МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ**

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ УПРАВЛІННЯ ПЕРСОНАЛОМ У СФЕРІ КІБЕРБЕЗПЕКИ”

на здобуття освітнього ступеня магістра
зі спеціальності 125 Кібербезпека
освітньо-професійної програми Управління інформаційною безпекою

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Олександр БОЙКО
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: Здобувач вищої освіти гр. УБДМ 61
Олександр БОЙКО

Керівник:
к.т.н. Юрій ЩАВІНСЬКИЙ

Рецензент:
д.т.н., професор Галина ГАЙДУР

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут захисту інформації

Кафедра Управління інформаційною та кібернетичною безпекою

Ступінь вищої освіти магістр

Спеціальність 125 Кібербезпека
Освітньо-професійна програма Управління інформаційною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедрою УІКБ
_____ Світлана ЛЕГОМІНОВА
"____" _____2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Бойко Олександру Олександровичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: "Підвищення ефективності управління персоналом у сфері кібербезпеки"

керівник кваліфікаційної роботи Юрій ЩАВІНСЬКИЙ, к.т.н.
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від "19" жовтня 2023 р. №145

2. Строк подання кваліфікаційної роботи "18" грудня 2023 р

3. Вихідні дані до кваліфікаційної роботи: *управління кібербезпекою, організації кібербезпеки, методи та засоби управління персоналом, корпоративні кодекси кібербезпеки нормативні документи, стандарти, міжнародні стандарти, наукова та технічна література*

4. Перелік питань, які потрібно розробити:
1. Здійснити аналіз наукової літератури та публікацій, пов'язаних із управлінням персоналом у сфері кібербезпеки та існуючими підходами до цієї проблеми.
2. Дослідити сучасний стан управління персоналом в організації кібербезпеки, основні потреби та вимоги до кваліфікації та компетентності персоналу, сучасні методи та практики управління персоналом в галузі кібербезпеки в організації.
3. Розробити стратегію, яка включає в себе процеси набору, навчання, розвитку та утримання персоналу в галузі кібербезпеки.
4. Здійснити моніторинг та оцінку ефективності нової стратегії управління персоналом, визначити досягнуті покращення та ідентифікувати можливі обмеження.

5. Перелік ілюстративного матеріалу: *презентація*

6. Дата видачі завдання "02" жовтня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	10.10.2023	
2.	Збір та аналіз літератури.	23.10.2023	
3.	Аналіз основних положень теорії управління персоналом	27.10.2023	
4.	Дослідження сучасного стану управління персоналом організацій кібербезпеки.	10.11.2023	
5.	Розроблення стратегії управління персоналом.	15.11.2023	
6.	Моніторинг та оцінка ефективності розробленої стратегії	22.11.2023	
7.	Оформлення роботи.	04.12.2023	
8.	Оформлення презентації.	14.12.2023	
9.	Отримання рецензії на роботу.	18.12.2023	
10.	Захист в ДЕК.	16.01.2024	

Здобувач вищої освіти _____ Олександр БОЙКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Юрій ЩАВІНСЬКИЙ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

,

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувач Бойко О.О. до захисту кваліфікаційної роботи
(прізвище та ініціали)

за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)

Освітньо-професійної програми Управління інформаційною безпекою
(назва)

на тему: “ Підвищення ефективності управління персоналом у сфері кібербезпеки ”
Кваліфікаційна робота і рецензія додаються.

Директор ННІЗІ _____ Віталій САВЧЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач **БОЙКО Олександр** у кваліфікаційній роботі дослідив сучасний стан управління персоналом у сфері кібербезпеки, здійснив аналіз наукової літератури, сучасних методів управління персоналом, що дало змогу зробити висновок про необхідність пошуку нових підходів з метою підвищення ефективності управління організаціями і підрозділами кібербезпеки. Розроблена удосконалена методика оцінювання ефективності управління персоналом кібербезпеки на основі визначених критеріїв та розробленої стратегії дозволять формувати стратегії управління персоналом кібербезпеки, здійснювати обґрунтований вибір методів і засобів підвищення ефективності управління персоналом організації при виконанні завдань кібербезпеки. **БОЙКО Олександр** показав розуміння проблеми дослідження та бачення основних теоретичних та практичних напрямів її вирішення, довів уміння самостійного застосування методів наукового дослідження, проявив себе як організований, відповідальний виконавець. Результати дослідження апробовані на науково-практичній конференції.

Це дозволяє оцінити виконану кваліфікаційну роботу здобувача **БОЙКА Олександра** на оцінку “відмінно” та присвоїти йому кваліфікацію “Магістр кібербезпеки за освітньо-професійною програмою “Управління інформаційною безпекою”.

Керівник кваліфікаційної роботи _____ Юрій ЩАВІНСЬКИЙ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

“___“_____2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Бойко О.О. допускається до захисту роботи в екзаменаційній комісії

Завідувач кафедрою
Управління інформаційною
та кібернетичною безпекою _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну магістерську роботу

здобувача вищої освіти Бойко Олександра Олександровича
на тему " ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ УПРАВЛІННЯ ПЕРСОНАЛОМ У СФЕРІ КІБЕРБЕЗПЕКИ "

Актуальність

Зроблений в роботі аналіз сучасного стану управління персоналом етичних аспектів кібербезпеки дозволив правильно обґрунтувати вибрану тему дослідження. У контексті динамічної інформаційної обстановки, ефективність управління персоналом у сфері кібербезпеки набуває особливої ваги. Зазначений напрямок досліджень передбачає вивчення сучасних методів навчання та розвитку кадрів, аналіз технологічних інновацій, що можуть поліпшити процеси виявлення та вирішення кіберзагроз, а також визначення оптимальних моделей співпраці та комунікації всередині команди кібербезпеки

Позитивні сторони

Здійснений аналіз наукової літератури та публікацій, пов'язаних із управлінням персоналом у сфері кібербезпеки дозволив визначити потребу у застосуванні комплексного підходу до управління персоналом. В магістерській роботі вперше запропоновані нові підходи до розроблення стратегії управління персоналом кібербезпеки, які відрізняються від відомих тим, що ґрунтуються на врахуванні особливостей людських ресурсів при формуванні команд кібербезпеки. Удосконалена методика оцінювання ефективності управління персоналом кібербезпеки на основі визначених критеріїв оцінювання ефективності розробленої стратегії. Застосування напрацювань дозволять формувати стратегії управління персоналом кібербезпеки, здійснювати обґрунтований вибір методів і засобів підвищення ефективності управління персоналом організації при виконанні завдань кібербезпеки.

Недоліки

Було б також доцільно у роботі зробити аналіз застосування етичних норм в управлінні персоналом кібербезпеки. Однак, зазначене зауваження не впливає на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки «відмінно» а її автор Бойко Олександр Олександрович - присвоєння кваліфікації «Магістр кібербезпеки» за освітньо-професійною програмою «Управління інформаційною безпекою».

Рецензент: завідувач кафедри
Інформаційної та кібернетичної
безпеки,
д.т.н, професор _____ Галина ГАЙДУР
підпис *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 69 стор., 19 рис., 8 табл., 56 джерел.

Метою роботи є розробка та обгрунтування шляхів підвищення ефективності управління персоналом в галузі кібербезпеки з метою забезпечення високого рівня захисту кіберінфраструктури.

Об'єктом дослідження є управління персоналом у сфері кібербезпеки.

Предмет дослідження – ефективність управління персоналом організацій кібербезпеки.

Методи дослідження. Для вирішення визначених наукових завдань в роботі при дослідженні процесів управління персоналом використані методи системного аналізу та теорії управління, SWOT-аналіз для оцінювання сильних та слабких сторін визначеної стратегії та при проведенні тестування якостей працівників кібербезпеки.

Короткий зміст роботи. Здійснено аналіз наукової літератури та публікацій, пов'язаних із управлінням персоналом у сфері кібербезпеки та існуючими підходами до цієї проблеми. Досліджено сучасний стан управління персоналом в організації кібербезпеки, основні потреби та вимоги до кваліфікації та компетентності персоналу, сучасні методи та практики управління персоналом в галузі кібербезпеки в організації.

В магістерській роботі вперше запропоновані нові підходи до розроблення стратегії управління персоналом кібербезпеки, які відрізняються від відомих тим, що ґрунтуються на врахуванні особливостей людських ресурсів при формуванні команд кібербезпеки.

Удосконалена методика оцінювання ефективності управління персоналом кібербезпеки на основі визначених критеріїв оцінювання ефективності розробленої стратегії.

Дістали подальшого розвитку способи процесу розробки кадрової стратегії, які включають поєднання мотиваційної складової і використання

інформаційних технологій, підвищення кваліфікації та отримання сертифікатів

Галузь застосування. Розроблені підходи можуть бути використані при плануванні та реалізації системи управління персоналом в організаціях кібербезпеки з метою підвищення ефективності протидії загрозам, пов'язаним із веденням інформаційного протиборства. Застосування напрацювань дадуть змогу формувати стратегії управління персоналом кібербезпеки, здійснити обґрунтований вибір методів і засобів підвищення ефективності управління персоналом організації при виконанні завдань кібербезпеки в умовах інформаційного протиборства.

КЛЮЧОВІ СЛОВА: КІБЕРБЕЗПЕКА, УПРАВІННЯ ПЕРСОНАЛОМ, ОРГАНЗАЦІЇ КІБЕРБЕЗПЕКИ, СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЄЮ ТА КІБЕРБЕЗПЕКОЮ.

ABSTRACT

The text part of the qualification work for obtaining a master's degree: 69 pages, 19 figures, 8 tables, 56 sources.

The purpose of the work is the development and justification of ways to improve the effectiveness of personnel management in the field of cyber security in order to ensure a high level of cyber infrastructure protection.

Object of research is personnel management in the field of cyber security.

Subject ***of research*** is the effectiveness of personnel management of cyber security organizations.

Research methods. The methods of system analysis and management theory, SWOT analysis for evaluating the strengths and weaknesses of the defined strategy and testing the qualities of cyber security workers were used to solve the identified scientific tasks in the study of personnel management processes.

Brief content of research. An analysis of scientific literature and publications related to personnel management in the field of cyber security and existing approaches to this problem was carried out. The modern state of personnel management in the cyber security organization, the main needs and requirements for personnel qualifications and competence, modern methods and practices of personnel management in the field of cyber security in the organization were studied.

In the master's thesis, for the first time, new approaches to the development of a cyber security personnel management strategy are proposed, which differ from the known ones in that they are based on taking into account the characteristics of human resources when forming cyber security teams.

An improved methodology for evaluating the effectiveness of cyber security personnel management based on defined criteria for evaluating the effectiveness of the developed strategy.

Methods of the personnel strategy development process, which include a combination of the motivational component and the use of information technologies, professional development and obtaining certificates, received further development

Field of research. The developed approaches can be used in the planning and implementation of the personnel management system in cyber security organizations in order to increase the effectiveness of countering threats related to the conduct of information warfare. The application of developments will make it possible to form cyber security personnel management strategies, to make a justified choice of methods and means of increasing the effectiveness of the organization's personnel management when performing cyber security tasks in the conditions of information warfare.

KEYWORDS: CYBER SECURITY, PERSONNEL MANAGEMENT, CYBER SECURITY ORGANIZATIONS, INFORMATION AND CYBER SECURITY MANAGEMENT SYSTEM.

ЗМІСТ

ВСТУП

Актуальність теми. Ефективне управління персоналом є однією з передумов досягнення високих результатів діяльності кожної організації (підприємства) в любій сфері діяльності.

У сучасному інформаційному суспільстві, де технологічний прогрес стрімко набуває обертів, питання кібербезпеки стає вельми актуальним та невід'ємним елементом функціонування підприємств та організацій. Зростання кількості та складності кіберзагроз, а також постійна зміна методів атак вимагають від організації не лише сучасних технічних засобів захисту, але й висококваліфікованих кадрів, які здатні ефективно управляти цим складним процесом.

Сьогодні перед дослідниками стоїть актуальне завдання розгляду ключових аспектів, які впливають на успішність управлінської діяльності в галузі кібербезпеки, а також визначення оптимальних стратегій та практик, спрямованих на забезпечення високого рівня захисту інформаційних ресурсів.

У контексті динамічної інформаційної обстановки, ефективність управління персоналом у сфері кібербезпеки набуває особливої ваги. Зазначений напрямок досліджень передбачає вивчення сучасних методів навчання та розвитку кадрів, аналіз технологічних інновацій, що можуть поліпшити процеси виявлення та вирішення кіберзагроз, а також визначення оптимальних моделей співпраці та комунікації всередині команди кібербезпеки.

У цьому контексті, проведення аналізу ефективності управління персоналом у сфері кібербезпеки надає можливість виявлення слабких точок та визначення шляхів їх вдосконалення. Відповідно, результати цього дослідження можуть служити основою для розробки рекомендацій щодо оптимізації управлінських практик та підвищення рівня кібербезпеки організації.

Дипломна робота висвітлює ключові виклики, з якими стикаються керівники у сфері кібербезпеки, і надає практичні рекомендації для покращення ефективності управління персоналом, що має визначальне значення для

забезпечення інформаційної безпеки в умовах сучасного цифрового середовища.

З огляду на зазначене тема кваліфікаційної роботи є актуальною, а використання її результатів сприятиме підвищенню рівня інформаційної безпеки суб'єктів підприємницької діяльності в умовах інформаційного протиборства.

Об'єкт дослідження - управління персоналом у сфері кібербезпеки.

Предмет дослідження – ефективність управління персоналом організацій кібербезпеки.

Мета роботи полягає у визначенні та обґрунтуванні шляхів підвищення ефективності управління персоналом у сфері кібербезпеки.

Для досягнення цієї мети в роботі виконано наступні *завдання:*

1. Здійснено аналіз наукової літератури та публікацій, пов'язаних із управлінням персоналом у сфері кібербезпеки та існуючими підходами до цієї проблеми.

2. Досліджено сучасний стан управління персоналом в організації кібербезпеки, основні потреби та вимоги до кваліфікації та компетентності персоналу, сучасні методи та практики управління персоналом в галузі кібербезпеки в організації.

3. Розроблена стратегія, яка включає в себе процеси набору, навчання, розвитку та утримання персоналу в галузі кібербезпеки.

4. Здійснений моніторинг та визначені критерії оцінювання ефективності нової стратегії управління персоналом, визначені досягнуті покращення та ідентифіковані можливі обмеження.

Методи дослідження. Для вирішення означених вище наукових завдань в роботі при дослідженні процесів управління персоналом використані методи системного аналізу та теорії управління, SWOT-аналіз для оцінювання сильних та слабких сторін визначеної стратегії та при проведенні тестування якостей працівників кібербезпеки.

Наукова новизна одержаних результатів.

1. В магістерській роботі вперше запропоновані нові підходи до розроблення стратегії управління персоналом кібербезпеки, які відрізняються від

відомих тим, що ґрунтуються на врахуванні особливостей людських ресурсів при формуванні команд кібербезпеки.

2. Удосконалена методика оцінювання ефективності управління персоналом кібербезпеки на основі визначених критеріїв оцінювання ефективності розробленої стратегії.

3. Дістали подальшого розвитку способи процесу розробки кадрової стратегії, які включають поєднання мотиваційної складової і використання інформаційних технологій, підвищення кваліфікації та отримання сертифікатів.

Практичне значення одержаних результатів. Розроблені підходи можуть бути використані при плануванні та реалізації системи управління персоналом в організаціях кібербезпеки з метою підвищення ефективності протидії загрозам, пов'язаним із веденням інформаційного протиборства. Застосування напрацювань дадуть змогу формувати стратегії управління персоналом кібербезпеки, здійснити обґрунтований вибір методів і засобів підвищення ефективності управління персоналом організації при виконанні завдань кібербезпеки в умовах інформаційного протиборства.

Апробація результатів кваліфікаційної роботи. Результати дослідження було оприлюднено:

на Всеукраїнській науково-практичної Інтернет-конференції «Стратегії кіберстійкості: управління ризиками та безперервність бізнесу» (м. Київ, 23 лютого 2023 року), яка проведена в Навчально-науковому інституті захисту інформації ДУТ;

на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки: (м. Київ, 27 жовтня 2023 року), яка проведена в Навчально-науковому інституті захисту інформації Державного університету інформаційно-комунікаційних технологій.

.

РОЗДІЛ 1
ТЕОРЕТИЧНІ АСПЕКТИ УПРАВЛІННЯ ПЕРСОНАЛОМ

1.1 Огляд основних теорій управління персоналом

Наука про управління персоналом існує більше сотні років і знаходиться на стику психології, економіки праці, організації управління, трудового права та інших дисциплін. Вона почала формуватися на початку періоду промислової революції. Першими авторами наукових робіт з теорії управління були Ф. Тейлор, який сформулював принципи наукового менеджменту, Ф. Гілберт, Г. Емерсон. За цей час роль людини в організації встигла істотно змінитися, а на світ з'явилося безліч теорій управління кадрами.

Сьогодні всі існуючі теорії управління персоналом умовно поділяють на три групи (рис.1.1)

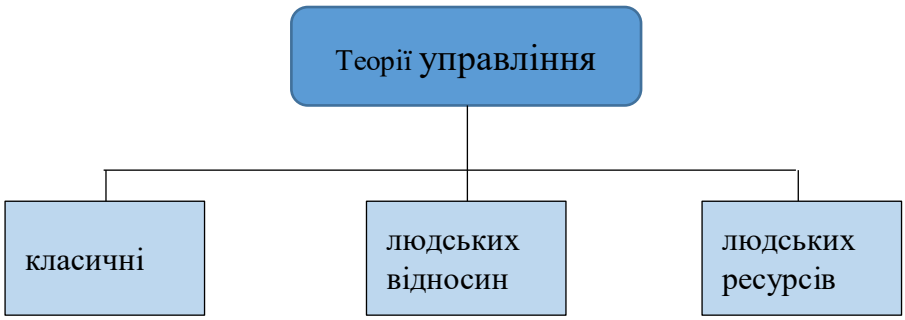

Рис. 1.1. Сучасні теорії управління персоналом

Класичні теорії, які розвинулися ще з минулого століття, зводилися переважно до розробки методів контролю за працівниками, за якість виконання покладених на них завдань. Незначна увага приділялась ефективності та підвищенню кваліфікації співробітників. Авторами класичної теорії управління персоналом вважаються Г. Форд, М. Вебер, А Файоль. Вони також започаткували дослідження передумов якісної роботи, впливу індивідуальних

особливостей працівників на результативність, застосування інструментів мотивації [1].

