СИЛАБУС КОМПОНЕНТИ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

«НАУКОВО-ТЕХНІЧНИЙ ПЕРЕКЛАД»

Лектор курсу	**Мужанова Тетяна Михайлівна**, кандидат наук з держ.упр., доц., доцент кафедри управління інформаційною та кібербезпекою	**Контактна інформація лектора (e-mail), сторінка курсу в Moodle**	**e-mail:** muzanovat@gmail.com; **сторінка курсу в Moodle –** https://dn.dut.edu.ua/course/view.php?id=715
Галузь знань	12 Інформаційні технології	**Рівень вищої освіти**	магістр
Спеціальність	125 Кібербезпека та захист інформації	**Семестр**	9-10
Освітньо-професійна програма	Управління інформаційною та кібернетичною безпекою	**Тип дисципліни**	Основна компонента освітньо-професійної програми

Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінарських занять	Практичних занять	Лабораторних занять	Самостійна підготовка
	10	300	-	-	72	-	228

АНОТАЦІЯ КУРСУ

Взаємозв'язок у структурно-логічній схемі

Освітні компоненти, які передують вивченню	Менеджмент інформаційної безпеки Іноземна мова професійного спрямування
Освітні компоненти для яких є базовою	Аудит інформаційної безпеки Ефективність управління інформаційною безпекою

Мета курсу: набуття студентами компетенцій, знань, умінь і навичок науково-технічного перекладу з іноземної (англійської) мови у сфері управління інформаційною безпекою, оволодіння професійною термінологією з метою подальшого використання у професійній діяльності.

Компетентності відповідно до освітньої програми

Загальні компетентності (КЗ)	**Фахові компетентності спеціальності (КФ)**
КЗ2. Здатність проводити дослідження на відповідному рівні. **КЗ5**. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності). **КЗ9**. Володіння навичками критичного мислення.	**КФ2**. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки. **КФ4**. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.

Програмні результати навчання (ПРН)

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.
РН26. Здатність використовувати професійно профільовані знання й практичні навички для розроблення та впровадження національних стандартів і технічних регламентів застосування інформаційно-комунікаційних технологій, гармонізованих із відповідними європейськими стандартами.

ОРГАНІЗАЦІЯ НАВЧАННЯ			
Тема, опис теми	**Вид заняття**	**Оцінювання за тему**	**Форми і методи навчання/питання до самостійної роботи**
Змістовий модуль 1			
Тема 1. Вступ та огляд кібербезпеки ***Знати***: 1. Сутність, еволюція та різниця між поняттями інформаційної та кібербезпеки. 2. Цілі кібербезпеки: цілісність, доступність, конфіденційність, невідмовність. 3. Засади управління кібербезпекою (управління, обробка ризиків, нормативна відповідність, розподіл ролей). 4. Домени кібербезпеки. ***Вміти:*** перекладати з англійської на українську мову науково-технічні тексти у сфері управління інформаційною безпекою; використовувати англійську науково-технічну лексику в інтернаціональному професійному спілкуванні. ***Формування компетенцій:*** К32, К35, К39, КФ2, КФ4 ***Результати навчання:*** РН1, РН3 ***Рекомендовані джерела:*** 1,4,7-9.	Практичне заняття 1 Практичне заняття 2 Практичне заняття 3 Практичне заняття 4 Практичне заняття 5	5,5*	Усний та/або письмовий переклад науково-технічних текстів за фахом з англійської на українську мову індивідуально або в міні-групах. Ведення словника, вивчення і повторення професійної науково-технічної термінології. Підготовка анотацій та повідомлень, виділення основних тез та узагальнення змісту опрацьованих текстів. Обговорення прочитаних науково-технічних публікацій англійською мовою, прослуховування аудіо- та відеоматеріалів за темою. Усне експрес-опитування за матеріалами попереднього заняття, перевірка знання науково-технічної термінології та виразів. **Проведення контрольної роботи № 1**
Тема 2. Концепції кібербезпеки. ***Знати***: 1. Види ризиків кібербезпеці. Управління ризиками. 2. Типові типи і вектори кібератак. 3. Політики кібербезпеки. 4. Заходи та засоби кібербезпеки. ***Вміти:*** перекладати з англійської на українську мову науково-технічні тексти у сфері управління інформаційною безпекою; використовувати англійську науково-технічну лексику в інтернаціональному професійному спілкуванні. ***Формування компетенцій:*** К32, К35, К39, КФ2, КФ4 ***Результати навчання:*** РН1, РН3, РН26 ***Рекомендовані джерела:*** 1,4,7-9.	Практичне заняття 6 Практичне заняття 7 Практичне заняття 8 Практичне заняття 9 Практичне заняття 10 Практичне заняття 11	5,5*	Усний та/або письмовий переклад науково-технічних текстів за фахом з англійської на українську мову індивідуально або в міні-групах. Ведення словника, вивчення і повторення професійної науково-технічної термінології. Підготовка анотацій та повідомлень, виділення основних тез та узагальнення змісту опрацьованих текстів. Обговорення прочитаних науково-технічних публікацій англійською мовою, прослуховування аудіо- та відеоматеріалів за темою. Усне експрес-опитування за матеріалами попереднього заняття, перевірка знання науково-технічної термінології та виразів. **Проведення контрольної роботи № 2**

