Журнал «Перспективи та інновації науки»
(Серія «Педагогіка», Серія «Психологія», Серія «Медицина»)
№ 2(48) 2025

УДК 811.161.2–047.22 + 004.056.5 + 378

https://doi.org/10.52058/2786-4952-2025-2(48)-965-977

Снігурова Ірина Іванівна старший викладач кафедри української мови, Національний технічний університет «Харківський політехнічний інститут», аспірантка, Харківський національний університет внутрішніх справ, спеціальність 011 Освітні, педагогічні науки, м. Харків, тел. (066) 806-60-90, https://orcid.org/0000-0002-9637-2428

МОВНОКОМУНІКАТИВНА КОМПЕТЕНТНІСТЬ МАЙБУТНІХ ФАХІВЦІВ ЗІ СПЕЦІАЛЬНОСТІ «КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ» ЯК СКЛАДОВА ЇХНЬОЇ УСПІШНОЇ ПРОФЕСІЙНОЇ ДІЯЛЬНОСТІ

Анотація. Мовнокомунікативна компетентність фахівців з кібербезпеки є вимогою стандартів вищої освіти та професійних стандартів і важливим чинником успішної професійної діяльності таких фахівців. Уміння створювати якісні документи (політики, інструкції, положення тощо), вести діалоги під час комунікацій зі співробітниками, постачальниками обладнання й послуг, стейкхолдерами, здійснювати монологічне мовлення під час проведення занять та інструктажів зі співробітниками з питань кібербезпеки є необхідною складовою під час виконання функціональних обов'язків таких фахівців.

Особливістю спеціальності «Кібербезпека та захист інформації» є значна кількість професійних ролей фахівців цього напряму підготовки. Зараз в Україні відбувається процес реформування системи підготовки фахівців з кібербезпеки. Реформа ґрунтується на створенні Національної рамки кваліфікації у сфері кібербезпеки та захисту інформації, запровадженні системи професійних стандартів, а також у створенні в Україні мережі незалежних кваліфікаційних центрів. Такий підхід враховує найкращі світові практики, спирається на досвід Європейської рамки кваліфікацій та американської Стратегічної освітньої ініціативи в кібербезпеці. Держспецзв'язком за підтримки проєкту USAID «Кібербезпека критично важливої інфраструктури України» було розроблено 21 професійний стандарт, які були схвалені Національним агентством кваліфікацій. Також необхідно відзначити, що в Європейській структурі навичок кібербезпеки (European Cybersecurity Skills Framework, ECSF) існує 12 профілів ролей для фахівців з кібербезпеки.

У таких умовах необхідно створити системний підхід щодо формування мовнокомунікативної компетентності студентів, які навчаються в закладах вищої освіти, враховуючи особливу професійну спрямованість фахівців спеціальності «Кібербезпека та захист інформації».

Журнал «Перспективи та інновації науки»
(Серія «Педагогіка», Серія «Психологія», Серія «Медицина»)
№ 2(48) 2025

У статті здійснено аналіз фахових компетентностей для ролей, прописаних в Європейській структурі навичок кібербезпеки, та вимог для формування професійної мовнокомунікативної компетентності студентів, які навчаються в закладах вищої освіти. Також у статті проаналізовано зміст завдань фахівців зі спеціальності «Кібербезпека та захист інформації», які вимагають високого рівня мовнокомунікативної компетентності, і розглянуто основні особливості комунікативних ситуацій фахівців даної спеціальності.

Ключові слова: Мовнокомунікативна компетентність, кібербезпека, комунікативні ситуації, професійна спрямованість фахівців, монологічне мовлення, діалог.

Snihurova Iryna Ivanivna senior lecturer of the Ukrainian language Department of the National Technical University "Kharkiv Polytechnic Institute", post-graduate student of the Kharkiv National University of internal affairs, specialty 011 Educational, Pedagogical Sciences, Kharkiv, tel.: (066) 806-60-90, https://orcid.org/0000-0002-9637-2428

LINGUISTIC AND COMMUNICATIVE COMPETENCE OF FUTURE SPECIALISTS IN THE SPECIALTY "CYBERSECURITY AND INFORMATION PROTECTION" AS A COMPONENT OF THEIR SUCCESSFUL PROFESSIONAL ACTIVITY

Abstract. The linguistic and communicative competence of cybersecurity specialists is a requirement of higher education standards and professional standards and an important factor in the successful professional activity of such specialists. The ability to create high-quality documents (policies, instructions, regulations, etc.), conduct dialogues in communications with employees, equipment and service providers, stakeholders, and deliver monologue speech during training and briefings with employees on cybersecurity issues is a necessary component of the functional responsibilities of such specialists.