Відомий своєю теорією наукового управління, Фредерік Тейлор у своїх дослідженнях зосереджувався на оптимізації робочих процесів та раціональному використанні ресурсів, впроваджував стандартизацію та розподіл обов'язків.

Анрі Файоль розробив концепцію функціональної організації, виділив п'ять функціональних областей управління: планування, організація, координація, командування та контроль.

Генрі Форд запровадив конвеєрну лінію та стандартизацію виробництва. Його підхід допоміг знизити вартість виробництва та зробити автомобілі доступнішими для широкої публіки

Ці класичні теорії внесли вагомий вклад у розвиток управління персоналом та сформували основи для подальших досліджень та практичного застосування

Основою *теорії людських відносин*, що застосовуються з початку 1930-х років до цього дня, є співробітництво і взаємодія між працівниками і керівниками. За цією теорією науковці [2,3] основними інструментами впливу на ефективність праці вважають залученість в загальну справу керівників та підлеглих, які об'єднані єдиною метою, наявність мотивації як моральної так і матеріальної. Теорія людських відносин організацій складається з трьох основних компонентів.

По-перше, теорія робить акцент на важливості особистості. Працівник – це не просто гвинтик у машині, а своєрідна особистість, яка реагує на навколишнє середовище. Максимізація продуктивності праці працівників вимагає врахування цих індивідуальних особливостей.

По-друге, теорія людських відносин враховує неформальні організації на робочому місці. Те, що важливо для працівника і що впливає на рівень його продуктивності, може бути не офіційна організаційна схема, а його зв'язки з іншими працівниками.

Організації все більше усвідомлюють той факт, що для виживання в умовах все більш жорсткого і конкурентного ділового середовища в сучасному

світі всі організаційні ресурси повинні бути повністю використані, використані і керовані для досягнення цілей організації. Зокрема, більша увага приділяється людському елементу організаційних ресурсів як кінцевій детермінанті успіху організацій, звідси випливає необхідність ефективного управління цим важливим ресурсом. У цій концептуальній роботі стверджується, ефективне управління людськими ресурсами ґрунтується на базовому розумінні природи працівників, перш за все, як людських істот з особливостями, і що таке розуміння можливе лише за умови адекватного знання основних принципів та внеску теорії людських відносин, започаткованої Елтоном Мейо. У статті також стверджується, що ця теорія має наслідки для ефективного управління людськими ресурсами в таких сферах, як розуміння природи людей, мотивація працівників, важливість лідерства, роль неформальних груп та ефективна комунікація на робочому місці. У статті зроблено висновок про те, що теорія людських відносин становить основу та забезпечує теоретичну основу ефективного управління людськими ресурсами в організаціях.

Одним із головних завдань керівника є науковий розподіл обов'язків з урахуванням індивідуальних психологічних особливостей, отриманих навичків і потреб співробітників, створення в колективі сприятливої атмосфери, що дозволяє кожному працівникові відчувати себе корисним і потрібним [4]. При цьому, діяльність з управління персоналом зосереджується на заходах контролю з боку начальства та на особистому самоконтролі працівника. Керівникам рекомендується забезпечувати підлеглим можливість самостійно приймати рішення і особисто відповідати за результати праці. Представниками такої теорії людських відносин стали М. Фоллетт, К. Арджеріс, Р. Блейк [5].

Сучасніші методики управління персоналом базуються переважно на *теоріях людських ресурсів*, які стверджують, що праця сама по собі здатна приносити задоволення більшості працівників. А завдання керівника полягає у раціональному використанні людських ресурсів на основі здатності до самоконтролю, творчості, самостійного прийняття рішень.

Література з управління людськими ресурсами (HRM) переважно

фокусується на аналізі взаємозв'язку між практиками управління людськими ресурсами та бізнес-продуктивністю. Однак менше досліджень спрямовано на визначення того, як і чому ці практики можуть бути пов'язані з однаковим патерном або моделлю поведінки.

У роботах [6,7] проаналізовано різні моделі управління людськими ресурсами, які визначають рамки дії будь-якої організації та обґрунтовують застосування різних практик управління людськими ресурсами. Ми розглядаємо м'які та жорсткі моделі управління людськими ресурсами та вказуємо на їхні основні обмеження. Крім того, ми встановлюємо типологію моделей, спрямованих на мотиваційну якість особи, де антропологічна модель представлена як більш повна модель порівняно з механістичною моделлю та психосоціологічною моделлю. Основна різниця між цими двома класифікаціями полягає в тому, що, в той час як м'які та жорсткі моделі представлені як виключні моделі, взаємозв'язок між механістичною, психосоціологічною та антропологічною моделями полягає в тому, що різні елементи кожної моделі включаються в наступну модель, встановлюючи більш схоже відображення з бізнес-реальністю та збільшуючи її пояснювальну здатність.

Важливо розуміти, що успіх будь-якої організації залежить від співпраці та координації зусиль всіх її членів. Компанія без добре злагодженої команди людей не здатна досягти відмінних результатів. Тому індивіди, які складають організацію, повинні співпрацювати, щоб отримати результати, які цікавлять всіх членів компанії Управлінцю (менеджеру) належить зробити працю максимально різноманітною і цікавою. На сучасному етапі зростає роль стратегічного планування і гнучких форм винагороди. Автори, які зробили значний внесок у розвиток теорії людських ресурсів - А. Маслоу, Д. Мак-Грегор, Ф. Герцберг [8].

Детальний аналіз відмінностей визначений в роботах [9-11] та згрупований в таблицю (табл. 1.1).

Таблиця 1.1.

Теорії управління персоналом і підходи до їх використання на підприємстві [9-11]

Найменування теорій	Постулати теорій	Завдання керівника підприємства	Очікувані результати
Класичні теорії	Праця для більшості персоналу не приносить задоволення, це властива для них якість. Те, що вони роблять, менш важливе для них, ніж те, що вони заробляють, роблячи це. Мало творчих, самостійних, ініціативних або здатних до самоконтролю	Завдання керівника: надмірний контроль і спостереження за підлеглими. Його завдання – спростити операції, що повторюються, розробити прості процедури праці і застосовувати їх на практиці	Для персоналу важливою є відповідна заробітна плата і справедливий керівник, що їх контролює. При цьому працівники підприємства зможуть дотримувати фіксовані норми виробництва
Теорії людських відносин	Прагнення працівників бути корисними і значущими, визнаними як особистості. Ці потреби є важливішими, ніж гроші щодо стимулювання і мотивації до праці	Головне завдання керівника зробити так, щоб кожен відчував себе корисним і потрібним. Він повинен інформувати своїх підлеглих про плани, а також враховувати їх пропозиції щодо поліпшення цих планів. Керівник повинен надавати своїм підлеглим можливість самостійності і особистого самоконтролю щодо виконання завдань, особливо рутинних операцій	Можливість обміну інформацією з підлеглими і їх участь у прийнятті рішень дозволяє керівнику задовольнити основні потреби щодо взаємодії працівників і відчутті їх власної значущості. Задоволення потреб мотивує їх і зменшує відчуття протидії керівництву, тобто, підлеглі більш охоче спілкуються з керівником

Найменування теорій	Постулати теорій	Завдання керівника підприємства	Очікувані результати
Теорії людських ресурсів	Праця для більшості працівників приносить задоволення. Люди прагнуть зробити внесок у реалізацію спільних цілей через особистісні. При цьому більшість працівників має здатність до самостійності у прийнятті рішень, творчості, відповідальності, самоконтролю	Головним завданням керівника є ефективне використання людських ресурсів. Це полягає у створенні сприятливої атмосфери щодо можливостей персоналу максимально проявляти свої здібності, брати участь у вирішенні важливих проблем, постійно розвиваючи їх самостійність і самоконтроль	Присутність самостійності і самоконтролю у працівників спричинятиме підвищення їх власної продуктивності та ефективності виробництва в цілому. Внаслідок цього - задоволення працею постійно має тенденцію до зростання, оскільки працівники повною мірою використовують власні ресурси

В науковій праці [12] зроблений більш детальний аналіз ідей засновників і послідовників концепцій і теорії управління персоналом (табл. 1.2)

Таблиця 1.2.

Основні концепції й школи управління персоналом

Концепції, школи й теорії управління персоналом	Засновники й послідовники	Основні ідеї, які використовувалися
Класичні концепції: наукове управління, наукова організація праці, соціальна інженерія, комплексний підхід до організації праці	Ф. Тейлор, Ф. Дунаєвський, М. Вітке, Ф. Гілберт, П. Керженцев, М. Емерсон, О. Гастев	Стандартизація і раціоналізація трудових операцій; персональна оцінка й оплата за результатами праці; максимальна ефективність використання робочої сили
Адміністративне управління	Ч. Барнард, М. Фоллет, А. Файоль	Науковцями розглядається управління – як особливий вид професійної діяльності, який включає планування, організацію, координацію й контроль; загальні принципи управління, які приводять до успіху; механізм

Концепції, школи й теорії управління персоналом	Засновники й послідовники	Основні ідеї, які використовувалися
		прийняття рішень і підпорядкування наказам розпорядженням; лідерство, взаємодопомога, етика тощо
Бюрократична організація	М. Вебер	Доцільний функціональний розподіл праці та ієрархія керівних відносин; кар'єрне зростання на основі кваліфікації й досвіду; письмове закріплення обов'язків персоналу; стратегія довічного наймання; мінімізація особистісних властивостей й суб'єктивізму
Концепція «людських відносин»	Р. Лайкерт Е. Мейо, Ф. Ротлісбергер,	Позитивне ставлення керівників до підлеглих, здоровий морально-психологічний клімат і задоволення вимог і потреб – головні фактори підвищення продуктивності праці
Концепція людських ресурсів і школа поведінкових наук (концепції X і Y управління; концепція Z – синтез американського і японського методів управління)	А. Маслоу, Д. Макгрегор, В. Скотт, М. Фоллет, У. Оучі	Ієрархія потреб людини; закономірності поведінки суб'єкта
Концепції ситуаційного підходу	М. Стівенсон, Ф. Фідлер, Дж. Вудворт, В. Врум П. Герсі й К. Бланчард, Р. Блейк і Д.Моутон	Ефективності управління залежить від умов конкретної ситуації функціонування підприємства; SWOT-аналіз; здатність аналізувати ринкову кон'юнктуру й приймати рішення; вибір адекватного стилю управління; лідерство й керівництво; «управлінська решітка»

Концепції, школи й теорії управління персоналом	Засновники й послідовники	Основні ідеї, які використовувалися
Концепції системного підходу (управління за цілями, концепція «7S»; сучасне підприємство як відкрита й закрита система)	П. Дракер, Р. Лайкерт, Т. Пітерс, Р. Уотерман, І. Ансофф	management by objectives (Управління за цілями) передбачає визначення цілей функціонування кожного структурного елемента організації (адміністрації, працівників) і реалізованих проектів, для спостереження й контролю результатів спільної діяльності. Сучасне підприємство розглядається як відкрита й закрита система Розроблена американською консультативною фірмою «МакКінси» Модель «7S» одержала свою назву від семи найважливіших проблем організації й управління: *strategy* (стратегія) – *skill* (навички, майстерність) – *shared values* (загальновизнані цінності) – *structure* (структура) – *systems* (система й процеси прийняття рішень) – *staff* (персонал, кадри) – *style* (стиль).
Концепції інституціонального підходу	Д. Норт	Ринок являє собою сукупність формальних і неформальних «правил гри», факторів (процедур) примусу й організацій («гравців»), що переслідують власні цілі
Сучасні концепції: теорія людського капіталу	Т. Шульц М. Беккер, Я. Мінсер,	Вплив інтелектуального капіталу на зростання доходу компанії
Теорія стратегічного управління персоналом	К. Легге, С. Фомбрун, Д. Сторі, М. Бір, Д. Гест, П. Боксалл, Д. Парселл,	Управління організаційною структурою та людськими ресурсами повинні відповідати організаційній стратегії

Ще один варіант аналізу та систематизації концепцій теорії управління персоналом поданий в роботі [13]. Сучасні підходи до управління персоналом, актуальні для різних типів організацій та підприємств, включаючи гуманістичну складову, представлені науковцем в таблиці 1.3.

Таблиця 1.3

Концепції управління персоналом

№	Період	Концепції	Підходи
1.	20–40 рр. XX ст.	Використання трудових ресурсів (labour resources use) Економічна	Економічний (працівник-носій трудової функції, «живий придаток машини»)
2.	50–70 рр. XX ст.	Управління персоналом (personnel management) Організаційно-адміністративна.	Органічний (працівник-суб'єкт трудових відносин, особистість)
3.	80–90 рр. XX ст.	Управління людськими ресурсами (human resource management) Організаційно-соціальна.	Органічний (працівник-ключовий стратегічний ресурс організації)
4.	XXI ст.	Управління людиною (human being management) Гуманістична	Гуманістичний (не люди для організації, а організація - для людей)

Зроблений науковцями аналіз основний теорії управління персоналом в генезі вказує суть теорії та дозволяє глибше здійснювати подальші теоретичні дослідження, розкриваючи основні поняття, завдання і функції управління.

1.2 Основні поняття, завдання і функції управління персоналом

Управління персоналом - це галузь управління, що вивчає і розвиває методи та практики керівництва людськими ресурсами в організації.

Основні поняття управління персоналом включають; трудові ресурси, трудовий колектив, персонал, кадри, людські ресурси, кадровий потенціал [14-15].

Під *трудовими ресурсами* розуміють частину населення, яка володіє розумовими здібностями і знаннями, що необхідні для роботи у народному господарстві. *Трудові ресурси підприємства* характеризують основну його потенційну робочу силу.

Під *кадровим потенціалом* підприємства розуміють граничну величину можливої участі працівників у діяльності підприємства з урахуванням компетентності, психофізичних особливостей, інтересів, мотивацій таких працівників.

Під *персоналом* підприємства розуміється сукупність його працівників (тимчасових і постійних, кваліфікованих та некваліфікованих), які працюють по найму та мають трудові відносини с роботодавцем.

Під визначенням *кадри* розуміють основний (штатний та постійний) кваліфікований склад працівників підприємства. У розвинених країнах поняття "*кадри*" спочатку замінили на термін "персонал", а з семидесятих років минулого століття поширення отримало поняття "людські ресурси". Така заміна ґрунтується на усвідомленні економічної доцільності вкладень у людину, орієнтацією на розвиток її компетентностей, як сукупності вмінь, навичок та здібностей [16].

Під людськими ресурсами підприємства сьогодні більшість науковців розуміють сукупність соціальних, психологічних і культурних якостей кожного працівника підприємства. На початку 80-х років минулого століття уже цей термін почав визначатися як "*трудовий потенціал працівника*" та застосовується до сьогодні.

Трудовий потенціал працівника визначається сукупністю фізичних і духовних якостей людини, що забезпечують можливість і межі її участі у трудовій діяльності, здатність досягати певних результатів у визначених умовах, а також удосконалюватися в процесі праці. Важливими елементами *трудового потенціалу* кожного працівника є [17]:

- особисті мотиви поведінки, цінності, ставлення до праці, творча активність тощо;
- соціально-демографічні характеристики, які включають стать, вік, національність і т.д.;
- психофізіологічні характеристики: стан здоров'я, тип темпераменту, працездатність і схильність до певного роду діяльності тощо;
- основні кваліфікаційні характеристики - рівень освіти, практичний досвід, професіоналізм, творчі здібності тощо.

Поняття "*трудовий колектив*" можна розглядати як:

- соціальну організацію, що може бути представлена адміністративно-правовою структурою;
- спільноту, що представляє структуру малих груп з їхніми міжособистісними зв'язками, а також поділом кадрів підприємства на соціальні групи.

На практиці з метою визначення діяльності з координації роботи людей використовують різні поняття [18]:

- "управління";
- "менеджмент";
- "адміністрування";
- "керування" тощо.

Управління – найбільш загальне поняття, яке поширюється на значне коло різноманітних об'єктів, явищ і процесів, наприклад: технічні системи; господарські системи; суспільні системи; державні системи тощо.

Під менеджментом розуміють самостійний вид професійної діяльності, який направлений на досягнення з обов'язковим застосуванням економічних

методів управління визначених цілей організації (підприємства) шляхом раціонального використання матеріальних, фінансових і трудових ресурсів. Це поняття використовують переважно для характеристики процесів управління господарськими організаціями (підприємствами).

Під адмініструванням розуміють поняття, що використовується для позначення процесів керування діяльністю апарата управління підприємства та поширюється на управління державними установами або організаціями.

Керування – поняття, яке поширюється на мистецтво тієї або іншої особи (менеджера) впливати на поведінку і мотиви діяльності підлеглих з метою досягнення цілей організації.

Під штатною структурою розуміють кількісно-професійний склад персоналу організації (підприємства), розмір оплати праці та фонд заробітної плати працівників.

Організаційна структура – це склад і підпорядкованість, взаємозалежність різних ланок управління. Організаційну структуру можна охарактеризувати через такі поняття:

- рівень управління;
- самостійна частина організаційної структури;
- апарат (орган) управління;
- структурний підрозділ;
- самостійна частина ланки управління (відділ, служба тощо).

Розподіл управлінських функцій між керівництвом і окремими підрозділами відображає *функціональна структура*.

Чисельність персоналу в організаціях (на підприємствах) визначається масштабами діяльності самої організації, її фінансовими можливостями, особливостями її конкурентного стану, рівнем механізації й автоматизації виробничих процесів тощо. Зазначені критерії визначають нормативну (планову) величину чисельності персоналу, за якою складається штатний розпис і в якому закріплюється посадовий (штатний) склад працівників, де конкретизуються [19-20]:

- перелік посад;
- чисельність штатних одиниць;
- розмір посадових окладів, надбавок і доплат (за умови, що надбавки та доплати передбачено відповідними нормативними документами).

Крім того, також можлива поява інших параметрів.