Тема 3. Принципи архітектури кібербезпеки ***Знати***: 1. Основи архітектури кібербезпеки. 2. Модель взаємодії відкритих систем OSI. 3. Сутність концепції ешелованого захисту. 3. Методи контролю інформаційних потоків, ізоляції та сегментації (VLAN). 4. Реєстрація, моніторинг і виявлення. 5. Основи, методи і застосування шифрування. ***Вміти:*** перекладати з англійської на українську мову науково-технічні тексти у сфері управління інформаційною безпекою; використовувати англійську науково-технічну лексику в інтернаціональному професійному спілкуванні. ***Формування компетенцій:*** КЗ2, КЗ5, КЗ9, КФ2, КФ4 ***Результати навчання:*** РН1, РН3, РН26 ***Рекомендовані джерела:*** 1,4,7-9.	Практичне заняття 12 Практичне заняття 13 Практичне заняття 14 Практичне заняття 15 Практичне заняття 16 Практичне заняття 17 Практичне заняття 18	5,5*	Усний та/або письмовий переклад науково-технічних текстів за фахом з англійської на українську мову індивідуально або в міні-групах. Ведення словника, вивчення і повторення професійної науково-технічної термінології. Підготовка анотацій та повідомлень, виділення основних тез та узагальнення змісту опрацьованих текстів. Обговорення прочитаних науково-технічних публікацій англійською мовою, прослуховування аудіо- та відеоматеріалів за темою. Усне експрес-опитування за матеріалами попереднього заняття, перевірка знання науково-технічної термінології та виразів. **Проведення контрольної роботи № 3**
Тема 1. Підходи до управління ризиками ISO, ISACA, NIST. **Тема 2.** Системи моніторингу та управління безпекою інформаційної мережі. **Тема 3.** Види міжмережевих екранів. Переваги і недоліки.	Самостійна робота		1. Ідентифікація та класифікація ризиків кібербезпеці. Управління ризиками відповідно до стандартів ISO, COBIT, спеціальних публікацій NIST. 2. Роль та функції систем управління інформацією та подіями безпеки (SIEM) та запобігання витоку даних у забезпеченні кібербезпеки (DLP). Засоби запобігання та виявлення вторгнень (IDS, IPS). 3. Призначення, види і функції міжмережевих екранів. Порівняльна характеристика продуктів різних виробників.
Змістовий модуль 2			
Тема 4. Безпека мереж, систем, додатків і даних Безпека мережі. Безпека.. ***Знати***: 1. Заходи з оцінки ризиків. Вразливості кібербезпеки. 2. Методи забезпечення безпеки мережі. 3. Заходи безпеки операційної системи та додатків. 4. Безпека даних. ***Вміти:*** перекладати з англійської на українську мову науково-технічні тексти у сфері управління інформаційною безпекою; використовувати англійську науково-технічну лексику в інтернаціональному професійному спілкуванні. ***Формування компетенцій:*** КЗ2, КЗ5, КЗ9, КФ2, КФ4	Практичне заняття 19 Практичне заняття 20 Практичне заняття 21 Практичне заняття 22	5,5*	Усний та/або письмовий переклад науково-технічних текстів за фахом з англійської на українську мову індивідуально або в міні-групах. Ведення словника, вивчення і повторення професійної науково-технічної термінології. Підготовка анотацій та повідомлень, виділення основних тез та узагальнення змісту опрацьованих текстів. Обговорення прочитаних науково-технічних публікацій англійською мовою, прослуховування аудіо- та відеоматеріалів за темою.

