэндфордского університету в 1984 році створили фірму Cisco Systems. Одночасно було створено освітній проект «Мережева академія Cisco» [36], спільно з освітніми установами й компанією Cisco, світовим лідером в області мережних Інтернет-рішень. На початку своєї діяльності академія планувалася для підготовки кваліфікованих кадрів по обслуговуванню мереж, однак надалі, у міру збільшення питомого важеля дисциплін, зв'язаних з інформаційною безпекою, вона придбала популярність як могутній центр підготовки фахівців із захисту інформації.

У даний час мережна академія Cisco є світовим лідером у мережних технологіях для Інтернет. Вона забезпечує фундаментальну підготовку фахівців з теорії й практики проектування, будівництва й технічного супроводу локальних і глобальних мереж з використанням загальновизнаних стандартів і рішень в області інформаційної безпеки.

Академії Cisco відкриті в 128 країнах, для того, щоб навчити своїх студентів проєктувати та створювати мережі.

Програма Мережної академії Cisco розрахована на 280 годин. Навчальні плани розроблені відповідно до освітніх стандартів США при участі кращих фахівців в області освіти і мережевих технологій. Після проходження навчального курсу проводитися іспит на звання сертифікованого Cisco фахівця (CCNA) чи сертифікованого Cisco мережного професіонала (CCNP).

У навчальному процесі використовуються самі прогресивні методики навчання і контролю рівня знань. Зокрема, широко

використовуються технології дистанційного навчання. Функціонує «Глобальна лабораторія по електронному навчанню», що в режимі on-line щодня здійснює близько 35000 тестів. Навчання проводиться на 9 мовах. Навчальний матеріал обновляється кожні 90 днів.

Одним з підходів до удосконалювання підготовки фахівців у США є використання передових технологій навчання, а саме – широке використання дистанційного навчання (e-learning).

Проведений порівняльний огляд технологій навчання [40] в США показує стрімкий розвиток системи дистанційного навчання. Дійсно, у США і Канаді, за даними Official MBA Guide, нараховується більш 800 програм ділового адміністрування. При цьому вони не зосереджені в Нью-Йорку або Вашингтоні, а розкидані по всій території Північної Америки. У США ринок дистанційної освіти зростає більш ніж на 40% щорічно. Приблизно 350 тис. чоловік, що вчаться винятково дистанційно, платять навчальним закладам за онлайн-курси $1,75 млрд. у рік. Зараз, оборот усього ринку дистанційного навчання складає в США $4,5 млрд., а до 2025 року він збільшиться до $17 млрд. Американські корпорації в 2025 році витратять на e-learning, за даними М. Бреннена з дослідницької фірми IDC, до $14,98 млрд [40].

Слід зазначити, що більш детальне вивчення навчальних програм ділового адміністрування показує, що в них знаходять серйозний розгляд питання інформаційної безпеки, а також питання, зв'язані з вивченням легальних методів одержання інформації про конкурентів (конкурентна розвідка).

Аналіз сайтів ведучих університетів США дозволяє зробити ще ряд цікавих висновків. Наявність одного диплома, виданого 10-15 років тому, у США вже недостатньо. Тому портрет американця що вчиться стрімко міняється. 42% усіх студентів приватних і державних вузів США старше 25 років. Більш того, число бажаючих вчитися дорослих людей росте непропорційно високими темпами. У період між 1970 і 2010 р. кількість

студентів у віці 18-24 років виросло на 41%. За цей же термін число «дорослих» учнів збільшилося на 170%. Цікаво відзначити, що серед них особливо багато жінок – 67%. При такому швидкому росту потреб в освіті, в американських коледжів незабаром просто не буде можливості прийняти на навчання всіх бажаючих. Тому характер самого освітнього ринку вже зараз істотно міняється, а в доступному для огляду майбутньому може перетерпіти дуже значні зміни. Комерційні онлайн-програми вузів відбирають учнів у традиційних коледжів. Уже зараз 33% усіх, хто вчитися дистанційно, вибирають платні тренінгові курси, а не програми університетів. На думку С. Данна, до 2025 р. «половина з нинішніх коледжів закриється, піде на злиття зі своїми конкурентами або кардинально змінить свою місію» .

Важливим фактором, що впливає на характер освіти, залишається розвиток технологій. До 2025 року, по оцінці М. Ситрона й О. Дэвью, майже 100% жителів міст США будуть комп’ютерно грамотними. Це неминуче впливає на освітні процеси. Учні дистанційних програм можуть легко користатися електронною поштою, форумами, чатами, онлайновими тестами й іншим мережевим інструментарієм. Усі ці механізми повинні обов'язково враховувати програми дистанційного навчання. Більш того, що ріст пропускної здатність мереж робить не тільки актуальним, але й необхідним використання ігрових і імітаційних методик, а також відеоматеріалів і відеоконференцій [40].

2.2. Особливості підготовки кадрів в області інформаційної та кібербезпеки в країнах ЄС.

Однією з найактуальніших галузей сучасного суспільства є інформаційна безпека. В умовах різкої зростаючої кількості кіберзагроз та інших викликів, пов'язаних з інформаційною сферою, питання підготовки висококваліфікованих кадрів в галузі інформаційної безпеки стає

надзвичайно важливим. Спроможність країн справлятися з цими викликами в значній мірі залежить від якості підготовки фахівців у даній області. Дослідження ґрунтується на аналізі літературних джерел, статистичних даних та результатів попередніх досліджень в галузі інформаційної безпеки в країнах ЄС. Аналіз проводиться на основі порівняльного підходу, що дозволяє виявити спільні риси та відмінності в підготовці кадрів в області інформаційної безпеки в країнах ЄС.

Система освіти в країнах ЄС відрізняється високим ступенем стандартизації та інтеграції. Вона включає в себе початкову, середню, вищу освіту та систему післядипломної підготовки. Аналізуючи структуру системи освіти, можна визначити місце та роль підготовки фахівців з інформаційної безпеки в цій системі. Країни ЄС пропонують різноманітні освітні програми з інформаційної безпеки, які охоплюють різні аспекти цієї галузі. Вони можуть бути представлені у вищих навчальних закладах, професійних школах та центрах підготовки.

Аналізуючи систему підготовки кадрів в Німеччині, варто відзначити важливу роль вищих навчальних закладів та індустрійних партнерств у наданні спеціалізованих програм з інформаційної безпеки. Окрема увага приділяється практичній складовій підготовки студентів.

У Німеччині система підготовки фахівців з інформаційної безпеки базується на високих стандартах та враховує актуальні потреби галузі. Основними характеристиками підготовки кадрів в галузі інформаційної безпеки в Німеччині є:

1. Вищі навчальні заклади. В Німеччині велика кількість вищих навчальних закладів пропонують програми з інформаційної безпеки. Студенти можуть отримати ступінь бакалавра, магістра або доктора в цій галузі. Освітні програми включають в себе вивчення криптографії, кібербезпеки, мережевої безпеки, а також дослідницьку роботу.

На приклад Університет Пассау [25] пропонує магістерську програму "Кібербезпека та медіа". Ця програма включає в себе вивчення

кібербезпеки, криптографії та кіберфізичних систем, Університет техніки Мюнхена [26] пропонує магістерську програму "Комп'ютерна наука та техніка", яка включає в себе спеціалізацію в галузі інформаційної безпеки. Студенти вивчають питання кібербезпеки та мережевої безпеки.

2. Практична підготовка. Однією з важливих особливостей підготовки фахівців в Німеччині є акцент на практичній підготовці. Студенти мають можливість виконувати стажування в інформаційних технологічних компаніях та організаціях, де вони можуть застосовувати свої знання на практиці.

3. Індустрійна підготовка. Співпраця з промисловістю в Німеччині грає важливу роль у підготовці фахівців з інформаційної безпеки. Багато вищих навчальних закладів укладають партнерські угоди з технологічними компаніями та організаціями, які спеціалізуються на кібербезпеці. Ця співпраця дозволяє студентам мати доступ до сучасних технологій та здобувати досвід роботи в реальних умовах.

Німеччина активно розвиває галузь підготовки фахівців з інформаційної безпеки, оскільки кіберзагрози стають все більш серйозними. Можна очікувати подальшого зростання числа освітніх програм та ініціатив, спрямованих на підготовку кадрів в цій галузі. Важливою є також співпраця з іншими країнами ЄС для обміну досвідом та ресурсами.

Франція має розвинуту систему вищої освіти в галузі інформаційної безпеки, яка включає магістерські програми та докторантуру. Особливий акцент робиться на дослідницькій роботі та співпраці з промисловістю. У Франції існують численні освітні програми з інформаційної безпеки, які пропонуються в університетах та вищих навчальних закладах. Франція відома своєю високою якістю освіти та акцентом на науковий підхід до вирішення проблем в галузі інформаційної безпеки.

Університет Парижа-Суд пропонує магістерську програму "Інформаційна безпека та кіберзахист" (Cybersecurity and Cyberdefense). Ця

програма надає студентам глибокі знання в галузі інформаційної безпеки та кібернетичного захисту. Студенти вивчають такі теми, як кібернетичні загрози, криптографія, захист мереж та інформаційна безпека в обчислювальних системах. Програма акцентує науковий підхід та дослідження в галузі кібербезпеки.

Інститут інформаційних наук та технологій (ISTY) [29] пропонує магістерську програму з інформаційної безпеки. Студенти отримують поглиблені знання з кібербезпеки, включаючи аспекти кібернетичних атак, захисту мереж, криптографії та етики в інформаційній безпеці. Програма розроблена з урахуванням актуальних тенденцій у галузі.

Інститут Телекомуникацій і інформаційних технологій (ITII) [30] надає програму бакалавра "Інженерія кібербезпеки". Ця програма спрямована на підготовку інженерів у галузі кібербезпеки. Студенти вивчають технічні аспекти кіберзахисту, включаючи захист мереж, інциденти кібербезпеки та криптографію.

Ці освітні програми в Франції допомагають студентам отримати високоякісну освіту та глибокі знання в галузі інформаційної безпеки. Вони також ставлять акцент на практичну підготовку та наукові дослідження, що робить їх ідеальними для тих, хто бажає працювати в цій важливій галузі.

Велика Британія відома своєю інноваційною підготовкою фахівців з інформаційної безпеки, де акцент робиться на сучасних технологіях та креативних підходах до захисту інформації. Країна має довгу історію в цій сфері та активно розвивається, щоб впроваджувати нові технології та методи захисту в інформаційній безпеці.

Національний центр кібербезпеки NCSC [37] – це важлива організація, що відповідає за кібернетичний захист у Великій Британії. Вони надають поради та рекомендації щодо кібербезпеки, вивчають загрози та координують дії в разі кібернетичних інцидентів. NCSC також веде дослідження та надає публічні звіти щодо кібербезпеки.

Велика Британія має численні університети, що пропонують освітні програми в галузі інформаційної безпеки та кібернетичного захисту. Імперський коледж Лондона пропонує магістерську програму "Кібербезпека". Студенти вивчають кібернетичні загрози, криптографію та захист мереж. Оксфордський університет проводить дослідження в галузі кібербезпеки та має програми для докторантів. Кембриджський університет також активно діє в галузі кібербезпеки та розробляє нові методи захисту.

Крім того Англія має розвинений промисловий сектор у галузі інформаційної безпеки. Багато компаній спеціалізуються на кібернетичному захисті, розробці програмного забезпечення та консалтингу в галузі інформаційної безпеки. Приклади таких компаній включають "BAE Systems Applied Intelligence," "Darktrace," "Palo Alto Networks," та інші.

У Великій Британії існують центри навчання та інкубатори стартапів, які спеціалізуються на кібербезпеці. Ці центри надають студентам, вченим та підприємцям можливість розвивати свої навички та створювати інноваційні продукти та послуги в галузі кібербезпеки.