Штатний розпис визначає можливість, складає своєрідний план та параметри можливої діяльності організації.

Фактично використовують показник *облікової* (фактичної) чисельності, як кількість працівників, що офіційно працюють в організації у певний період часу.

У складі облікової чисельності, як правило, виділяють три категорії працівників - постійні, тимчасові, сезонні [17].

Постійними вважаються прийняті безстроково або на термін більше одного року за контрактом. Тимчасові – прийняті на термін до 2 місяців, а для заміщення тимчасово відсутньої особи – до 4 місяців. Сезонні – це прийняті на роботу, яка носить сезонний характер, на термін до 6 місяців.

Таким чином, управління персоналом – це професійна діяльність, спрямована на максимально ефективне функціонування працівників в організації. Управління персоналом передбачає основні етапи, які показані на рис.1.2 та виконується в процесі певних цілеспрямованих завдань.

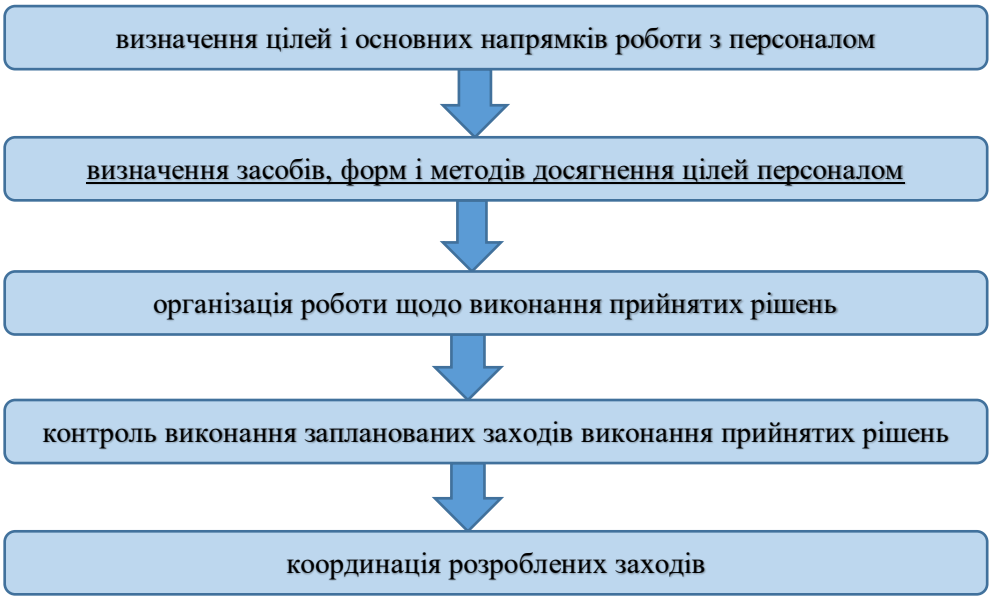

Рис.1.2. Етапи управління персоналом

Основні завдання управління персоналом [21]:

- забезпечення відповідності потребам організації через здійснення рекрутингу і підбір кадрів, необхідних для досягнення стратегічних цілей;
- розвиток персоналу, забезпечення можливостей для навчання та професійного зростання працівників;
- створення мотиваційної системи, розробка та впровадження системи стимулювання, що підтримує високий рівень мотивації працівників;
- збереження та розвиток талантів, розробка та впровадження заходів для утримання ключових працівників і розвиток їхнього потенціалу.
- управління відносинами з персоналом, вирішення конфліктів, підтримка комунікації та створення позитивного організаційного клімату;
- ефективне використання трудового потенціалу, оптимізація розподілу завдань та визначення оптимального використання трудового потенціалу.

Основні функції управління персоналом вказані на рис.1.3

Рис. 1.3. Функції управління персоналом

Управління персоналом спрямоване на оптимізацію взаємовідносин між

організацією та її працівниками для досягнення стратегічних цілей і підвищення ефективності виробничих процесів.

Вдосконаленої системи управління персоналом є досить складним явищем. Відсутність практичних рекомендацій щодо управління персоналом в компаніях в умовах війни і трансформацій, які базувались би на успішних прикладах застосування. Більшість рекомендацій, як визначено в дослідженні [22] застарілі, носять теоретичний характер, та не враховують проблеми сучасних реалій – міграційні процеси, політична та економічна нестабільність, законодавчі зміни та неадаптованість законодавства про працю до нових умов.

1.3 Сучасні моделі управління персоналом і їх особливості

Сучасне управління персоналом включає різноманітні моделі та підходи, які допомагають ефективно використовувати потенціал працівників. Шлях розвитку, який пройшли теорії управління персоналом, демонструє поступове зростання впливу людського фактору на організацію трудового процесу. Сучасні організації (підприємства, компанія) нагадують складний організм, життєдіяльність якого безпосередньо залежить від злагодженості роботи окремих елементів. Щоб забезпечити ефективну взаємодію на всіх рівнях, застосовуються комплексні моделі управління персоналом. Фахівці з менеджменту організацій ділять моделі на чотири основні групи: німецьку (європейську), американську, японську і сімейну [24].

Американська (англо-американська або аутсайдерська) модель корпоративного управління ґрунтується на використанні зовнішніх інструментів контролю. Така компанія, менеджмент якої побудований на базі даної моделі, в значній мірі попадає під вплив зовнішніх факторів (фондового ринку або ринку праці). На всі виробничі процеси і всіх учасників спільноти здійснюється вплив з боку безпосередніх керівників організації. Сьогодні ця модель найбільш поширена в США, Швеції, Великобританії.

Соціальна рівність характерна для *німецької* (*німецької, інсайдерської*) моделі управління персоналом. У цій моделі вплив факторів зовнішнього управління, навпаки, зменшується. На перший план виступають такі аспекти управління персоналом, як забезпечення абсолютної зацікавленості кожного акціонера або співробітника в результатах роботи компанії. Принципи німецької моделі управління персоналом покладено в основу корпоративної культури країн Центральної Європи.

Японська модель корпоративного управління зосереджена на пріоритеті колективних інтересів над особистими і на верховенстві корпоративного духу, відданості роботодавцю, вона підкріплюється наданням працівникам ряду соціальних гарантій та інших благ, характеризується досягненням балансу інтересів трьох сил - інвесторів, керівників і працівників. При цьому, у багатьох японських компаніях практикується система довічного найму. Слід зауважити, що далеко не в кожній компанії приживається таке управління персоналом, кадри, підібрані стихійним чином, далеко не завжди готові вбудуватися в систему настільки ж щільно, як японські працівники, яких з раннього віку готують до роботи на конкретному підприємстві.

Сімейний капіталізм (або *сімейна модель управління компанією*) поширений в країнах Латинської Америки, Азії, Канаді, нерідко зустрічається у Франції, Італії та інших країнах Європи. Суть системи зводиться до концентрації і розподілу капіталу за сімейними каналах. Сімейна модель корпоративного управління забезпечує жорсткий контроль над бізнесом, але має ряд недоліків: навіть якщо на практиці застосовується найсучасніша теорія управління персоналом організації, основною метою існування компанії залишається задоволення інтересів однієї сім'ї при слабкій інформаційній прозорості всіх бізнес-процесів.

Описані моделі корпоративного менеджменту не є взаємовиключними, кадрова політика з управління персоналом будь-якого окремо взятого підприємства може містити елементи двох і більше моделей, оскільки жодна з них не має суттєвих переваг перед іншими і не може вважатися універсальною.

Якісно нові вимоги до кадрових менеджерів, які висуваються сучасними умовами діяльності підприємств, пред'являють і обумовлюють потребу більш високої інтенсивності їхньої праці, раціонально використовувати час, володіння комплексом організаційних і психологічних якостей, застосовувати креативний підхід до роботи в управлінні персоналом [25-27].

Сьогодні в Україні управлінню персоналом приділяється недостатньо уваги. Склалася ситуація, при якій технології розробки і прийняття кадрових рішень є недосконалими і науково недостатньо необґрунтованими. В управлінні персоналом у переважній більшості випадків менеджерам з персоналу не вистачає орієнтації на досягнення ефективності такого управління. Це визначається рядом об’єктивних факторів:

- служби управління персоналом організацій і підприємств мають недостатній організаційний статус і розглядаються керівниками організації як обслуговуючий підрозділ з обмеженим колом виконуваних функцій;
- працівники кадрових органів мають недостатньо високий рівень компетентності в галузі;
- низький рівень організаційно-правової і соціально-психологічної культури працівників кадрових служб.

Менеджери з персоналу у більшості випадків не мають достатніх навиків в зосередженні кадрової роботи на кінцеві фінансово-господарські показники підприємства. Ця проблема обумовлена низьким рівнем професійної і соціальної компетентності менеджерів з персоналу. Вона також є причиною недостатнього нерозуміння керівниками підприємств місця і ролі кадрових служб у вирішенні загальних задач на досягнення цілей підприємства. Перераховані проблеми тягнуть за собою недостатньо ефективне виконання таких важливих функцій управління персоналом, як:

- визначення якісного і кількісного складу працівників;
- інформаційне забезпечення створеної на підприємстві системи управління персоналом;

- психологічна діагностика персоналу;
- регулювання та аналіз взаємовідносин у колективі, управління виробничими і соціальними конфліктами;
- планування ділової кар'єри працівників;
- професійна і соціально-психологічна адаптація нових працівників;
- аналіз і оцінка потенціалу персоналу;
- формування стабільного трудового колективу;
- формування кадрового резерву;
- аналіз попиту та задоволень персоналу.

Сьогодні у переважній більшості підприємств і організацій середнього рівня немає в наявності положень про кадрову службу, недостатньо відпрацьовані кадрові технології, низький рівень координації діяльності кадрової служби з іншими структурними підрозділами організацій (підприємств). Недостатнє впровадження у практику кадрових служб наукових методів відбору, оцінювання, навчання кадрів фатально знижує як економічну, так і соціальну ефективність управління персоналом.

Ще одною проблемою у сфері управління персоналом є відсутність цікавості керівників кадрових служб до засобів виявлення та розуміння очікувань і намагань, настроїв, соціальних орієнтацій працівників і цілих колективів, що значно обмежує можливості керівника підприємства по створенню "єдиної команди" для ефективного вирішення завдань, які стоять перед підприємством, організацією.

Враховуючи зазначений аналіз, у сучасних умовах виникла нагальна об'єктивна необхідність в удосконаленні управління персоналом в організаціях (на підприємствах). Для підвищення ефективності управління персоналом на всіх рівнях необхідно розробити відповідні заходи. Потрібно зазначити, що в умовах ринку розвиток людських ресурсів потребує кооперації і співробітництва, тому що зв'язки між організаціями дозволяють об'єднати інтелектуальні ресурси підприємств з метою впровадження вливань різного роду у їхню діяльність.

Для підвищення ефективності всередині організації керівники і менеджери повинні усвідомити та врахувати недоліки традиційних концепцій управління персоналом і сформувати нову кадрову політику корпоративної філософії керівництва. Такі підходи будуть сприяти узгодженню економічних і соціальних інтересів окремих працівників і робочих груп та досягненню соціального партнерства в колективі.

ВИСНОВОК до розділу 1. Таким чином, стає очевидним, що розглянуті теорії (класична, людських ресурсів, людських відносин) зробили значний внесок у ефективне управління персоналом та є фундаментальною основою для ефективного управління організаціями, наголошуючи на важливості людського фактору в успіху організації. Ефективна практика управління персоналом передбачає повне знання людини на робочому місці, її взаємодії з керівниками та колегами як на офіційному, так і на неформальному рівнях, а також організаційних питань, здатних мотивувати працівника до підвищення продуктивності. Теорія дає розуміння природи та характеристик людей, які необхідно розуміти, маніпулювати ними та використовувати, щоб отримати від людей найбільшу ефективність при виконанні ними обов’язків.

Керівники організацій повинні бути повністю обізнаними щодо принципів теорії людських відносин і тих факторів, які є загальними для людей, щоб ними було легше керувати в процесі досягнення організаційних цілей і завдань. Особливості функціонування організацій і підрозділів кібербезпеки вимагають детального аналізу проблем управління персоналом через призму завдань, які специфічні для інформаційної безпеки.

РОЗДІЛ 2
АНАЛІЗ МЕТОДІВ ТА МОДЕЛЕЙ ОЦІНКИ ЕФЕКТИВНОСТІ УПРАВЛІННЯ ПЕРСОНАЛОМ В КІБЕРБЕЗПЕЦІ

2.1 Особливості управління персоналом у сфері кібербезпеки

Протягом останніх кількох років відбувається безперервний розвиток інформаційно-комунікаційних технологій, які визначають зміни у сучасному світі. Прогресуюча комп'ютеризація та перенесення діяльності в кіберпростір є невід'ємними аспектами функціонування окремих осіб, організацій, держав та міжнародного співтовариства. Як визначають дослідники [28-29], ці елементи стали мішенню для країн, що розвиваються, і відмінною рисою високорозвинених країн.

Кібербезпека сьогодні є міждисциплінарним питанням, оскільки потребує скоординованих дій у технологічній, правовій, організаційній, процедурній та соціальній сферах. Разом з тим, багато науковців у своїх дослідженнях визнають, що людський фактор є найслабшою ланкою в системі кібербезпеки. Агентство Європейського Союзу з кібербезпеки (ENISA) наголошує, що підвищення рівня навичок та знань є обов'язковим елементом у побудові стійкості суспільства до загроз кіберпростору [30-32].

Управління персоналом - це процес розробки кадрової стратегії впливу на персонал для підвищення його ефективності та досягнення цілей організацій (підприємства). Одним із інструментів підвищення ефективності вважають мотивацію. Наприклад, в дослідженні [33] висвітлюються питання підвищення ефективності мотивації персоналу підприємства, проведений аналіз та надана характеристика основних зарубіжних моделей мотивації працівників, уточнено визначення сутності поняття “мотиваційний механізм в управлінні персоналом підприємства”, розглянуто категорії матеріального та нематеріального

стимулювання. Автором обґрунтовано тезу про те, що комплексне застосування роботодавцями методів прямої і непрямої мотивації дозволяє зберегти персонал і підвищити ефективність трудової діяльності, сприяє збільшенню інклюзії працівників в трудовий процес. Розроблено структуру мотиваційного механізму та її складові елементи, запропоновано напрями вдосконалення мотиваційного механізму в управлінні персоналом підприємства. Систематизовано та узагальнено пріоритетні види матеріального та нематеріального стимулювання працівників. Розроблені пріоритетні напрями мотиваційного механізму що дозволять підвищити ефективність системи управління персоналом підприємства та покращити організацію соціально-трудових відносин між працівниками і роботодавцями

Хороша кібербезпека починається зі співробітників. Людські ресурси часто є ресурсом для вдосконалення навичок працівників, пов'язаних з роботою, що може включати спеціалізоване навчання для внутрішніх систем. 0Не всі співробітники мають однаковий досвід або знання про технології, якими вони користуються щодня. Це може зробити організацію відкритою для загроз.

Управління ІТ персоналом – наріжний камінь, на якому тримається діяльність всього ІТ-відділу і залежить успішність застосування ІТ-інфраструктури у всій компанії. Часто цьому питанню приділяється дуже мало уваги. Керівники вважають, що у цьому випадку важлива техніка, а не люди. Однак саме від правильної організації праці людей залежить, наскільки добре та правильно функціонуватиме техніка.

Питання керівництва кадрами невеликого підрозділу інформаційної безпеки мало означає на початковому етапі розвитку становлення. Для більшого контингенту працівників у певний момент виявляється, що керівник не може одноосібно керувати всіма організаційними сторонами захисту інформації. У цей час в організації створюється структура менеджменту, від продуманості якої залежить вся подальша доля ефективності виконання завдань, які постають перед колективом. Управлінням персоналом займається галузь управління під назвою Human Resource (HR). Існує й спеціальний термін позначення керівництва

професіоналами інформаційної сфери: ITHR.

Сьогодні в кадровому менеджменті виділяють декілька етапів роботи ITHR, від якості яких в подальшому буде залежати ефективність роботи організації (рис. 2.1):

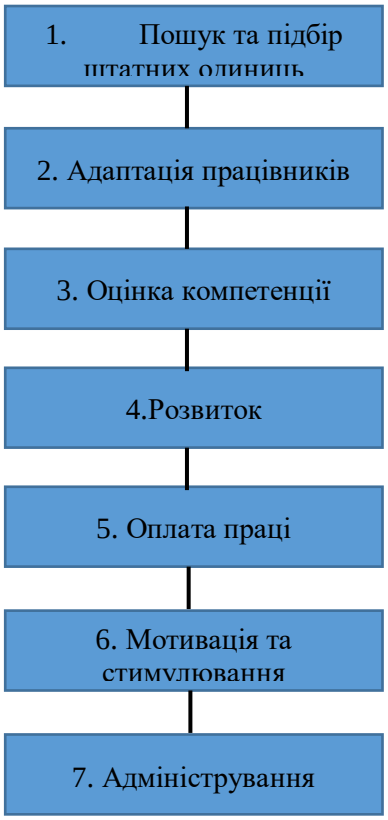

Рис. 2.1. Етапи кадрового менеджменту у IT-сфері

1. Необхідно знати, де IT-фахівці розміщують резюме, де варто публікувати оголошення про вакансії, які існують інші способи пошуку потрібних фахівців (контакти у професійній спільноті, рекомендації ділових партнерів). З потенційними співробітниками необхідно проводити співбесіди, застосовувати тестування та пропонувати пробні завдання.

2. Досвідчений HR-менеджер знає, які завдання поставити перед новачком спочатку, як включити його в робочий процес, як познайомити його з особливостями діяльності фірми, які навчальні матеріали запропонувати, з ким із колег насамперед познайомити.

3. На цьому етапі стає зрозуміло, які професійні навички та особисті

особливості співробітника, яким чином їх найкраще застосувати. Оцінка проводиться не лише щодо новачків, а й на постійній основі щодо всіх працівників. Це може бути як формальна регулярна атестація, так і неформальні бесіди та спостереження.

4. Далі, оцінивши компетенцію, HR-менеджер може дійти висновку, що комусь із фахівців треба запропонувати підвищити кваліфікацію, а когось навпаки варто перевести на більш високу посаду, тому що стару посаду він явно переріс. Іноді курси перенавчання проводяться масово – наприклад, у разі впровадження нових технологій.

