Силабус освітнього компонента
Програма навчальної дисципліни

Англійська мова в академічних застосунках

Шифр та назва спеціальності
F5 – Кібербезпека та захист інформації

Інститут
ННІ комп`ютерних наук та інформаційних технологій

Спеціалізація

Кафедра
Кібербезпеки (328)

Освітня програма
Кібербезпека

Тип дисципліни
Загальна підготовка, Обов'язкова

Рівень освіти
Другий (магістерський)

Форма навчання
Денна

Семестр
1

Мова викладання
Українська

Викладачі, розробники

МІЛЕВСЬКИЙ Станіслав Валерійович
stanislav.milevskyi@khpi.edu.ua
Доктор технічних наук, доцент, професор кафедри кібербезпеки НТУ «ХПІ».

Автор понад 100 наукових та навчально-методичних праць. Гарант освітньо-наукової програми «Кібербезпека» другого (магістерського) рівня вищої освіти. Провідний лектор з дисциплін: «Основи математичного моделювання систем безпеки», «Англійська мова в академічних застосунках», «Моделювання кіберфізичних дій» у студентів бакалавріата та магістратури.

Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Сучасні вимоги до підготовки магістра потребують від нього перш за все бути плідним учасником міжкультурної комунікації і мати необхідні навички та вміння професійного, ділового та ситуативного спілкування в усній і письмовій формах, бути спроможними оволодіти новітньою фаховою інформацією через іноземні джерела.

Мета та цілі дисципліни

Поглиблення набутих мовленнєвих компетентностей з англійської мови та формування професійно-оріентованої іншомовної комунікативної компетентності зі спеціальності F5 “Кібербезпека та захист інформації”.

Формат занять

Практичні заняття, самостійна робота, консультації. Підсумковий контроль – іспит.

Компетентності

КЗ-1. Здатність застосовувати знання у практичних ситуаціях.

Результати навчання

РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.
РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.
РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв’язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.
РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.
РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.
РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.
РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об’єктах інформаційної діяльності та критичної інфраструктури.
РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.
РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.
РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.
РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.

РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.
РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.
РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.
РН25. Оцінювати ефективність та практичну цінність результатів наукових і практичних досліджень та інновацій.

Обсяг дисципліни

Загальний обсяг дисципліни 90 год. (3 кредити ECTS): практичні заняття – 32 год., самостійна робота – 58 год.

Передумови вивчення дисципліни (пререквізити)

Володіти базовими навичками читання, письма, аудіювання та говоріння англійською мовою, знати основні граматичні структури, лексику загального вжитку та термінологію своєї спеціальності, уміти користуватися електронними ресурсами та довідковими матеріалами англійською мовою для навчальних і наукових цілей.

Особливості дисципліни, методи та технології навчання

В ході викладання дисципліни викладачем застосовуються пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний методи навчання. В якості методів викладання, які направлені на активізацію та стимулювання навчально-пізнавальної діяльності здобувачів, застосовуються презентації, бесіди, індивідуальні групові проєкти, майстер-класи.

Програма навчальної дисципліни

Навчальні заняття

Практичні заняття

Теми практичних/семінарських занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Кіберпростір і кібербезпека – головні ознаки нової інформаційної цивілізації у полікультурному середовищі. Ознайомлення з поняттями кіберпростору та кібербезпеки, їхньою роллю у формуванні сучасного інформаційного суспільства. Аналіз впливу цифрових технологій на полікультурне середовище.	8	0,1
Тема 2. Кібератаки та кібертероризм у полікультурному середовищі. Розгляд основних видів кібератак і проявів кібертероризму, приклади з практики. Вивчення впливу кіберзагроз на суспільну безпеку та міжкультурну взаємодію.	8	0,1
Тема 3. Канали несанкціонованого доступу до інформації. Аналіз основних каналів витоку інформації в кіберпросторі. Вивчення типових способів несанкціонованого доступу та практичних методів їх виявлення і запобігання.	8	0,1

Тема 4. Методи та засоби протидії соціотехнічним атакам і захисту від них: переваги та недоліки. Ознайомлення з видами соціотехнічних атак (фішинг, маніпуляції, інженерія довіри). Практичний аналіз ефективності методів захисту, їхніх сильних і слабких сторін.	8	0,1
Загальна кількість годин	**32**	$\sum_{i=1}^{n} a_i = 0{,}4$

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Особливості академічного письма англійською мовою. Аналіз структурних та мовних особливостей академічного тексту. Практичне опрацювання правил оформлення есе, звітів, анотацій і наукових статей англійською мовою.	0,1
Тема 2. Академічна комунікація: презентації, дискусії та публічні виступи. Вивчення принципів ефективної усної академічної комунікації. Формування навичок створення та представлення презентацій, участі в наукових обговореннях і дебатах англійською мовою.	0,1
Загалом	$\sum_{i=1}^{m} b_i = 0{,}2$

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

Опрацювання теоретичного матеріалу

Теми для самостійного вивчення	Кількість годин
Тема 1. Академічна лексика та термінологія. Вивчення основної академічної лексики, уживаної у наукових статтях, звітах та виступах. Розширення словникового запасу для академічного письма та комунікації.	8
Тема 2. Структура та стиль наукового тексту. Ознайомлення з особливостями побудови наукових текстів англійською мовою, принципами логічності, послідовності й формального стилю.	10
Тема 3. Академічна доброчесність і запобігання плагіату. Вивчення правил цитування, оформлення бібліографії та способів перевірки оригінальності наукових робіт.	10
Тема 4. Читання та аналіз наукових джерел англійською мовою. Розвиток навичок роботи з автентичними академічними текстами, аналіз основних ідей, аргументів та висновків.	10
Тема 5. Написання анотацій, резюме та рефератів англійською мовою. Формування вмінь стисло передавати зміст наукових текстів відповідно до академічних стандартів.	10
Тема 6. Використання цифрових ресурсів для академічного навчання. Ознайомлення з онлайн-інструментами для покращення академічної англійської — словниками, корпусами, платформами для публікацій і навчання.	10

Загальна кількість годин	58

Неформальна освіта

Здобувач має можливість перезарахувати окремі теми або курс шляхом: проходження професійних курсів чи тренінгів, онлайн-освіти, професійних стажувань, у сфері, що відповідає навчальним цілям дисципліни.
Для зарахування необхідно надати: сертифікат (електронний або друкований) про проходження курсу/стажування, опис програми тренінгу із зазначенням змісту тем, обсягу та тривалості..