Результати навчання: РН1, РН3, РН26 ***Рекомендовані джерела:*** 1,5,7-9.	Практичне заняття 23 Практичне заняття 24 Практичне заняття 25		Усне експрес-опитування за матеріалами попереднього заняття, перевірка знання науково-технічної термінології та виразів. **Проведення контрольної роботи № 4**
Тема 5. Реагування на інциденти кібербезпеки ***Знати***: 1. Події та інциденти кібербезпеки. 2. Реагування на інциденти безпеки. 3. Розслідування, юридичні затримання та збереження. Криміналістична експертиза. 4. Плани аварійного відновлення та безперервності бізнесу. ***Вміти:*** перекладати з англійської на українську мову науково-технічні тексти у сфері управління інформаційною безпекою; використовувати англійську науково-технічну лексику в інтернаціональному професійному спілкуванні. ***Формування компетенцій:*** КЗ2, КЗ5, КЗ9, КФ2, КФ4 ***Результати навчання:*** РН1, РН3, РН26 ***Рекомендовані джерела:*** 1,5,7-9.	Практичне заняття 26 Практичне заняття 27 Практичне заняття 28 Практичне заняття 29 Практичне заняття 30	5,5*	Усний та/або письмовий переклад науково-технічних текстів за фахом з англійської на українську мову індивідуально або в міні-групах. Ведення словника, вивчення і повторення професійної науково-технічної термінології. Підготовка анотацій та повідомлень, виділення основних тез та узагальнення змісту опрацьованих текстів. Обговорення прочитаних науково-технічних публікацій англійською мовою, прослуховування аудіо- та відеоматеріалів за темою. Усне експрес-опитування за матеріалами попереднього заняття, перевірка знання науково-технічної термінології та виразів. **Проведення контрольної роботи № 5**
Тема 6. Перспективи кібербезпеки та впровадження новітніх технологій Орієнтація ІТ та мобільних пристроїв на споживання. Хмарна та цифрова співпраця. ***Знати***: 1. Сучасний ландшафт загроз. Розширені постійні загрози. Основні функції підсистем захисту операційної системи. 2. Вразливості, загрози та ризики для мобільних технологій. 3. Взаємодія у сфері хмарних та мобільних технологій. 4. Напрями знань у сфері кібербезпеки. ***Вміти:*** перекладати з англійської на українську мову науково-технічні тексти у сфері управління інформаційною безпекою; використовувати англійську науково-технічну лексику в інтернаціональному професійному спілкуванні. ***Формування компетенцій:*** КЗ2, КЗ5, КЗ9, КФ2, КФ4 ***Результати навчання:*** РН1, РН3, РН26 ***Рекомендовані джерела:*** 1,5,7-9.	Практичне заняття 31 Практичне заняття 32 Практичне заняття 33 Практичне заняття 34 Практичне заняття 35 Практичне заняття 36	5,5*	Усний та/або письмовий переклад науково-технічних текстів за фахом з англійської на українську мову індивідуально або в міні-групах. Ведення словника, вивчення і повторення професійної науково-технічної термінології. Підготовка анотацій та повідомлень, виділення основних тез та узагальнення змісту опрацьованих текстів. Обговорення прочитаних науково-технічних публікацій англійською мовою, прослуховування аудіо- та відеоматеріалів за темою. Усне експрес-опитування за матеріалами попереднього заняття, перевірка знання науково-технічної термінології та виразів. **Проведення контрольної роботи № 6**