5. Фахівець, відповідальний за управління кадрами, повинен брати участь у виборі системи оплати праці, у визначенні рівня зарплат, у присудженні премій. Принаймні він повинен чітко розуміти, скільки фірма може витратити на оплату праці і як ці кошти розподіляються.

6. Організація успішно розвивається, якщо більшість співробітників зацікавлені у своїй роботі та добре ставляться до колег. Однак до питань мотивації, особливо в IT-сфері, не можна підходити формально та нав'язливо. Люди, які звикли працювати з комп'ютерами та програмами, найчастіше насторожено ставляться до ідеї участі у стандартних корпоративних розвагах. Але до них можна знайти підхід, якщо розібратися в їхній професійній культурі та традиціях.

7. Багато нюансів роботи з персоналом чітко прописані у законах, і некомпетентність у цій сфері може призвести до негативних наслідків у разі візиту контролюючих органів. Тому HR-менеджер повинен розбиратися у трудовому законодавстві, він уміє укладати трудові договори, складати інструкції та звіти.

Виділяють п'ять основних функцій HR-менеджерів у сфері IT, що займаються управлінням персоналу: Адаптація; Навчання; Розвиток; Мотивація; Оцінка (рис.2.2).

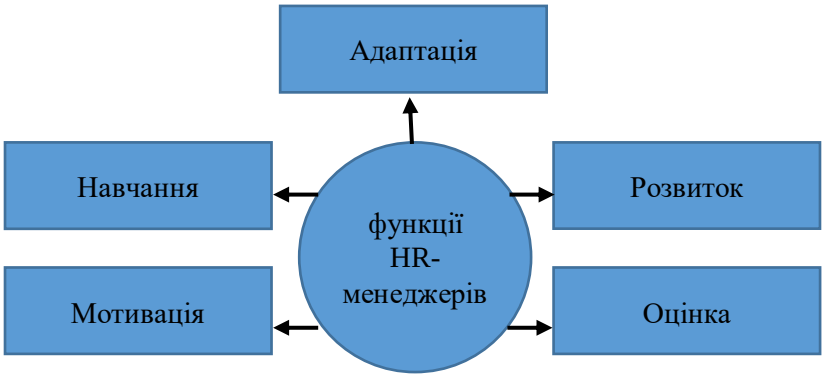

Рис. 2.2. Функції HR-менеджерів у сфері IT

У сфері кібербезпеки особливо важливо ефективно управляти персоналом через постійне зростання загроз в інтернеті та вимог до захисту цифрових активів.

Деякі ключові аспекти, які визначають актуальність підвищення ефективності управління персоналом у цій сфері детально описані у Загальних принципах управління персоналом у сфері кібербезпеки (Загальні принципи NICE - Національної ініціативи з освіти у сфері кібербезпеки) [34], що були розроблені основним авторським колективом, який включав представників багатьох міністерств і державних органів Федерального уряду Сполучених Штатів Америки.

Вони можуть включати (рис.2.3):

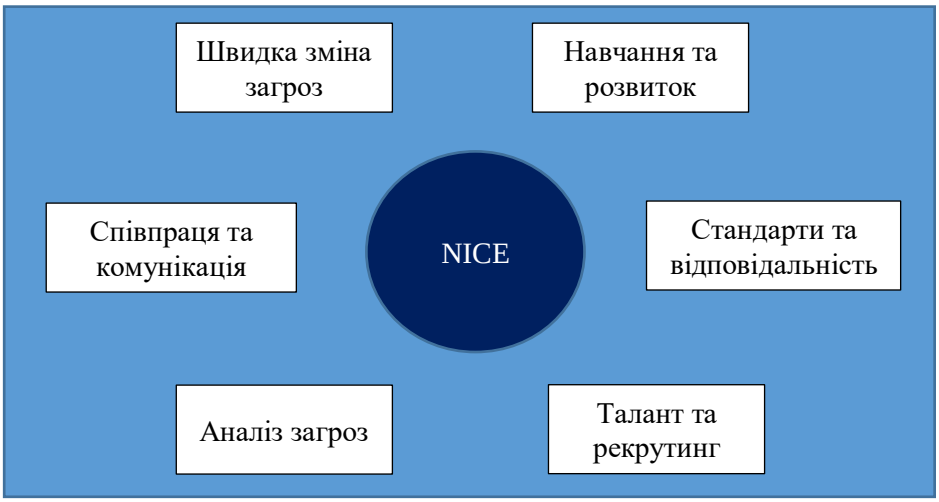

Рис. 2.3. Ключові аспекти ефективності управління персоналом у сфері кібербезпеки

У цій публікації (NICE) описується загальна структура управління персоналом кібербезпеки (NICE Framework). NICE Framework допомагає організаціям подолати бар'єр опису своєї робочої сили багатьом зацікавленим сторонам, представляючи підхід до будівельних блоків. Завдяки використанню концептуальних будівельних блоків NICE Framework представляє можливість спільного внутрішнього та зовнішнього використання для організацій. Цей підхід дозволяє організаціям адаптувати та впроваджувати NICE Framework відповідно до свого унікального робочого середовища. Більше того, створюючи спільну мову, NICE Framework знижує бар'єр входу для організацій, які прагнуть вступити та співпрацювати з іншими організаціями.

За принципами NICE організація управління персоналом у сфері кібербезпеки здійснюється для всіх учасників, як поточних працівників так і студентів або тих, хто навчається. Навчання їх здійснюється постійно, включаючи і осіб, які шукають роботу та претендують на вакантні місця. Два основних типи концепцій NICE показані на рис. 2.4.

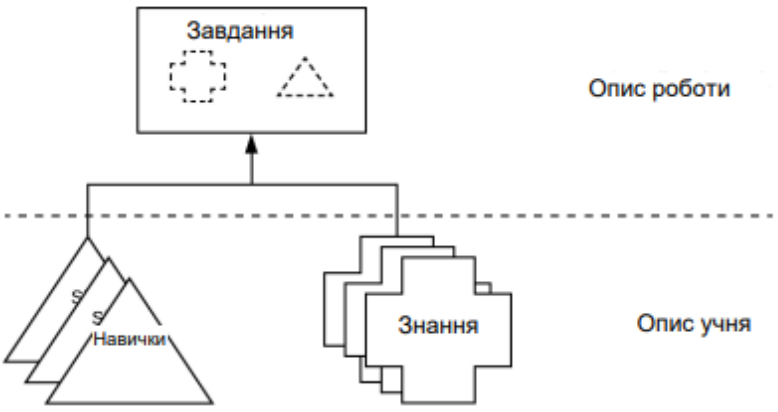

Рис. 2.4. Підхід до навчання за принципом NICE

Аналіз рисунку 2.4. вказує на те, що за принципами NICE навчання персоналу здійснюється на всіх рівнях: учня а також працівника при виконанні функціональних обов'язків.

Цей документ виражає цю роботу у формі формулювання Завдань та

описує формулювання компетентностей, які створюють основу для тих, хто навчається, включаючи студентів та осіб, які шукають роботу, і працівників. Використання цих формулювань допоможе студентам розвивати навички, особам, які шукають роботу, демонструвати потрібну компетентність, а працівникам - виконувати завдання [34].

Workforce Framework for Cybersecurity побудовано на наборі окремих будівельних блоків, які описують роботу, яку потрібно виконати (у формі завдань), і те, що потрібно для виконання цієї роботи - як знання та навички (рис. 2.5)

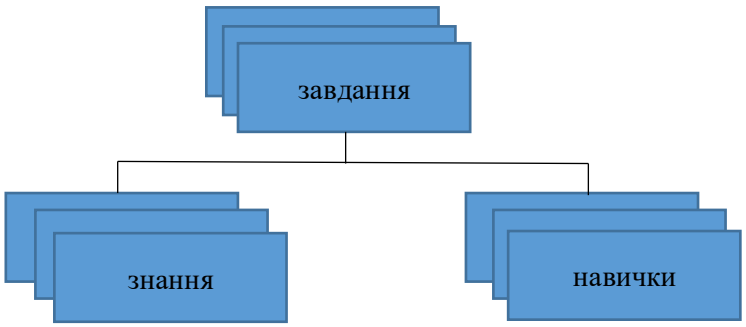

Рис.2.5. Побудова блоків за принципом NICE

Формулювання завдань призначені для опису роботи, яка повинна бути виконана у відповідності з контекстом організації.

При формулювання знань за принципом NICE, як набір понять в пам'яті, описуються базові або спеціальні знання, що можуть знадобитися для виконання завдання. При цьому, для завдання може знадобитися декілька формулювань знань або одне формулювання знань може бути використане для виконання багатьох різних завдань.

При формулюванні навичок, як здатність виконувати потрібну діяльність, описують прості чи складні навички і для виконання завдання можуть знадобитися декілька формулювань навичок або одне формулювання навички може застосовуватися для виконання більш ніж одного завдання.

Ці будівельні блоки є організаційними конструкціями, які підтримують зручність використання та реалізацію NICE Framework. Вони забезпечують

механізм, за допомогою якого як організації, так і окремі особи можуть зрозуміти обсяг і зміст NICE Framework.

Такий підхід має на меті надання менеджерам персоналу IT загального набору складових, на основі яких можна розробити модель, яка тісніше пов'язана з унікальним контекстом конкретної організації.

Ключові аспекти (рис. 2.3, 2.4) також за результатами дослідження науковців [35-36] забезпечують ефективність управління ризиками інформаційної безпеки організацій.

Враховуючи швидку зміну загроз, кіберзлочинці постійно змінюють свої методи та техніки. Тому ефективне управління персоналом повинно бути гнучким і готовим відповідати на нові виклики.

Іншим аспектом є навчання та розвиток працівників. Забезпечення постійного навчання та розвитку персоналу є важливим елементом. Кадри повинні поряд із змінами технологій вивчати нові методи боротьби з кіберзагрозами.

Кібербезпека є конкурентною сферою, і здобуття та утримання висококваліфікованих фахівців стає дедалі важливішим завданням. Визначення чітких стандартів та відповідальних ролей може покращити ефективність управління персоналом у кібербезпеці.

Використання аналітики для прогнозування та аналізу потенційних кіберзагроз може допомогти підготуватися та запобігти інцидентам.

Ефективна співпраця між різними відділами та комунікація в межах команди є ключовими факторами успіху управління персоналом у сфері кібербезпеки.

Одним із напрямків підвищення ефективності може бути використання сучасних технологій, таких як штучний інтелект для аналізу загроз, автоматизації завдань та виявлення аномалій у поведінці мережі. Подальший розвиток і вдосконалення методів управління персоналом у цій галузі може допомогти забезпечити більш ефективний захист від кіберзагроз.

2.2 Аналіз сучасних підходів та проблем у виборі, навчанні, мотивації та управлінні персоналом в галузі кібербезпеки

Аналіз сучасних проблем управління персоналом в галузі кібербезпеки може бути корисним для розуміння того, які виклики стоять перед організаціями, що займаються кібербезпекою. Згідно з дослідженням, проведеним CSIS (Центр стратегічних і міжнародних досліджень), 82% роботодавців повідомляють про нестачу кадрів у галузі кібербезпеки, а 71% вважають, що ця нестача талантів призводить до прямої і вимірюваної шкоди для їх організацій. За даними CyberSeek, США стикаються з нестачею майже 314 000 фахівців з кібербезпеки на січень 2019 року. Це при тому, що загальна кількість працюючих фахівців з кібербезпеки в країні становить лише 716 000. За даними, отриманими з вакансій, кількість вакансій з кібербезпеки, які не були заповнені, зросла більш ніж на 50% з 2015 року. За прогнозами, до 2022 року глобальна нестача кадрів у галузі кібербезпеки може досягти понад 1,8 мільйона незаповнених посад. Нестача кадрів існує для майже кожної посади в галузі кібербезпеки, але найбільш гострої потреби є для висококваліфікованого технічного персоналу (рис. 2.6).

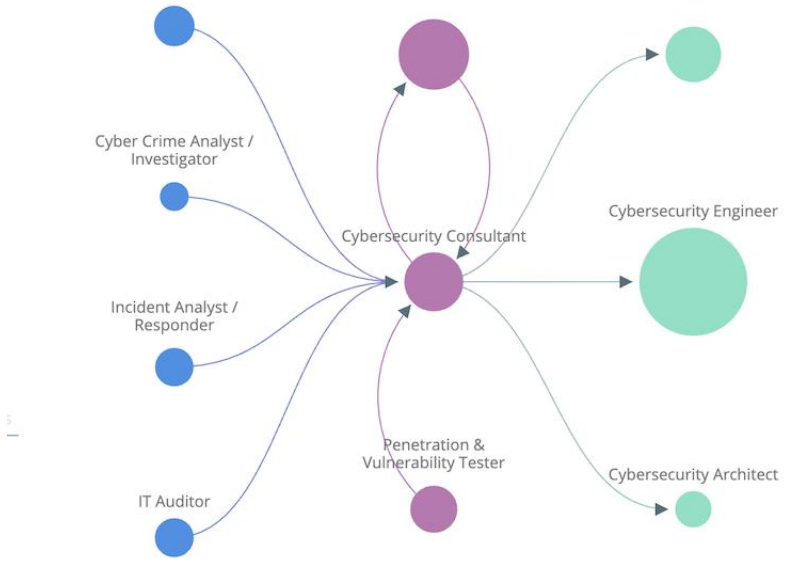

Рис. 2.6. Основні посади висококваліфікованих фахівців кібербезпеки

З вересня 2022 року по серпень 2023 року на кожні 100 вакансій припадало лише 72 працівники з кібербезпеки, затребувані роботодавцями.

Рис. 2.7. Укомплектованість посад фахівцями кібербезпеки в організаціях США

В ENISA наголошують, що в останні кілька років діяльність, що сприяє кібербезпеці, полягала переважно в технічній безпеці систем і пристроїв. Важливість людського фактору в системі кібербезпеки була обмежена насамперед процедурами та санкціями [37]. Можливо, це сприяло низькому рівню компетенцій у запобіганні кібератакам.

У науковій літературі та ініціативах багатьох країн та міжнародних організацій почали помічати необхідність удосконалення компетенцій у сфері кібербезпеки. У цьому контексті з'явилося поняття «кібергігієна», що означає знання та поведінку, спрямовані на зменшення ризикованої поведінки в кіберпросторі [38] . Належний рівень кібергігієни знижує вразливість системи до загроз і включає здатність запобігати потенційній атаці [39]. Кібергігієна – це набір правил і поведінки, дотримання яких підвищує безпеку окремих користувачів і позитивно впливає на організацію. Ефективні практики

кібергігієни були запропоновані як цінні для подолання кіберризиків, але на сьогоднішній день ці практики набули західної або американської номології. Для людей незахідного походження відмінності в культурних нормах, вимогах і обмеженнях, швидше за все, вимагатимуть від них іншого підходу до кібергігієни і, можливо, переосмислення того, що означає її ефективна практика. Використовуючи вибірку користувачів домашніх інформаційних систем у США та Саудівській Аравії, це дослідження перевіряє гіпотезу про те, що національна культура пом'якшує вплив очікувань та цінності людей на їхню мотивацію дотримуватися практик кібергігієни. Пропаганда принципів кібергігієни може допомогти уникнути великої кількості інцидентів безпеки.

Важливе значення для забезпечення кібербезпеки мають компетенції. Як брак знань, так і відсутність відповідних навичок може сприяти виникненню кіберзагроз. Кіберпростір є предметом подальшої еволюції, тому важливо вдосконалювати компетенції, щоб мінімізувати ризик виникнення загроз.

Загрози кіберпростору стають все більш витонченими і охоплюють широкий спектр методів і прийомів атак. Таким чином, кіберпростір є середовищем позитивної і негативної співпраці, оскільки він не тільки створює умови для прогресу в широкому розумінні, але також є джерелом або об'єктом загроз. Забезпечення технологічного розвитку з одночасною необхідністю забезпечення кібербезпеки є значним викликом. Це питання знайшло своє відображення в стратегіях і нормативно-правових актах багатьох країн і міжнародних організацій.

Національний інститут стандартів і технологій заснував Національну ініціативу з освіти в галузі кібербезпеки (NICE), яка є форумом для співпраці між урядом, науковими колами та приватним сектором. NICE розробила модель компетенцій у сфері кібербезпеки, яка є спробою визначити, класифікувати та нормалізувати знання, навички та ставлення, пов'язані з кібербезпекою [40, 41].

Модель представлена у вигляді піраміди, що складається з декількох рівнів (рис. 2.8).

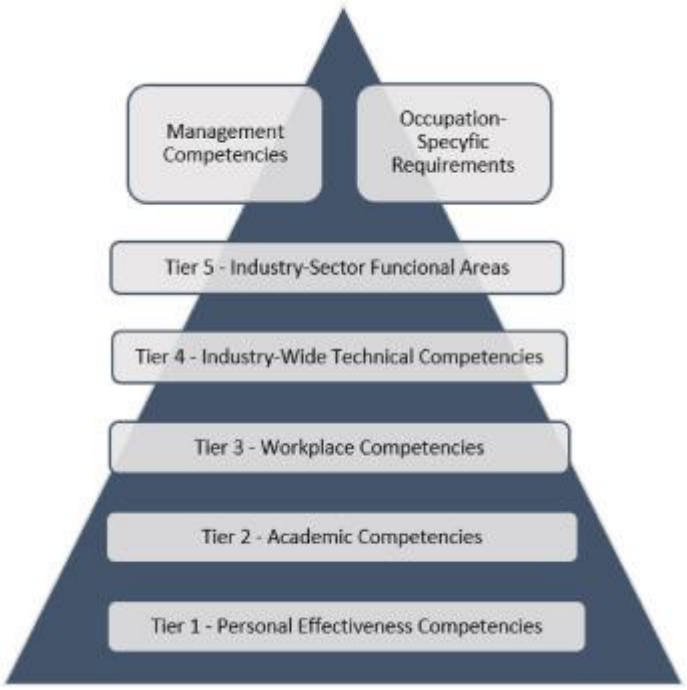

Рис. 2.8. Модель компетенцій у сфері кібербезпеки [42].