The specific feature of the speciality ‘Cybersecurity and Information Protection’ is a significant number of professional roles of specialists in this field of study. Ukraine is currently in the process of reforming its cybersecurity training system. The reform is based on the creation of a National Qualification Framework in Cybersecurity and Information Protection, the introduction of a system of professional standards, and the establishment of a network of independent qualification centres in Ukraine. This approach takes into account the best international practices and draws on the experience of the European Qualifications Framework and the US Strategic Cybersecurity Education Initiative. With the support of the USAID project ‘Cybersecurity of Ukraine's Critical Infrastructure’, the State Service for Special Communications and Information Protection of Ukraine developed 21 professional standards that were approved by the National

Qualifications Agency. It should also be noted that the European Cybersecurity Skills Framework (ECSF) has 12 role profiles for cybersecurity professionals.

In such conditions, it is necessary to create a systematic approach to the formation of linguistic and communicative competence of students studying in higher education institutions, taking into account the special professional orientation of specialists in the speciality 'Cybersecurity and Information Protection'.

The article analyses the professional competences for the roles prescribed in the European Cybersecurity Skills Framework and the requirements for the development of professional linguistic and communicative competence of students studying in higher education institutions. The article also analyses the content of the tasks of specialists in the speciality 'Cybersecurity and Information Protection', which require a high level of linguistic and communicative competence, and considers the main features of communicative situations of specialists in this speciality.

Keywords: linguistic and communicative competence, cybersecurity, communicative situations, professional orientation of specialists, monologue speech, dialogue.

Постановка проблеми. Спеціальність «Кібербезпека та захист інформації» є на даний момент однією з найважливіших у забезпеченні захисту інформаційних ресурсів державних і приватних структур нашої країни, персональних даних громадян України. Стандартом вищої освіти бакалавра за даною спеціальністю [1] визначені загальна компетентність «Здатність спілкуватися державною мовою як усно, так і письмово» і результат навчання «Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків». Стандартом вищої освіти магістра за цією спеціальністю визначена загальна компетентність «Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами інших галузей знань / видів економічної діяльності)» і результат навчання «Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення й обговорення результатів досліджень та інновацій, забезпечення бізнес/операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки» [2].

Підготовка мовнокомунікативної компетентності студентів у технічних закладах вищої освіти (ЗВО) здійснюється в рамках навчальних дисциплін, таких, наприклад, як «Українське фахове мовлення», «Українська мова (за професійним спрямуванням)», «Українська мова» або інших на рішення ЗВО. Метою таких навчальних дисциплін є формування інтелектуально розвиненої, морально досконалої, національно свідомої, духовно багатої мовної особистості, яка вільно володіє виражальними засобами сучасної української літературної мови, її стилями, різновидами, жанрами в усіх видах мовленнєвої діяльності, відзначається готовністю до подальшого професійно-орієнтова-

Журнал «Перспективи та інновації науки»
(Серія «Педагогіка», Серія «Психологія», Серія «Медицина»)
№ 2(48) 2025

ного навчання, спроможна самостійно визначити цілі самоосвіти, самовиховання й саморозвитку та їх реалізувати [3]. Акцент таких дисциплін робиться на формуванні мовних компетентностей, практичних навичок володіння культурою мови й мовлення, дотримання в усних і письмових висловлюваннях орфоепічних, орфографічних, лексичних, морфологічних, стилістичних, пунктуаційних норм, уміння користуватися лінгвістичними словниками тощо. Програми цих дисциплін в технічних ЗВО, як правило, однакові для усіх технічних спеціальностей.

У рамках освітніх компонентів базової та вибіркової частин за спеціальністю при опануванні спеціальних (фахових) компетентностей також підвищується мовнокомунікативна компетентність студентів. Майбутні фахівці опановують навички відпрацювання письмових текстів і доповідей своїх результатів під час захисту лабораторних робіт навчальних дисциплін, курсових робіт (проєктів), кваліфікаційних робіт (проєктів) та інших освітніх компонентів. Водночас необхідно відзначити, що, як правило, основна увага науково-педагогічних працівників спрямована на формування фахових компетентностей, а не мовнокомунікативної.

Спеціальність «Кібербезпека та захист інформації» має свою специфіку з погляду професійної діяльності випускника цієї спеціальності. Він може працювати керівником підрозділу, менеджером, аудитором, дослідником, технічним фахівцем тощо, тобто для такого спеціаліста існує значне різноманіття комунікативних ситуацій, для яких він має бути готовим.

Тому актуальним завданням є розроблення методології формування мовнокомунікативної компетентності для виконання професійних функцій у студентів ЗВО, які навчаються за спеціальністю «Кібербезпека та захист інформації».

Аналіз останніх досліджень і публікацій. Питанням мовної підготовки особистості присвячено чимало праць С. Єрмоленко, Л. Мацько, Н. Колодій, В. Мельничайка, Л. Струганець, О. Семеног, Н. Голуб, Т. Симоненко, Н. Остапенко, К. Климової, Ю. Лукаш, І. Чеботарьової та інших науковців, але питання формування мовнокомунікативної компетентності майбутніх фахівців з кібербезпеки не розглядалися.

