СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«УПРАВЛІННЯ БЕЗПЕКОЮ ІНФОРМАЦІЇ ТА ІНФРАСТРУКТУРИ»

Лектор курсу			**Мужанова Тетяна Михайлівна**, кандидат наук з держ.упр., доцент кафедри управління інформаційною та кібербезпекою		**Контактна інформація лектора (e-mail), сторінка курсу в Moodle**	**e-mail:**muzanovat@gmail.com; **сторінка курсу в Moodle –** http://dl.dut.edu.ua/course/view.php?id=1742	
Галузь знань			12 Інформаційні технології		**Рівень вищої освіти**	бакалавр	
Спеціальність			125 Кібербезпека		**Семестр**	8	
Освітня програма			Управління інформаційною та кібернетичною безпекою		**Тип дисципліни**	Вибіркова	
Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінарських занять	Практичних занять	Лабораторних занять	Самостійна підготовка
	5	150	-	-	40	-	110

АНОТАЦІЯ КУРСУ

Мета курсу:	набуття студентами компетенцій, знань, умінь і навичок щодо використання іноземної мови у сфері управління інформаційною безпекою з метою подальшого використання зазначених знань та навиків у подальшій практичній діяльності

Компетентності відповідно до освітньої програми

Soft- skills / Загальні компетентності (ЗК)	**Hard-skills / Спеціальні компетентності (СК)**
ЗК 1. Здатність застосовувати знання у практичних ситуаціях **ЗК 2.** Знання та розуміння предметної області та розуміння професії. **ЗК 3.** Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. **ЗК 4.** Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.	**ПП 5.** Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики безпеки. **ПП 8.** Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку **ПП 12.** Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам .

Програмні результати навчання (ПРН)

ПРН 5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.
ПРН 12. Розробляти моделі загроз та порушника.
ПРН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку якості прийнятих рішень.
ПРН 19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.
ПРН 22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і кібербезпеки.
ПРН 27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.
ПРН 29. Виконувати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та

ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів.
ПРН 36. Виявляти небезпечні сигнали технічних засобів.
ПРН 44. Застосовувати різні класи політик інформаційної безпеки та кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів.
ПРН 46. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.
ПРН 51. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.
ПРН 52. Вирішувати задачі аналізу програмного коду на наявність можливих вразливостей.

ОРГАНІЗАЦІЯ НАВЧАННЯ			
Тема, опис теми	**Вид заняття**	**Оцінювання за тему**	**Форми і методи навчання/питання до самостійної роботи**
Розділ 1 «БЕЗПЕКА ОПЕРАЦІЙ ТА КОМУНІКАЦІЙ»			
Тема 1. ***Управління функціонуванням інформаційних систем*** ***Знати***: базову професійно-орієнтовану лексику за темою. ***Вміти:*** 1.читати спеціалізовані тексти нормативного характеру за темою; 2.спілкуватися на зазначену тему; 3.писати повідомлення, документи, пов'язані з професією; 4.сприймати на слух і розуміти спеціалізовану інформацію за фахом. ***Формування компетенцій:*** ЗК1, ЗК2, ЗК3, ЗК5, ПП5, ПП8, ПП12 ***Результати навчання:*** ПРН5, ПРН12, ПРН14, ПРН19, ПРН22, ПРН27, ПРН29, ПРН36, ПРН44, ПРН46, ПРН51,ПРН52 ***Рекомендовані джерела:*** 1-6, 8, 9, 10.	Практичне заняття 1 Практичне заняття 2 Практичне заняття 3 Практичне заняття 4	5,5*	Читання і переклад зі словником спеціалізованих текстів нормативного характеру за темою Вивчення спеціалізованої лексики за темою, ведення словника, перевірка знання термінології Розповідь, ведення дискусії на зазначену тему Підготовка повідомлень, ессе з теми Прослуховування спеціалізованих текстів за фахом, обговорення змісту почутого, вивчення лексики Опитування за результатами вивчення теми
Тема 2***. Управління комунікаціями*** ***Знати***: базову професійно-орієнтовану лексику за темою. ***Вміти:*** 1.читати спеціалізовані тексти нормативного характеру за темою; 2.спілкуватися на зазначену тему; 3.писати повідомлення, документи, пов'язані з професією; 4.сприймати на слух і розуміти спеціалізовану інформацію за фахом. ***Формування компетенцій:*** ЗК1, ЗК2, ЗК3, ЗК5, ПП5, ПП8, ПП12 ***Результати навчання:*** ПРН5, ПРН12, ПРН14, ПРН19, ПРН22, ПРН27, ПРН29, ПРН36, ПРН44, ПРН46, ПРН51,ПРН52 ***Рекомендовані джерела:*** 1-6, 8, 9, 10.	Практичне заняття 5 Практичне заняття 6 Практичне заняття 7 Практичне заняття 8	5,5*	Читання і переклад зі словником спеціалізованих текстів нормативного характеру за темою Вивчення спеціалізованої лексики за темою, ведення словника Індивідуальні розповіді, ведення дискусії на зазначену тему Прослуховування спеціалізованих текстів за фахом, обговорення змісту почутого, вивчення лексики Опитування за результатами вивчення теми