Результати емпіричних даних свідчать, що у 2016-2017 роках [41] в органах державного управління були присутні певні проблемні місця в аспекті управління інформаційною безпекою, до яких, зокрема, належать:

- відсутність організації СУІБ;
- неповна або застаріла документація СУІБ;
- відсутність регулярного аналізу ризиків;
- відсутність перевірок, аудитів або контролю;
- обмежене використання заходів фізичного та технологічного захисту;
- *недостатня підготовка або професійний розвиток*.

У 2018-2019 роках рішення Європейського Союзу, а саме Регламент GDPR (General Data Protection Regulation - Загальний регламент про захист даних в межах законодавства Європейського Союзу) та Директива NIS (Директива про мережеву та інформаційну безпеку [43]) вплинули на підвищення рівня безпеки інформації в державному управлінні та мають значно обмежену кількість виявлених порушень. Результати дослідження дозволяють припустити, що забезпечення інформаційної безпеки в державному управлінні потребує

системного підходу, що випливає з необхідності постійного вдосконалення.

Методи оцінки при відборі персоналу можна умовно розділити на суб'єктивні та об'єктивні методи.

Суб'єктивні методи включають:

- особистісні показники;
- опитувальники стресу та стилю подолання стресу;
- інтерв'ю та оцінки супервізора.

Об'єктивні показники включають:

- вибірки робіт;
- біографічні дані, такі як стать і вік;
- тести ситуаційних суджень;
- тести здібностей;

У цьому розділі представлено кілька традиційних підходів, які використовуються при відборі персоналу в різних організаціях, командах і на підприємствах.

Для формування методик підбору персоналу на початковому етапі науковцями проведено низку досліджень взаємозв’язку психологічних характеристик та станом інформаційної та кібербезпеки організацій, підприємств. Так у дослідженні [44] вивчався взаємозв'язок між ризикованою поведінкою у сфері кібербезпеки, ставленням до кібербезпеки в бізнес-середовищі, інтернет-залежністю та імпульсивністю. 538 учасників, які працюють неповний або повний робочий день у Великій Британії, заповнили онлайн-анкету, при аналізі даних були використані відповіді 515 осіб. Опитування включало ставлення до кіберзлочинності та кібербезпеки в масштабах бізнесу, міру імпульсивності, інтернет-залежності та шкали «ризикованої» поведінки у сфері кібербезпеки. Результати продемонстрували, що інтернет-залежність є важливим предиктором ризикованої поведінки в галузі кібербезпеки. Позитивне ставлення до кібербезпеки в бізнесі було негативно пов'язане з ризикованою поведінкою у сфері кібербезпеки. Нарешті, показник імпульсивності показав, що як увага, так і моторна імпульсивність були

значними позитивними предикторами ризикованої поведінки кібербезпеки. Результати є подальшим кроком у розумінні індивідуальних відмінностей, які можуть регулювати належну практику кібербезпеки, підкреслюючи необхідність зосередитися безпосередньо на більш ефективних механізмах навчання та обізнаності.

Обізнаність про інформаційну безпеку (ISA - Information Security Awareness) є невід'ємною частиною захисту організації від кіберзагроз. Метою цієї статті є подальше встановлення валідності опитувальника з людських аспектів інформаційної безпеки (HAIS-Q), як ефективного інструменту для вимірювання МСА.

Опитувальник з людських аспектів інформаційної безпеки (HAIS-Q) [44,45], який складається з 63 пунктів, вимірює МСА в 21 конкретній області, які згруповані в одну з семи основних областей інформаційної безпеки. HAIS-Q має як теоретичні, так і прикладні наслідки. З теоретичної точки зору, інструмент був розроблений і вдосконалений з використанням різних груп населення, включаючи студентів, широку громадськість і співробітників державних і фінансових установ. У дослідженні [46] 1112 студентів університету пройшли тест HAIS-Q, а також взяли участь в емпіричному лабораторному експерименті з фішингу. Результати показали, що учасники, які набрали більш високі бали за HAIS-Q, мали кращу продуктивність в експерименті з фішингом. Це означає, що HAIS-Q може передбачити аспект поведінки інформаційної безпеки та надати докази його конвергентної валідності. У дослідженні 2 HAIS-Q було проведено для більш репрезентативної популяції з 505 працюючих австралійців для подальшого встановлення конструктної валідності інструменту. Результати факторного аналізу та інших статистичних методів свідчать про валідність HAIS-Q як надійного показника ISA. Практичні наслідки HAIS-Q, як вважають дослідники [44-47], підтверджують висновок про те, що опитувальник може бути використаний фахівцями з інформаційної безпеки.

Висновки до розділу 2. Аналіз сучасних проблем управління персоналом в галузі кібербезпеки може бути корисним для розуміння того, які виклики стоять перед організаціями, що займаються кібербезпекою.

Загальна структура управління персоналом кібербезпеки (NICE Framework) з її будівельними блоками допомагає організаціям подолати бар'єр опису своєї робочої сили багатьом зацікавленим сторонам. Цей підхід дозволяє організаціям адаптувати та впроваджувати NICE Framework відповідно до свого унікального робочого середовища. Більше того, створюючи спільну мову, NICE Framework знижує бар'єр входу для організацій, які прагнуть вступити та співпрацювати з іншими організаціями, що важливо при побудові системи управління персоналом кібербезпеки в Україні, адаптованої до міжнародних правил.

Опитувальник інформаційної безпеки (HAIS-Q), включаючи людський фактор, є інструментом для вимірювання рівня інформаційної безпеки в організації допомагає визначити, наскільки добре організація захищена від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки запису чи знищення інформації.

РОЗДІЛ 3
РОЗРОБКА СТРАТЕГІЇ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ УПРАВЛІННЯ ПЕРСОНАЛОМ

3.1 Визначення ключових потреб та вимог щодо компетентностей персоналу в галузі кібербезпеки

Професійне вдосконалення, кіберобізнане суспільство України є одним із пріоритетних напрямків посилення кіберстійкості держави. Україна сьогодні проводить докорінну реформу системи підготовки та підвищення кваліфікації фахівців у сфері кібербезпеки, а також здійснює заходи щодо збереження наявного кваліфікованого кадрового потенціалу суб'єктів кібербезпеки. Цифрові навички, кіберобізнаність щодо сучасних кіберзагроз та протидії ним сьогодні є невід'ємними елементами освіти кожного громадянина України [48].

Стратегічні напрямки професійного розвитку фахівців кібербезпеки постійно вдосконалюються у нормативно-правових актах держави. Згідно з Проєктом Стратегії кібербезпеки України (2023 – 2025 роки), модель компетенцій у сфері кібербезпеки визначається як сукупність знань, навичок та досвіду, необхідних для забезпечення кібербезпеки відповідно до вимог національних та міжнародних стандартів. Для забезпечення кібербезпеки України, Проєкт Стратегії кібербезпеки України визначає пріоритети, цілі та завдання забезпечення кібербезпеки України з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави [49].

У сфері кібербезпеки існує кілька ключових компетенцій, якими повинен володіти персонал, щоб забезпечити безпечне функціонування систем безпеки компанії. Деякі з основних навичок включають:

- бажання вникати в технічні питання і розглядати їх з усіх боків;
- ентузіазм і високий ступінь адаптивності;
- сильні аналітичні та діагностичні навички;

- сучасне розуміння поширених веб-вразливостей;
- обізнаність та знання про сучасні стандарти, практики, процедури та методи.

Крім того, володіння такими компетенціями може допомогти претендувати на посаду в цій галузі:

- фундаментальні технологічні навички, такі як конфігурація та керування мережею, встановлення брандмауера, програмування та адміністрування різних операційних систем;
- мови програмування та сценаріїв, такі як JavaScript, є основними компетенціями для експертів з кібербезпеки;
- навички визначення та управління ризиками є постійним обов'язком, який потребує регулярного моніторингу та аналізу.

Багато роботодавців вимагають або вважають за краще, щоб персонал із кібербезпеки мав сертифікати у своїй сфері діяльності. На думку західних фахівців, щоб отримати будь-яку посаду в організації кібербезпеки, необхідно мати одну або декілька з наведених нижче поширених сертифікатів кібербезпеки на рисунках 3.1-3.4.

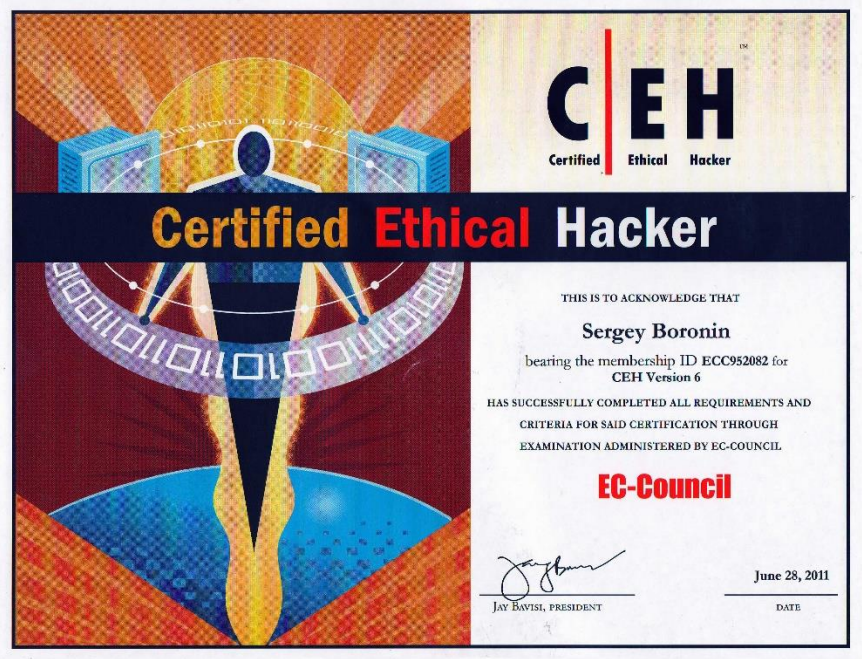

Рис. 3.1. Сертифікат етичного хакера (CEH)

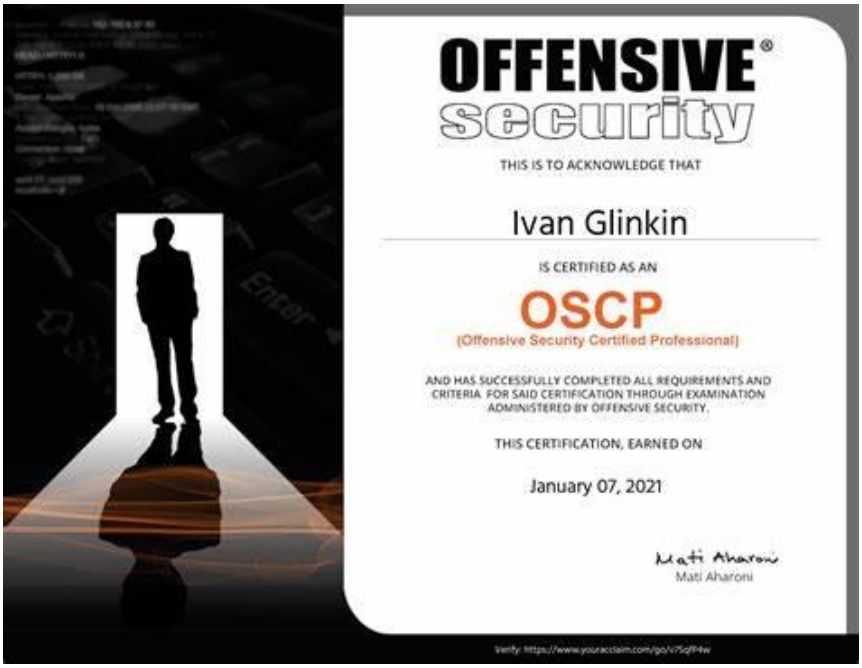

Рис. 3.2. Сертифікат спеціаліста з наступальної безпеки (OSCP)

Рис. 3.3. Сертифікат аудитора з інформаційної безпеки (CISA)

Рис. 3.4. Сертифікат обробника інцидентів GIAC (GCIH)

Одна з причин, чому компанії не можуть знайти потрібних їм досвідчених фахівців з кібербезпеки: просто не так багато технічних фахівців, які оволоділи не тільки необхідними технічними здібностями, але й «м'якими навичками» (наприклад, чіткою комунікацією), а ті, хто вже працевлаштований (часто з високими зарплатами та пільгами, призначеними для того, щоб утримувати їх на місці в довгостроковій перспективі). Фахівцям з безпеки часто доводиться спілкуватися на складні теми з людьми, які можуть не мати достатньої технічної освіти (наприклад, керівникам вищої ланки). Маючи це на увазі, оволодіння наступними зазвичай є необхідною умовою для сходження на більш просунуті позиції на сходах кібербезпеки:

- відмінні презентаційні та комунікативні навички для ефективного спілкування з керівництвом та клієнтами;
- здатність чітко формулювати складні поняття (як письмово, так і усно);
- уміння, розуміння та використання навичок активного слухання (особливо з клієнтами!).

З точки зору кібербезпеки, м'які навички також дозволять вам визначити

приклади та пояснити соціальну інженерію, яка є поширеною проблемою в спільноті безпеки. Ви можете запровадити всі види апаратних і програмних заходів безпеки, але хакери все одно можуть використовувати соціальну інженерію, щоб переконати нічого не підозрюючих співробітників надати їм паролі, облікові дані та доступ до безпечних систем.

Старші фахівці з кібербезпеки, тим часом, повинні організовувати та координувати технічні оцінки вразливостей, включаючи оцінку вразливостей систем та мережі, тестування на проникнення, оцінку веб-додатків, оцінку соціальної інженерії, оцінку фізичної безпеки, оцінку безпеки бездротового зв'язку та впровадження рішень безпечної інфраструктури.

Вони рекомендують і встановлюють технічний напрямок управління інцидентами безпеки, а також забезпечують цілісність отриманого процесу і підходу. З точки зору використання м'яких навичок, їм потрібно буде пояснити керівництву (і показати криміналістично), як була проведена атака.

3.2 Аналіз структури і професійного складу персоналу організацій кібербезпеки

Структура національної системи кібербезпеки України визначена у Законі України Про основні засади забезпечення кібербезпеки України У систему кібербезпеки входять (рис. 3.5) [50]:

- Президент України;
- Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України;
- Кабінет Міністрів України;
- міністерства та інші центральні органи виконавчої влади;
- місцеві державні адміністрації;
- органи місцевого самоврядування;
- правоохоронні, розвідувальні і контррозвідувальні органи, суб’єкти

оперативно-розшукової діяльності;

- Збройні Сили України, інші військові формування, утворені відповідно до закону;
- Державна служба спеціального зв'язку та захисту інформації України;
- Національний банк України;
- підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури;
- суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом.

Рис. 3.5. Національна система кібербезпеки України

Склад Національного координаційного центру кібербезпеки, як робочого органу Ради національної безпеки і оборони України, показаний на рис. 3.6.

Рис. 3.6. Склад Національного координаційного центру кібербезпеки України

Модель Національної системи кібербезпеки України показана на рис. 3.7.

Рис. 3.7. Модель Національної системи кібербезпеки

Щоб забезпечити безпеку інформації, компанії можуть мати різні підрозділи, які займаються кібербезпекою. Склад таких підрозділів може включати такі професії, як:

- розробник систем захисту інформації, який відповідає за розробку та впровадження систем захисту інформації.
- адміністратор мереж і систем, який відповідає за налаштування та підтримку мереж і систем.
- фахівець з питань безпеки, який відповідає за аналіз та оцінку ризиків, пов’язаних з безпекою інформації;
- аналітик з безпеки інформаційно-телекомунікаційних систем, який відповідає за аналіз та оцінку ризиків, пов’язаних з безпекою інформаційно-телекомунікаційних систем;
- інструктор – методист з інформаційної безпеки та кібербезпеки, який відповідає за підготовку та проведення навчань з питань інформаційної безпеки та кібербезпеки.

Це не повний список професій, які можуть бути включені в склад підрозділів кібербезпеки. Для кожної компанії можуть бути свої вимоги до професійного складу персоналу кібербезпеки.

3.3 Розробка навчальних програм і програми навчання для персоналу

Ефективне впровадження сучасних технологій потребує реалізації багатьох проектів управління персоналом у сфері кібербезпеки, його підготовки та розвитку компетенцій. За деякими прогнозами, за деякими оцінками, вартість кіберзлочинності зростає на 15% щорічно, а до 2025 року може сягнути понад 10 трильйонів доларів щорічно. Тому питання кібербезпеки є значним глобальним викликом. Організація Об'єднаних Націй рекомендує розвивати цифрові можливості, включаючи компетенції у сфері кібербезпеки. На рівні Європейського Союзу також є потреба у вдосконаленні рішень у цій сфері. У

таблиці 3.1 представлені окремі нормативно-правові акти та ініціативи Європейського Союзу, що стосуються, серед іншого, компетенції у сфері кібербезпеки. В ініціативах наголошується, що досягнення прийнятного рівня кібербезпеки вимагає дій у юридичній, технічній, фізичній та соціальній сферах. Документи свідчать про те, що компетенції у сфері кібербезпеки занадто низькі. Отже, важливим політичним викликом є поширення знань і навичок для розбудови оборонних спроможностей у сфері кібербезпеки.

Таблиця 3.1.

Компетенції у сфері кібербезпеки – вибрані нормативно-правові акти ЄС.

Ініціатива	**Ознака**
Директива про безпеку мереж та інформаційних систем (Директива NIS)	Директива встановлює зобов'язання держав-членів щодо підвищення загального рівня кібербезпеки в ЄС. До завдань групи співробітництва входить обмін інформацією та кращими практиками з підвищення обізнаності та навчання. У документі вказується, що національна стратегія безпеки мереж та інформаційних систем повинна містити керівні принципи, що стосуються освіти, інформації та навчальних програм (O.J. EU L 191/1, 19.7.2016, 6 липня 2016 року)
Закон про кібербезпеку	Положення вказує на те, що необхідні додаткові зусилля для підвищення обізнаності громадян про кібербезпеку. Рекомендованим рішенням є сприяння кібергігієні в державах-членах. ENISA підтримує держави-члени у підвищенні обізнаності про кібербезпеку. ENISA сприяє просуванню найкращих практик та рішень, у тому числі у сфері кібергігієни та цифрових навичок, на рівні громадян, організацій та підприємств. Громадські інформаційні кампанії повинні поширювати знання про такі загрози, як фішингові атаки, ботнети, фінансове та банківське шахрайство, інциденти шахрайства з даними. Крім того, слід пропагувати методи безпеки, включаючи багаторівневу автентифікацію, шифрування, анонімізацію та захист даних (O.J. EU L 151, 7.6.2019, 17 квітня 2019 р.)