Мета статті – дослідження особливостей формування мовнокомунікативної компетентності майбутніх фахівців зі спеціальності «Кібербезпека та захист інформації» в контексті їх професійних ролей.

Виклад основного матеріалу. Комунікативна компетентність — це сукупність знань про спілкування в різноманітних умовах і з різними комунікантами, а також уміння їх ефективного застосування в конкретному спілкуванні в ролі адресанта й адресата [3, 4, 5]. Професійна комунікативна компетентність формується на базі комунікативної компетентності та передбачає наявність знань, умінь професійного спілкування. Мовнокомунікативна компетентність – це здатність особистості ефективно використовувати

мовні засоби для виконання комунікативних завдань у різних ситуаціях спілкування [6].

У літературі виділено низку компонентів мовнокомунікативної (або комунікативної) компетентності. Найчастіше названо такі види, як: мовна (знання учасниками комунікації норм і правил літературної мови та вміле використання їх у продукуванні висловлювань); соціолінгвістична (здатність розуміти та продукувати мовлення в конкретному соціолінгвістичному контексті спілкування); прагматична, дискурсивна, жанрова (спроможність поєднувати дискурси у зв'язні тексти й залучати їх до відповідних дискурсів); іллокутивна (здатність формувати й реалізовувати комунікативні наміри в повідомлення); стратегічна (уміння брати ефективну участь у спілкуванні, обираючи правильну стратегію і тактику); соціокультурна, лінгвокультурна, міжкультурна (здатність розуміти і використовувати різні складники національної культури (звичаї, норми) у конкретних ситуаціях з урахуванням специфіки національних культур у міжкультурному спілкуванні); когнітивно-гносеологічна (здатність пізнавати мовну картину світу); паравербальна (володіння невербальними засобами (фонаційними, кінетичними, графічними), що супроводжують мовлення й беруть участь у передаванні інформації) та ін. [6].

Для рішення поставленого в статті завдання необхідно спочатку зрозуміти, які професійні вимоги й комунікативні ситуації та яких потенційних комунікантів може мати майбутній фахівець зі спеціальності «Кібербезпека та захист інформації».

Європейська структура навичок кібербезпеки (European Cybersecurity Skills Framework, ECSF) [7] визначила 12 профілів ролей для фахівців з кібербезпеки, які потрібні та застосовуються в організаціях, що використовують фахівців із кібербезпеки. Кожен профіль визначається загальним шаблоном, який містить ключові критерії набору (тобто посада, альтернативні назви, підсумкова заява, місія, основні завдання, ключові навички, ключові знання, електронні компетентності). Зміст кожного критерію адаптовано до кожної ролі, але підлягає можливій адаптації, щоб забезпечити гнучку реалізацію відповідно до конкретних ситуацій і вимог.

До цих профілів відносяться: керівник інформаційної безпеки, реагувальник на кіберінциденти, офіцер з питань кіберюриспруденції, політики та відповідності, спеціаліст з аналізу кіберзагроз, педагог із кібербезпеки, реалізатор кібербезпеки, архітектор з кібербезпеки, аудитор із кібербезпеки, дослідник із кібербезпеки, менеджер ризиків з кібербезпеки, дослідник із цифрової криміналістики, тестувальник проникнення.

Зараз у нашій країні йде реформування системи підготовки кадрів у сфері кібербезпеки з урахуванням найкращих світових підходів [8, 9]. У 2022 році за підтримки Проєкту USAID «Кібербезпека критично важливої інфраструктури України» були розроблені та затверджені перші шість нових

Журнал «Перспективи та інновації науки»
(Серія «Педагогіка», Серія «Психологія», Серія «Медицина»)
№ 2(48) 2025

професійних стандартів у сфері кібербезпеки. У 2023 році Держспецзв'язку підготувала професійні стандарти ще для 15 нових професій у сфері кібербезпеки, які були схвалені Нацагентством кваліфікацій. До цих професійних стандартів відносяться: аналітик загроз безпеки, аудитор інформаційних технологій (з кібербезпеки), фахівець з оцінки заходів захисту інформації (кібербезпеки), фахівець з підтримки інфраструктури кіберзахисту, фахівець з кібердосліджень та розробок систем безпеки, фахівець з реагування на інциденти кібербезпеки, конструктор систем кібербезпеки, фахівець з планування політики та стратегії кібербезпеки, керівник структурного підрозділу з питань безпеки інформації та кіберзахисту; фахівець з криптографічного захисту інформації, фахівець з технічного захисту інформації, уповноважений з авторизації безпеки інформації, аналітик з оцінки вразливостей, фахівець з тестування систем захисту інформації, кібероператор. Загалом всього схвалено 21 професійний стандарт.