Разом з тим в Британії уряд і приватні компанії активно працюють над підвищенням своєї кібербезпеки та підготовкою фахівців у цій галузі. Це робить країну однією з провідних у світі у галузі інформаційної безпеки та кібернетичного захисту.

У Ірландії також існують відмінні освітні програми з інформаційної безпеки. Приклади таких програм: Дублінський університет технологій пропонує магістерську програму "Кібербезпека". Студенти вивчають теми, такі як етика в інформаційній безпеці, кіберзахист та безпека мереж. Університет Лімеріка має магістерську програму "Інформаційна та кібербезпека". Студенти отримують знання в галузі кібербезпеки та захисту інформації. Ці ірландські програми надають студентам можливість

навчатися в інноваційному середовищі та розвивати навички, необхідні для кар'єри в галузі інформаційної безпеки.

2.3. Основні вимоги до підготовки фахівців з технічного захисту у сфері інформаційної безпеки

Проблема удосконалювання підготовки фахівців в області інформаційної безпеки є багатоплановою. Успішно вирішити її можливо тільки комплексно, на основі системного підходу.

Основні принципи підготовки кадрів з урахуванням вимог сьогоднішнього дня можна сформулювати таким чином: рівень теоретичних знань повинен наближатися до міжнародного, підготовку слід орієнтувати на придбання практичних навиків ведення справи у вітчизняних кризових умовах, істотна увага повинна бути приділена питанням забезпечення безпеки і стійкого розвитку суб'єкта господарювання і регіону. Останнє диктується наступним обставинами:

а) необхідністю збільшення чисельності професійних фахівців, оскільки той контингент, підготовка якого забезпечується у даний час, вже недостатня для задоволення всіх потреб у цих фахівцях;

б) потребою безперервного вдосконалення учбового процесу в цілях підвищення якості підготовки фахівців, оскільки теорія і практика захисту інформації безперервно і інтенсивно розвивається, і нові досягнення повинні швидше відображатися в навчальних планах і програмах;

с) необхідністю розширення номенклатури спеціальностей по захисту, оскільки сучасні системи захисту стають все більш складними і комплексними як по цілях, так і по використовуваних методах і засобах захисту.

Кажучи загалом про підготовку системотехніка по захисту інформації, нагадаємо, що під системотехнікою в теорії систем розуміють науковий напрям, що охоплює питання проектування, створення,

випробування і експлуатації великих систем. Остання, у свою чергу, визначається як організована сукупність великого числа взаємозв'язаних елементів, що мають загальну мету функціонування. Причому відомо, що ефективність функціонування сукупності елементів, організованих на користь досягнення певної мети, причому чим вищий рівень організації системи, тім більше системний ефект. Забезпечення такої організації для отримання найбільшого ефекту і складає головне завдання системотехніка.

Стосовно системотехніка по захисту інформації перерахуємо основні завдання, які він повинен вміти вирішувати на різних стадіях створення і експлуатації систем захисту інформації

У процесі проектування систем захисту:

а) обстеження об’єкту в цілях кваліфікованого визначення необхідності застосування спеціальних заходів захисту;

б) визначення потенційно можливих загроз інформації;

в) визначення і прогнозування значень показників уразливості інформації;

г) обґрунтування рівня необхідного захисту інформації на об’єкті і найбільш доцільних способів його забезпечення;

д) вибір засобів, необхідних для раціонального вирішення завдань захисту;

е) розробка загального проекту системи захисту інформації на об’єкті і рекомендацій по його реалізації;

ж) розробка технологічних схем функціонування системи захисту в різних режимах діяльності об’єкту;

з) розробка пропозицій по практичній реалізації проекту системи захисту.

На стадії реалізації проекту системи захисту:

а) участь в розробці, замовленні і перевірці засобів захисту;

б) участь в монтажі системи і у пуско-налагоджувальних роботах;

в) участь у випробуваннях і прийманні системи захисту;

г) участь в навчанні і інструктажах користувачів і персоналу автоматизованої системи обробки даних.

У процесі функціонування системи захисту:

а) участь в організації і здійсненні контролю за функціонуванням системи захисту;

б) участь у вживанні невідкладних заходів при появі нештатних ситуацій;

в) збір, накопичення і обробка статистичних даних про функціонування систем захисту;

г) розробка рекомендацій і участь в процесі вдосконалення систем захисту.

Об'єктами професійної діяльності випускника ВУЗу із спеціалізації по захисту інформації є автоматизовані системи обробки, зберігання і передачі інформації певного рівня конфіденційності, методи і засоби забезпечення інформаційної безпеки автоматизованих систем.

Одним з перших питань підготовки кадрів є формування моделі спеціаліста відповідних спеціальностей (спеціалізації). Тому професійні вимоги або кваліфікаційна характеристика спеціаліста в галузі захисту інформації з обмеженим доступом повинні відображати:

– кваліфікаційні вимоги до знань і умінь;

– професійне призначення та сферу діяльності фахівця.

В міру того, як перелік спеціальностей і спеціалізацій буде уточнюватись, а також з урахуванням досвіду підготовки спеціалістів та пропозицій відповідних міністерств і відомств, кваліфікаційні характеристики повинні корегуватись і доповнюватись. Розробка повного переліку кваліфікаційних характеристик в галузі захисту інформації повинна вестись з урахуванням розвитку галузі інформаційної безпеки і ринку праці. Модель спеціаліста з захисту інформації є основою для розробки навчальних програм і навчальних планів, а також для корегування вимог до спеціалістів у відповідних довідниках.

І. Кваліфікаційна характеристика спеціаліста в галузі захисту інформації в комп'ютерних системах та мережах.

1. Професійне призначення і сфера діяльності.

Фахівець призначений для:

Професійної діяльності в галузі комплексного захисту інформації від несанкціонованого доступу до засобів електронної обчислювальної техніки, автоматизованих систем різного рівня та призначення, банків даних і знань, мереж електронних обчислювальних машин шляхом використання апаратних, програмних, програмно-апаратних, програмно-математичних, криптографічних засобів захисту, а також захисту інформації від витоку каналами побічних електромагнітних випромінювань та наведень шляхом використання інженерно-технічних та програмних засобів захисту.

Фахівця підготовлено для:

Професійної діяльності на посадах, передбачених типовими номенклатурами посад для фахівців з вищою спеціальною освітою у структурних підрозділах із захисту інформації з обмеженим доступом центральних і місцевих органів державної влади, підприємств, організацій, установ; головних і базових організацій системи захисту інформації, працюючих в галузі захисту інформації в комп'ютерних системах та мережах; наукових, проектних і конструкторських організацій, що розробляють засоби електронної обчислювальної техніки, автоматизовані системи різного рівня та призначення, програмні та технічні засоби захисту інформації для цих систем; фінансово-банківських та комерційних структур державного і недержавного секторів економіки, що використовують автоматизовані системи та комп'ютерні засоби; державних і недержавних організацій, які займаються сервісним обслуговуванням захищених комп'ютерних систем та мереж; виробничих структур управління рухом усіма видами транспорту (повітряного, водного, залізничного, автомобільного) та продуктопроводів, що

використовують засоби обчислювальної техніки; структур управління енергетичними комплексами (АЕС, ДРЕС, ТЕЦ), що використовують засоби обчислювальної техніки; структур управління виробництвом і технологіями у промисловості, що використовують засоби обчислювальної техніки; структур управління з використанням засобів обчислювальної техніки – військових частин різного підпорядкування (для спеціалістів, що закінчили військові навчальні заклади).

2. Кваліфікаційні вимоги до знань спеціаліста.

На додаток до базових знань факультетів кібернетики, інформатики, обчислювальної техніки, прикладної математики тощо, спеціаліст повинен знати:

а) загально інженерні дисципліни:

математичну логіку; математичну статистику; теорію алгоритмів і автоматів; теорію інформаційних процесів; теорію та технологію програмування; моделювання об’єктів та процесів; електро- та радіовимірювання; теорію розповсюдження радіохвиль; теоретичні основи радіотехніки;

б) загально спеціальні дисципліни:

електроніку та схемотехніку електронних обчислювальних машин; цифрову обробку сигналів; дискретну математику; методи системного аналізу; основи автоматизованого проектування; методи та засоби штучного інтелекту; системи передачі даних; теорію випадкових процесів; теорію управління; теорію надійності;

в) вузькоспеціальні дисципліни:

теорію комплексного захисту інформації в комп’ютерних системах та мережах; методологію комплексного захисту інформації в комп’ютерних системах та мережах; основи теорії криптографії і криптоаналізу, використання криптографічних засобів з метою захисту інформації в комп’ютерних системах та мережах; математичні методи захисту інформації в комп’ютерних системах та мережах; методологію захисту

операційних систем, систем управління банками даних і знань, телемоніторів, мережевого програмного забезпечення; основи проектування захищеного системного програмного забезпечення; методи захисту програмно-інформаційного продукту від несанкціонованого впливу (з метою крадіжки, руйнування, цілеспрямованого спотворення) у тому числі вірусного характеру; методи захисту програмного забезпечення від несанкціонованого копіювання; методи оцінки захищеності програмного забезпечення систем обчислювальної техніки і автоматизованих систем; канали витоку інформації, методи і засоби несанкціонованого доступу до інформації в комп'ютерних системах та мережах; методику оцінки вразливості інформації в комп'ютерних системах та мережах; технічні канали витоку інформації в комп'ютерних системах та мережах побічним електромагнітним випромінюванням і наведеннями; методи оцінки захищеності інформації в комп'ютерних системах та мережах від витоку каналами побічних електромагнітних випромінювань і наведень; методи здійснення спецдосліджень засобів електронної обчислювальної техніки і спецперевірок для виявлення закладок; інженерно-технічні засоби захисту інформації в комп'ютерних системах та мережах від витоку каналами побічних електромагнітних випромінювань і наведень; основи проектування захищених від витоку каналами побічних електромагнітних випромінювань і наводок засобів електронної обчислювальної техніки та автоматизованих систем, а також технічні засоби захисту; методи контролю ефективності комплексного захисту інформації в комп'ютерних системах та мережах; методику техніко-економічного забезпечення заходів з комплексного захисту інформації в комп'ютерних системах та мережах; вимоги стандартів та нормативно-технічних матеріалів з комплексного захисту інформації в комп'ютерних системах та мережах; основи організаційно-правового забезпечення безпеки інформації; іноземний досвід комплексного захисту інформації в комп'ютерних системах та мережах.

Спеціаліст повинен вміти:

– аналізувати інформаційні потоки в комп'ютерних системах та мережах; оцінювати міру захищеності інформації від несанкціонованого доступу і витоку технічними каналами;

– формулювати і обґрунтовувати вимоги з комплексного захисту інформації у таких системах;

– експлуатувати захищені засоби електронної обчислювальної техніки та технічні засоби захисту, програмно-апаратні та криптографічні засоби захисту інформації в комп'ютерних системах та мережах;

– розробляти технічні вимоги з комплексного захисту інформації в комп'ютерних системах та мережах; конструювати та організаційно оформляти локальні системи комплексного захисту інформації в комп'ютерних системах та мережах;

– розробляти програмно-апаратні та криптографічні засоби захисту інформації в комп'ютерних системах та мережах;

– розробляти захищені засоби електронної обчислювальної техніки та технічні засоби захисту інформації від витоку каналами побічних електромагнітних випромінювань і наведень;

– розробляти техніко-економічне обґрунтування з комплексного захисту інформації в комп'ютерних системах та мережах;

– розробляти технічну документацію на засоби комплексного захисту інформації в комп'ютерних системах та мережах;

– здійснювати спецдослідження засобів електронної обчислювальної техніки з метою визначення ступеню їх захищеності;

– здійснювати спецдослідження засобів електронної обчислювальної техніки з метою виявлення закладок;

– здійснювати контроль ефективності захисту інформації в комп'ютерних системах та мережах від витоку каналами побічних електромагнітних випромінювань і наводок;

– розробляти технічні вимоги з інженерного захисту об'єктів з

комп'ютерними системами та мережами, що будуються і реконструюються;

– вести наукові дослідження зі створення сучасних ефективних засобів комплексного захисту інформації в комп'ютерних системах та мережах;

– освоювати науково-технічну документацію сучасних засобів комплексного захисту інформації в комп'ютерних системах та мережах, оцінювати їх ефективність і реалізовувати у практичній діяльності.