Ініціатива	Ознака
План дій з цифрової освіти на 2021–2027 роки	У документі зроблено висновок, що всім державам-членам не вистачає цифрових експертів, включаючи аналітиків з кібербезпеки. Попит на електронні навички зростатиме, а також будуть потрібні, серед іншого, компетенції у сфері кібербезпеки (COM/2020/0624).
Стратегія ЄС з кібербезпеки на період цифрового десятиліття	У стратегії наголошується, що компетенції у сфері кібербезпеки низькі. Крім того, у співробітників спостерігається значний дефіцит навичок кібербезпеки. Компетенція та гігієна кібербезпеки мають лежати в основі цифрової трансформації (JOIN, 2020)

Нормативно-правові акти Європейського Союзу мають значний вплив на правову систему держав-членів. В результаті вжитих ініціатив спостерігається підвищення рівня безпеки мережевих та інформаційних систем в державах-членах. Значне значення в цьому плані відіграв, зокрема, детектив NIS.

Сьогодні продовжується реформування вищої освіти України в галузі кібербезпеки, запроваджуються найкращі світові практики, які враховують досвід Європейської рамки кваліфікації та американської Стратегічної освітньої ініціативи у сфері кібербезпеки, відповідність стандартам в Європейському Союзі та США. Реформа ґрунтується на запровадженні системи професійних стандартів і створенні в Україні мережі незалежних кваліфікаційних центрів, які поліпшуватимуть можливості професійного зростання та підтвердження кваліфікації наявних на ринку фахівців.

У 2021 році Державною службою спеціального зв’язку та захисту інформації було додано до державного класифікатора професій ще 17 професій у галузі кіберзахисту та інформаційної безпеки. У 2022 році за підтримки Проекту USAID (англ. - UNITED STATES AGENCY INTERNATIONAL DEVELOPMENT - Агентство США з міжнародного розвитку) «Кібербезпека критично важливої інфраструктури України» були розроблені шість професійних стандартів для цих професій:

- фахівець сфери захисту інформації;

- фахівець з питань безпеки;
- розробник систем захисту інформації;
- адміністратор мереж і систем;
- аналітик з безпеки інформаційно-телекомунікаційних систем;
- інструктор-методист з інформаційної безпеки та кібербезпеки.

Вони пройшли перші етапи публічного обговорення та отримали позитивні висновки експертів Національного агентства кваліфікацій і затверджені головою Державної служби спеціального зв'язку та захисту інформації, що дозволяє закладам вищої освіти впроваджувати спеціалізації та використовувати ці стандарти для вдосконалення освітніх програм. Запровадження професійних стандартів має істотно підвищити якість підготовки фахівців кібербезпеки, які так необхідні сьогодні державі.

У 2023 році було заплановано збільшення кількості професій у сфері кібербезпеки та захисту інформації до 20 а також розробити стандарти до 14 професій.

До кінця 2023 року повинні з'явитися незалежні кваліфікаційні центри. У них фахівці, які здобули освіту в закладах формальної освіти або самостійно, зможуть підтвердити відповідність своїх знань, навичок та компетенцій посадам, на які претендують. Затверджені стандарти допоможуть роботодавцям створювати плани кар'єрного розвитку для своїх працівників.

Розробка стратегії управління персоналом

Ефективне управління персоналом стає стратегічно важливим фактором для забезпечення кібербезпеки, оскільки персонал виступає як перший захист від кіберзагроз і визначає, наскільки успішно організація може захистити свою інформацію та реагувати на інциденти. Ефективне управління персоналом дозволяє швидко мобілізувати та орієнтувати команди для відповіді на кіберінциденти, зменшуючи час реакції на загрози та мінімізуючи шкоду. Правильно підготовлений і мотивований персонал допомагає забезпечити сталість і надійність систем кібербезпеки, зменшуючи ризик людських помилок

або недбалості [51].

За даними NIST 800-181 [34], загальні принципи управління персоналом у сфері кібербезпеки включають такі аспекти як:

- *розробка та впровадження стратегій управління персоналом*;
- забезпечення безпеки інформації;
- визначення кваліфікацій та навичок персоналу;
- підготовка персоналу;
- оцінка ефективності та забезпечення сталого розвитку персоналу.

Стратегія управління персоналом - це систематичний підхід до управління людськими ресурсами в організації з метою досягнення стратегічних цілей компанії. Основна суть стратегії управління персоналом полягає у забезпеченні відповідності людських ресурсів (персоналу організації) потребам і цілям організації.

В дослідженнях [52,53] ефективність управління персоналом визначається в розрізі 9 функцій управління персоналом за відповідними індикаторами:

- аналіз та планування персоналу;
- набір персоналу;
- відбір персоналу;
- атестація та оцінювання кадрів;
- організація трудових відносин; мотивація персоналу;
- створення умов праці;
- інформаційне забезпечення;
- розвиток і навчання персоналу.

Ключовим елементом успішної стратегії забезпечення кібербезпеки організації є правильний підбір персоналу на основі професійних стандартів, які визначають вимоги до знань умінь і навичок на основі КВЕД-2010 «Класифікація видів економічної діяльності» [54] та Національного класифікатору України ДК 003:2010 «Класифікатор професій» [55]. Для цього в організації для фахівців кібербезпеки створюються карти компетенцій (професіограми) – портрет ідеального співробітника, які дозволяють уникнути недоліків підбору і

полегшують роботу співробітників відділу кадрів, що зайняті прийомом на роботу.

Важливим аспектом ефективності управління персоналом у сфері кібербезпеки є його підготовка та навчання із застосуванням сучасних технологій та інструментів, таких як системи виявлення та реагування на інциденти (IDS/IPS), SIEM-системи, проведення обов'язкових регулярних тренінгів персоналу щодо дій в непередбачуваних або кризових ситуаціях, пов'язаних з кібербезпекою. Підготовка персоналу може здійснюватись як за планом всередині організації так і на курсах з отриманням сертифікатів, які будуть підтвердженням компетентності та необхідних навичок. Одним із варіантів є напрацьовані фахівцями пропозиції загальних принципів управління персоналом у сфері кібербезпеки, відображені у Національній освітній ініціативі у сфері кібербезпеки (NICE) [56].

Загальні принципи NICE допомагають організаціям подолати проблему з описом своїх працівників для багатьох зацікавлених сторін шляхом використання підходу на основі стандартних блоків.

Здобуття сертифікатів у галузі кібербезпеки може підвищити компетентність персоналу та підтвердити їхні навички. Сертифікація може включати крім перерахованих у розділі 3 (рис.3.1-3.4), CISSP, CompTIA Security+, і багато інших.

CISSP (Certified Information Systems Security Professional) - це міжнародно визнана сертифікація, яка підтверджує знання та навички у галузі інформаційної безпеки. Ця сертифікація була розроблена для професіоналів, які мають досвід у галузі інформаційної безпеки та бажають поглибити свої знання.

CompTIA Security+ - це сертифікація, яка показує наявність знань та навичок, необхідних для розуміння основних принципів безпеки комп'ютерних систем. Ця сертифікація допоможе вам зрозуміти загальну структуру безпеки комп'ютерних систем.

Крім курсів, у плані ефективного управління персоналом для підвищення кваліфікації керівникам підрозділів інформаційного захисту підприємства

доцільно використовувати ресурси Інтернету та платформи, на яких можна знайти тести та вправи для вивчення кібербезпеки (рис. 3.8 – 312):

- Hack The Box (HTB) - платформа для віртуальних лабораторій і тестів з кібербезпеки (рис. 3.8).

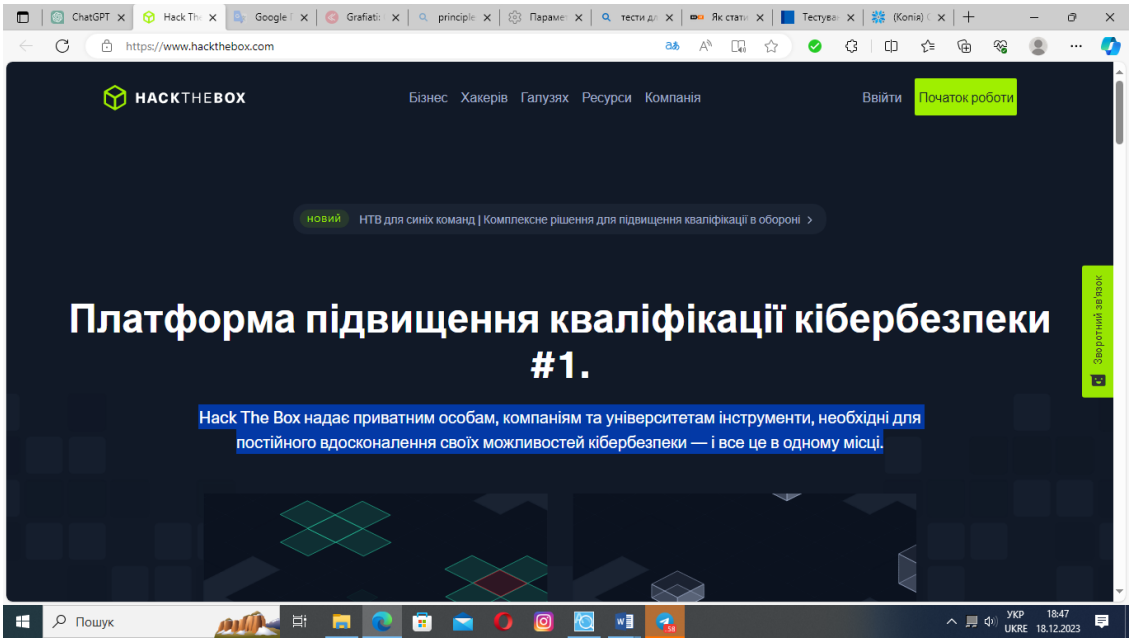

Рис. 3.8. Hack The Box

- TryHackMe - інша платформа для віртуальних лабораторій та навчання кібербезпеці;

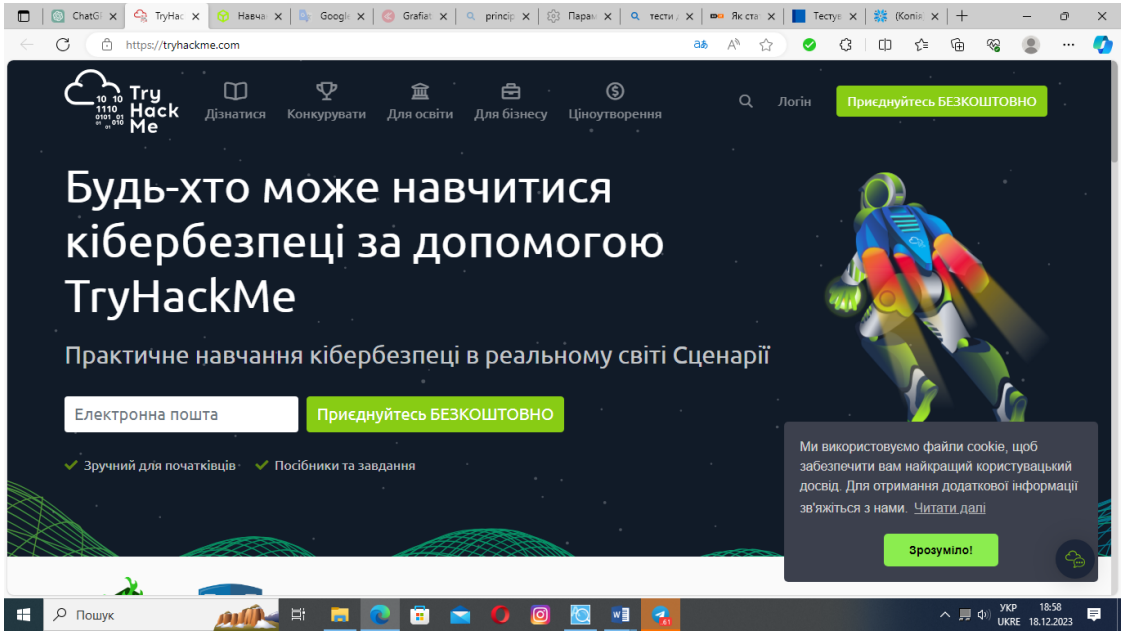

Рис. 3.9. Платформа TryHackMe

- OverTheWire - набір грифів (wargames) для вивчення аспектів кібербезпеки, вивчити та практикувати концепції безпеки у формі веселих ігор;

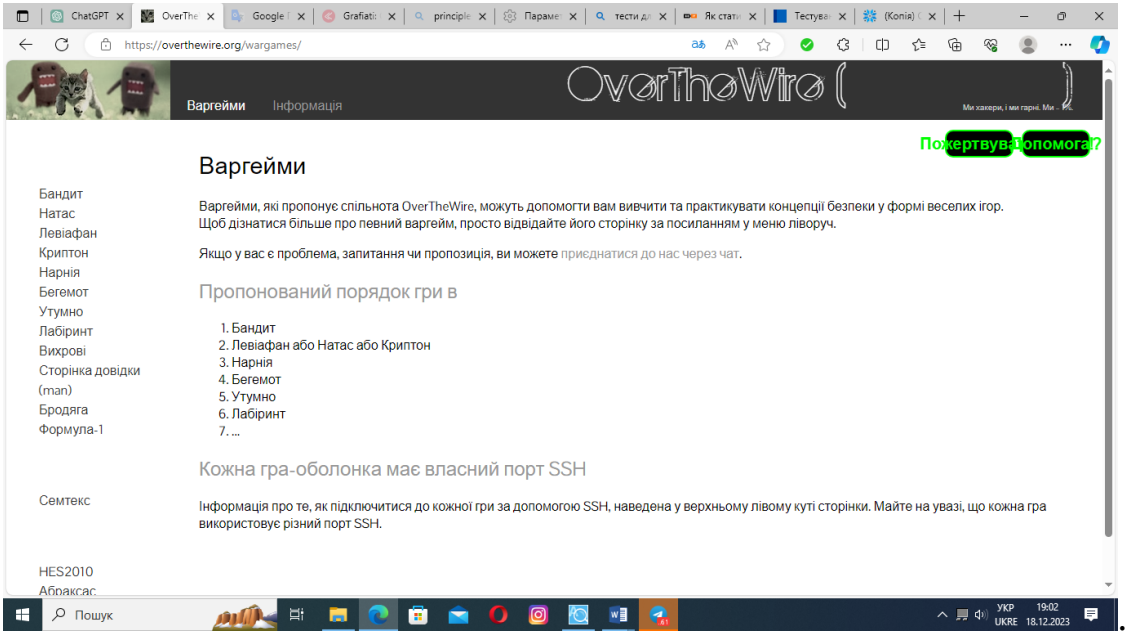

Рис. 3.10. Навчальна платформа OverTheWire

- PentesterLab - лабораторії для навчання вразливостям веб-додатків та іншим аспектам кібербезпеки;

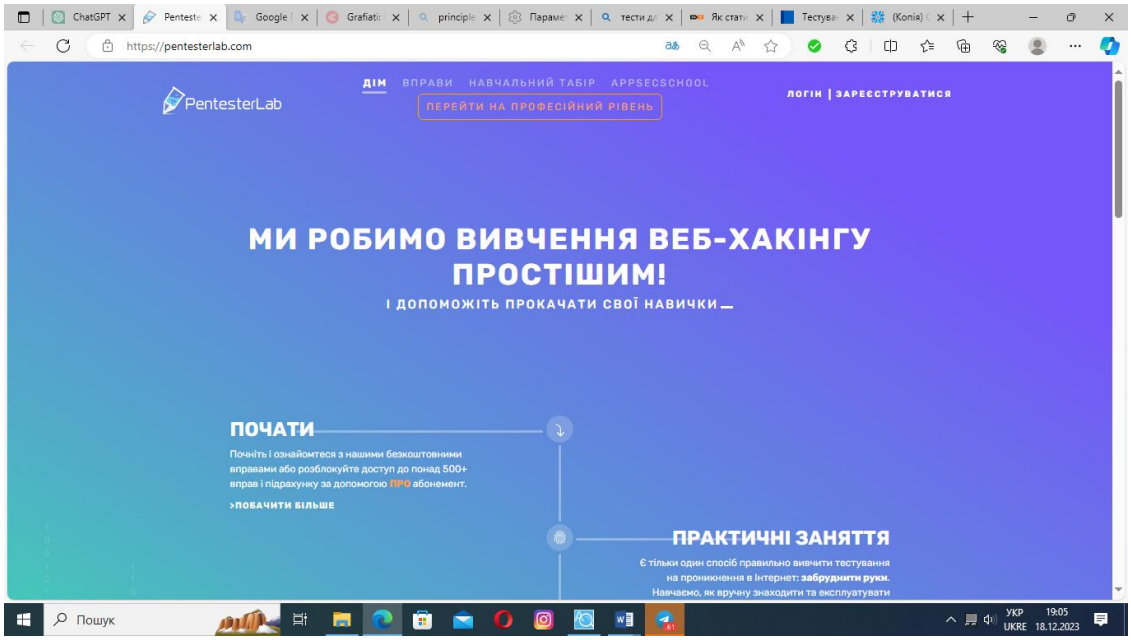

Рис. 3.11. Навчальна лабораторія PentesterLab

- Cybrary - платформа із курсами з кібербезпеки, які можуть включати тести.