Проведемо аналіз фахових компетентностей для зазначених вище ролей, прописаних в Європейській структурі навичок кібербезпеки, і вимог для мовленнєвої компетентності. Перелік ключових компетентностей по кожному з профілей фахівця з кібербезпеки представлений в таблиці 1 [10].

Таблиця 1.

Перелік ключових компетентностей фахівця з кібербезпеки відповідно ECSF

ID	Профіль фахівця з кібербезпеки	Призначення	Ключові професійні компетентності ECSF
1	2	3	4
2.1	Керівник інформаційної безпеки (Chief Information Security Officer (CISO))	Керує стратегією кібербезпеки організації та її реалізацією, щоб гарантувати належну безпеку та захист цифрових систем, послуг і активів.	• Оцінка та покращення стану кібербезпеки організації; • Аналіз та впровадження політики кібербезпеки, сертифікації, стандартів, методологій та рамок; • Аналіз законів, нормативних актів та законодавства, зв'язок з кібербезпекою і дотримання їх; • Впровадження рекомендацій та найкращих практик щодо кібербезпеки; • Управління ресурсами кібербезпеки; • Розробка, підтримка та керування виконанням стратегії кібербезпеки; • Вплив на культуру кібербезпеки організації; • Розробка, застосовування, контроль та переглядання Системи управління інформаційною безпекою (СУІБ) безпосередньо або через аутсорсинг; • Перегляд та покращення документів безпеки, звітів, SLA та забезпечення цілей безпеки; • Виявлення та вирішення проблем, пов'язаних з кібербезпекою; • Створення плану кібербезпеки; • Спілкування, координація та співпраця з внутрішніми та зовнішніми зацікавленими сторонами; • Передбачення необхідних змін до стратегії інформаційної безпеки, організації та формулювання нових планів.

Продовження табл. 1

1	2	3	4
2.2	Реагувальник на кіберінциденти (Cyber Incident Responder)	Відстеження стану кібербезпеки організації, обробка інцидентів під час кібератак і забезпечення безперервної роботи систем ІКТ.	• Практика технічних, функціональних та операційних аспектів обробки і реагування на інциденти кібербезпеки; • Збір, аналіз та співставлення інформації про кіберзагрози, що надходить із багатьох джерел; • Робота над операційними системами, серверами, хмарами та відповідними інфраструктурами; • Робота під тиском; • Спілкування, презентація та звітування перед відповідними зацікавленими сторонами; • Керування файлами журналів і аналіз їх.
2.3	Офіцер з питань кібер-юриспруденції, політики та відповідності (Cyber Legal, Policy & Compliance Officer)	Керування дотриманням стандартів кібербезпеки, законодавчої та нормативної бази на основі стратегії організації та правових вимог.	• Повне розуміння бізнес-стратегії, моделей і продуктів і здатність враховувати законодавчі, нормативні вимоги та вимоги стандартів; • Виконання практики захисту даних і конфіденційності, пов'язані з реалізацією організаційних процесів, фінансів і бізнес-стратегії; • Очолювання розробки належної політики та процедур кібербезпеки та конфіденційності, які доповнюють бізнес-потреби та законодавчі вимоги; забезпечення його прийняття, розуміння та реалізацію та повідомлення про це залученим сторонам; • Проведення, контроль та переглядання оцінки впливу на конфіденційність, використовуючи стандарти, рамки, визнані методології та інструменти; • Пояснення та повідомлення зацікавленим сторонам і користувачам теми захисту даних і конфіденційності; • Розуміння, практикування та дотримування етичних вимог і стандартів; • Розуміння наслідків змін законодавчої бази для кібербезпеки організації та стратегії та політики захисту даних • Співпрацювання з іншими членами команди та колегами.
2.4	Спеціаліст з аналізу кіберзагроз (Cyber Threats Intelligence Specialist)	Збір, обробка, аналіз даних та інформації для створення дієвих звітів розвідки та розповсюджуйте їх серед зацікавлених сторін.	• Співпраця з іншими членами команди та колегами; • Збір, аналіз та співставлення інформації про кіберзагрози, що надходить із багатьох джерел; • Визначення TTP і кампанії загрозливих осіб; •Автоматизація процедур керування розвідкою про загрози; • Проведення технічного аналізу та звітності; • Виявлення некібернетичних подій, що мають наслідки, пов'язані з кібернетичною діяльністю; • Моделювання загроз, акторів і TTP; • Спілкування, координація та співпраця з внутрішніми та зовнішніми зацікавленими сторонами; • Спілкування, презентація та звітування перед відповідними зацікавленими сторонами; • Використання та застосовування платформ та інструментів CTI.
2.5	Архітектор з кібербезпеки (Cybersecurity Architect)	Планування та проектування рішення безпеки за проектом (інфраструктури, системи, активи, програмне забезпечення, апаратне забезпечення та послуги) і засоби контролю кібербезпеки.	• Проведення аналізу вимог безпеки користувачів і бізнесу; • Намалювання архітектурних та функціональних специфікацій кібербезпеки; • Декомпонування та аналіз системи для розробки вимог безпеки та конфіденційності та визначення ефективних рішень; • Розробка системи та архітектури на основі принципів безпеки та конфіденційності за проектом і за замовчуванням кібербезпеки; • Керівництво та спілкування з розробниками та IT/OT персоналом; • Спілкування, презентація та звітування перед відповідними зацікавленими сторонами; • Пропонування архітектури кібербезпеки на основі потреб і бюджету зацікавлених сторін; • Вибір відповідних специфікацій, процедури та засобів контролю; • Створення стійкості до точок збою в усій архітектурі; • Координування інтеграції рішень безпеки.