Ця кваліфікаційна характеристика може бути базовою для формування кваліфікаційних характеристик спеціалістів таких спеціалізацій, як: "Програмно-апаратні засоби захисту інформації в комп'ютерних системах", "Інженерно-технічні засоби захисту інформації в комп'ютерних системах", "Захист інформації в спеціалізованих комп'ютерних системах", "Комплексний захист інформації в комп'ютерних системах та мережах" тощо. Крім того, вона також може бути використана з відповідними змінами, що відображають специфіку галузі, під час підготовки спеціалістів з захисту інформації в комп'ютерних системах та мережах для управління виробництвом, технологічними та енергетичними комплексами, рухом транспорту тощо [32].

Професійне призначення та сфера діяльності фахівця.

Випускник відповідно до фундаментальної і спеціальної підготовки повинен здійснювати наступні види професійної діяльності: проектно-конструкторська; організаційно-технологічна; експлуатаційна; організаційно-управлінська.

Проектно-конструкторська діяльність:

– розробка проектів нормативних і методичних матеріалів, що регламентують роботи по захисту інформації, а також положень, інструкцій і інших організаційно-розпорядливих документів;

– участь у розробці нових систем апаратури контролю, засобів автоматизації контролю, моделей і систем захисту інформації;

– участь в аналізі технічних завдань на проектування, виконання технічних і робочих проектів підсистем інформаційної безпеки автоматизованих систем, з урахуванням діючих нормативних і методичних документів;

Організаційно-технологічна діяльність:

– виконання повного робіт, пов'язаних з комплексним забезпеченням інформаційної безпеки конкретних автоматизованих систем на основі розроблених програм і методик, зокрема із забезпеченням вимог нормативних документів, що регламентують режим дотримання державної таємниці;

– аналіз матеріалів організацій і підрозділів відомства з метою підготовки рішень по забезпеченню захисту інформації;

– аналіз існуючих методів і засобів, які вживалися для контролю і захисту інформації, розробка пропозицій по їх вдосконаленню і підвищенню їх ефективності;

– участь в роботах по проведенню оцінки техніко-економічного рівня і ефективності пропонованих і реалізованих організаційно-технічних рішень.

Експлуатаційна діяльність:

– здійснення регламентних робіт, пов'язаних з комплексним забезпеченням інформаційної безпеки конкретних автоматизованих систем, і робіт, здійснюваних у режимах нештатних ситуацій, зокрема заходів, обов'язкових для автоматизованих систем, що містять відомості, що становлять державну таємницю;

– аналіз експлуатаційної та іншої документації організації і підрозділів відомства з метою підготовки рішень по вдосконаленню підсистем, що забезпечують захист інформації;

– забезпечення ефективного використання засобів автоматичного контролю, виявлення і закриття можливих каналів витоку конфіденційних відомостей;

Організаційно-управлінська діяльність:

– виконання оперативного управління діяльністю організацій по комплексному забезпеченню інформаційної безпеки конкретних автоматизованих систем на основі розроблених програм і методик;

– поточний аналіз матеріалів з метою підготовки рішень по оперативному управлінню процесами забезпечення режиму захисту конфіденційної інформації;

– робота за оцінкою техніко-економічного рівня і ефективності запропонованих і реалізуємих організаційно-управлінських рішень.

Фахівець із захисту інформації винний вміти:

– вирішувати основні задачі на обчислення меж функцій, їх диференціювання і інтеграцію, на розкладання функцій у, включаючи оцінку якості рішень прикладних завдань; вирішувати прості звичайні диференціальних рівняння і лінійні системи рівнянь;

– оперувати з елементами числових і кінцевих полів, кілець, підстановками, багаточленами, матрицями; вирішувати системи рівнянь над полями і кільцями вирахувань;

– досліджувати прості геометричні об'єкти по їх рівняннях у різних системах координат; описувати будову основних класів геометричних груп;

– застосовувати стандартні методи і моделі до рішення типових теоретико-імовірнісних завдань і стандартних завдань математичної статистики;

– використовувати стандартні статистичні пакети і давати змістовне пояснення одержуваним результатам;

– працювати на сучасних ПЕОМ на рівні користувача під управлінням основних операційних систем;

– застосовувати на практиці основні законі загальної фізики і оцінювати чисельні порядки величин, характерних для різних розділів природознавства;

– використовувати сучасні засоби розробки програмного забезпечення, включаючи сучасний призначений для користувача інтерфейс, на мовах високого рівня і мовах СУБД, бібліотеки об'єктів і класів для вирішення завдань створення і супроводу автоматизованих систем;

– виявляти можливі способи порушення інформаційної безпеки при роботі автоматизованих систем обробки інформації і використовувати засоби і можливості сучасних ЕОМ і їх мереж, мікропроцесорів, операційних систем, СУБД для проектування і реалізації засобів забезпечення інформаційної безпеки;

– реалізовувати основні структури даних на мовахпрограмування високого рівня;

– ефективно програмувати основні алгоритми сортування і пошуку на мовах програмування високого рівня;

– вибирати оптимальні в конкретних умовах структури даних і алгоритми;

– аналізувати основні механізми, реалізовані в сучасних операційних системах і СУБД, і модифікувати їх для вирішення завдань забезпечення інформаційної безпеки;

– проектувати бази даних і розподілені системи обробки інформації, забезпечення безпеки даних, що володіють необхідними характеристиками;

– аналізувати технології обробки даних у розподілених системах з метою оптимізації їх продуктивності й підвищення надійності функціонування;

– у рамках завдань забезпечення інформаційної безпеки вирішувати питання використання радіоелектронної апаратури і інших технічних засобів;

– застосовувати основні методи аналізу радіоелектронних систем, що становлять технічну базу комплексних систем забезпечення інформаційної безпеки;

– ставити завдання і інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів контролю характеристик автоматизованих систем;

– застосовувати типові методи проектування й оцінки ефективності складних систем в області своєї діяльності, застосовувати стандарти за оцінкою захищеності автоматизованих систем при їх аналізі й проектуванні;

– застосовувати діючу законодавчу базу в області інформаційної безпеки для забезпечення необхідних дій професійної діяльності, застосовувати правові акти в області інформаційної безпеки й захисту державної таємниці в конкретній сфері діяльності, включаючи адекватні організаційні заходи;

– застосовувати стандартні криптографічні рішення для захисту інформації і кваліфіковано оцінювати їх якість;

– використовуючи сучасні методи і засоби розробляти і оцінювати моделі і політику безпеки;

– реалізовувати системи захисту інформації в автоматизованих системах відповідно до стандартів за оцінкою захищених систем;

– практично вирішувати задачі захисту програм і даних програмно-апаратними засобами і давати оцінку якості пропонованих рішень;

– визначати і вимірювати параметри небезпечних сигналів для технічних каналів просочування інформації і визначати ефективність захисту від просочування інформації;

– застосовувати системний підхід до забезпечення інформаційної безпеки в різних сферах діяльності, включаючи комплекс організаційних заходів, що враховують особливості функціонування підприємства й вирішуваних ними завдань;

– проектувати й реалізовувати комплексну систему захисту інформації оцінювати її якість.

Інформаційна безпека стала однією з ключових складових національної безпеки в сучасному світі. Зростання кількості кіберзагроз, кібератак та порушень інформаційної безпеки свідчить про необхідність надійного захисту інформації та критичних інфраструктур. Країни Європейського Союзу (ЄС) не є винятком і активно працюють над розвитком спеціалізованих програм та ініціатив з підготовки фахівців у галузі інформаційної безпеки.

Одним із основних методів підготовки фахівців в галузі інформаційної безпеки в ЄС є запровадження спеціалізованих освітніх програм. Багато університетів та вищих навчальних закладів пропонують магістерські програми та курси, які спеціалізуються саме на кібербезпеці. Ці програми зазвичай включають в себе вивчення таких тем, як кібернетичні загрози, криптографія, захист мереж та кібернетичні атаки. Студенти отримують поглиблені знання та навички, необхідні для роботи у галузі інформаційної безпеки.

Для ефективної підготовки фахівців в галузі інформаційної безпеки, країни ЄС розвивають партнерські відносини з приватним сектором. Багато компаній, що спеціалізуються на кібербезпеці, активно взаємодіють з університетами та навчальними закладами, надаючи їм доступ до актуальних технологій та знань. Це сприяє практичній підготовці студентів та сприяє розвитку інновацій в галузі кібербезпеки.

Багато країн ЄС створюють спеціалізовані центри кібернетичного навчання, які надають підтримку та ресурси для навчання та дослідження в галузі інформаційної безпеки. Ці центри забезпечують доступ до сучасних

лабораторій, тренувальних площадок та експертних знань. Вони також відіграють важливу роль у поширенні найкращих практик та стандартів кібербезпеки

Країни ЄС активно інвестують у наукові дослідження в галузі інформаційної безпеки. Університети та наукові інститути здійснюють дослідження, спрямовані на виявлення нових загроз, розробку нових методів захисту та покращення існуючих систем. Це сприяє розвитку інновацій та підвищенню рівня інформаційної безпеки в ЄС.

Організація спеціалізованої підготовки в галузі інформаційної безпеки в країнах ЄС включає в себе широкий спектр ініціатив, від спеціалізованих освітніх програм до наукових досліджень та співпраці з приватним сектором. Ці заходи спрямовані на забезпечення надійного захисту інформації та кіберінфраструктури в умовах зростаючих кіберзагроз. Розвиток галузі інформаційної безпеки в ЄС є ключовим завданням для забезпечення стабільності та безпеки в цифровому світі.

Аналіз інформації, представленої на сайтах ведучих ВУЗів ЄС, що займаються підготовкою фахівців з напрямку “Інформаційна безпека”, дозволив виявити ряд висновків, реалізація яких дозволяє забезпечити якісну підготовку фахівців в області захисту інформації.

Забезпечення тісного зв'язку навчального процесу з науковими дослідженнями в області інформаційної безпеки. Як відомо, якість навчання багато в чому визначається глибиною відповідних наукових досліджень. Надзвичайна наукоемкість інформаційних технологій вимагає залучення великого числа фахівців і могутнього технічного забезпечення. Дослідження в області інформаційної безпеки до недавніх часів проводилися тільки в закритих і військових вузах. Стрімкий розвиток інформаційних технологій стимулює цивільні вузи до інтенсивного нагромадження власного досвіду, створенню своїх наукових шкіл. На сьогоднішній день склалася наукова школа в області криптографії; по

технічних засобах захисту; правовим питанням захисту інформації; захисту комп'ютерних систем від шкідливих програм.