Тема 3. ***Управління інцидентами інформаційної безпеки*** ***Знати***: базову професійно-орієнтовану лексику за темою. ***Вміти:*** 1.читати спеціалізовані тексти нормативного характеру за темою; 2.спілкуватися на зазначену тему; 3.писати повідомлення, документи, пов'язані з професією; 4.сприймати на слух і розуміти спеціалізовану інформацію за фахом. ***Формування компетенцій:*** ЗК1, ЗК2, ЗК3, ЗК5, ПП5, ПП8, ПП12 ***Результати навчання:*** ПРН5, ПРН12, ПРН14, ПРН19, ПРН22, ПРН27, ПРН29, ПРН36, ПРН44, ПРН46, ПРН51,ПРН52 ***Рекомендовані джерела:*** 1-6, 8, 9.	Практичне заняття 9 Практичне заняття 10 Практичне заняття 11 Практичне заняття 12	5,5*	Читання і переклад зі словником спеціалізованих текстів нормативного характеру за темою Вивчення спеціалізованої лексики за темою, ведення словника, перевірка знання термінології Індивідуальні розповіді, ведення дискусії на зазначену тему Підготовка повідомлень про різні підходи до управління інцидентами ІБ Проведення презентацій про різні підходи до управління інцидентами ІБ Опитування за результатами вивчення теми Проведення модульного контролю № 1 «БЕЗПЕКА ОПЕРАЦІЙ ТА КОМУНІКАЦІЙ»
Тема 1. Засоби захисту від шкідливого коду. **Тема 2.** Процедури резервного копіювання. **Тема 3**. Управління технічними вразливостями систем. **Тема 4**. Моніторинг та відстеження подій в системах. **Тема 5**. Реагування на інциденти інформаційної безпеки.	Самостійна робота		1. Роль антивірусів у захисті від шкідливого ПЗ. 2. ПЗ для відновлення даних та систем після впливу шкідливих програм. 3. Обсяги й частота резервного копіювання даних. 4. Засади управління технічними вразливостями 5. Використання оновлень для ПЗ: переваги і загрози. 6. Засади моніторингу подій у системах та мережах. 7. Вимоги до безпечного передавання електронних повідомлень. 8. Звітування про інциденти ІБ. 9. Схема реагування на інциденти інформаційної безпеки NIST.
Розділ 2 «КОНТРОЛЬ ДОСТУПУ ДО ЗАСОБІВ ОБРОБКИ ІНФОРМАЦІЇ»			
Тема 4. ***Контроль доступу*** ***Знати***: базову професійно-орієнтовану лексику за темою. ***Вміти:*** 1.читати спеціалізовані тексти нормативного характеру за темою; 2.спілкуватися на зазначену тему; 3.писати повідомлення, документи, пов'язані з професією; 4.сприймати на слух і розуміти спеціалізовану інформацію за фахом. ***Формування компетенцій:*** ЗК1, ЗК2, ЗК3, ЗК5, ПП5, ПП8, ПП12 ***Результати навчання:*** ПРН5, ПРН12, ПРН14, ПРН19, ПРН22, ПРН27, ПРН29, ПРН36, ПРН44, ПРН46, ПРН51,ПРН52 ***Рекомендовані джерела:*** 1-6, 8, 9.	Практичне заняття 13 Практичне заняття 14 Практичне заняття 15 Практичне заняття 16	5,5*	Читання і переклад зі словником спеціалізованих текстів нормативного характеру за темою Вивчення спеціалізованої лексики за темою, ведення словника Індивідуальні розповіді, ведення дискусії на зазначену тему Прослуховування спеціалізованих текстів за фахом, обговорення змісту почутого, вивчення лексики Опитування за результатами вивчення теми