Журнал «Перспективи та інновації науки»
(Серія «Педагогіка», Серія «Психологія», Серія «Медицина»)
№ 2(48) 2025

Продовження табл. 1

1	2	3	4
2.6	Аудитор з кібербезпеки (Cybersecurity Auditor)	Проведення аудиту кібербезпеки екосистеми організації. Забезпечення відповідності законодавчій, нормативній, політичній інформації, вимогам безпеки, галузевим стандартам і найкращим практикам.	• Організація та праця систематично та детерміновано на основі доказів; • Дотримування і практикування аудиторських рамок, стандартів та методологій; • Застосовування інструментів та методів аудиту; • Аналіз бізнес-процесів, оцінювання та перевірка безпеки програмного чи апаратного забезпечення, а також технічних та організаційних засобів контролю; • Декомпонування та аналіз системи для виявлення слабких місць і неефективних засобів контролю; • Повідомлення, пояснювання та адаптування правових та нормативних вимог та потреб бізнесу; • Збирання, оцінювання, зберігання та захищення аудиторської інформації; • Чесне, неупереджене та незалежне проводення аудиту.
2.7	Педагог з кібербезпеки (Cybersecurity Educator)	Покращує знання, навички та компетенцію людей з кібербезпеки.	• Визначення потреб в обізнаності, навчанні та освіті з кібербезпеки; • Розроблення та запровадження навчальних програм для задоволення потреб у кібербезпеці; • Розроблення навчань з кібербезпеки, включаючи моделювання з використанням кіберсередовища; • Забезпечення навчань щодо отримання професійних сертифікатів із кібербезпеки та захисту даних; • Використовування наявних і навчальних ресурсів, пов'язаних з кібербезпекою; • Розроблення програм оцінки діяльності з підвищення обізнаності, навчання та освіти; • Спілкування, презентація та звітування перед відповідними зацікавленими сторонами; • Визначення та вибір відповідних педагогічних підходів для цільової аудиторії; • Мотивування та заохочування людей.
2.8	Реалізатор кібербезпеки (Cybersecurity Implementer)	Розробка, розгортання та керування рішеннями кібербезпеки (системами, активами, програмним забезпеченням, елементами керування та послугами) в інфраструктурі та продуктах.	• Спілкування, презентація та звітування перед відповідними зацікавленими сторонами; • Інтегрування рішень з кібербезпеки в інфраструктуру організації; • Налаштування рішень відповідно до політики безпеки організації; • Оцінка безпеки та продуктивності рішень; • Розробка коду, сценаріїв та програм; • Виявлення та вирішення проблем, пов'язані з кібербезпекою; • Співпрацювання з іншими членами команди та колегами.
2.9	Дослідник з кібербезпеки (Cybersecurity Researcher)	Покращення знань, навичок та компетенцій людей з кібербезпеки.	• Визначення потреб в обізнаності, навчанні та освіті з кібербезпеки; • Розроблення, розроблення та запровадження навчальних програм для задоволення потреб у кібербезпеці; • Розроблення навчання з кібербезпеки, включаючи моделювання з використанням кіберсередовища; • Забезпечення навчання щодо отримання професійних сертифікатів із кібербезпеки та захисту даних; • Використовування наявних навчальних ресурсів, пов'язаних з кібербезпекою; • Розроблення програм оцінювання діяльності з підвищення обізнаності, навчання та освіти; • Спілкування, презентація та звітування перед відповідними зацікавленими сторонами; • Визначення та вибір відповідних педагогічних підходів для цільової аудиторії; • Мотивування та заохочування людей.