Матеріально-технічне забезпечення навчального процесу. Додаткові труднощі при підготовці фахівців із захисту інформації виникають і через суворість існуючих вимог до матеріально-технічного забезпечення навчального процесу. Практичні й лабораторні заняття повинні проводитися в спеціально обладнаних приміщеннях, із застосуванням сучасної обчислювальної техніки. Для забезпечення занять з дисциплін спеціалізації потрібні спеціальні технічні засоби (заставні пристрої, скануючи радіоприймачі, прилади нічного бачення, портативні металодетектори тощо), придбання яких для більшості вузів просто не представляється можливим. Значних витрат вимагає ліцензійне програмне забезпечення, видаткові матеріали, доступ в Інтернет. Рішення цієї проблеми знаходять шляхом інтеграції з промисловими підприємствами, що, з одногу боку, беруть на себе матеріально-технічне забезпечення ВУЗів, а з іншої, задовольняють власні потреби в молодих фахівцях.

Забезпечення навчального процесу педагогічними кадрами вищої кваліфікації. Рішення даної проблеми вирішується за допомогою організації короткострокових курсів підвищення кваліфікації, проведення семінарів і конференцій по обміну досвідом. Нестачу кадрів вищої кваліфікації вимагає без зупинного моніторингу якості навчання.

Висновки до розділу 2

Для розробки обґрунтованих рекомендацій з оптимізації підготовки фахівців в сфері захисту інформації в Україні порівняємо технології навчання в США й країнах ЄС й виділимо ряд моментів, що доцільно використовувати в нашій державі.

У США позитивними моментами підготовки фахівців у галузі захисту інформації є:

1) широке використання міжнародних консорціумів;

2) використання для навчання самих передових технологій;

3) здійснення навчального процесу на найсучаснішому устаткуванні;

4) акцент на проведення курсів, орієнтованих на використання власних програмних продуктів для захисту інформації;

5) висока мобільність навчальних програм;

6) включення в навчальні плани підготовки менеджерів і фахівців з бізнесу дисциплін, безпосередньо зв'язаних із захистом інформації бізнес-структур;

7) регулярне проведення семінарів, тренінгів, конференцій із проблем захисту інформації.

Аналіз програм підготовки фахівців в галузі інформаційної безпеки країн ЄС дозволяє виділити наступні особливості навчання:

1) багато напрямків підготовки й перепідготовки з інформаційної безпеки;

2) спрямованість навчання на заглиблену теоретичну підготовку фахівців з найбільш загальних аспектів безпеки і ознайомлення з відносно повним спектром методів і систем захисту інформації;

3) акцент на практичну спрямованість навчання;

4) орієнтація на вивчення конкретних продуктів і правил їхньої експлуатації;

5) висока мобільність змісту курсів, що читаються, (швидка реакція на нові технології захисту інформації);

6) міжнародна співпраця (організація закордонних стажувань);

7) фінансова підтримка (Багато країн ЄС надають фінансову підтримку студентам у вигляді стипендій, грантів та інших видів фінансування. Це допомагає знизити фінансове навантаження на студентів та зробити освіту більш доступною).

РОЗДІЛ 3
АНАЛІЗ СТАНУ ЦИФРОВИХ СИСТЕМ КІБЕРЗАХИСТУ ТА ПІДГОТОВКИ КАДРІВ З ЦИФРОВОЇ БЕЗПЕКИ В УКРАЇНІ

3.1. Новітні тенденції та перспективи розвитку цифрових інструментів кіберзахисту в Україні

Мінливість ландшафту кіберзагроз, частоти їх появи, складність і цільовий характер кібератак вимагає еволюції діючих правил кібербезпеки та переходу до поєднання технологій запобігання, виявлення і реагування на кібератаки.

Класичні цифрові інструменти кіберзахисту дозволяють, як правило, виявляти відомі кібератак, однак їх можливості, нажаль, не завжди дозволяють зупинити невідомі атаки, спеціально створені з метою обходу наявної системи захисту за рахунок зміни сигнатур і шаблонів поведінки.

Традиційним рішенням кіберзахисту у більшості випадків властиві такі моменти, як захист на основі сигнатурних файлів, виявлення переважно відомі кіберзагрози, базування, як правило, на поведінці старих кіберзагроз і кібератак (не здійснюють глибокий моніторинг активності з аналізом причинно-наслідкового зв'язку), ненадання інформації про кібератаки тощо.

У підсумку ми бачимо все наростаючий розрив у виявленні невідомих кіберзагроз і кібератак. Зокрема, за даними Verizon Data Breach Investigations Report 2016, спостерігається стійке зростання кіберінцидентів, за яких час компрометації системи займав день чи навіть кілька годин, причому загроза може скомпрометувати систему за хвилини або години, в той час як реакція власника системи зазвичай займає тижні, місяці або навіть роки [69].

Зазначене говорить про те, що кіберзловмисники стають все більш

ефективними, а шкідливе програмне забезпечення все більш витонченим. Також розвиваються і техніки виконання кібератак, кібератаки стали цілеспрямовані, скоординовані і з використанням різноманітних векторів.

Тому ми все частіше чуємо про рішення кіберзахисту «наступного покоління», до яких прийнято відносити, зокрема:

– системи міжмережевого екранування нового покоління (англ. *Next Generation Firewall, NGFW*);

– системи уніфікованого управління загрозами (англ. *Unified Threat Management, UTM*);

– системи запобігання вторгненням нового покоління (англ. *Next Generation Intrusion Prevention System, NGIPS)*.

Такі системи представляють собою безпековий продукт, який може виконувати одночасно кілька функцій безпеки в рамках одного пристрою: брандмауер мереж, запобігання вторгнень в мережу, антивірусний шлюз, антиспамовий шлюз, VPN, фільтрація контенту, балансування навантаження, запобігання витоку даних і звітність (таблиця 2.2).

У галузі захисту від сучасних кібератак на думку експертів [70] однією із новітніх тенденцій є використання аналітичних систем кібербезпеки із застосуванням систем машинного навчання і штучного інтелекту на великих обсягах даних (англ. *Machine Learning-based Security Analytics using Big Data*). Ці системи дозволяють виявляти відхилення у поведінці систем чи користувачів від норми і таким чином виявляти більшість небезпечних кібератак.

Перспективним є застосування таких систем для завдань кібербезпеки у вигляді платформ UEBA (*User Entity and Behavior Analytics*). Сучасні так звані детектори аномальної активності персоналу підвищують імовірність виявлення мотивованого інсайдера, що зменшує ризики виникнення кіберінцидентів.

Таблиця 2.2 – Порівняльний аналіз функцій систем NGFW, UTM та NGIPS

NGFW	**UTM**	**NGIPS**
міжмережеве екранування (firewall)	міжмережеве екранування (firewall)	–
аналіз програм та за стосунків та повна видимість стека	аналіз програм та за стосунків та повна видимість стека	аналіз програм та за стосунків та повна видимість стека
запобігання вторгненням (IPS)	запобігання вторгненням (IPS)	запобігання вторгненням (IPS)
розблокування зашифрованих сеансів, перевірка зашифрованих пакетів, виявлення та блокування загроз (SSL and SSH inspection)	розблокування зашифрованих сеансів, перевірка зашифрованих пакетів, виявлення та блокування загроз (SSL and SSH inspection)	–
перевірка та фільтрація пакетів (DPI)	фільтрація веб-контенту (Web content filtering)	аналіз і поінформованість про вміст контенту (Content awareness)
	антиспам, антивірусний та антишпигунський захист	
виявлення зловмисного програмного забезпечення на основі репутації (reputation-based malware detection)	–	аналіз і поінформованість про вміст контенту (Content awareness)
забезпечення якості обслуговування (Quality of Service (QoS) functionality)	–	–
–	формування трафіку (traffic shaping) / управління пропускною здатністю (bandtwith control)	–
–	запобігання витоку даних (Data Loss Prevention, DLP)	–

Зустрічаються й суто унікальні цифрові інструменти кіберзахисту, серед яких, за власними спостереженнями автора роботи, найбільшої уваги заслуговують:

– системи виявлення загроз на кінцевих точках (англ. *Endpoint Detection and Response, EDR*) [71];

– технологія *ESET LiveGrid* [72];

– технологія *Arbor Peakflow SP* для запобігання DDoS-атак [73];

– технологія розширеного захисту від зловмисних програм (англ. *Advanced Malware Protection, AMP*) [74];

– програмне забезпечення для полювання на кіберзагрози (англ. *cyber threat hunting*) [75];

– технологія *Cyber Threat Defense (CTD)* на базі аналізу мережевої телеметрії для забезпечення захисту від кіберзагроз [76].

Як бачимо, на ринку наявна значна кількість ефективних цифрових інструментів кіберзахисту. Однак в Україні існує ряд проблемних питань щодо механізмів впровадження та легітимного використання таких цифрових інструментів для кіберзахисту ДІР.

3.2. Питання стратегії і тактики ведення інформаційних війн фахівцями з інформаційної та кібербезпеки

Інформаційні війни, що виявляються в сфері інформаційної безпеки, в сучасному світі стають не тільки актуальними, але й невід'ємною складовою геополітичного ландшафту. Розуміння стратегій і тактик, використовуваних у цих війнах, вкрай важливе для розвитку ефективних заходів інформаційного захисту. Комп'ютерні злочини є одним зі способів ведення інформаційної війни з метою ідеологічного й психологічного впливу на свідомість окремого індивіда, соціальних груп, розпалення етнічної й релігійної ворожнечі. Тому при підготовці фахівців в області захисту інформації пропонується включити питання, зв'язані методологічними принципами ведення інформаційних операцій. Фахівець із захисту інформації зобов'язаний знаті стратегію й тактикові ведення інформаційної війни, що уражають фактори інформаційної зброї й прийоми протидії інформаційним операціям.

Стратегічний аспект інформаційних війн включає в себе планування і довгострокове визначення цілей. Однією з ключових стратегій є

маніпуляція інформаційним простором для досягнення політичних, економічних або військових переваг. Це може включати розповсюдження дезінформації, кероване впливання на громадську думку та атаки на інформаційні системи. Стратегічна адаптація полягає в визначенні слабких місць супротивника і виборі оптимальних методів впливу, таких як психологічна війна або формування публічної думки через мас-медіа.

Тактика інформаційних війн включає конкретні дії, спрямовані на досягнення стратегічних цілей. Однією з тактик є кібератаки на інформаційні системи. Це може виявитися у витоку чутливої інформації, розповсюдженні вірусів чи атаках на критичні інфраструктурні об'єкти. Іншою тактикою є використання соціальних мереж та мас-медіа для формування сприятливого образу або дискредитації супротивника. Важливою тактичною складовою є також контроль за потоком інформації, яка потрапляє до громадськості.

Сучасні інформаційні війни вимагають від експертів інформаційної безпеки розуміння та вироблення стратегічних та тактичних відповідей. Ефективна боротьба із загрозами в інформаційному просторі вимагає поєднання технічних засобів захисту інформаційних систем із стратегічним мисленням, що враховує глибинні аспекти інформаційних війн. Дослідження та розвиток таких стратегій і тактик є невід’ємною частиною забезпечення інформаційної безпеки у сучасному світі.

Важливим аспектом стратегічного аналізу інформаційних війн є розгляд аспектів гібридної війни, де використовуються не лише технічні, але й соціальні, економічні та політичні засоби впливу. Розвиток глибокого розуміння соціокультурного контексту є стратегічною перевагою при аналізі інформаційних кампаній.

Стратегічні відповіді повинні орієнтуватися на вдосконалення методів виявлення та відвернення кіберзагроз, в тому числі шляхом розвитку технологій штучного інтелекту та машинного навчання для попередження інцидентів.

На тактичному рівні, кіберзаходи, такі як моніторинг мережі, аналіз збоїв безпеки, інцидент-відгуки та відновлення після атак, стають невід’ємною частиною стратегій інформаційної безпеки. Застосування інтелектуальних систем, які можуть передбачати та реагувати на нові загрози, є ключовим елементом тактичного заходу.