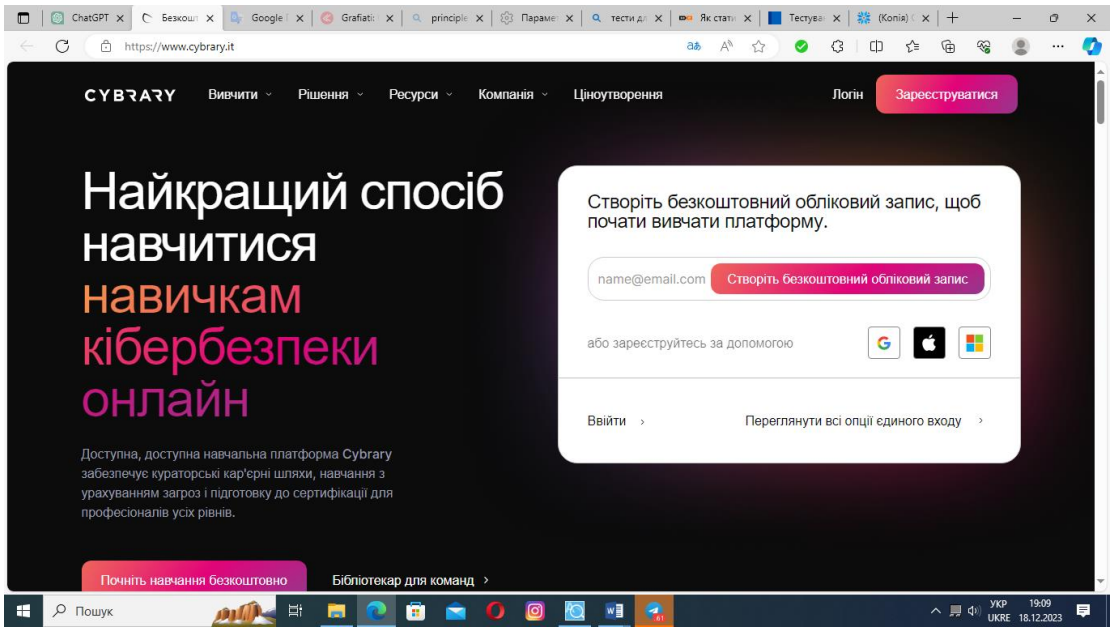

Рис. 3.12. Платформа з тестами Cybrary

Розробка та впровадження стандартів і процедур у сфері кібербезпеки допомагає створити структурований підхід до управління персоналом. Це може включати плани реагування на інциденти, політики безпеки та моніторинг загроз.

Одним із важливих механізмів підвищення ефективності управління персоналом є розробка та впровадження професійного кодексу кібербезпеки та корпоративного етичного кодексу організації кібербезпеки, в яких визначені етичні правила професійної діяльності.

Також важливим напрямком підвищення ефективності є мотивація персоналу, розроблена система оцінки результативності співробітників.

Таким чином, враховуючи результати аналізу теорії управління персоналом та основних моделей оцінки ефективності метод, що розглянуті у розділах 1,2 можна сформувати стратегію управління персоналом, яка буде включати основні аспекти (рис. 3.13):

Рис. 3.13. Основні аспекти стратегії управління персоналом

Врахування цих аспектів дозволяє організації ефективно використовувати свої людські ресурси для досягнення стратегічних цілей та забезпечення сталого успіху.

Управління персоналом в галузі кібербезпеки має свої особливості, оскільки це сфера, де ключову роль відіграють висококваліфіковані інформаційні та технічні спеціалісти. Такі особливості формують додаткові вимоги до ключових аспектів формування стратегії управління персоналом:

- високий рівень компетентності кваліфікованих фахівців у команді кібербезпеки, здатних ефективно захищати інформаційні ресурси вимагає необхідності розвитку та утримання талановитих інженерів, експертів з безпеки та аналітиків;
- з урахуванням швидкої зміни технологій важливо забезпечувати постійне професійне навчання та підвищення кваліфікації працівників,

розробляти програми стажування, тренінгів та сертифікацій для підтримки розвитку навичок персоналу;

- для формування постійної готовності до реагування на кіберінциденти та відновлення роботи після їхнього виникнення необхідно розробляти та удосконалювати нові методики для виявлення, оцінки та управління кіберризиками;
- для забезпечення конфіденційності і захисту даних розробляти політики безпеки, які будуть включати найновіші технології та практики кібербезпеки на основі штучного інтелекту;
- для ефективної роботи в команді, співпраці з різними відділами та фахівцями і реагування на постійні зміни необхідно створювати команди з урахуванням психологічної сумісності та особливостей характеру особистості;
- при формуванні політики безпеки та процедур враховувати дотримання вимог вітчизняного та міжнародного законодавства.

Загальна мета стратегії полягає в створенні ефективної та відповідальної команди кібербезпеки, яка забезпечить надійний захист інформації та ресурсів організації.

Однією з ефективних стратегій управління персоналом в організації кібербезпеки може бути:

- створення програми "Центр експертизи та розвитку", який буде відповідати за професійний розвиток експертів у сфері кібербезпеки та працівників. Така програма спрямована на забезпечення високого рівня компетентності персоналу та постійного розвитку їхніх навичок у сфері кібербезпеки;
- розробка індивідуальних планів професійного розвитку для кожного працівника з урахуванням його поточних навичок та стратегічних цілей організації;
- забезпечення можливостей для отримання сертифікатів та участі в конференціях та тренінгах;

- менторство та навчання, зосереджене на практичність і направлене на підтримку та допомогу новачкам;
- організація практичних занять та сценаріїв, що відповідають реальним загрозам та інцидентам в галузі кібербезпеки;
- визначення ключових компетенцій та критеріїв успіху для оцінки рівня знань та навичок працівників, проведення регулярних оцінок та звітів з метою виявлення успіхів та визначення областей для подальшого розвитку;
- встановлення системи стимулювання та винагород за досягнення високих результатів у професійному розвитку та вирішенні кібербезпекових завдань;
- забезпечення конкурентоспроможної заробітної плати та бонусів для високопрофесійних працівників;
- встановлення партнерських відносин з університетами та навчальними закладами для забезпечення постачання кваліфікованих випускників.
- участь у галузевих ініціативах та обміні знаннями для підтримки розвитку працівників.

Ця стратегія сприяє створенню внутрішнього експертного середовища, розвитку навичок та знань працівників, а також сприяє вирішенню глобальних викликів у сфері кібербезпеки.

Одним із важливих напрямків стратегії управління персоналом є формування ефективної команди реагування на кіберінциденти. При проведенні переддипломної практики в ТзОВ «ФОРА» застосований тест, наведений в табл. 3.2. для визначення здатності до співпраці та комунікації фахівців кібербезпеки.

Таблиця 3.2

Тест на здатність до співпраці та комунікації в галузі кібербезпеки

Вид здатності	Завдання
Комунікаційні навички	Як ви поясните неспеціалістам (наприклад, керівництву компанії чи користувачам) потенційну загрозу кібербезпеки та заходи, які потрібно прийняти для її запобігання?
Ситуаційна задача	Ви працюєте в кібербезпековому відділі організації і стали

Вид здатності	Завдання
	свідком потенційної кібератаки. Як ви підходите до розв'язання цієї проблеми в співпраці з іншими відділами (наприклад, відділом IT, юридичним відділом та вищим керівництвом)? Опишіть ваш план дій.
Робота в команді	Уявіть, що ви працюєте в команді кібербезпеки. Як ви плануєте обговорення та рішення проблеми в разі кібератаки разом з іншими членами команди? Як ви розподілите завдання та забезпечите ефективну співпрацю?
Співпраця з іншими відділами	Як ви взаємодієте з відділами, які не є прямо пов'язаними з кібербезпекою (наприклад, відділом розробки, відділом маркетингу) для впровадження політик безпеки та попередження інцидентів?
Реагування на інцидент	Ваша команда стала об'єктом кібератаки, і вам треба швидко приймати рішення. Як ви організуєте комунікацію та співпрацюєте з колегами під час кризової ситуації?
Рішення конфліктів	Якщо виникає конфлікт думок в команді з кібербезпеки, як ви його вирішуєте? Як ви зберігаєте конструктивний характер обговорення та сприяєте досягненню компромісу?

Ці питання орієнтовані на виявлення не лише технічних навичок, але й здатності співпрацювати, ефективно комунікувати та вирішувати завдання в командному середовищі. Вони допоможуть визначити, наскільки кандидат може успішно взаємодіяти з іншими у ситуаціях, пов'язаних з кібербезпекою.

Критерії для оцінювання тесту наведені в таблиці 3.3.

Таблиця 3.3

Оцінка тесту на здатність до співпраці та комунікації в галузі кібербезпеки

Критерій оцінювання	Зміст критерію	Шкала оцінювання
1. Ясність та логіка відповідей	Оцініть, наскільки ясно та логічно кандидат висловлює свої думки та ідеї у відповіді на кожне питання.	0-5
2. Комунікаційні навички	Перевірте, як кандидат може пояснити складні концепції кібербезпеки простим та зрозумілим мовою, особливо коли він звертається до непрофесіоналів чи колег, які не мають технічного бекграунду	0-10
3. Здатність до співпраці	Оцініть, як кандидат реагує на ситуації співпраці та чи може він успішно працювати в команді. Зверніть увагу на його здатність розподіляти завдання та	0-10

Критерій оцінювання	Зміст критерію	Шкала оцінювання
	ефективно співпрацювати з іншими членами команди	
4. Управління конфліктами	Оцініть, як кандидат вирішує конфліктні ситуації, чи може зберегти конструктивний характер обговорення та сприяти досягненню компромісу	0-5
5. Стратегічне мислення	Оцініть, як кандидат може стратегічно підходити до рішення проблем та вирішення кібербезпечних завдань у великій організації	0-5
6. Етика та конфіденційність	Важливо звертати увагу на те, як кандидат розглядає етичні аспекти та зберігає конфіденційність під час відповідей. Обов'язково відзначайте конкретні приклади та сценарії, що їх вказав кандидат, оскільки це допоможе вам зробити більш об'єктивну оцінку його чи її навичок та здатностей. Важливо також брати до уваги контекст та умови, у яких відбувалася відповідь, і оцінювати їх у контексті конкретної організації та вакансії	0-5

За результатами тестування претендентів групи реагування на інциденти із 5 фахівців інформаційної безпеки визначені тільки 4, які зможуть працювати в команді (рис. 3.9).

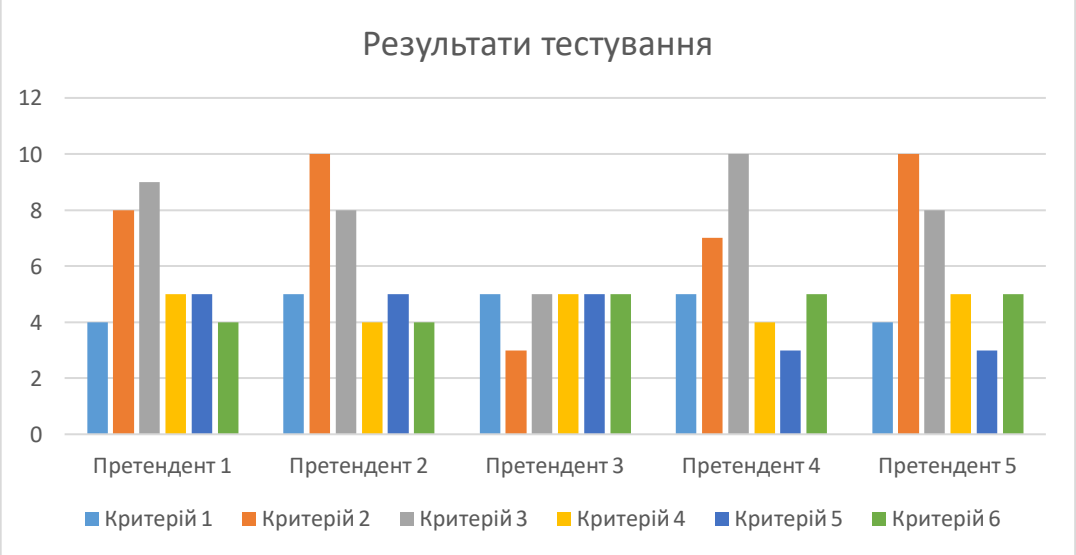

Рис. 3.9. Результати тестування здатності роботи в команді

ВИСНОВОК до 3 розділу. Загалом, ефективне управління персоналом стає стратегічно важливим фактором для забезпечення кібербезпеки, оскільки персонал виступає як перший захист від кіберзагроз і визначає, наскільки успішно організація може захистити свою інформацію та реагувати на інциденти.

Пошук нових відповідей на проблему поведінки в галузі безпеки даних вимагає виходу за рамки того, що наразі відомо про підвищення обізнаності та дотримання нормативних вимог, двох відмінностей, які накладаються на дискурс безпеки, що часто в кінцевому підсумку виснажує практики людей і завдає дискомфорту співробітникам у різних сферах своїми розмовами про ризик і загрозу небажаних подій.

Запропонований тест психологічної сумісності у поєднанні із визначенням фахових компетентностей дозволяє створити ефективну команду спеціалістів кібербезпеки для реагування на кіберінциденти.

Визначені положення стратегії управління персоналом кібербезпеки сприяють створенню внутрішнього експертного середовища, розвитку навичок та знань працівників, а також вирішенню глобальних викликів у сфері кібербезпеки.

РОЗДІЛ 4
ПРОПОЗИЦІЇ ТА РЕКОМЕНДАЦІЇ

4.1 Оцінка ефективності запропонованої стратегії

Оцінка ефективності стратегії управління персоналом в організації кібербезпеки вимагає системного підходу та врахування різних показників. При оцінюванні ефективності необхідно врахувати наступні питання та критерії (табл.4.1).

Таблиця 4.1.

Перелік питань і критеріїв для оцінювання ефективності стратегій управління персоналом кібербезпеки

Перелік критеріїв оцінювання	Зміст питань оцінювання
Досягнення стратегічних цілей	Наскільки успішно організація досягла своїх стратегічних цілей у сфері кібербезпеки? Чи було зменшено кількість кібератак або їхні наслідки завдяки впровадженню стратегії?
Склад та якість персоналу	Як висококваліфікований та мотивований персонал у компанії? Якість найму нових фахівців і їхнє відповідність потребам організації?
Розвиток навичок і навчання	Наскільки ефективно реалізована програма навчання та розвитку для працівників? Які навички були успішно розвинені у персоналу?
Утримання та задоволеність персоналу	Які механізми використовуються для утримання та стимулювання ключових талантів? Як висока рівень задоволеності працівників за останній час?
Успішність управління інцидентами	Як ефективно працює команда під час кіберінцидентів? Чи були прийняті заходи для уникнення подібних інцидентів у майбутньому?
Впровадження політик та процедур	Наскільки успішно впроваджені політики безпеки та процедури в організації? Як ефективно вони дотримуються працівниками?
Співпраця та комунікація	Як ефективно співпрацює персонал між собою та з іншими відділами? Чи існують ефективні механізми комунікації в

Перелік критеріїв оцінювання	Зміст питань оцінювання
	організації?
Реакція на зміни в індустрії	Як ефективно організація реагує на зміни в технологіях та трендах кібербезпеки? Чи забезпечено постійне оновлення навичок персоналу?
Співвідношення витрат та результатів	Як відповідає стратегія бюджетним обмеженням, і які результати вона демонструє?
Оцінка здатності до інновацій	Чи існують новаторські підходи та рішення в галузі управління персоналом? Наскільки організація відкрита до впровадження нових ідей та технологій?

Для оцінки ефективності стратегії важливо регулярно проводити огляди та внутрішні аудити, спілкуватися з персоналом, знаходити способи вдосконалення та вносити корективи в стратегію на основі отриманих результатів. Також слід враховувати особливості конкретної організації та її цілей при оцінці.

4.2 Формулювання практичних рекомендацій для організацій у галузі кібербезпеки щодо підвищення ефективності управління персоналом

Підвищення ефективності управління персоналом в галузі кібербезпеки вимагає комплексного підходу, що враховує специфіку цієї галузі. Для підвищення ефективності управління персоналом за результатами досліджень можна сформулювати кілька практичних рекомендацій, застосування яких при створенні системи інформаційної безпеки організації (підприємства) забезпечить стійкість самої системи та виконання завдань кібербезпеки (табл.4.2).

Таблиця 4.2

Практичні рекомендації щодо підвищення ефективності управління персоналом організації кібербезпеки

Напрямки стратегії управління персоналом	Зміст заходів
Розробка Центру експертизи та навчання	Створення спеціалізованого Центру експертизи та навчання для розвитку навичок персоналу в галузі кібербезпеки. Забезпечення доступу до актуальних ресурсів, тренінгів та

Напрямки стратегії управління персоналом	Зміст заходів
	інших освітніх засобів.
Програма професійного розвитку	Розробка індивідуальних планів професійного розвитку для кожного працівника, враховуючи його поточні навички та стратегічні цілі організації. Забезпечення доступу до курсів, сертифікацій та ресурсів для постійного навчання.
Менторство та програми обміну досвідом	Запровадження програм менторства, де досвідчені фахівці надають підтримку та поради новачкам. Організація програм обміну досвідом для сприяння взаємному навчанню та обміну кращими практиками.
Практичні тренування та сценарії	Проведення практичних тренувань та сценаріїв, що відповідають реальним загрозам та інцидентам в галузі кібербезпеки. Використання симуляцій для тренування реакції на кібератаки та інші кризові ситуації.
Оцінка та звітність	Розробка системи оцінки та звітності, щоб визначати рівень знань та навичок працівників. Регулярна оцінка прогресу та подальших потреб у навчанні.
Стимулювання та винагороди	Встановлення системи стимулювання та винагород за досягнення високих результатів у професійному розвитку та вирішенні кібербезпекових завдань. Забезпечення конкурентоспроможної заробітної плати та бонусів для висококваліфікованих працівників.
Співпраця з навчальними закладами	Установлення партнерських відносин з університетами та іншими навчальними закладами для забезпечення потоку кваліфікованих випускників. Участь у галузевих ініціативах та обміні знаннями для підтримки розвитку працівників.
Внутрішнє експертне середовище	Створення внутрішнього експертного середовища, де фахівці можуть обмінюватися досвідом та знаннями. Організація регулярних технічних форумів та зустрічей для обговорення актуальних питань.
Формування робочого середовища	Створення позитивного та стимулюючого робочого середовища, що сприяє розвитку та інноваціям. Забезпечення можливостей для розвитку soft skills, таких як ефективна комунікація та робота в команді.
Оцінка конкурентоспроможності	Постійна оцінка конкурентоспроможності стратегії управління персоналом у порівнянні з іншими галузевими лідерами. Аналіз реакції на нові технологічні та галузеві тренди.