Продовження табл. 1

1	2	3	4
2.10	Менеджер ризиків з кібербезпеки (Cybersecurity Risk Manager)	Управління ризиками організації, пов'язаними з кібербезпекою, відповідно до стратегії організації. Розробка, підтримка та повідомлення про процеси та звіти з управління ризиками.	• Впровадження основ управління ризиками кібербезпеки, методології та вказівок та забезпечення дотримання правил і стандартів; • Аналіз та консолідування методів управління якістю та ризиками організації; • Надання дозволу власникам бізнес-активів, керівникам та іншим зацікавленим сторонам приймати рішення з урахуванням ризиків для управління та пом'якшення ризиків; • Створення середовища кібербезпеки з урахуванням ризиків; • Спілкування, презентація та звітування перед відповідними зацікавленими сторонами; • Пропонування та керування варіантами розподілу ризиків
2.11	Дослідник з цифрової криміналістики (Digital Forensics Investigator)	Переконання, що розслідування кіберзлочинців виявить усі цифрові докази, які підтверджують зловмисну діяльність.	• Працювання етично та незалежно; не піддаватися впливу та упередженості внутрішніх чи зовнішніх акторів; • Збір інформації, зберігаючи її цілісність; • Визначення, аналіз та співвідносин подій кібербезпеки; • Пояснювання та представлення цифрових доказів простим, зрозумілим і зрозумілим способом; • Розроблення та повідомлення детальних та аргументованих звітів про розслідування.
2.12	Тестувальник проникнення (Penetration Tester)	Оцінка ефективності засобів контролю безпеки, виявлення та використання вразливостей кібербезпеки, оцінка їх критичності в разі використання загрозами.	• Розробка кодів, сценаріїв та програм; • Проведення соціальної інженерії; • Виявлення та використання вразливостей; • Виконання етичного хакерства; • Розуміння творчо та нестандартно; • Виявлення та вирішення проблем, пов'язаних із кібербезпекою; • Спілкування, презентація та звітування перед відповідними зацікавленими сторонами; • Ефективне використання засобів тестування на проникнення; • Проведення технічного аналізу та звітності; • Декомпонування та аналізування системи для виявлення слабких місць і неефективних засобів контролю; • Перегляд кодів, оцінка їх безпеки

Як бачимо в таблиці 1, професійні компетентності фахівців з кібербезпеки включають взаємозалежну комбінацію професійних технічних або організаційно-технічних компетентностей і мовнокомунікативну компетентність залежно від профілю.

Проведемо більш глибокий аналіз завдань, які має фахівець із кібербезпеки й захисту інформації та які вимагають мовнокомунікативної компетентності, і комунікаторів, з якими цей фахівець має спілкуватися. Результати аналізу представлені в таблиці 2.

Журнал «Перспективи та інновації науки»
(Серія «Педагогіка», Серія «Психологія», Серія «Медицина»)
№ 2(48) 2025

Таблиця 2.

Зміст завдань фахівців зі спеціальності «Кібербезпека та захист інформації», які вимагають високого рівня мовнокомунікативної компетентності

№ з/п	Завдання	Особливості контенту комунікації	Цільова аудиторія
1.	Розробка основної політики організації	Письмовий документ, який містить цілі і завдання СУІБ, принципи, регуляторні вимоги та інше.	1. Співробітники компанії. 2. Стейкхолдери (зовнішні сторони, клієнти) компанії.
2.	Розробка детальних політик процесів СУІБ – оцінки ризику інформаційної безпеки, проведення аудиту, обробки інцидентів та інших	Письмові документи, які містять організаційні та організаційно-технічні аспекти реалізації процесу.	Співробітники компанії (за необхідності зовнішні сторони). Можуть бути не фахівцями з кібербезпеки. Як приклад для оцінки ризиків ІБ залучаються менеджери, юристи та інші.
3.	Розробка детальних політик, процедур, рекомендацій, найкращих практик з кібербезпеки та інших документів	Письмові документи залежно від типу документа містять технічні та організаційні аспекти реалізації механізмів кіберзахисту, інших процесів в рамках спеціальності.	Технічні фахівці організації, які відповідають за реалізацію процесів в рамках профілів спеціальності (наприклад, Web-безпека, захист від шкідливих програм, криптографічний захист інформації та інші).
4.	Проведення тренінгів, навчань, інструктажів	Усна комунікативна діяльність у вигляді монологу/діалогу з однією особою або групою.	Співробітники компанії (технічні і нетехнічні фахівці).
5.	Комунікація зі внутрішніми та зовнішніми зацікавленими сторонами	Усна комунікативна діяльність у вигляді діалогу з однією особою або групою.	Співробітники компанії та зовнішні зацікавлені сторони (технічні і не- технічні фахівці).
6.	Комунікація в команді	Усна комунікативна діяльність у вигляді діалогу з однією особою або групою.	Члени колективу (наприклад, підрозділу з інформаційної безпеки – фахівці з цієї сфери).
7.	Проведення внутрішнього аудиту у вигляді письмового опитування	Письмовий опитувальник з питаннями по організаційним/організаційно-технічним аспектам організації процесів в компанію.	Співробітники компанії (технічні і нетехнічні фахівці).
8.	Презентація та звітування перед відповідними зацікавленими сторонами	Письмовий звіт, письмова презентація, усна презентація Наприклад, реагувальник на кіберінциденти звітує результати розслідування кіберінцидента перед керівництвом компанії.	Співробітники компанії та зовнішні зацікавлені сторони (технічні і не- технічні фахівці).
9.	Комунікація з постачальниками програмних, апаратних засобів, послуг	Усна у вигляді діалогу та письмова комунікативна діяльність з однією особою або групою.	Співробітники компанії та зовнішні сторони (в основному технічні фахівці).