У сфері контролю за інформаційним впливом, акцент робиться на розвитку аналітичних інструментів, що дозволяють виявляти та аналізувати масові потоки даних для ідентифікації дезінформації та маніпуляцій громадською думкою.

Невід'ємною частиною стратегії відповіді на інформаційні війни є освіта та тренування. Створення кваліфікованих інформаційних аналітиків та спеціалістів із кібербезпеки, які здатні розпізнавати та протидіяти інформаційним загрозам, відіграє важливу роль у забезпеченні безпеки в інформаційному просторі.

Створення кваліфікованих інформаційних аналітиків та фахівців із кібербезпеки є стратегічно важливим етапом у забезпеченні безпеки в інформаційному просторі. Отримання необхідних компетенцій та навичок для розпізнавання та протидії інформаційним загрозам може відігравати вирішальну роль в боротьбі з сучасними викликами інформаційної безпеки.

1. Професійна Освіта та Навчання

Розвиток програм професійної освіти та навчання є критичним для формування експертів у галузі інформаційної безпеки. Навчальні заклади повинні надавати високоякісні курси з аналізу даних, кібербезпеки та кіберінтелігенції для формування необхідних компетенцій.

2. Сертифікація та Спеціалізовані Курси

Проведення сертифікаційних програм та спеціалізованих курсів дозволяє фахівцям вдосконалювати свої навички та підтримувати їхню актуальність у світі швидкозмінюючих технологій. Здобуття акредитованих сертифікатів стає маркером високого професійного рівня.

3. Практичний Досвід та Симуляційні Вправи

Важливою частиною підготовки фахівців є можливість отримати практичний досвід у реальних або симулюваних умовах. Спеціалізовані тренувальні площадки дозволяють аналізувати та вирішувати ситуації, пов'язані з інформаційною безпекою, без реального ризику.

4. Міждисциплінарний Підхід

Забезпечення повноцінної підготовки передбачає міждисциплінарний підхід. Фахівці з інформаційної безпеки повинні мати знання не лише у сфері технологій, а й в галузі права, психології та соціології, оскільки інформаційні загрози мають комплексний характер.

5. Співпраця з Приватним Сектором

Активна співпраця з приватним сектором є важливою для адаптації навчальних програм до сучасної реальності. Взаємодія з компаніями, які активно займаються кібербезпекою, дозволяє фахівцям вивчати передові технології та стратегії.

6. Сприяння Дослідженням та Інноваціям

Підтримка наукових досліджень та інновацій у галузі інформаційної безпеки сприяє розвитку нових технологій та методів, що можуть використовуватися для протидії загрозам.

Створення кваліфікованих кадрів є стратегічно важливою складовою глобальної інформаційної безпеки, оскільки це дозволяє ефективно відповідати на виклики та забезпечувати стійкість інформаційного простору.

Загрози інформаційної безпеки стають все більш складними і виразними. Стратегії та тактики відповіді на ці загрози повинні бути не лише реактивними, але й передбачливими та інноваційними. Здатність адаптуватися до нових викликів і поєднання технічних та соціокультурних засобів захисту стають визначальними для забезпечення інформаційної безпеки в сучасному світі.

3.3. Шляхи удосконалення цифрового інструментарію кіберзахисту державних інформаційних ресурсів

З набуттям у 2018 році чинності Законом України «Про основні засади забезпечення кібербезпеки України» настав новий етап розвитку організаційно-правових основ забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі. Можна з упевненістю стверджувати, що цей Закон здійснив запуск комплексного процесу розбудови національної системи кібербезпеки, у тому числі системи захисту від кіберагресії.

Система кіберзахисту в Україні поки що лише будується. І основні наступні завдання – цілком зрозумілі. Першочергово Уряду необхідно визначити вимоги щодо кіберзахисту ОКІІ, у тому числі ОКІІ, в яких обробляються ДІР, порядок формування переліку ОКІІ, перелік таких об’єктів та порядок їх внесення до державного реєстру ОКІІ, порядок формування та забезпечення функціонування цього реєстру. Натомість власникам ІТС, в яких обробляються ДІР, в свою чергу, необхідно впровадити достатньо надійну систему кіберзахисту, з урахуванням усіх вимог законодавства у сфері захисту інформації.

На сьогодні розробити і впровадити абсолютно дієву КСЗІ, що дозволить забезпечувати належний рівень кіберзахисту ДІР, навряд чи можливо, оскільки при наявності достатнього обсягу часу і сучасних програмно-технічних засобів можна подолати будь-який опір системи кіберзахисту. Тому взагалі йдеться про достатній рівень якості роботи КСЗІ, при якому фінансові витрати на її побудову та експлуатацію, ризик успішної реалізації кібератак і розмір можливого збитку від них були б співрозмірними між собою та прийнятними.

При обмеженому обсязі коштів, що виділяються на утримання органів державної влади, та за умови недостатнього усвідомлення значною

частиною керівників цих органів значення кіберзахисту ДІР для національної безпеки, фінансування заходів із захисту ДІР здійснюється, як правило, за залишковим принципом. Це не дозволяє своєчасно і в повному обсязі здійснити в органах державної влади передбачені законодавством заходи щодо захисту ДІР.

Найбільш характерним порушенням є функціонування ДІР, які підключені до глобальної мережі передачі даних Інтернет, без дотримання вимог законодавства у сфері захисту інформації. Стан захисту ДІР залишається на досить низькому рівні, що, у разі здійснення успішних кібератак на ДІР, підвищує ймовірність нанесення шкоди інтересам громадян, суспільства та держави в цілому.

Загалом система КСЗІ потребує істотного осучаснення, аж до її заміни на інші системи захисту. Сама ідея, внутрішня структура й модель впровадження КСЗІ здебільшого не відповідає вимогам сучасного кіберзахисту. Складно ігнорувати той факт, що КСЗІ була побудована для значної частини ДІР, на які було здійснено успішні кібератаки в 2015-2017 роках. Це вкотре спонукає до здійснення ґрунтовного перегляду чинних законодавчих документів і технічних вимог щодо побудови систем захисту інформації з метою підвищення стану кіберзахищеності ДІР в державних установах.

В умовах сьогодення цінності інформаційного суспільства, євроінтеграційні процеси, що впливають на подальший розвиток України, її національної інформаційної інфраструктури, електронного врядування, забезпечення кібербезпеки, вимагають від держави дієвих кроків щодо належного правового, організаційного та науково-технічного забезпечення реформування системи захисту інформації, націленого на забезпечення кіберзахищеності ДІР.

На сьогодні у рамках роботи виділено такі проблемні питання у сфері кіберзахисту ДІР:

– невідповідність інфраструктури електронних комунікацій держави,

рівня її розвитку та захищеності сучасним вимогам;

– недостатній рівень захищеності ДІР від кіберзагроз;

– безсистемність заходів кіберзахисту ДІР;

– інертність до питань кіберзахисту ДІР в цілому (спочатку відбувається кібератака, а тоді вже вживаються заходи щодо ліквідації наслідків кібератаки та впроваджуються, як правило, мінімальні механізми кіберзахисту ДІР);

– недостатній рівень координації, взаємодії та інформаційного обміну між суб'єктами забезпечення кібербезпеки;

– висока залежність від іноземних засобів захисту і продукції у ІТ-сфері, відсутність власних розробок та виробництва засобів захисту і продукції у ІТ-сфері та сфері кібербезпеки;

– відсутність дієвої державної системи сертифікації засобів захисту інформації;

– низький рівень цифрової грамотності, кібергігієни обслуговуючого персоналу функціонування ДІР;

– безсистемність підготовки кадрів у сфері кібербезпеки.

За результатами проведення дослідження стану кіберзахисту ДІР пропонуються наступні шляхи удосконалення цифрового інструментарію кіберзахисту ДІР:

– оновлення системних механізмів реалізації Національної програми інформатизації, яка тривалий час фактично не виконувалася;

– впровадження єдиної платформи захищених електронних комунікацій для органів державної влади;

– визначення єдиних правил та вимог до створення, ведення і функціонування ДІР, а також електронної взаємодії ДІР;

– закріплення на законодавчому рівні можливості використання міжнародних стандартів кібербезпеки (на кшталт ISO/IEC 27001 та ISO/IEC 15408);

– забезпечення функціонування єдиного дата-центру резервного

збереження інформації і відомостей ДІР;

– налагодження якісного рівня координації, взаємодії та інформаційного обміну між суб'єктами забезпечення кіберзахисту ДІР та командою CERT-UA;

– налагодження комплексної співпраці з міжнародними урядовими організаціями для обміну досвідом щодо впровадження кращих рішень цифрового інструментарію кіберзахисту ДІР;

– збільшення напрямків прикладних та фундаментальних досліджень у галузі ТЗІ та КЗІ;

– сприяння виробництву вітчизняних програмних продуктів, зокрема вітчизняної операційної системи, вітчизняного антивірусного програмного забезпечення тощо;

– сприяння виробництву конкурентоспроможних вітчизняних засобів захисту інформації;

– завершення робіт з розроблення технічних регламентів засобів ТЗІ / КЗІ та оцінки їх відповідності, а також впровадження системи їх сертифікації відповідно до кращих міжнародних практик;

– впровадження механізмів визнання в Україні іноземних сертифікатів на засоби ТЗІ / КЗІ, а також взаємного визнання українських та іноземних сертифікатів;

– розроблення механізмів залучення фізичних і юридичних осіб до виконання завдань кіберзахисту ДІР у рамках державно-приватного партнерства на умовах аутсорсингу (краудфандингу тощо), у тому числі у сфері оцінювання відповідності засобів захисту.

Висновки до розділу 3

У 2018 році повноцінно запрацювали Стратегія кібербезпеки України, і прийнятий у 2017 році Закон України «Про основні засади забезпечення кібербезпеки України» – державні органи активно

здійснюють їх реалізацію, у тому числі в частині забезпечення кіберзахисту державних інформаційних ресурсів.

За результатами аналізу державної політики в сфері захисту інформації встановлено, що кіберзахист державних інформаційних ресурсів має забезпечуватися власником інформаційно-телекомунікаційної системи, в якій обробляються державних інформаційних ресурсів, шляхом впровадження в такій інформаційно-телекомунікаційній системі комплексної системи захисту інформації з підтвердженою відповідністю. При цьому для створення комплексної системи захисту державних інформаційних ресурсів повинні використовуватися засоби захисту інформації, що мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері технічного та криптографічного захисту інформації.

Виявлено високу залежність України від іноземних засобів захисту і продукції у ІТ-сфері, відсутність власних розробок та виробництва засобів захисту і продукції у ІТ-сфері та сфері кібербезпеки, що можуть застосовуватися для кіберзахисту державних інформаційних ресурсів. Означене питання є критичним, оскільки для держав, які не володіють власними розробками та виробництвом засобів і продукції у ІТ-сфері, у тому числі у сфері кіберзахисту, загрози від використання таких технологій збільшуються, по-перше, у зв’язку з постійним відставанням від технологічного прогресу, по-друге, внаслідок можливих «вбудованих» та незадокументованих недружніх функцій в іноземних засобах та технологіях.

Проведений аналіз міжнародних стандартів у сфері інформаційних технологій, безпеки та захисту інформації, кібербезпеки, безпеки мережевих та інформаційних систем свідчить про те, що нормативно-правові акти, що забезпечують державне регулювання та контроль за додержанням законодавства у сфері захисту інформації, потребують постійного оновлення і вдосконалення з урахуванням євроінтеграційних

процесів, які сьогодні відбуваються в нашій країні. Також потребує істотного осучаснення базова система комплексної системи захисту інформації, оскільки вона не завжди відповідає сучасним викликам і загрозам у кіберпросторі.

