ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«УЖГОРОДСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ»
ФАКУЛЬТЕТ СУСПІЛЬНИХ НАУК
КАФЕДРА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ СИСТЕМ

«ЗАТВЕРДЖУЮ»
Проректор з наукової роботи
_____ / Іван МИРОНЮК/
«___» _____ 2024 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«ТЕХНОЛОГІЇ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ» / «SOFTWARE OF INFORMATION SECURITY TECHNOLOGIES»

Рівень вищої освіти	**Третій (освітньо-науковий)**
Галузь знань	**12 Інформаційні технології**
Спеціальність	**121 Інженерія програмного забезпечення**
Освітня програма	**Інженерія програмного забезпечення**
Статус дисципліни	**Обов'язкова**
Мова навчання	**Українська**

Ужгород 2024

Робоча програма навчальної дисципліни «Технології програмного забезпечення інформаційної безпеки»/«Software of Information Security Technologies») розроблена для здобувачів третього рівня вищої освіти галузі знань 12 Інформаційні технології, спеціальності 121 Інженерія програмного забезпечення, освітньо-наукової програми «Інженерія програмного забезпечення».

Розробник: Поліщук В.В., д.т.н., проф., професор кафедри програмного забезпечення систем

Робочу програму розглянуто та затверджено на засіданні кафедри програмного забезпечення систем
протокол №12 від «31» січня 2024 р.
Завідувач кафедри _____ Юрій БІЛАК

Схвалено науково-методичною комісією факультету інформаційних технологій
протокол №8 від «20» лютого 2024 р.
Т.в.о. голови науково-методичної комісії _____ Ігор ПОВХАН

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

<table>
<tr><td rowspan="2">Найменування показників</td><td colspan="2">Розподіл годин за навчальним планом</td></tr>
<tr><td>Денна форма навчання</td><td>Заочна форма навчання</td></tr>
<tr><td>Кількість кредитів ЄКТС – 3</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td>Загальна кількість годин – 90</td><td>1</td><td>1</td></tr>
<tr><td>Кількість модулів – 2</td><td colspan="2">Семестр:</td></tr>
<tr><td rowspan="5">Тижневих годин:
для денної форми навчання:
аудиторних – 2,77
самостійної роботи здобувача – 3</td><td>2</td><td>2</td></tr>
<tr><td colspan="2">Лекції:</td></tr>
<tr><td>22</td><td>8</td></tr>
<tr><td colspan="2">Практичні (семінарські):</td></tr>
<tr><td>14</td><td>2</td></tr>
<tr><td rowspan="2">Вид підсумкового контролю:
екзамен</td><td colspan="2">Лабораторні:</td></tr>
<tr><td>0</td><td>0</td></tr>
<tr><td rowspan="2">Форма підсумкового контролю:
письмова або тестова</td><td colspan="2">Самостійна робота:</td></tr>
<tr><td>54</td><td>80</td></tr>
</table>

2. МЕТА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Навчальна дисципліна спрямована на поглиблене вивчення моделей, методів, процесів та програмних засобів забезпечення інформаційної безпеки на всіх етапах життєвого циклу програмного забезпечення. Особлива увага приділяється інженерії безпечного програмного забезпечення, аналізу активів, загроз, вразливостей та інцидентів, розробленню програмних систем підтримки прийняття рішень, а також оцінюванню ризиків і керованості складних інформаційних систем в умовах невизначеності.

У результаті вивчення дисципліни аспіранти повинні знати та вміти:

• застосовувати принципи безпечного життєвого циклу програмного забезпечення та Secure-by-Design;

• формалізувати активи, загрози, вразливості, наслідки та інциденти інформаційної безпеки;

• проєктувати архітектуру програмних засобів захисту, моніторингу й підтримки прийняття рішень;

• використовувати експертні, нечіткі та багатокритеріальні моделі оцінювання ризиків;

• розробляти програмні технології оцінювання керованості та безпечного стану складних систем;

• реалізовувати, тестувати, верифікувати та візуалізувати результати роботи програмних моделей;

• документувати результати, дотримуватися вимог академічної доброчесності, ліцензування та захисту інтелектуальної власності.

Практична складова дисципліни базується на створенні двох програмних прототипів: експертної моделі оцінювання ризиків та інцидентів безпеки мережевих й інформаційних систем об’єктів критичної інфраструктури та програмної технології оцінювання керованості систем у різних режимах функціонування для забезпечення інформаційної безпеки. Під час розроблення програмних прототипів здобувачі повинні передбачити валідацію вхідних даних, розмежування доступу, безпечне оброблення помилок, журналювання подій, тестування вразливостей, верифікацію результатів та документування прийнятих проєктних рішень із забезпечення інформаційної безпеки.

