



Силабус курсу УПРАВЛІННЯ ІНФОРМАЦІЙНО БЕЗПЕКОЮ

Ступінь вищої освіти – бакалавр

Галузь знань – 12 Інформаційні технології

Спеціальність - 125 Кібербезпека та захист інформації

Освітньо-професійна програма – «Кібербезпека»

Рік навчання: 3

Семестр: 6

Кількість кредитів: 5

Мова викладання: українська

Керівник курсу

ППП

Аліна ДАВЛЕТОВА

Контактна інформація

a.davletova@wunu.edu.ua

Опис дисципліни

Курс «Управління інформаційною безпекою» орієнтований на формування компетентностей та умінь щодо основних підходів захисту інформації, концептуальної моделі інформаційної безпеки, розроблення, впровадження та експлуатації систем управління інформації на об'єктах інформаційної діяльності, формування навичок аналізу систем забезпечення інформаційної безпеки з метою впровадження найкращих практик захисту інформації. Вивчення курсу вимагає цілеспрямованої роботи над вивченням спеціальної літератури, активної роботи на лекціях та практичних заняттях, самостійної роботи та виконання індивідуальних завдань. Метою курсу є формування комплексу знань щодо підходів до визначення джерел загроз та об'єктів захисту, методів та механізмів захисту інформаційних ресурсів, нормативно-методичної бази в галузі захисту інформації, набуття теоретичних знань та практичних навичок щодо управління інформаційною безпекою в інформаційно-телекомунікаційних (автоматизованих) системах для реалізації встановленої політики безпеки..

Структура курсу

Години лек/пр	Тема	Результати навчання	Завдання
2/2	Інформаційні ресурси, що підлягають захисту	Визначати інформаційні ресурси, що потребують захисту, і класифікувати їх за типами.	Поточне опитування
2/2	Загрози безпеці інформації	Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно телекомунікаційних (автоматизованих) системах.	Поточне опитування
2/2	Характеристики захищеності інформаційних ресурсів.	Вирішувати задачі захисту потоків даних в інформаційних, інформаційно телекомунікаційних (автоматизованих) системах.	Поточне опитування
2/2	Політика інформаційної безпеки	Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно телекомунікаційних системах згідно встановленої політики	Поточне опитування

		інформаційної та/або кібербезпеки.	
2/2	Соціотехнічна безпека	Виявляти, аналізувати та класифікувати загрози соціотехнічного характеру, застосовувати методи протидії соціальному інжинірингу та захисту інформаційних ресурсів від соціотехнічних атак. Організовувати моніторинг соціальних мереж і реалізовувати стратегії управління персоналом та інформаційною безпекою з урахуванням соціального фактору.	Поточне опитування
2/2	Національна безпека	Аналізувати категорії, принципи та фактори забезпечення національної безпеки, оцінювати її характеристики та застосовувати засоби захисту в контексті інформаційної та кібербезпеки.	Поточне опитування
2/2	Кіберзлочинність	Ідентифікувати та класифікувати види кіберзлочинів, аналізувати їх вплив на національні інтереси в інформаційній сфері та оцінювати державні механізми протидії в контексті захисту національних інтересів України.	Поточне опитування
2/2	Інформаційне протиборство. Інформаційна війна.	Розуміти концепцію та форми інформаційної війни на державному рівні, ідентифікувати засоби інформаційної зброї та оцінювати стратегії захисту інформаційних систем.	Поточне опитування
2/2	Аналіз ризиків	Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем	Поточне опитування
2/2	Управління ризиками інформаційної безпеки.	Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).	Поточне опитування
2/2	Аналіз інцидентів інформаційної безпеки	Застосовувати методи аналізу та оцінки ризиків, документувати результати і формувати реєстр ризиків для забезпечення інформаційної безпеки.	Поточне опитування
2/2	Реагування на інциденти інформаційної безпеки	Здійснювати ідентифікацію інцидентів інформаційної безпеки, планувати та реалізовувати процес реагування.	Поточне опитування
2/2	Стимування та пом'якшення наслідків інцидентів	Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність.	Поточне опитування
2/2	Розслідування інцидентів	Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/або кібербезпеки для розслідування інцидентів.	Поточне опитування
2/2	Система управління інформаційною безпекою	Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.	