Запропоновано шляхи удосконалення цифрового інструментарію кіберзахисту державних інформаційних ресурсів, а також розроблено пропозиції та рекомендації щодо забезпечення кіберзахисту державних інформаційних ресурсів в Україні в умовах сьогодення. Ці пропозиції та рекомендації можуть бути використані в роботі Адміністрації Державної служби спеціального зв'язку та захисту інформації України з метою вдосконалення функціонування державних інформаційних ресурсів. Крім того, зазначені пропозиції та рекомендації можуть допомогти керівникам органів державної влади і фахівцям сфери захисту інформації підвищити рівень обізнаності щодо особливостей кіберзахисту державних інформаційних ресурсів та інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом.

ВИСНОВКИ

Відповідно до поставлених завдань було досліджено ключові аспекти використання цифрових інструментів кіберзахисту в системах публічного управління. Отримані результати аналізу дозволили зробити висновки щодо перспектив їх розвитку в контексті публічного управління.

1. Визначено організаційно-правові засади формування державної політики у сфері інформаційної безпеки та кіберзахисту.

Аналіз існуючих законодавчих актів та стратегій, які регулюють формування державної політики у сфері інформаційної безпеки, дозволяє зробити важливі висновки. Україна визнає необхідність вдосконалення своїх механізмів кіберзахисту через прийняття та впровадження ключових законодавчих актів, які орієнтовані на забезпечення ефективного контролю та реагування на кіберзагрози. Законодавчі ініціативи, спрямовані на регулювання кібербезпеки, надають правовий фундамент для розвитку стратегічних напрямків у цій галузі.

Визначення ключових компонентів та принципів організаційно-правового забезпечення кіберзахисту свідчить про необхідність комплексного підходу до цього питання. Впровадження сучасних організаційних та правових механізмів базується на розумінні важливості співпраці між державними органами, приватним сектором та громадськістю. Основні компоненти організаційно-правового забезпечення включають створення ефективної системи моніторингу, вдосконалення процедур реагування на інциденти та визначення чіткої відповідальності між різними структурами.

Загальний висновок полягає в тому, що для успішного формування державної політики у сфері інформаційної безпеки та кіберзахисту важливо поєднати сучасний законодавчий підхід з інноваційними методами управління та технологіями. Визначення конкретних заходів та покращень у цих двох напрямах дозволить країні ефективно протистояти

викликам у кіберпросторі та забезпечити стабільність її інформаційної безпеки.

2. Проведено аналіз цифрових інструментів, що використовуються для протидії кіберзагрозам та забезпечення нормальної функціонування систем управління.

В результаті проведеного аналізу цифрових інструментів кіберзахисту у сфері публічного управління визначено ключові аспекти, які визначають їхню важливу роль як складової частини забезпечення національної безпеки України. Ефективність цих інструментів виявилася критичною для протидії кіберзагрозам та забезпечення нормальної функціонування систем управління.

Серед ефективних інструментів кіберзахисту виділено такі:

– Фаєрвол: контролює трафік мережі та фільтрує його для запобігання несанкціонованому доступу.

– Антивірусне програмне забезпечення: виявляє, блокує та видаляє віруси, шкідливі програми та інші загрози для комп'ютерної системи.

– Системи виявлення та запобігання вторгнень: моніторять мережевий трафік для виявлення та запобігання атакам.

– Шифрування даних: застосування алгоритмів шифрування для захисту конфіденційної інформації під час передачі та зберігання.

– Мультифакторна аутентифікація: застосування декількох методів для перевірки ідентичності користувача.

– Системи моніторингу та журналювання подій: аналізують та реагують на події в інформаційних системах для виявлення загроз.

– Засоби аналізу вразливостей: сканують системи на предмет потенційних слабких місць та вразливостей.

Розширення та постійне оновлення цифрових інструментів є важливою складовою стратегії кіберзахисту в сфері публічного управління. Їх аналіз надає підстави для подальших стратегічних розробок

та удосконалення заходів кіберзахисту, а також формулювання конкретних рекомендацій щодо забезпечення національної безпеки в кіберпросторі.

3. Розглянуто актуальні вимоги до фахівців у сфері кіберзахисту з урахуванням специфіки публічного управління та сучасних викликів у кіберпросторі.

Підсумовуючи розгляд актуальних тенденцій та вимог до фахівців у сфері кіберзахисту з урахуванням специфіки публічного управління та сучасних викликів у кіберпросторі, можна визначити, що динамічний характер кіберзагроз та зростання інтерконектованості публічних інформаційних систем створюють унікальні виклики для фахівців у цій галузі.

Актуалізація навичок у сфері кіберзахисту вимагає врахування специфічних потреб публічного сектору, де діє державна чутливість і конфіденційність даних. Забезпечення кібербезпеки в публічному управлінні потребує не лише технічної експертизи, але й глибокого розуміння сучасних викликів, таких як кібершпигунство, кібертероризм та інші форми атак.

Зазначені вимоги висувають великі виклики перед системами підготовки фахівців у сфері кіберзахисту, вимагаючи гнучкості та постійного оновлення програм та педагогічних підходів. У контексті ростущого кількісного та якісного рівня кіберзагроз, важливість адаптивності та широкого спектру компетенцій у фахівців кіберзахисту в публічному управлінні визначається як стратегічний елемент забезпечення національної кібербезпеки.

4. Виокремлено важливі аспекти стратегії і тактики використання цифрових інструментів кіберзахисту у сфері публічного управління.

В контексті кіберзахисту у сфері публічного управління можуть бути розглянуті різноманітні стратегії, спрямовані на ефективне використання цифрових інструментів для забезпечення інформаційної безпеки. Деякі із можливих стратегій включають:

– стратегію адаптації: розробка інструментів, які можуть адаптуватися до кіберзагроз, що швидко змінюються. та вимог публічного сектору;

– стратегію захисту критичних інфраструктур: спрямована на захист та забезпечення безпеки ключових об'єктів та інфраструктури публічного управління;

– стратегію співпраці та обміну інформацією: закладання механізмів для ефективного обміну інформацією про кіберзагрози між публічними організаціями та іншими секторами;

– стратегію навчання та підготовки: розробка програм навчання та підготовки фахівців, які відповідають унікальним вимогам публічного сектору;

– стратегію інтеграції інновацій: впровадження новітніх цифрових технологій та інновацій для покращення кіберзахисту;

– стратегію взаємодії з приватним сектором: забезпечення співпраці та обміну інформацією з приватним сектором для спільного забезпечення кібербезпеки;

– стратегію забезпечення публічної свідомості: розробка заходів для підвищення рівня обізнаності та свідомості громадськості щодо кіберзагроз та заходів захисту.

Ефективна реалізація цих стратегій спрямована на досягнення високого рівня інформаційної безпеки в сфері публічного управління. Особлива увага приділяється взаємодії з іншими секторами, забезпечуючи стійке функціонування та ефективний захист критичних інформаційних ресурсів.

5. Запропонувати шляхи вдосконалення цифрових інструментів кіберзахисту у сфері публічного управління.

На основі проведеного аналізу цифрових інструментів кіберзахисту у сфері публічного управління запропоновано конкретні шляхи їх вдосконалення. Розглянуті проблеми та виклики виявили необхідність

вдосконалення функціоналу та ефективності застосування цих інструментів. Запропоновані шляхи включають в себе впровадження передових технологій, розробку інтегрованих систем захисту, підвищення кваліфікації фахівців та розширення співпраці з приватним сектором і міжнародними партнерами. Такі заходи спрямовані на забезпечення високого рівня кібербезпеки в публічному управлінні та покращення реакції на сучасні та еволюючі кіберзагрози.

Впровадження передових технологій передбачає проведення систематичного аналізу та оновлення існуючих технічних рішень для адаптації до сучасних кіберзагроз, а також використання штучного інтелекту, машинного навчання та аналітики для розпізнавання та протидії новим видам атак.

Розробка інтегрованих систем захисту включає створення комплексних систем, які об'єднують технічні та організаційні аспекти кіберзахисту для ефективного управління та реагування, а також впровадження механізмів миттєвого виявлення та реагування на інциденти за допомогою автоматизованих систем.

Підвищення кваліфікації фахівців вимагає організації систематичного професійного навчання та перепідготовки кадрів у галузі кіберзахисту; сприяння участі фахівців у міжнародних конференціях, тренінгах та обміні досвідом для ознайомлення з передовими практиками.

Розширення співпраці з приватним сектором і міжнародними партнерами має на меті встановлення ефективного механізму обміну інформацією та досвідом з приватним сектором щодо виявлення та запобігання кіберзагрозам. Цьому сприяє також активна участь у міжнародних ініціативах та партнерстві для обміну найкращими практиками та впровадження стандартів кібербезпеки.

Ці рекомендації спрямовані на вироблення комплексного підходу до кіберзахисту в публічному управлінні та забезпечення стійкості

інформаційних систем державного сектора перед сучасними загрозами кіберпростору.

СПИСОК ВИКОРИСТАНОЇ ЛИТЕРАТУРИ

1. Про інформацію: Закон України від 02.10.92 № 2657-XII // [Електронний ресурс]. Режим доступу: http://zakon.rada.gov.ua/laws/show/2657-12.

2. Про телекомунікації: Закон України від 18.11.2003 № 1280-IV // [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/1280-15.

3. Енциклопедичний словник з державного управління / уклад. : Ю.П. Сурмін, В.Д. Бакуменко, А.М. Михненко та ін.; за ред. Ю.В. Ковбасюка, В.П. Трощинського, Ю.П. Сурміна. – К. : НАДУ, 2010. – 820 с.

4. Маслянко П.П., Ліссов П.М. Інформаційні ресурси та засоби їх створення [Текст] // Вісн. Східноукр. нац. ун-ту ім. В. Даля – № 5 (111) – 2007. – с. 141-145. [Електронний ресурс]. – Режим доступу: http://lissov.kiev.ua/files/publications/kpi/Maslyanko_Lissov_InformativeResourcesCreation.pdf.

5. Марутян Р.Р. Інформаційні ресурси у системі забезпечення національної безпеки України. // [Електронний ресурс]. – Режим доступу: http://www.dsaua.org/index.php?option=com_content&view=article&id=114%3A2010-11-30-17-18-49&catid=66%3A2010-12-13-08-48-53&Itemid=90&lang=uk.

6. Кунанець Н., Липак Г. Європейський досвід створення консолідованих інформаційних ресурсів // [Електронний ресурс]. – Режим доступу: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/bv_2016_6_5.pdf.

7. Биков В.Ю. Відкрите навчальне середовище та сучасні мережні інструменти систем відкритої освіти // [Електронний ресурс]. – Режим доступу: http://lib.iitta.gov.ua/id/eprint/1159.

8. Пунченко О.П., Лазаревич А.А. Інформатизація як засіб репрезентації інформаційних ресурсів суспільства // [Електронний ресурс]. Режим доступу: http://vestnikzgia.com.ua/article/view/57498.

9. Кравченко М.С, Кєтриш О.С. Управління інформаційними ресурсами як інструмент управляння соціальними та економічними процесами в Україні // [Електронний ресурс]. Режим доступу: http://ves.pstu.edu/article/viewFile/105569/100702.

10. Про Національну програму інформатизації: Закон України від 04.02.98 № 74/98-ВР // [Електронний ресурс]. Режим доступу: http://zakon2.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80.

11. Угода про співробітництво у формуванні інформаційних ресурсів і систем, реалізації міждержавних програм держав - учасниць Співдружності Незалежних Держав у галузі інформатизації від 24.12.99 // [Електронний ресурс]. Режим доступу: http://zakon.rada.gov.ua/laws/show/997_842.

12. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII // [Електронний ресурс]. Режим доступу: http://zakon3.rada.gov.ua/laws/show/2163-19.

