**Силабус курсу**

# УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

**Ступінь вищої освіти –** бакалавр
**Галузь знань –** 15 Автоматизація та приладобудування
**Спеціальність** - 152 Метрологія та інформаційно-вимірювальна техніка
**Освітньо-професійна програма –** «Технології інтернету речей»
**Рік навчання:** 4
**Семестр**: 8
**Кількість кредитів:** 5
**Мова викладання:** українська

## Керівник курсу


| | |
|---|---|
| **ПІП** | 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 | Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації | Поточне опитування |

| | | | |
|---|---|---|---|
| | безпеки | процесів і користувачів в інформаційно телекомунікаційних системах згідно встановленої політики інформаційної і\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 | Стримування 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 | Поточне опитування |

| | | | |
|---|---|---|---|
| | | інцидентів. | |
| 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.

## Політика щодо визнання результатів навчання

Відповідно до «Положення про визнання в Західноукраїнському національному університеті результатів попереднього навчання» (https://www.wunu.edu.ua/pdf/pologenya/Polozhennya_ruzult_poper_navch.pdf) здобувачам вищої освіти може бути зараховано результати навчання (неформальної/інформальної освіти, академічної мобільності тощо) на підставі підтвердних документів (сертифікати, довідки, документи про підвищення кваліфікації тощо). Рішення про зарахування здобувачу результатів (певного освітнього компонента в цілому, або ж окремого виду навчальної роботи за таким освітнім компонентом) приймається уповноваженою Комісією з визнання результатів навчання за процедурою, визначеною вищезазначеним положенням.

## Оцінювання

| Модуль 1 | | Модуль 2 | | Модуль 3 | Модуль 4 |
|---|---|---|---|---|---|
| 20% | 20% | 20% | 20% | 5% | 15% |
| Поточне оцінювання | Модульний контроль 1 | Поточне оцінювання | Модульний контроль 2 | Тренінги | Самостійна робота |
| Середнє арифметичне оцінок, отриманих за поточне опитування та підсумкове модульне тестування за темами №1-7. | Середнє арифметичне за виконання та захист лабораторних робіт №1-7. | Середнє арифметичне оцінок, отриманих за поточне опитування та підсумкове модульне тестування за темами №8-14. | Середнє арифметичне за виконання та за захист лабораторних робіт №8-14. | Середнє арифметичне з оцінок за виконання та презентацію одного завдання тренінгу. | Середнє арифметичне за виконання та презентацію одного завдання самостійної роботи. |

**Шкала оцінювання:**

| За шкалою університуту | 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) |