Отже, у результаті аналізу можна виділити декілька основних особливостей ситуацій при реалізації мовнокомунікативної компетентності фахівця зі спеціальності «Кібербезпека та захист інформації».

По-перше, у якості цільової аудиторії можуть бути як технічні фахівці, які більш-менш володіють спеціальною термінологією та спеціальними знаннями в галузі кібербезпеки, так і нетехнічні фахівці.

По-друге, такі фахівці повинні мати уміння відпрацьовувати письмові документи, які, з одного боку, мають бути написані технічно грамотно, а з іншого – враховувати цільову аудиторію, яка може не володіти технічною термінологією, знанням певних технічних інструментів і процесів. Як приклад наведемо вимоги стандарту ISO/IEC27001 [11] щодо політики інформаційної безпеки: політика інформаційної безпеки має бути оформлена як документована інформація, бути поширена в організації, бути доступною для зацікавлених сторін. Стандарт ISO/IEC27002 [12] вимагає, щоб політика інформаційної безпеки була схвалена керівництвом компанії, опублікована й доведена до відома всіх співробітників і зацікавлених сторонніх організацій, тобто текст документа має бути написаний зрозумілою мовою для усієї цільової аудиторії.

По-третє, фахівці з цієї спеціальності повинні мати навички усного діалогічного та монологічного мовлення, презентації свої результатів, коли цільова аудиторія – це технічні фахівці та співробітники компанії, а також зацікавлені зовнішні сторони, які є фахівцями в інших галузях економіки. Як приклад можна навести ситуації, коли дослідник із цифрової криміналістики доповідає результати цифрової криміналістичної експертизи в суді, де його комунікаторами є судові працівники, адвокати, прокурори, інші залучені до судового процесу особи.

Висновки. Отже, на підставі сучасних досліджень із мовнокомунікативної компетентності, вимог наявних вітчизняних і міжнародних нормативних документів щодо рівня фахової компетентності фахівця з кібербезпеки та захисту інформації, комунікативних ситуацій у професійній діяльності таких фахівців буде розроблений методологічний підхід підготовки студентів, які навчаються в ЗВО.

Література:

1. Стандарт вищої освіти для першого (бакалаврського) рівня вищої освіти зі спеціальності 125 Кібербезпека. МОН України, 2024 р. 18 с.

2. Стандарт вищої освіти для другого (магістерського) рівня вищої освіти зі спеціальності 125 Кібербезпека. МОН України, 2021 р. 16 с.

3. Колодій Н. В. Професійна мовнокомунікативна компетенція / Н. В. Колодій // Проблеми та перспективи розвитку економіки і підприємництва та комп'ютерних технологій в Україні: збірник тез доповідей XIV Науково-практичної конференції, 17-20 квітня 2018 року. Львів: Видавництво Львівської політехніки, 2018. С. 144–146.

4. Чеботарьова І.О. Комунікативна компетентність: Теоретичний аспект / І.О. Чеботарьова// Наукові записки кафедри педагогіки, вип. XXXVI, Харків, 2014. С. 205 – 215.

5. Мацько Л. І. Культура української фахової мови: навчальний посібник / Л. І. Мацько, Л. В. Кравець. К. : ВЦ «Академія», 2007. 360 с.

6. Струганець Л.В. Мовнокомунікативна компетентність лідера в освітній галузі (теоретичний ракурс) / Л. Струганець // Університети і лідерство. 2015. № 1. С. 52-55.

7. European Cybersecurity Skills Framework User Manual / ENISA, 2022 p. 53. с. https://www.enisa.europa.eu/sites/default/files/publications/European%20Cybersecurity%20Skills%20Framework%20User%20Manual.pdf.

8. Реформування системи підготовки кадрів у сфері кібербезпеки: Нацагентство кваліфікацій схвалило 8 нових професійних стандартів. Державна служба спеціального зв'язку та захисту інформації України.

https://cip.gov.ua/ua/news/reformuvannya-sistemi-pidgotovki-kadriv-u-sferi-kiberbezpeki-nacagentstvo-kvalifikacii-skhvalilo-8-novikh-profesiinikh-standartiv.