Метою вивчення навчальної дисципліни «Технології програмного забезпечення інформаційної безпеки» є формування у здобувачів третього рівня вищої освіти системних теоретичних знань і дослідницько-практичних умінь щодо аналізу, проєктування, реалізації та оцінювання програмних технологій інформаційної безпеки, а також створення нових моделей, методів і програмних засобів підтримки прийняття рішень в умовах ризику та невизначеності.

Дисципліна поєднує інженерні, програмно-технологічні та аналітичні підходи до забезпечення інформаційної безпеки. Програмні технології інформаційної безпеки розглядаються як сукупність моделей, методів, архітектурних рішень, процесів та інструментальних засобів, інтегрованих у життєвий цикл програмного забезпечення — від формування вимог і моделювання загроз до реалізації, тестування, розгортання, моніторингу та реагування на інциденти.

Відповідно до освітньо-наукової програми, вивчення дисципліни сприяє формуванню таких компетентностей:

Інтегральна компетентність (ІК):

Здатність продукувати нові ідеї, розв'язувати комплексні проблеми професійної та/або дослідницько-інноваційної діяльності у сфері інженерії програмного забезпечення та з дотичних до неї міждисциплінарних напрямів, застосовувати методологію наукової та педагогічної діяльності, проводити власне наукове дослідження, результати якого мають наукову новизну, теоретичне та практичне значення.

Загальні компетентності (ЗК):

ЗК01. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

- Спеціальні (фахові, предметні) компетентності (СК):
- СК04. Здатність відстежувати тенденції розвитку інженерії програмного забезпечення та критично переосмислювати наявні технології.
- СК05. Здатність до розроблення нових та вдосконалення існуючих моделей, методів, засобів, процесів у сфері інженерії програмного забезпечення, які забезпечують розвиток або надають нові можливості технологіям розробки та супроводження програмного забезпечення.
- СК12. Здатність аналізувати та забезпечувати інформаційну безпеку програмних продуктів, розуміти основні принципи кібербезпеки та конфіденційності даних, вміти використовувати новітні технології та інструменти.

3. ПЕРЕДУМОВИ ДЛЯ ВИВЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Передумовою вивчення навчальної дисципліни «Технології програмного забезпечення інформаційної безпеки» є здобутий другий рівень вищої освіти (магістр). Бажаними є базові знання з інженерії програмного забезпечення, комп'ютерних мереж, баз даних, алгоритмів, математичного моделювання та основ інформаційної безпеки.

4. ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ

Відповідно до освітньо-наукової програми «Інженерія програмного забезпечення», вивчення навчальної дисципліни повинно забезпечити досягнення здобувачами таких програмних результатів навчання (РН):

Програмні результати навчання	Шифр РН
Мати передові концептуальні та методологічні знання з інженерії програмного забезпечення та дотичних до неї міждисциплінарних напрямів, а також дослідницькі навички, достатні для проведення наукових і прикладних досліджень на рівні останніх світових досягнень з відповідного напряму, отримання нових знань та/або здійснення інновацій.	**РН01**
Пропонувати нові ефективні методи і моделі розроблення, впровадження, супроводу та забезпечення якості програмного забезпечення та управління відповідними процесами на всіх етапах життєвого циклу.	**РН03**
Застосовувати сучасні інструменти і технології пошуку, оброблення та аналізу інформації, зокрема, статистичні методи аналізу даних великого обсягу та/або складної структури, спеціалізовані бази даних та інформаційні системи для покращення ефективності програмних систем.	**РН05**
Забезпечувати захист інтелектуальної власності у сфері інженерії програмного забезпечення.	**РН12**

Очікувані результати навчання, які повинні бути досягнуті здобувачами після опанування навчальної дисципліни «Технології програмного забезпечення інформаційної безпеки»:

Програмні результати навчання	Шифр РН
Пояснювати передові концепції та методології безпечної розробки програмного забезпечення; критично аналізувати сучасні технології інформаційної безпеки, моделі загроз і ризиків; обґрунтовувати вибір методів та інструментів для наукових і прикладних досліджень.	**РН01**
Розробляти й удосконалювати моделі, методи та програмні прототипи оцінювання ризиків, інцидентів, фінансових збитків і керованості складних інформаційних систем; виконувати фазифікацію,	**РН03**