13. Концепція формування системи національних електронних інформаційних ресурсів: затверджено Розпорядженням Кабінету Міністрів України від 05.05.2003 № 259-р // [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/259-2003-%D1%80.

14. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 23.02.2006 № 3475-IV // [Електронний ресурс]. Режим доступу: http://zakon3.rada.gov.ua/laws/show/3475-15.

15. Про затвердження Положення про Реєстр інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління: Постанова Кабінету Міністрів України

від 03.08.2005 № 688 // [Електронний ресурс]. Режим доступу: http://zakon2.rada.gov.ua/laws/show/688-2005-%D0%BF.

16. Правові аспекти формування системи державних інформаційних ресурсів // [Електронний ресурс] / О.К. Юдін, С.С. Бучик // Безпека інформації. – 2014. – Т. 20 (1). – С. 76–82. – Режим доступу: http://jrnl.nau.edu.ua/index.php/Infosecurity/article/view/6578.

17. Гладиш С.В. Формування вимог щодо безпеки державних інформаційних ресурсів в телекомунікаційній мережі загального користування // Науково-технічний збірник «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні», вип. 1 (14), 2007.

18. Порядок взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах: затверджено постановою Кабінету Міністрів України від 16.11.2002 № 1772 // [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/1772-2002-%D0%BF. http://zakon.rada.gov.ua/laws/show/1772-2002.

19. Про захист інформації в автоматизованих системах: Закон України від 05.07.94 № 80/94-ВР // [Електронний ресурс]. Режим доступу: http://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80/ed19940705.

20. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.94 № 80/94-ВР // [Електронний ресурс]. Режим доступу: http://zakon2.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.

21. Порядок оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади: затверджено постановою Кабінету Міністрів України від 04.01.2002 № 3 // [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/3-2002-%D0%BF/ed20020104.

22. Порядок підключення до глобальних мереж передачі даних: затверджено постановою Кабінету Міністрів України

від 12.04.2002 № 522 // [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/522-2002-%D0%BF.

23. Про електронні документи та електронний документообіг: Закон України від 22.05.2003 № 851-IV // [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/851-15/ed20181107.

24. Про електронний цифровий підпис: Закон України від 22.05.2003 № 852-IV // [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/852-15.

25. Про електронні довірчі послуги: Закон України від 05.10.2017 № 2155-VIII // [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/2155-19.

26. Положення про Національний реєстр електронних інформаційних ресурсів: затверджено постановою Кабінету Міністрів України від 17.03.2004 № 326 // [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/326-2004-%D0%BF/ed20180529.

27. Національний реєстр електронних інформаційних ресурсів // [Електронний ресурс]. Режим доступу: https://e-resurs.gov.ua.

28. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 09.01.2007 № 537-V // [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/537-16.

29. Стратегія розвитку інформаційного суспільства в Україні: схвалено розпорядженням Кабінету Міністрів України від 15.05.2013 № 386-р // [Електронний ресурс]. Режим доступу: https://zakon2.rada.gov.ua/laws/show/386-2013-%D1%80.

30. Концепція розвитку електронного урядування в Україні: схвалено Розпорядженням Кабінету Міністрів України від 20.09.2017 № 649-р // [Електронний ресурс]. Режим доступу: http://zakon2.rada.gov.ua/laws/show/649-2017-р.

31. Доповідь Єврокомісії ЄС 2016 року «The EU Data Protection

Reform and Big Data: Factsheet» // [Електронний ресурс]. – Режим доступу: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwjT7dHn_9bfAhWIxIsKHb5eB-8QFjAAegQIBxAC&url=http%3A%2F%2Fec.europa.eu%2Fnewsroom%2Fjust%2Fdocument.cfm%3Fdoc_id%3D41523&usg=AOvVaw0ST2KcGgcpQzrQ8t4JTG3F.

32. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: затверджено постановою Кабінету Міністрів України від 29.03.2006 № 373 // [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF. http://zakon2.rada.gov.ua/laws/show/649-2017-%D1%80

33. Про доступ до публічної інформації: Закон України від 13.01.2011 № 2939-VI // [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/2939-17.

34. Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України»: затверджено постановою Кабінету Міністрів від 03.09.2014 № 411 // [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/411-2014-%D0%BF.

35. Голова Держспецзв'язку: кібератаки на другому місці в рейтингу глобальних світових ризиків // [Електронний ресурс]. – Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=299367&cat_id=284576&mustWords=%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA&searchPublishing=1.

36. Росс Алек. Індустрії майбутнього / пер. з англ. Н. Кошманенко. – К. : Наш формат, 2017.

37. Збитки від кібератак по всьому світу страховики оцінюють в $1 трлн на рік // [Електронний ресурс]. – Режим доступу: https://news.finance.ua/ua/news/-/426280/zbytky-vid-kiberatak-po-vsomu-svitu-strahovyky-otsinyuyut-v-1-trln-na-rik.

38. США звинуватили Росію в атаці вірусу NotPetya і пообіцяли наслідки: // [Електронний ресурс]. – Режим доступу: https://www.unian.ua/politics/10009301-ssha-zvinuvatili-rosiyu-v-ataci-virusu-notpetya-i-poobicyali-naslidki.html.

39. Про рішення Ради національної безпеки і оборони України від 06.05.2015 «Про Стратегію національної безпеки України: Указ Президента України від 26.05.2015 № 287 // [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/287/2015.

40. Про рішення Ради національної безпеки і оборони України від 27.01.2016 «Про Стратегію кібербезпеки України»: Указ Президента України від 15.03.2016 № 96 // [Електронний ресурс]. – Режим доступу: https://zakon3.rada.gov.ua/laws/show/96/2016.

41. Про Національний координаційний центр кібербезпеки: Указ Президента України від 07.06.2016 № 242 // [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/242/2016.

42. Про затвердження Порядків формування переліку об'єктів критичної інформаційної інфраструктури, внесення об'єктів критичної інформаційної інфраструктури до державного реєстру об'єктів критичної інформаційної інфраструктури, формування та забезпечення функціонування державного реєстру об'єктів критичної інформаційної інфраструктури: проект постанови Кабінету Міністрів України // [Електронний ресурс]. Режим доступу: http://195.78.68.84/dsszzi/control/uk/publish/article?showHidden=1&art_id=292848&cat_id=38837&ctime=1532005123380.

43. Про затвердження Загальних вимог з кіберзахисту об'єктів критичної інфраструктури, критеріїв та порядку віднесення об'єктів до об'єктів критичної інфраструктури проект постанови Кабінету Міністрів України // [Електронний ресурс]. Режим доступу: http://195.78.68.84/dsszzi/control/uk/publish/article?showHidden=1&art_id=290116&cat_id=38837&ctime=1526660658491.

44. Аналітична доповідь до Щорічного Послання Президента України до Верховної Ради України «Про внутрішнє та зовнішнє становище України в 2017 році» // [Електронний ресурс]. – Режим доступу: http://www.niss.gov.ua/public/File/book_2017/Poslanya_druk_fin.pdf.

45. Держспецзв'язку візьме участь у забезпеченні надійного функціонування ЄІАС «Вибори» // [Електронний ресурс]. – Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=116093&cat_id=112509&mustWords=%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA&searchPublishing=1.

46. Аналітична доповідь до Щорічного Послання Президента України до Верховної Ради України «Про внутрішнє та зовнішнє становище України в 2018 році» // [Електронний ресурс]. – Режим доступу: http://www.niss.gov.ua/public/File/analit_dopovid_POSLANNYA_2018_FINAL_Oct_02.pdf.

47. Відбулась міжнародна конференція «Кібербезпека та вибори в Україні» // [Електронний ресурс]. – Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=300828&cat_id=284576&mustWords=%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA&searchPublishing=1.

48. НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі: наказ ДСТСЗІ СБ України від 08.11.2005 № 125 // [Електронний ресурс]. Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=46074&cat_id=38835.

49. Про Положення про технічний захист інформації в Україні: затверджено Указом Президента України від 27.09.99 № 1229 // [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/1229/99.

50. Аналіз загроз державним інформаційним ресурсам // [Електронний ресурс] // О.К. Юдін, С.С. Бучик // Проблеми інформатизації та управління. – 2013. – № 4 (44). – С. 93-99. – Режим доступу: http://jrnl.nau.edu.ua/index.php/PIU/article/view/6404.

51. Державні інформаційні ресурси. Методологія побудови класифікатора загроз: монографія // Юдін О.К., Бучик С.С. – К.: НАУ, 2015. – 214 с. // [Електронний ресурс] // Режим доступу: http://er.nau.edu.ua:8080/handle/NAU/31911.

52. НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу»: наказ ДСТСЗІ СБ України від 28.04.99 № 22 (зі змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806) // [Електронний ресурс]. Режим доступу: www.dsszzi.gov.ua/dsszzi/doccatalog/document?id=106340.

53. НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу»: наказ ДСТСЗІ СБ України від 28.04.99 № 22 (зі змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806) // [Електронний ресурс]. Режим доступу: www.dsszzi.gov.ua/dsszzi/doccatalog/document?id=106342.

54. X.800 : Security architecture for Open Systems Interconnection for CCITT applications // [Електронний ресурс]. Режим доступу: https://www.itu.int/rec/T-REC-X.800-199103-I/en.

55. Мережева модель OSI // [Електронний ресурс]. Режим доступу: https://uk.wikipedia.org/wiki/Мережева_модель_OSI.

56. НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні профілі захищеності оброблювальної інформації від несанкціонованого доступу»: наказ ДСТСЗІ СБ України від 28.04.99 № 22 (зі зміною № 1, затвердженою наказом Адміністрації Держспецзв'язку від 15.10.2008 № 172) // [Електронний ресурс]. Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_

id=101870&cat_id=89734&ctime=1344501089407.

57. Конвенція Ради Європи про кіберзлочинність від 23.11.2001 № 994: ратифіковано Законом України від 07.09.2005 № 2824-IV // [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/994_575.

58. Палаева Л.В., Хафизов А.М., Гилязетдинова А.М., Вахитова А.Р., Давыдова К.Н., Сиротина Е.Р. Основные виды кибератак на автоматизированные системы управления технологическим процессом и средства защиты от них // Фундаментальные исследования. – 2017. – № 10-3. – С. 507-511 // [Електронний ресурс]. Режим доступу: http://www.fundamental-research.ru/ru/article/view?id=41866.

59. «Трояни» та сніфери: якими бувають віруси та як від них позбутися? // [Електронний ресурс]. Режим доступу: https://cybercalm.org/novyny/troyany-ta-snifery-yakymy-buvayut-virusy-ta-yak-vid-nyh-pozbutysya.

60. Infrastructure Attacks and Stealthy Mining – Threats Go Big and Small // [Електронний ресурс]. Режим доступу: https://www.symantec.com/security-center/threat-report.

61. Розвинена стала загроза // [Електронний ресурс]. Режим доступу: https://uk.wikipedia.org/wiki/Розвинена_стала_загроза#Відомі_приклади.

62. Спеціалісти Держспецзв'язку відбили всі атаки на сервери ЦВК // [Електронний ресурс]. Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=114136&cat_id=112509.

63. Хакерська атака Росії на українську енергосистему: як це було // [Електронний ресурс]. Режим доступу: http://texty.org.ua/pg/article/newsmaker/read/66125/Hakerska_ataka_Rosiji_na_ukrajinsku_jenergosystemu_jak.

64. В.И. Даль. Толковый словарь живого великорусского языка / Зав. редакцией В.В. Пчелкина. – Т. 1-4. – М.: Рус. яз., 1981. – Т. 2. И – О. 1981. 779 с.