Тема 5. ***Фізична безпека та безпека інфраструктури*** ***Знати***: базову професійно-орієнтовану лексику за темою. ***Вміти:*** 1.читати спеціалізовані тексти нормативного характеру за темою; 2.спілкуватися на зазначену тему; 3.писати повідомлення, документи, пов'язані з професією; 4.сприймати на слух і розуміти спеціалізовану інформацію за фахом. ***Формування компетенцій:*** ЗК1, ЗК2, ЗК3, ЗК5, ПП5, ПП8, ПП12 ***Результати навчання:*** ПРН5, ПРН12, ПРН14, ПРН19, ПРН22, ПРН27, ПРН29, ПРН36, ПРН44, ПРН46, ПРН51,ПРН52 ***Рекомендовані джерела:*** 1-6, 8, 9, 11.	Практичне заняття 17 Практичне заняття 18 Практичне заняття 19 Практичне заняття 20	5,5*	Читання і переклад зі словником спеціалізованих текстів нормативного характеру за темою Вивчення спеціалізованої лексики за темою, ведення словника, перевірка знання термінології Індивідуальні розповіді, ведення дискусії на зазначену тему Підготовка анотацій статей з Інтернет-ресурсів про актуальні проблеми фізичній безпеці інфраструктури Представлення анотацій, відповіді на запитання Опитування за результатами вивчення теми Проведення модульного контролю № 2 «КОНТРОЛЬ ДОСТУПУ ДО ЗАСОБІВ ОБРОБКИ ІНФОРМАЦІЇ»
Тема 6. Технічні засоби захисту зон фізичної безпеки організації. **Тема 7**. Управління доступом до інформаційно-комунікаційних систем. **Тема 8.** Придбання, розробка та підтримка систем обробки й передачі інформації. **Тема 9.** Дотримання відповідності нормативно-правовим вимогам інформаційної безпеки.	Самостійна робота		1. Технічні засоби захисту різних зон безпеки периметру та входу. 2. Технічні засоби безпеки приміщень та місць розташування засобів обробки інформації. 2. Методи захисту обладнання організації. 3. Політика «чистого» столу та «чистого» екрана. 4. Управління доступом користувачів ІКС. 5. Контроль доступу до систем і додатків. 6. Дотримання вимог безпеки у процесі придбання та розробки програмного й апаратного забезпечення. 7. Безпечний технічний супровід систем обробки й передачі інформації. 8. Виконання норм законодавства і контрактних умов у процесі управління ІБ.

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

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

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

1. Pauline Bowen, Joan Hash, Mark Wilson. Information Security Handbook: A Guide for Managers, NIST, 178 p. http://www.dut.edu.ua/uploads/l_1889_44919882.pdf
2. Tony Campbell, Burns Beach. Practical Information Security Management: A Complete Guide to Planning and Implementation. Apress. 237 p. http://www.dut.edu.ua/uploads/l_1888_50813661.pdf
3. Cybersecurity Fundamentals Study Guide, 2nd Edition. ISACA. 194 p. https://www.studocu.com/nl-be/document/odisee-hogeschool/cybersecurity-fundamentels/college-aantekeningen/cybersecurity-fundamentals-with-notes/7343872/view
4. Cyber-Security Standards, Benchmarking & Best Practices Overview. SAINT Consortium, 2018. 155 p. 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. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
7. ISO/IEC 27000:2018(E) Information technology - Security techniques - Information security management systems - Overview and vocabulary. 27 p.
8. ISO/IEC 27001:2013(E) Information technology - Security techniques - Information security management systems – Requirements. 34 p.
9. ISO/IEC 27002:2013 Information technology - Security techniques - Code of practice for information security controls. 80 p.
10. ISO/IEC 27005:2008 Information technology - Security techniques - Information security risk management. 55 p.
11. Vitalii Savchenko, Halyna Haidur, Sergii Gakhov, Svitlana Lehominova, Tetiana Muzhanova, Iryna Novikova. Model of Control in a UAV Group for Hidden Transmitters Detection on the Basis of Local Self-Organization : International Journal of Advanced Trends in Computer Science and Engineering. Volume-9 Issue-4. July-August 2020. P 6167-6174. http://www.warse.org/IJATCSE/static/pdf/file/ijatcse291942020.pdf
12. Мужанова Т.М. Організаційне забезпечення інформаційної безпеки підприємства: основні засади. Сучасний захист інформації. 2016. № 2. С.78-82. http://www.dut.edu.ua/uploads/p_1739_99516793.pdf