агрегування, дефазифікацію, тестування та верифікацію отриманих результатів.	
Застосовувати сучасні інструменти пошуку, оброблення та аналізу інформації про стан інформаційної безпеки програмних систем, використовувати статистичні методи аналізу даних, спеціалізовані бази даних та інформаційні системи для виявлення закономірностей, оцінювання ризиків і підвищення ефективності засобів захисту програмного забезпечення.	**РН05**
Застосовувати принципи авторського права, ліцензування програмного забезпечення і даних, належного цитування та захисту результатів інтелектуальної діяльності під час розроблення й оприлюднення програмних засобів інформаційної безпеки.	**РН12**

Досягнення СК12 забезпечується через виконання здобувачами завдань із моделювання загроз, формування вимог інформаційної безпеки, проєктування програмних механізмів захисту, оцінювання ризиків та інцидентів, тестування вразливостей, перевірки безпечності програмного коду та верифікації результатів роботи розроблених програмних прототипів.

5. ЗАСОБИ ДІАГНОСТИКИ ТА КРИТЕРІЇ ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Засобами оцінювання та методами демонстрування результатів навчання є: практичні роботи; теоретичні модульні контролі; аналіз вихідного коду; звіти зі структурною схемою, інструкцією користувача, лістингом і скриншотами; презентація та захист результатів; екзамен.

Форми контролю та критерії оцінювання результатів

Форми поточного контролю: виконання, тестування, демонстрація та захист практичних програмних робіт; письмове або тестове виконання теоретичних модульних контрольних робіт.

Форма підсумкового семестрового контролю: екзамен.

Екзамен проводиться у письмовій або тестовій формі та охоплює теоретичний і практичний зміст двох модулів навчальної дисципліни. До складання підсумкового контролю допускаються здобувачі, які виконали, оформили та захистили обидві практичні роботи.

Особливості використання засобів діагностики та контролю за умов дистанційного навчання

В умовах використання формату онлайн-навчання (дистанційного навчання) із застосуванням корпоративної мережі Google Meet названі засоби, методи і форми визначаються за домовленістю зі студентським колективом і, в залежності від зручного виду взаємодії, застосовуються з допомогою існуючих функцій групових чатів та відео-конференцій.

Для ефективного засвоєння тематики є можливість демонстрації необхідних матеріалів на робочому столі комп'ютерного технічного засобу під час занять.

Зокрема, у разі потреби, під час онлайн-заняття можна надати доступ до свого екрану, щоб показати презентації або іншу тематичну інформацію на робочому столі.

Планування лекційних і лабораторних занять, модульних контрольних робіт, а також підсумкова перевірка знань у формі екзамену здійснюється заздалегідь за допомогою прив'язки до гугл-календаря. Синхронізація запланованих заходів виконується автоматично на всіх зручних для їх проведення пристроях.

Розподіл балів, які отримують здобувачі вищої освіти

Змістовий модуль	**Практична робота**	**Теоретичний модульний контроль**	**Максимум за модуль**
Модуль 1 (Т1–Т6)	Практична робота №1 – 30 балів	Модульний контроль №1 – 70 балів	100 балів
Модуль 2 (Т7–Т12)	Практична робота №2 – 30 балів	Модульний контроль №2 – 70 балів	100 балів

Оцінювання окремих видів навчальної роботи з дисципліни

Вид діяльності здобувача вищої освіти		
	Кількість	Максимальна кількість балів (сумарна)
Практичні заняття	**3 заняття по 10**	**30**
Модульна контрольна робота №1	**1**	**70**
Разом		**100**
Практичні заняття	**3 заняття по 10**	**30**
Модульна контрольна робота №2	**1**	**70**
Разом		**100**

Критерії оцінювання підсумкового семестрового контролю.

Оцінювання здійснюється окремо за кожним змістовим модулем за 100-бальною шкалою. Результат модуля 1 формується як сума балів за практичну роботу №1 (30 балів) і теоретичний модульний контроль №1 (70 балів). Результат модуля 2 формується як сума балів за практичну роботу №2 (30 балів) і теоретичний модульний контроль №2 (70 балів). Підсумкова семестрова оцінка та оцінка за екзамен визначаються як середнє арифметичне результатів двох модулів.

- Практична робота (30 балів): коректність програмної реалізації та обчислень – 12 балів; повнота виконання завдання – 6 балів; тестування і верифікація результатів – 4 бали; якість звіту та програмної документації – 4 бали; презентація і захист – 4 бали.
- Теоретичний модульний контроль (70 балів): у письмовій формі – 5 описових питань по 14 балів; у тестовій формі – 20 тестових завдань по 3,5 бала. Максимальна сума за кожний теоретичний модульний контроль становить 70 балів.