Тема 5. Тестування на проникнення. **Тема 6.** Основні засади шифрування, криптографічні техніки і додатки. **Тема 7.** Новітні підходи до захисту мобільних пристроїв у корпоративних інформаційних мережах.	Самостійна робота		1. Завдання пентестингу. Етапи і методологія тестування на проникнення. 2. Класифікація алгоритмів шифрування. Принципи роботи симетричних та асиметричних алгоритмів шифрування, їх недоліки. 3. Використання мобільних пристроїв. Загрози використання й методи захисту мобільних пристроїв в корпоративних мережах.

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

- Мультимедійний проектор;
- Комп'ютерний клас для проведення практичних занять.

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

1. Cybersecurity Fundamentals Study Guide, 2nd Edition. ISACA. 194 p. URL: https://www.studocu.com/nl-be/document/odisee-hogeschool/cybersecurity-fundamentels/college-aantekeningen/cybersecurity-fundamentals-with-notes/7343872/view
2. Pauline Bowen, Joan Hash, Mark Wilson. Information Security Handbook: A Guide for Managers, NIST, 178 p. URL: http://www.dut.edu.ua/uploads/l_1889_44919882.pdf
3. Tony Campbell, Burns Beach. Practical Information Security Management: A Complete Guide to Planning and Implementation. Apress. 237 p. URL: http://www.dut.edu.ua/uploads/l_1888_50813661.pdf
4. Cyber-Security Standards, Benchmarking & Best Practices Overview. SAINT Consortium, 2018. 155 p. URL: https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5bab62342&appId=PPGMS
5. Information Security Management Handbook. Sixth Edition. Volume 7. Edited by Richard O'Hanley, James S. Tiller. CRC Press Taylor & Francis Group. 400 p.
6. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. National Institute of Standards and Technology, 2018. 48 p. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
7. ISACA. URL: http://www.isaca.org/
8. SpringerOpen. URL: https://www.springeropen.com/
9. Sciencedirect. URL: https://www.sciencedirect.com/search?qs=cybersecurity
10. Technology Innovation Management Review (TIM Review). URL: https://www.timreview.ca/
11. V.Savchenko, H.Haidur, S.Gakhov, S.Lehominova, T.Muzhanova, I.Novikova. Model of Control in a UAV Group for Hidden Transmitters Detection on the Basis of Local Self-Organization : IJATCSE. Volume-9 Issue-4. July-August 2020. P 6167-6174. URL: http://www.warse.org/IJATCSE/static/pdf/file/ijatcse291942020.pdf

ПОЛІТИКА КУРСУ («ПРАВИЛА ГРИ»)

- Курс передбачає роботу індивідуально і в групах.
- Середовище в аудиторії є інтерактивним, творчим, відкритим до дискусії та взаємодопомоги.
- Освоєння дисципліни передбачає обов'язкове відвідування практичних занять, а також самостійну роботу.
- Самостійна робота включає в себе індивідуальний переклад науково-технічних текстів за спеціалізацією, вивчення професійної термінології та виразів, що стосуються тем, які не ввійшли в теоретичний курс, або були розглянуті коротко, їх поглиблене опрацювання на основі рекомендованої літератури, практичне оволодіння навичками науково-технічного перекладу, анотування, методами роботи з літературою.
- Усі завдання, передбачені програмою, мають бути виконані у встановлений термін.
- Якщо студент відсутній з поважної причини, він надає викладачу виконані завдання в індивідуальному порядку.
- Під час роботи над завданнями не допустимо порушення вимог академічної доброчесності: при використанні Інтернет-ресурсів та інших джерел інформації студент має посилатися на використане джерело. Не допускається підказування й допомога студенту з боку одногрупників під час виконання індивідуальних

завдань. У разі виявлення факту плагіату студент отримує за завдання 0 балів, аналогічну оцінку отримують автори тотожних робіт.