ПОЛІТИКА КУРСУ («ПРАВИЛА ГРИ»)

- Курс передбачає роботу індивідуально і в групах.
- Середовище в аудиторії є інтерактивним, творчим, відкритим до дискусії.
- Освоєння дисципліни передбачає обов'язкове відвідування практичних занять, а також самостійну роботу.
- Самостійна робота включає в себе теоретичне вивчення питань, що стосуються тем, які не ввійшли в теоретичний курс, або були розглянуті коротко, їх поглиблене опрацювання на основі рекомендованої літератури.
- Усі завдання, передбачені програмою, мають бути виконані у встановлений термін.
- Якщо студент відсутній з поважної причини, він презентує 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. 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 фахової термінології	за кожну правильну відповідь 0,25 бала
	• доповідь з презентацією за темою, в тому числі вивченою самостійно (оцінка залежить від повноти розкриття теми, якості інформації, самостійності та креативності матеріалу, якості презентації і доповіді),	за кожну презентацію (реферат) максимум 3 бали
	• підготовка повідомлення, тез, ессе, анотації тощо	за кожну правильну відповідь 2 бали
	• участь у дискусії, обговоренні положень нормативних актів, статей, відеоматеріалів	за кожну участь 1 бал
РУБІЖНЕ	Модульний контроль № 1 «БЕЗПЕКА ОПЕРАЦІЙ ТА КОМУНІКАЦІЙ»	максимальна оцінка – 15 балів

ОЦІНЮВАННЯ (МОДУЛЬНИЙ КОНТРОЛЬ)	Модульний контроль № 2 «КОНТРОЛЬ ДОСТУПУ ДО ЗАСОБІВ ОБРОБКИ ІНФОРМАЦІЇ»	максимальна оцінка – 15 балів
Додаткова оцінка	Участь у наукових конференціях, підготовка наукових публікацій, участь у Всеукраїнських та Міжнародних конкурсах наукових студентських робіт за спеціальністю, створення кейсів тощо.	Звільняється від заліку
ПІДСУМКОВЕ ОЦІНЮВАННЯ ***Залік***	Метою заліку є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання професійних обов'язків. Залік проходить 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 спілкування з використанням спеціалізованої лексики, здатність вести діалог і дискусію на професійну тематику, повне сприйняття змісту прослуханих спеціалізованих текстів за фахом. За час навчання при проведенні практичних занять та виконанні індивідуальних / контрольних завдань студент проявляє вміння самостійно вирішувати поставлені завдання, 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 теоретичних положень.	**Високий** Повністю забезпечує вимоги до знань, умінь і навичок, що викладені в робочій програмі дисципліни. Власні пропозиції студента щодо виконання завдань підвищують його вміння використання знань, отриманих при вивчені інших дисциплін, а також знань, набутих при самостійному поглибленому вивченні питань, що відносяться до дисципліни, яка вивчається.	Відмінно / Зараховано (А)
82-89	Студент демонструє гарні знання змісту та професійної термінології, добре володіє матеріалом, що відповідає робочій програмі дисципліни, вміє застосовувати набуті знання та використовувати 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 вирішувати поставлені завдання, долучатися до обговорення фахових питань іноземною мовою із незначними прогалинами у володінні практичними навичками.	**Достатній** Забезпечує студенту самостійне виконання основних завдань за умов, коли вихідні дані в них змінюються порівняно з наданими у матеріалах дисципліни	Добре / Зараховано (В)
75-81	Студент загалом добре володіє матеріалом та професійною термінологією, знає основні теоретичні положення 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 та 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** Конкретний рівень, за вивченим матеріалом робочої програми дисципліни. Додаткові питання про можливість використання теоретичних положень для практичного використання викликають утруднення.	Добре / Зараховано (С)
4 - 7	Студент засвоїв більшу частину теоретичного матеріалу та спеціалізованої лексики,	**Середній**	Задовільно /

	передбачених 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 може усунути з допомогою викладача. .	Забезпечує достатньо надійний рівень відтворення основних положень дисципліни	Зараховано (D)
60-63	Студент володіє певними неґрунтовними знаннями, 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** Є мінімально допустимим у всіх складових навчальної програми з дисципліни	Задовільно / Зараховано (E)
35-59	Студент може відтворити окремі фрагменти матеріалів курсу й окремі терміни. Незважаючи на те, що програму навчальної дисципліни студент виконав, працював він пасивно, його відповіді під час практичних робіт в більшості є невірними, необґрунтованими. 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.	**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*