Висновки до 4 розділу. Розроблені критерії та питання, за якими потрібно оцінити ефективність запропонованих стратегій управління персоналом, дозволяють постійно удосконалювати систему управління персоналом організацій у відповідності до нових викликів та загроз інформаційній безпеці.

Рекомендації в таблиці 4.2 можуть служити основою для розвитку ефективної стратегії управління персоналом в галузі кібербезпеки. Важливо постійно адаптувати підходи до змін в галузі та специфіці організації.

ВИСНОВКИ

Розглянуті теорії (класична, людських ресурсів, людських відносин) є фундаментальною основою для ефективного управління організаціями, наголошуючи на важливості людського фактору в успіху організації.

Особливості функціонування організацій і підрозділів кібербезпеки вимагають детального аналізу проблем управління персоналом через призму завдань, які специфічні для інформаційної безпеки та потребують розроблення стратегій управління персоналом, характерних для кожної організації, яка потребує проведення заходів інформаційної безпеки. Теорія дає розуміння природи та характеристик людей, які необхідно розуміти, маніпулювати ними та використовувати, щоб отримати від людей найбільшу ефективність при виконанні ними обов’язків. Ефективна практика управління персоналом передбачає повне знання людини на робочому місці, її взаємодії з керівниками та колегами як на офіційному, так і на неформальному рівнях.

Здійснений аналіз наукової літератури та публікацій, пов'язаних із управлінням персоналом у сфері кібербезпеки та існуючими підходами до цієї проблеми і досліджений сучасний стан управління персоналом в організації кібербезпеки виявив основні потреби та вимоги до кваліфікації та компетентності персоналу, необхідність застосування сучасних методів та практик управління персоналом в галузі кібербезпеки. Проаналізовані підходи різних дослідників, що стосуються визначення сутності «управління персоналом» визначили складність та багатогранність проблеми формування ефективної системи управління персоналом у сфері кібербезпеки в сучасних умовах. Розкриті шляхи підвищення ефективності управління персоналом, які дозволять якісно організувати кібербезпеку.

В магістерській роботі вперше запропоновані підходи до розроблення стратегії управління персоналом кібербезпеки, які відрізняються від відомих тим, що ґрунтуються на врахуванні особливостей людських ресурсів при формуванні команд кібербезпеки. Удосконалена методика оцінювання ефективності управління персоналом кібербезпеки на основі визначених

критеріїв оцінювання ефективності розробленої стратегії.

Дістали подальшого розвитку способи процесу розробки кадрової стратегії, які включають поєднання мотиваційної складової і використання інформаційних технологій, підвищення кваліфікації та отримання сертифікатів.

Удосконалена методика підбору команд реагування на кіберінциденти шляхом проведення тестування.

Розроблені підходи можуть бути використані при плануванні та реалізації системи управління персоналом в організаціях кібербезпеки з метою підвищення ефективності протидії загрозам, пов’язаним із веденням інформаційного протиборства. Застосування напрацювань дадуть змогу формувати стратегії управління персоналом кібербезпеки, здійснити обґрунтований вибір методів і засобів підвищення ефективності управління персоналом організації при виконанні завдань кібербезпеки в умовах інформаційного протиборства.

Запропонована стратегія управління персоналом може зменшити ризики інформаційної безпеки, навчаючи співробітників правилам кібербезпеки та вдосконалюючи їхні навички.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Борданова Л.С. Навчальний посібник: Конспект лекцій з навчальної дисципліни «Управління персоналом» – Київ : КПІ ім. Ігоря Сікорського, 2020. – 103 с.

2. Cooley S. Human Relations Theory of Organizations. SpringerLink. 2016. URL: https://doi.org/10.1007/978-3-319-31816-5_2998-1 (date of access: 16.12.2023).

3. Бендіксон, Дж., Малдун, Дж., Лігурі, Е.В., Девіс, П.Е. Теорія агентства: передумови та епістемологія. Журнал історії менеджменту, том 22, No 4, 2016. с. 437-449.

4. Okafor, E.E., Imnonopi, D. & Obor, D. Introduction to Industrial Relations and PersonnelManagement. in Okafor, E.E., Adetola, O., Aborisade, R.A, Adebiyi, A. (eds). Human Resources:Industrial Relations and Management Perspectives. Ago-Iwoye: OOU Publishing House. 2020. pp. 1-29 URL: https://www.researchgate.net/publication/370215005 accessed Nov 19 2023

5. Duru, J.I. Teamwork: Strategy for Improving Employee and Organisational Performance. HumanResource Management Journal. 2017. 9 (1):11-26.

6. Gutiérrez-Broncano, S., Jiménez-Estévez, P., Rubio-Andrés, M.. Theoretical Models of Human Resource Management: The Anthropological Model as a Full Model to Manage Human Resources. In: Machado, C., Davim, J. (eds) Organizational Behaviour and Human Resource Management. Management and Industrial Engineering. Springer, Cham. 2018. URL: https://doi.org/10.1007/978-3-319-66864-2_7

7. Wright P. M., Ulrich M. D. A Road Well Traveled: The Past, Present, and Future Journey of Strategic Human Resource Management. Annual Review of Organizational Psychology and Organizational Behavior. 2017. Vol. 4, no. 1. P. 45–65. URL: https://doi.org/10.1146/annurev-orgpsych-032516-113052 (date of access: 16.12.2023).

8. Igwe, Anthony, Josaphat Uchechukwu Joe Onwumere and Obiamaka P. Egbo. “Effective Human Resource Management As Tool For Organizational Success.”

European Journal of Business and Management. no. 6. 2014. pp. 210-218.

9. Потьомкіна О.В., Дорош В.Ю. Дослідження теорій управління персоналом та їх застосування в сучасній практиці. Економічні науки. Серія «Економічна теорія та економічна історія». Збірник наукових праць. Луцький НТУ. – Випуск 14(56). – Луцьк, 2017. С. 156-162.

10. Потьомкіна О.В. Управління персоналом підприємства: навч. посіб. / О. В. Потьомкіна. – Луцьк: РВВ ЛНТУ, 2013. – 228 с. (Протокол №3 від 31.10.2013 р. ЛНТУ).

11. Давидова В. С. Від людського потенціалу до потенціалу управлінського – прогнозні характеристики можливостей країни, регіону, підприємства /Давидова В. С. Живодьор В. Ф. Менеджмент за умов трансформаційних інновацій: виклики, реформи, досягнення. – у 2 ч. – Ч. 1. – 2007. – Секція №4 «Людський потенціал – менеджмент інноваційної адекватності темпами змін» // [Електронний ресурс]. – Режим доступу: http://all-sci.net/menedjment/vid-lyudskogo-potentsialu-potentsialu.html

12. Бутенко І. Еволюція й генезис основних концепцій управління персоналом. Вісник економічної науки України. 2013. № 2 (24). С. 20–25.

13. Кармінська-Бєлоброва М. В. Особливості сучасних концепцій управління персоналом. Вісник Національного технічного університету "ХПІ" (економічні науки) - Bulletin of the National Technical University "KhPI" (economic sciences) : зб. наук. пр. – Харків : НТУ "ХПІ", 2018. – № 37 (1313). – С. 36-40.

14. Pfohl H.-C. Basics of Personnel Management. SpringerLink. 2023. pp. 343-369. URL: https://doi.org/10.1007/978-3-662-66564-0_10 (date of access: 16.12.2023).

15. Щербак В. Г. Управління персоналом підприємства : Наук. вид. Харків: ХНЕУ, 2005. 220 с.

16. Заклекта-Барестовенко О. С. Підвищення ефективності інвестицій у розвиток персоналу як результат вдосконалення управління. Вісник Тернопільського національного економічного університету. – Тернопіль: Економічна думка, 2009. – Вип. 4. – С. 77–84.

17. Кодекс законів України про працю. – К., 2018. [Електронний ресурс] : режим доступу: URL: https://zakon.rada.gov.ua/laws/show/322-08 .

18. Управління персоналом: підручник. В.М. Данюк. А.М. Колот, Г.С. Суков та ін. за заг. та наук. ред. к.е.н., проф. В.М. Данюка. – К.: КНЕУ; Краматорськ: НКМЗ, 2013. – 665 с.

19. Дяків О. П., Островерхов В. М. Управління персоналом : навчально методичний посібник (видання друге, переробл. і доповнено). – Тернопіль : ТНЕУ, 2018. – 288 с.

20. Селютін В. М., Яцун Л. М. Управління персоналом: Практикум [Електронний ресурс] : навч. посібник. – Харків: ХДУХТ 2018. – 188 с. URL: https://dut.edu.ua/uploads/l_1829_32362479.pdf (дата звернення 17.12.2023 р.)

21. Dobrianska N.A., Fomina N.M. The newest theories of personnel competitiveness management in the conditions of digitalization and COVID-19. Review article. ECONOMICS: time realities. №1(59), 2022. P. 37-45. URL: http://doi.org10.5281/zenodo.7226672.

22. Тимошенко В. Тенденції у сфері управління персоналом компаній в умовах трансформацій. Економіка та суспільство. Випуск # 52 / 2023. URL: https://doi.org/10.32782/2524-0072/2023-52-11.

23. Управління персоналом : підручник. О. М. Шубалий, Н. Т. Рудь, А. І. Гордійчук, І. В. Шубала, М. І. Дзямулич, О. В. Потьомкіна, О. В. Середа; за заг. ред. О. М. Шубалого. – Луцьк : ІВВ Луцького НТУ, 2018. – 404 с

24. Kapitanets S., Varenia N. Korolchuk O. Kulinich T., Kilnitska O. Holovchak H. Problems of Ensuring Personnel Stability and Security in the Government Authorities of Countries with Economies in Transition. Wseas transactions on environment and development. Vol. 17. Pp. 554-560. 2021. URL: https://doi.org/10.37394/232015.2021.17.53.

25. Parkhomenko-Kutsevil, O. Personnel security inthe system of public governance of Ukraine: theoretical fundamentals, Collection ofscientific works. Efficacy publicadministration, 37, 2013, pp. 13-20.

26. Довгань Л.Є., Ведута Л.Л., Мохонько Г.А. Технології управління

людськими ресурсами: підручник. Київ: КПІ ім. Ігоря Сікорського, 2018. 512 с. URL: https://ela.kpi.ua/bitstream/1679/25275/1/TULR_navch_posibn.pdf

27. Mishchuk I., Zinchenko O. Zinchenko D.,Pawliszczy D., Pohrebniak A., Differences inthe Assessment of Economic Security of Personnel and Security of Enterprise StaffInterests, WSEAS Transactions on Environmentand Development, Vol. 16, 2020, pp. 454-463. URL: https://doi.org/10.37394/232015.2020.16.46.

28. Appiah-Otoo I., Song N. The impact of ICT on economic growth-Comparing rich and poor countries. Telecommunications Policy. – 2021. – Vol.. 45. – №. 2. – p. 102082. URL: https://doi.org/10.1016/j.telpol.2020.102082.

29. Vu K., Hanafizadeh P., Bohlin E. ICT as a driver of economic growth: A survey of the literature and directions for future research. Telecommunications Policy. – 2020. – Т. 44. – №. 2. – С. 101922. URL: https://doi.org/10.1016/j.telpol.2020.101922.

30. Di Franco F. Analysis of the European R & D Priorities in Cybersecurity: Strategic Priorities in Cybersecurity for a Safer Europe. – ENISA, 2018. URL: https://www.enisa.europa.eu/publications/analysis-of-the-european-r-d-priorities-in-cybersecurity.

31. Брич В.Я., Гугул О.Я. Теоретичні аспекти розвитку персоналу. Вісник Хмельницького національного університету. – 2009. – № 5. – Т. 2. – С. 13-16.

32. Виноградський М.Д. Управління персоналом : [навч. посіб.] / М.Д. Виноградський, А.М. Виноградська, О.М. Шканова ; 2-ге вид. – К. : Центр учбової літератури, 2009. – 502 с.

33. Корольков В. В. Удосконалення мотиваційного механізму управління персоналом підприємства Ефективна економіка. 2020. № 11. URL http://nbuv.gov.ua/UJRN/efek_2020_11_45 . (дата звернення 26.11.2022.)

34. NIST SP 800-181 REV. 1. Загальні принципи управління персоналом у сфері кібербезпеки (загальні принципи NICE). URL: https://doi.org/10.6028/NIST.SP.800-181r1.ukr.

35. Stine K, Quinn S, Witte G, Gardner RK. Integrating Cybersecurity and Enterprise Risk Management (ERM). (National Institute of Standards and

Technology,Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8286. 2020. URL: https://doi.org/10.6028/NIST.IR.8286

36. Dodson D.F., Souppaya M.P., Scarfone K.A. Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF).(National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper. 2020. URL: https://doi.org/10.6028/NIST.CSWP.04232020

37. Enisa. Cybersecurity culture guidelines: behavioural aspects of cybersecurity. European Union Agency for Network and Information Security. – 2018. URL: https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity

38. Neigel A. R. et al. Holistic cyber hygiene education: Accounting for the human factors. Computers & Security. – 2020. – Vol. 92. – pp. 101731. URL: https://doi.org/10.1016/j.cose.2020.101731

39. Kalhoro S. et al. Extracting key factors of cyber hygiene behaviour among software engineers: A systematic literature review. IEEE Access. – 2021. – Vol. 9. – pp. 99339-99363. URL: https://doi.org/10.1109/ACCESS.2021.3097144 .

40. Whitman M. E. Industry priorities for cybersecurity competencies. Journal of The Colloquium for Information Systems Security Education. – 2018. – Vol. 6. – №. 1. – C. 21-21. URL: https://cisse.info/journal/index.php/cisse/article/view/91/CISSE_v06_i01_p06.pdf

41. Szczepaniuk E. K., Szczepaniuk H., Rokicki T., Klepacki B. Information security assessment in public administration. Computers & Security, – 2020. – vol. 90. – p. 101709. URL: https://doi.org/10.1016/j.cose.2019.101709 .

42. Vu K., Hanafizadeh P., Bohlin E. ICT as a driver of economic growth: A survey of the literature and directions for future research. Telecommunications Policy. – 2020. – T. 44. – №. 2. – C. 101922. URL: https://doi.org/10.1016/j.telpol.2020.101922.

43. Директива (ЄС) 2016/1148 Європейського Парламенту та Ради від 6 липня 2016 року про заходи для високого загального рівня безпеки мережевих та

інформаційних систем на всій території Союзу. Директива набула чинності 8 серпня 2016 року. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2017:476:FIN.

44. Hadlington L. Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon. – 2017. – Vol. 3. – №. 7. URL: https://doi.org/10.1016/j.heliyon.2017.e00346.

45. А. Зульфія, Р. Адавія, А. Н. Хідаянто, Н. Фітрія Аюнінг Буді. Вимірювання обізнаності співробітників про інформаційну безпеку за допомогою опитувальника людських аспектів інформаційної безпеки (HAIS-Q): тематичне дослідження в PT. PQS, 2019 5th International Conference on Computing Engineering and Design (ICCED), Сінгапур, 2019, с. 1-5, URL: https://doi.org/10.1109/ICCED46541.2019.9161120 .

46. Н. С. Сафа, Р. Фон Солмс і С. Фернелл. Модель дотримання політики інформаційної безпеки в організаціях. Comput Secur, Vol. 56, с. 70-82, 2016.

47. Парсонс, К. та ін. Опитувальник «Людські аспекти інформаційної безпеки» (HAIS-Q). Комп'ютери та безпека. – 2017. – Т. 66. – No B. – С. 40-51. URL: https://doi.org/10.1016/j.cose.2017.01.004

48. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України". Указ Президента України від 26 серпня 2021 року № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021?find=1&text=%D0%BC%D0%BE%D0%B4%D0%B5%D0%BB%D1%8C#w1_1.

49. Стратегія кібербезпеки України (2023 – 2025 роки). Безпечний кіберпростір – запорука успішного розвитку країни. (ПРОЄКТ). URL: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf.

50. Про основні засади забезпечення кібербезпеки України: Закон України. (Відомості Верховної Ради (ВВР), 2017, № 45, ст.403). URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

51. Бойко О.О. Шляхи підвищення ефективності управління персоналом у сфері кібербезпеки. Актуальні проблеми кібербезпеки: Матеріали Всеукраїнської науково-практичної конференції (м. Київ, 27 жовтня 2023 року). Навчально-науковий інститут захисту інформації, Державний університет інформаційно-комунікаційних технологій. Київ, 2023. С. 29-31.

52. Рульєв В.А., Гуткевич С. О., Мостенська Т. Л. Управління персоналом: підручн.,– Київ: КОНДОР, 2017. – 324 с

53. Дудукало Г.О. Механізм забезпечення ефективності управління персоналом машинобудівних підприємств : автореф. дис. на здобуття наук. ступеня канд. ек. наук : спец. 08.00.04. – Київ, 2015. – 20 с.

54. Класифікація видів економічної діяльності ДК 009:2010. Наказ Держспоживстандарту України від 11.10.2010 N 457. [Електронний ресурс] Режим доступу: URL: https://zakon.rada.gov.ua/rada/show/vb457609-10#Text. (дата звернення – 22.10.23).

55. Національний класифікатор України ДК 003:2010. Класифікатор професій. Наказ Держспоживстандарту України від 28.07.2010 № 327. [Електронний ресурс] Режим доступу: URL: https://zakon.rada.gov.ua/rada/show/va327609-10#Text. (дата звернення – 22.10.23).

56. Бойко О.О. Загальні принципи управління персоналом у сфері кібербезпеки. Стратегії кіберстійкості: управління ризиками та безперервність бізнесу: Матеріали Всеукраїнської науково-практичної Інтернет-конференції (м. Київ, 23 лютого 2023 року) / Навчально-науковий інститут захисту інформації ДУТ. Київ, 2023. С. 129-131.