- Студент, який спізнився, вважається таким, що пропустив заняття з неповажної причини з виставленням 0 балів за заняття, і при цьому має право бути присутнім на занятті.
- Використання телефонів і комп'ютерних засобів без дозволу викладача забороняється.

***КРИТЕРІЇ ТА МЕТОДИ ОЦІНЮВАННЯ**

Умовою допуску до підсумкового контролю є набрання студентом 30 балів у сукупності за всіма темами дисципліни

Форми контролю	Види навчальної роботи	Оцінювання
ПОТОЧНИЙ КОНТРОЛЬ	***Робота на заняттях,*** *у т.ч.:*	
	• присутність на заняттях (при пропусках занять з поважних причин допускається відпрацювання пройденого матеріалу)	за кожне відвідування 0,55 бала
	• опитування за результатами вивчення теми, перевірка знання термінології	за кожну правильну відповідь 0,25 бала
	• індивідуальний виступ за результатами самостійного перекладу науково-технічних текстів	за кожен виступ максимум 2 бали
	• доповідь з презентацією за темою, в тому числі вивченою самостійно (оцінка залежить від повноти розкриття теми, якості інформації, самостійності і креативності презентації і доповіді)	за кожну доповідь максимум 3 бали
	• підготовка повідомлення, анотації, аналіз основних тез науково-технічної публікації	за кожну правильну відповідь 2 бали
	• участь у дискусії, обговоренні основних тез науково-технічної публікації	за кожну участь 1 бал
РУБІЖНЕ ОЦІНЮВАННЯ (МОДУЛЬНИЙ КОНТРОЛЬ)	Модульний контроль № 1,2,3	максимальна оцінка – 15 балів
	Модульний контроль № 4,5,6	максимальна оцінка – 15 балів
Додаткова оцінка	Участь у наукових конференціях, підготовка наукових публікацій, участь у всеукраїнських та міжнародних конкурсах наукових студентських робіт за спеціальністю тощо.	Звільняється від заліку. іспиту
ПІДСУМКОВЕ ОЦІНЮВАННЯ ***Залік, іспит***	Метою заліку, іспиту є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання професійних обов'язків. Залік та іспит проходять у письмовій формі.	30 балів

ПІДСУМКОВА ОЦІНКА ЗА ДИСЦИПЛІНУ

бали	**Критерії оцінювання**	**Рівень компетентності**	**Оцінка** /*запис у заліковій відомості*
90-100	Студент демонструє повні й міцні знання навчального матеріалу й термінології в обсязі, що відповідає робочій програмі дисципліни, правильно й обґрунтовано відповідає на поставлені запитання за темою. Студент показує високу якість перекладу текстів науково-технічного спрямування, використання спеціалізованої лексики, повне сприйняття змісту матеріалів за темою. За час навчання при проведенні практичних занять та виконанні індивідуальних / контрольних завдань студент проявляє вміння самостійно виконувати поставлені завдання щодо науково-технічного перекладу текстів за фахом, активно долучатися до обговорення фахових питань іноземною мовою. Зменшення 100-бальної оцінки може бути пов'язане з недостатнім розкриттям питань, що стосується дисципліни, яка вивчається, але виходить за рамки обсягів матеріалу, передбаченого робочою програмою, або невпевненістю у тлумаченні окремих положень.	**Високий** Повністю забезпечує вимоги до знань, умінь і навичок, що викладені в робочій програмі дисципліни. Власні пропозиції студента щодо виконання практичних завдань підвищують його вміння використання знань, отриманих при вивченні інших дисциплін, а також знань, набутих при самостійному поглибленому вивченні питань у межах дисципліни, яка вивчається.	Відмінно / Зараховано (А)