65. Інструмент (визначення) // [Електронний ресурс]. Режим доступу: https://uk.wikipedia.org/wiki/Інструмент.

66. Деякі питання ліцензування господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації, за переліком, що визначається Кабінетом Міністрів України: затверджено Постановою Кабінету Міністрів України від 16.11.2016 № 821 // [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/821-2016-%D0%BF.

67. Методи виявлення вторгнень системами IDS: https://uk.wikipedia.org/wiki/Система_виявлення_вторгнень#Методи_виявлення.

68. У Windows 10 з'явиться своя «пісочниця» // [Електронний ресурс]. Режим доступу: https://news.finance.ua/ua/news/-/440947/u-windows-10-zyavytsya-svoya-pisochnytsya.

69. Что такое Cyber-Kill Chain и почему ее надо учитывать в стратегии защиты // [Електронний ресурс]. Режим доступу: https://habr.com/ru/company/panda/blog/327488.

70. Експерт: кіберзахист - це не параноя // [Електронний ресурс]. Режим доступу: https://www.bbc.com/ukrainian/features-39364360.

71. Reviews for Endpoint Detection and Response Solutions // [Електронний ресурс]. Режим доступу: https://www.gartner.com/reviews/market/endpoint-detection-and-response-solutions.

72. ESET LiveGrid // [Електронний ресурс]. Режим доступу: https://help.eset.com/ess/10/uk-UA/idh_config_charon.html.

73. Arbor DDoS Protection // [Електронний ресурс]. Режим доступу: https://www.netscout.com/ddos-protection.

74. Cisco Advanced Malware Protection Solution Overview // [Електронний ресурс]. Режим доступу:

https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/solution-overview-c22-734228.html?dtid=osscdc000283.

75. Полювання на кіберзагрози // [Електронний ресурс]. Режим доступу: https://uk.wikipedia.org/wiki/Полювання_на_кіберзагрози.

76. Сетевая телеметрия Cisco против киберугроз // [Електронний ресурс]. Режим доступу: https://habr.com/ru/company/cisco/blog/229073.

77. Положення про державну експертизу в сфері технічного захисту інформації: затверджено наказом Адміністрації Держспецзв'язку від 16.05.2007 № 93, зареєстрованим в Міністерстві юстиції України 16.07.2007 за № 820/14087 // [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/z0820-07.

78. Положення про державну експертизу в сфері криптографічного захисту інформації: затверджено наказом Адміністрації Держспецзв'язку від 23.06.2008 № 100, зареєстрованим в Міністерстві юстиції України 16.07.2008 за № 651/15342 // [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/z0651-08.

79. Про технічні регламенти та оцінку відповідності: Закон України від 15.01.2015 № 124-VIII // [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/124-19.

80. Правила проведення робіт із сертифікації засобів захисту інформації: затверджено спільним наказом Держспоживстандарту та Адміністрації Держспецзв'язку від 25.04.2007 № 75/91, зареєстрованим в Міністерстві юстиції України 14.05.2007 за № 498/13765) // [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/z0498-07.

81. Про затвердження Технічного регламенту засобів криптографічного захисту інформації: проект постанови Кабінету Міністрів України // [Електронний ресурс]. Режим доступу: http://195.78.68.84/dsszzi/control/uk/publish/article?showHidden=1&art_id=288501&cat_id=38837&ctime=1524467875297.

82. Zero Day Exploits. Holy Grail Of The Malicious Hacker // [Електронний ресурс]. Режим доступу: https://www.lifewire.com/zero-day-exploits-2487435.

83. Порядок використання комп'ютерних програм в органах виконавчої влади: затверджено постановою Кабінету Міністрів України від 10.09.2003 № 1433 // [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/1433-2003-п.

84. СБУ викрила вісім компаній на використанні шпигунського програмного забезпечення виробництва РФ // [Електронний ресурс]. Режим доступу: https://ssu.gov.ua/ua/news/1/category/1/view/3240#.hqI8tfBE.dpbs.

85. Про санкції: Закон України від 14.08.2014 № 1644-VII // [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/1644-18.

86. Порядок оновлення антивірусних програмних засобів, які мають позитивний експертний висновок за результатами державної експертизи в сфері технічного захисту інформації: затверджено наказом Адміністрації Держспецзв'язку від 26.03.2007 № 45, зареєстрованим в Міністерстві юстиції України 10.04.2007 за № 320/13587 // [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/z0320-07.

UNICHECK
by Turnitin

Ім'я користувача:
Національної економіки та публічного управління О...

ID перевірки:
1015967831

Дата перевірки:
04.12.2023 15:09:10 EET

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
04.12.2023 15:36:06 EET

ID користувача:
100005719

Назва документа: Тодорюк О.Д._магістр_2023

Кількість сторінок: 59 Кількість слів: 12259 Кількість символів: 101185 Розмір файлу: 316.00 KB ID файлу: 1015646580

24.5%
Схожість

Найбільша схожість: 6.55% з Інтернет-джерелом (http://nnvc.nuczu.edu.ua/images/topmenu/science/specrada/707.23.2..

23.6% Джерела з Інтернету 454 ..... Сторінка 61

5.29% Джерела з Бібліотеки 263 ..... Сторінка 67

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи 12

Національний технічний університет України
КПІ ім. Ігоря Сікорського
Інститут спеціального зв'язку та захисту інформації

Вроцлавський Університет
Факультет права, управління та економіки
Інститут адміністративних наук

Київський національний економічний університет
імені Вадима Гетьмана
Факультет економіки та управління

II Міжнародна
науково-практична конференція

КІБЕРБЕЗПЕКА ДЕРЖАВНИХ ІНСТИТУЦІЙ ТА ПОДОЛАННЯ КРИЗОВИХ СТАНІВ

ТОМ 2

ОСОБЛИВОСТІ ДІЯЛЬНОСТІ ОРГАНІВ ДЕРЖАВНОЇ ВЛАДИ В УМОВАХ КРИЗИ

збірник тез
(Київ – Вроцлав. Травень 2023)

Електронне видання

«ОФІС ЦІФРОВОГО ВРЯДУВАННЯ»

Київ – Вроцлав. 2023

УДК 621:351/354

Рекомендовано до друку Вченою радою ІСЗЗІ КПІ ім. Ігоря Сікорського
(протокол № 12 від 23.05.2023)

Тези публікуються в авторській редакції.
Організаційний комітет залишає за собою право не поділяти думку авторів.

Матеріали ІІ Міжнародної науково-практичної конференції «Кібербезпека державних інституцій та подолання кризових станів» в 2 т. Том 2. Особливості діяльності органів державної влади в умовах кризи зб. тез наук. доп. (Київ – Вроцлав. Травень 2023). [Електронне видання]. – Київ : «ОФІС ЦИФРОВОГО ВРЯДУВАННЯ», 2023. Т.2. 148 с.

Матеріали ІІ Міжнародної науково-практичної конференції «Кібербезпека державних інституцій та подолання кризових станів» присвячена 125-річчю Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», видані 2-х томах. На конференції обговорено актуальні проблеми та узагальнено отримані наукові результати у сферах інформаційної та кібербезпеки, кіберзахисту, інформаційних і інформаційно-комунікаційних технологій а також питання діяльності органів держаної влади в умовах кризи. В матеріалах опубліковано тези доповідей, що є фундаментом для подальшого розвитку освітньої, наукової та професійної діяльності учасників конференції в справі наближення Перемоги України.

РЕЦЕНЗЕНТИ:

Олександр ПУЧКОВ	к.філос.н., професор
Сергій КОНЮШОК	к.т.н., доцент
Вадим РОМАНЕНКО	к.т.н., доцент
Дмитро МОГИЛЕВИЧ	д.т.н., професор
Олена УВАРКІНА	д.філос.н., професор
Ігор СУБАЧ	д.т.н., доцент
Сергій ІВАНЧЕНКО	д.т.н., професор
Ярослав ЗІНЧЕНКО	к.т.н., с.н.с.

УДК 621:351/354

© «ОФІС ЦИФРОВОГО ВРЯДУВАННЯ», 2023

Олександр ТОДОРЮК
Київський національний економічний університет
імені Вадима Гетьмана

ОСОБЛИВОСТІ ПІДГОТОВКИ ФАХІВЦІВ З КІБЕРЗАХИСТУ У СФЕРІ ПУБЛІЧНОГО УПРАВЛІННЯ

Однією з важливих складових підвищення якості підготовки фахівців в області інформаційної безпеки є формування високих моральних якостей у студентів. Недостатня увага до людського фактора, як правило, являє собою більш значну загрозу, чим використання новітніх технічних засобів для добування конфіденційної інформації. Під поняттям «людський фактор» психологи розуміють «сукупність властивостей людини оператора, що впливають на ефективність системи «людина-машина» [10]. Представляється доцільним розширити визначення - це інтегральна характеристика особистості, що визначає надійність захисту інформації при її одержанні, збереженні й переробці в автоматизованих техніко-біологічних системах. Незважаючи на розмаїтість і постійне удосконалювання спеціальної техніки для захисту інформації, люди залишаються самою слабкою ланкою в людино-машинних системах, одним із самих ймовірних джерел витоку інформації.

Проблему людського фактора при підготовці фахівців в області інформаційної безпеки доцільно вирішувати у двох напрямках: удосконалювання технології профвідбору на спеціальності, зв'язані з захистом інформації й оптимізації виховної роботи в процесі навчання. У навчальних закладах, зв'язаних з підготовкою фахівців в області інформаційної безпеки доцільно створювати спеціальні підрозділи (лабораторії, групи, служби й т.п.), що змогли б займатися вивченням мотивації студентів до здійснення протиправних дій в області інформаційних технологій і виробленням рекомендацій для оперативного корегування навчально-виховної роботи серед молоді. Одним з головних напрямків діяльності таких підрозділів повинне бути проведення профорієнтованої роботи серед молоді й обов'язкового тестування абітурієнтів на їхню професійну придатність. Такі підрозділи змогли б вирішувати ще одне досить важливе завдання - використання впливу лідерів соціальних груп для боротьби й запобігання комп'ютерних злочинів. Такий напрямок успішне розвивається в США. Як показали соціологічні дослідження, проведені в США [11], вплив авторитетів у соціальних групах діє на поводження людей. Так, зниження кількості курців у США в значній мірі зв'язано із соціальним «клеймом» курця.

Таким чином, одним з важливих факторів підвищення якості підготовки фахівців в області інформаційної безпеки повинні бути заходи для

жорсткості режиму добору на спеціальності, зв'язані з захистом інформаційних технологій. Можна запропонувати наступні шляхи розвитку технології профвідбіру:

1) створення еталонних моделей студента й фахівців у багатомірному просторі професійно важливих якостей;
2) відображення в змісті професійно важливих якостей пізнавальних здібностей особистості, адаптаційних можливостей у професійній спрямованості кандидата;
3) розробка алгоритму оцінки близькості реальних і еталонних зразків кандидата з розрахунком, як узагальненого інтегрального показника, так і рівнів розвитку складових кожного показника.

н а у к о в е в и д а н н я

збірник тез
ІІ Міжнародної науково-практичної конференції

КІБЕРБЕЗПЕКА ДЕРЖАВНИХ ІНСТИТУЦІЙ ТА ПОДОЛАННЯ КРИЗОВИХ СТАНІВ

СЕКЦІЯ 5

ОСОБЛИВОСТІ ДІЯЛЬНОСТІ ОРГАНІВ ДЕРЖАВНОЇ ВЛАДИ В УМОВАХ КРИЗИ

Київ – Вроцлав. Травень 2023

Електронне видання

Авторська редакція

Упорядник
ГО «ОФІС ЦИФРОВОГО ВРЯДУВАННЯ»
digital.gov.office@gmail.com