Літературні джерела

1. Опорний конспект лекцій з дисципліни “Управління інформаційною безпекою” для здобувачів освітньо-професійної програми підготовки бакалавра галузі знань 12 Інформаційні спеціальності 125 «Кібербезпека» / Укл.: Давлетова А.Я., Драпак В.І., Возняк С.І. – Тернопіль 2022. – 76с.
2. Яцків В.В., Івасьєв С.В., Давлетова А.Я., Тимошенко Л.М. Методологія впровадження системи управління інформаційною безпекою на основі багаторівневої моделі кіберзахисту згідно з вимогами законодавства України.- Інформатика та математичні методи в моделюванні Том 15, № 1, 2025, 137-149.
3. Шумейко О.О. Інформаційна безпека. Дніпровський державний технічний університет, 2019. - 155 с.
4. Лісовська Ю. Кібербезпека. Ризики та заходи. - К.: Кондор, 2019. - 272 с.
5. Мужанова Т.М. Інформаційна безпека держави. Київ: Державний університет телекомунікацій, 2019. - 131 с.
6. Bender David. Bender on Privacy and Data Protection. LexisNexis, 2020. - 2940 p.
7. Schreider Tari. Building an Effective Security Program. 2nd Edition. - Rothstein Associates Inc., 2020. - 406 p.
8. Alassouli Hidaia. Common Windows, Linux and Web Server Systems Hacking Techniques. Independently published, 2021. - 181 p.
9. Barnum Todd. The Cybersecurity Manager's Guide: The Art of Building Your Security Program. O'Reilly Media, Inc., 2021. - 168 p.
10. Daimi K., Peoples C. Advances in Cybersecurity Management. Springer, 2021.- 497 p.
11. Alexandrou Alex. Cybercrime and Information Technology: The Computer Network Infrastructure and Computer Security, Cybersecurity Laws, Internet of Things (IoT), and Mobile Devices. CRC Press, 2022. - 455 p.
12. Goyal D., Balamurugan S., Senthilnathan K., Annapoorani I., Israr M. (Eds.) Cyber-Physical Systems and Industry 4.0: Practical Applications and Security Management. Apple Academic Press Inc., CRC Press, 2022. - 290 p.

Політика оцінювання

Політика щодо дедлайнів та перескладання: Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку (-10 балів). Перескладання модулів відбувається із дозволу деканату за наявності поважних причин (наприклад, лікарняний).

Політика щодо академічної доброчесності: Здобувач освіти зобов’язаний виконувати усі роботи та завдання самостійно. Під час контрольного заходу він може користуватися лише дозволеними допоміжними матеріалами або засобами; йому забороняється в будь-якій формі обмінюватися інформацією з іншими здобувачами, а також використовувати, розповсюджувати або збирати варіанти чужих робіт чи контрольних завдань.

Політика щодо відвідування: Відвідування занять є обов’язковим компонентом оцінювання. За об’єктивних причин (наприклад, хвороба, карантин, воєнний стан, міжнародне стажування) навчання може відбуватись в дистанційній формі за погодженням із керівником курсу та з дозволу дирекції факультету.