Рекомендовані курси, тренінги, стажування

1. Онлайн-курс CISCO «English For IT 1 and 2»
https://www.netacad.com/catalogs/learn?category=course.

Література, навчальні матеріали та інформаційні ресурси

Основна література

1. Словник термінів із кібербезпеки / За заг. ред. О. В. Копана, €. Д. Скулиша - К.: ВБ «Аванпост-Прим», 2012.-214 с. [Електронний ресурс].- Режим доступу:
https://www.nas.gov.ua/siaz/Ways_of_development_of_Ukrainian_science/article/12058.016.pdf
2. Borova T. English for Business Analysts: textbook: in 3 parts, Part 3. Business Intelligent Tools / T. Borova, O. Milov. – Kharkiv: S. Kuznets KhNUE, 2018. – 179 P. [Електронний ресурс].- Режим доступу:
http://repository.hneu.edu.ua/bitstream/123456789/21467/1/2018-%D0%91%D0%BE%D1%80%D0%BE%D0%B2%D0%B0%20%D0%A2%20%D0%90%2C%20%D0%9C%D1%96%D0%BB%D0%BE%D0%B2%20%D0%9E%20%D0%92.pdf
3. Journal of Information Security [Електронний ресурс].- Режим доступу: https://www.scirp.org/journa/home.aspx?issueid=l4294#103116.

Додаткова література

4 Key Private and Public Cyber Expectations Need to be Consistently [Електронний ресурс].- Режим доступу: http ://web.ebscohost.com.
5. Latest Cybersecurity News And Articles [Електронний ресурс].- Режим доступу: https://cyware.com/cyber-security-news-articles.

Система оцінювання

Підсумкова оцінка з освітнього компонента визначається відповідальним лектором за темами, видами занять, тощо у відповідності до силабусу і є інтегральною оцінкою результатів усіх вид навчальної діяльності здобувача вищої освіти. Підсумкова оцінка повинна відображати всі оцінки за складовими навчального процесу з урахуванням їх вагових показників k:

Поточний контроль (практичні, семінарські, лабораторні заняття), k_1	Контрольні роботи (за наявності), k_2	Індивідуальне завдання (за наявності), k_3	Підсумковий контроль (для ОК з іспитом), k_4
0,4	0,2		0,4

Сума коефіцієнтів повинна складати одиницю: $k_1 + k_2 + k_3 + k_4 = 1$. Підбір вагових коефіцієнтів підсумкової оцінки здійснює розробник курсу.

Розрахунок підсумкової оцінки проводиться за формулою:

$$О = П \cdot k_1 + K \cdot k_2 + І \cdot k_3 + Пк \cdot k_4$$

де: П – середньозважена середня оцінка за поточний контроль
І – оцінка за виконання індивідуального завдання
K – середньозважена оцінка за контрольні роботи
Пк – оцінка за підсумковий контроль

$$П = \frac{П_1 \cdot a_1 + П_2 \cdot a_2 + ... + П_n \cdot a_n}{\sum_{i=1}^{n} a_i}$$

де: a_i - ваговий коефіцієнт за кожне практичне (семінарське) або лабораторне заняття.

$$K = \frac{K_1 \cdot b_1 + K_2 \cdot b_2 + ... + K_m \cdot b_m}{\sum_{i=1}^{m} b_i}$$

де: b_i - ваговий коефіцієнт за кожну контрольну роботу.

Поточні оцінки за кожну складову (П, K, І,...) виставляються за 100-бальною шкалою згідно з положенням «Про критерії та систему оцінювання знань та вмінь і про рейтинг здобувачів вищої освіти» НТУ «ХПІ».

Підсумкова оцінка виставляється відповідно до розрахованої О з округленням до найближчого цілого числа в більшу сторону.

Шкала оцінювання

Сума балів	Національна оцінка	ECTS
90–100	Відмінно	A
82–89	Добре	B
75–81	Добре	C
64–74	Задовільно	D
60–63	Задовільно	E
35–59	Незадовільно (потрібне додаткове вивчення)	FX
1–34	Незадовільно (потрібне повторне вивчення)	F

Норми академічної етики і політика курсу

Здобувач вищої освіти повинен дотримуватися «Кодексу етики академічних взаємовідносин та доброчесності НТУ «ХПІ»: виявляти дисциплінованість, вихованість, доброзичливість, чесність, відповідальність. Конфліктні ситуації повинні відкрито обговорюватися в навчальних групах з викладачем, а при неможливості вирішення конфлікту – доводитися до відома співробітників дирекції інституту.
Нормативно-правове забезпечення впровадження принципів академічної доброчесності НТУ «ХПІ» розміщено на сайті: http://blogs.kpi.kharkov.ua/v2/nv/akademichna-dobrochesnist/

Погодження

Силабус погоджено	30.08.2025		**Завідувач кафедри** Сергій ЄВСЕЄВ
	30.08.2025		**Гарант ОП** Станіслав МІЛЕВСЬКИЙ