9. Завершено черговий етап реформування системи підготовки кадрів у сфері кібербезпеки: Нацагентство кваліфікацій схвалило ще 7 профстандартів**.** Державна служба спеціального зв'язку та захисту інформації України. https://qc.csi.cip.gov.ua/uk/posts/7.

10. European Cybersecurity Skills Framework Role Profiles / ENISA, 2022. 26 с.

https://www.enisa.europa.eu/sites/default/files/publications/European%20Cybersecurity%20Skills%20Framework%20Role%20Profiles.pdf.

11. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection. Information security management systems. https://www.iso.org/standard/27001.

12. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls. https://www.iso.org/standard/75652.html.

References:

1. Standart vyshchoyi osvity dlya pershoho (bakalavrs′koho) rivnya vyshchoyi osvity zi spetsial′nosti 125 Kiberbezpeka. [Higher education standard for the first (bachelor's) level of higher education in specialty 125 Cybersecurity. Ministry of Education and Science of Ukraine]. (2024). MON Ukrayiny [in Ukrainian].

2. Standart vyshchoyi osvity dlya druhoho (mahisters′koho) rivnya vyshchoyi osvity zi spetsial′nosti 125 Kiberbezpeka. [Higher education standard for the second (master's) level of higher education in specialty 125 Cybersecurity. Ministry of Education and Science of Ukraine]. (2021). MON Ukrayiny [in Ukrainian].

3. Kolodiy, N.V. (2018). *Profesiyna movnokomunikatyvna kompetentsiya [Professional linguistic and communicative competence]* – Problemy ta perspektyvy rozvytku ekonomiky i pidpryyemnytstva ta komp″yuternykh tekhnolohiy v Ukrayini: zbirnyk tez dopovidey KHIV Naukovo-praktychnoyi konferentsiyi – Problems and prospects of the development of the economy and entrepreneurship and computer technologies in Ukraine collection of abstracts of the 14th Scientific and Practical Conference - (pp. 144 – 146). L′viv: Vydavnytstvo L′vivs′koyi politekhniky [in Ukrainian].

4. Chebotar′ova, I.O. (2014) Komunikatyvna kompetentnist′: Teoretychnyy aspekt [Communicative competence: Theoretical aspect]. *Naukovi zapysky kafedry pedahohiky – Scientific notes of the Department of Pedagogy*, XXXVI, 205 – 215 [in Ukrainian].

5. Mats′ko L. I. (2007) *Kul'tura ukrayins'koyi fakhovoyi movy: navchal'nyy posibnyk [The culture of the Ukrainian professional language]*. Kyiv: VTS «Akademiya», 2007. [in Ukrainian]..

6. Struhanets′, L.V. (2015) Movnokomunikatyvna kompetentnist′ lidera v osvitniy haluzi (teoretychnyy rakurs) [Linguistic competence of a leader in the field of education (theoretical perspective)]. *Universytety i liderstvo – Universities and leadership*. 2015, 1, 52-55 [in Ukrainian].

7. European Cybersecurity Skills Framework User Manual / ENISA, 2022 p. 53. с. https://www.enisa.europa.eu/sites/default/files/publications/European%20Cybersecurity%20Skills%20Framework%20User%20Manual.pdf.

8. Reformuvannya systemy pidhotovky kadriv u sferi kiberbezpeky: Natsahent·stvo kvalifikatsiy skhvalylo 8 novykh profesiynykh standartiv. Derzhavna sluzhba spetsial′noho zv″yazku ta zakhystu informatsiyi Ukrayiny [Reforming the cybersecurity training system: The National Qualifications Agency approved 8 new professional standards. State Service for Special Communications and Information Protection of Ukraine]. https://cip.gov.ua/ua/news/reformuvannya-sistemi-pidgotovki-kadriv-u-sferi-kiberbezpeki-nacagentstvo-kvalifikacii-skhvalilo-8-novikh-profesiinikh-standartiv [in Ukrainian]..

9. Zaversheno cherhovyy etap reformuvannya systemy pidhotovky kadriv u sferi kiberbezpeky: Natsahent·stvo kvalifikatsiy skhvalylo shche 7 profstandartiv. Derzhavna sluzhba spetsial′noho zv″yazku ta zakhystu informatsiyi Ukrayiny [Another stage of reforming the cybersecurity training system has been completed: the National Qualifications Agency approved 7 more professional standards. State Service for Special Communications and Information Protection of Ukraine.]. https://qc.csi.cip.gov.ua/uk/posts/7.

10. European Cybersecurity Skills Framework Role Profiles / ENISA, 2022. 26 с. https://www.enisa.europa.eu/sites/default/files/publications/European%20Cybersecurity%20Skills%20Framework%20Role%20Profiles.pdf.

11. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection. Information security management systems. https://www.iso.org/standard/27001.

12. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls. https://www.iso.org/standard/75652.html.