Оцінювання

Модуль 1		Модуль 2		Модуль 3	Модуль 4	Модуль 5
10%	10%	10%	10%	5%	15%	40%
Поточне оцінювання	Модульний контроль 1	Поточне оцінювання	Модульний контроль 2	Тренінги	Самостійна робота	Екзамен
Середнє арифметичне оцінок, отриманих	Середнє арифметичне за виконання та захист	Середнє арифметичне оцінок, отриманих	Середнє арифметичне за виконання	Середнє арифметичне з оцінок за виконання	Середнє арифметичне за виконання	Теоретичні питання: 2 питання по 30

за поточне опитування та підсумкове модульне тестування за темами №1-7.	лабораторних робіт №1-7.	за поточне опитування та підсумкове модульне тестування за темами №8-14.	та за захист лабораторних робіт №8-14.	та презентацію одного завдання тренінгу.	та презентацію одного завдання самостійної роботи.	балів - мах 60 балів. Практичне завдання - мах 40 балів
---	--------------------------	--	--	--	--	---

Шкала оцінювання:

За шкалою
університету

За національною
шкалою

За шкалою ECTS

90–100

відмінно

A (відмінно)

85–89

добре

B (дуже добре)

75–84

C (добре)

65–74

задовільно

D (задовільно)

60–64

E (достатньо)

35–59

незадовільно

FX (незадовільно з можливістю повторного складання)

1–34

F (незадовільно з обов'язковим повторним курсом)

Виконання лабораторних робіт:

90–100 балів – робота виконана самостійно, без помилок, усі етапи задокументовано, правильне використання інструментів.

75–89 балів – виконання із незначними помилками, що не вплинули на результат; часткова потреба в підказках.

60–74 бали – виконання із суттєвими помилками; поверхнєве розуміння завдань.

1–59 балів – робота не виконана або результат неправильний; відсутність навичок.

Поточне опитування:

90–100 балів – повне володіння матеріалом, аргументовані й логічні відповіді, глибоке розкриття змісту.

75–89 балів – загалом повне володіння матеріалом, але окремі відповіді поверхнєві або з незначними неточностями.

65–74 бали – знання основного змісту без достатньої глибини та аргументації, суттєві неточності.

60–64 бали – фрагментарне володіння матеріалом, недостатнє розкриття питань.

1–59 балів – відсутність знань, нездатність розкрити зміст теоретичних питань.

Тренінг, самостійна робота:

90–100 балів – повне володіння матеріалом, аргументоване застосування знань, правильне виконання завдань, наявність елементів власного дослідження, творчий підхід.

75–89 балів – здебільшого правильне виконання, незначні помилки, достатньо аргументоване використання матеріалу, частково присутні елементи власного дослідження.

65–74 бали – розв'язання завдань з помилками, недостатня аргументація, поверхнєве опрацювання теми, обмежена самостійність.

60–64 бали – часткове або фрагментарне виконання завдань, відсутність повного обґрунтування, мінімальний авторський внесок.

1–59 балів – завдання практично не виконано, повністю неправильне розв'язання, відсутність дослідницького або творчого підходу.

Підсумкове модульне тестування:

90–100 балів – правильно виконано 90–100% завдань тесту.

75–89 балів – правильно виконано 75–89% завдань тесту.

60–74 бали – правильно виконано 60–74% завдань тесту.

1–59 балів – правильно виконано менше 60% завдань тесту.

Екзамен – підсумковий контроль, який проводиться з метою оцінювання засвоєння здобувачем вищої освіти теоретичного та практичного матеріалу. Екзаменаційне завдання складається з двох блоків:

Відповіді на теоретичні питання (максимум 60 балів):

25–30 балів – повне володіння матеріалом, аргументована та всебічна відповідь, демонстрація глибокого розуміння;

15–24 бали – достатнє володіння матеріалом, відповідь здебільшого правильна, допускаються незначні неточності;

0–14 балів – фрагментарне або неправильне викладення матеріалу, суттєві недоліки в аргументації.

Практичне завдання (тестове, максимум 40 балів):

30–40 балів – всі завдання виконані правильно, повне розуміння практичного матеріалу;

15–29 балів – завдання виконані частково правильно, допускаються незначні або суттєві помилки;

0–14 балів – завдання виконано неправильно або не виконано взагалі.