82-89	Студент демонструє гарні знання змісту та професійної термінології, добре володіє навичками науково-технічного перекладу матеріалів за фахом, що відповідає робочій програмі дисципліни, вміє застосовувати набуті знання професійну лексику для самостійної роботи над текстами, але допускає одиничні неточності. Вміє самостійно виправляти допущені помилки, число яких є незначним. За час навчання при проведенні практичних занять, виконанні індивідуальних / контрольних завдань студент проявляє хорошу здатність самостійно виконувати завдання щодо перекладу науково-технічних текстів, долучатися до їх обговорення іноземною мовою із незначними прогалинами у володінні практичними навичками.	**Достатній** На достатньо високому рівні забезпечує вимоги до знань, умінь і навичок, що викладені в робочій програмі дисципліни. Забезпечує студенту самостійне виконання практичних завдань у разі незначної зміни умов, порівняно з наданими у матеріалах дисципліни	Добре / Зараховано (B)
75-81	Студент загалом добре володіє матеріалом та професійною термінологією, вміє добре перекладати матеріали науково-технічного спрямування відповідно до робочої програми дисципліни, вміє застосовувати набуті знання та професійну лексику для самостійної роботи над текстами, але допускає окремі неточності, вміє пояснити основні положення виконаних завдань і дати правильні відповіді у ході опитування. Помилки у відповідях не є системними. Студент знає основні положення матеріалу, що мають визначальне значення при виконанні індивідуальних / контрольних завдань та поясненні представлених думок в межах дисципліни, що вивчається.	**Достатній** На достатньому рівні забезпечує вимоги до знань, умінь і навичок вивченим матеріалом робочої програми дисципліни. Додаткові питання про можливість використання теоретичних положень для практичного використання викликають утруднення.	Добре / Зараховано (C)
64-74	Студент засвоїв більшу частину навичок науково-технічного перекладу та вивчив спеціалізовану лексику, передбачені робочою програмою дисципліни, розуміє постановку стандартних завдань, має уявлення щодо способів їх виконання. У ході виконання завдань допускає значну кількість неточностей і грубих помилок, які усуває з допомогою викладача.	**Середній** Забезпечує помірний рівень відтворення основних положень дисципліни	Задовільно / Зараховано (D)
60-63	Студент володіє певними неґрунтовними знаннями та навичками науково-технічного перекладу, передбаченими в робочій програмі дисципліни, на мінімально допустимому рівні. З використанням основних теоретичних положень студент з труднощами виконує поставлені викладачем завдання. У ході виконання практичних / індивідуальних / контрольних завдань демонструє формальне ставлення, відсутність глибокого розуміння роботи та взаємозв'язків з іншими темами.	**Середній** Забезпечує мінімально допустимий рівень у всіх складових навчальної програми з дисципліни	Задовільно / Зараховано (E)
35-59	Студент може перекласти окремі фрагменти матеріалів науково-технічного характеру, знає окремі терміни. Незважаючи на те, що програму навчальної дисципліни студент виконав, працював він пасивно, його відповіді під час практичних робіт в більшості є неточними, не відображають специфіку науково-технічних текстів. Цілісність розуміння матеріалу з дисципліни та знання фахової лексики у студента відсутні.	**Низький** Не забезпечує практичної реалізації завдань, що формуються при вивченні дисципліни	Незадовільно з можливістю повторного складання) / Не зараховано (FX) *В залікову книжку не проставляється*
1-34	Студент повністю не виконав вимог робочої програми навчальної дисципліни. Його знання на підсумкових етапах навчання є фрагментарними. Студент не допущений до здачі заліку, іспиту.	**Незадовільний** Студент не підготовлений до самостійного вирішення завдань, які встановляє програма дисципліни	Незадовільно з обов'язковим повторним вивченням / Не допущений (F) *В залікову книжку не проставляється*