Підсумкова оцінка = (Модуль 1 + Модуль 2) / 2.

Підсумкова екзаменаційна оцінка визначається за накопичувальною системою як середнє арифметичне результатів першого і другого змістових модулів.

Переведення даних 100-бальної шкали оцінювання у оцінки за національною шкалою та шкалою ЄКТС

<table>
<tr><th rowspan="2">Сума балів</th><th rowspan="2">Оцінка ЄКТС</th><th colspan="2">Оцінка за національною шкалою</th></tr>
<tr><th>екзамен, диф. залік</th><th>залік</th></tr>
<tr><td>90 -100</td><td>A</td><td>відмінно</td><td rowspan="5">зараховано</td></tr>
<tr><td>82 - 89</td><td>B</td><td rowspan="2">добре</td></tr>
<tr><td>74 - 81</td><td>C</td></tr>
<tr><td>64 - 73</td><td>D</td><td rowspan="2">задовільно</td></tr>
<tr><td>60 - 63</td><td>E</td></tr>
<tr><td>35 - 59</td><td>FX</td><td rowspan="2">незадовільно</td><td rowspan="2">не зараховано</td></tr>
<tr><td>0 - 34</td><td>F</td></tr>
</table>

Відповідно до Положення про порядок та методику проведення семестрових (курсових) екзаменів і заліків в Ужгородському національному університеті, затвердженого наказом ректора ДВНЗ «УжНУ» від 08.05.2015 р. № 698/01-17, знання здобувачів оцінюється як з теоретичної, так і з практичної підготовки за такими критеріями:

оцінку «відмінно» (90-100 балів, А) заслуговує здобувач, який:

всебічно і глибоко володіє навчально-програмовим матеріалом;

вміє самостійно виконувати завдання, передбачені програмою, використовує набуті знання і вміння у нестандартних ситуаціях;

засвоїв основну і ознайомлений з додатковою літературою, яка рекомендована програмою;

при виконанні практичного завдання застосовує системні знання навчального матеріалу, передбачені навчальною програмою.

оцінку «добре» (82-89 балів, В) – заслуговує здобувач, який:

повністю опанував і вільно (самостійно) володіє навчально-програмовим матеріалом, в тому числі застосовує його на практиці, має системні знання в достатньому обсязі відповідно до навчально-програмового матеріалу, аргументовано використовує їх у різних ситуаціях;

має здатність до самостійного пошуку інформації, а також до аналізу, постановки і розв’язування проблем професійного спрямування;

під час відповіді допустив деякі неточності, які самостійно виправив, добирає переконливі аргументи на підтвердження вивченого матеріалу;

оцінку «добре» (74-81 бал, С) − заслуговує здобувач, який:

в цілому навчальну програму засвоїв, але відповідає з певною кількістю помилок;

вміє порівнювати, узагальнювати, систематизувати інформацію під керівництвом викладача, в цілому самостійно застосовувати на практиці, контролювати власну діяльність;

опанував навчально-програмовий матеріал, успішно виконав завдання, передбачені програмою, засвоїв основну літературу, яка рекомендована програмою;

оцінку «задовільно» (64-73 бали, D) – заслуговує здобувач, який:

знає основний навчально-програмовий матеріал в обсязі, необхідному для подальшого навчання і використання його у майбутній професії;

виконує завдання непогано, але зі значною кількістю помилок;

ознайомлений з основною літературою, яка рекомендована програмою;

допускає помилки при виконанні завдань, але під керівництвом викладача знаходить шляхи їх усунення.

оцінку «задовільно» (60-63 бали, E) – заслуговує здобувач, який:

володіє основним навчально-програмовим матеріалом в обсязі, необхідному для подальшого навчання і використання його у майбутній професії, а виконання завдань задовольняє мінімальні критерії. Знання мають репродуктивний характер.

оцінка «незадовільно» (35-59 балів, FX) – виставляється здобувачу, який:

виявив суттєві прогалини в знаннях основного програмового матеріалу, допустив принципові помилки у виконанні передбачених програмою завдань.

оцінка «незадовільно» (35 балів, F) – виставляється здобувачу, який:

володіє навчальним матеріалом тільки на рівні елементарного розпізнавання і відтворення окремих фактів або не володіє зовсім;

допускає грубі помилки при виконанні завдань, передбачених програмою;

не може продовжувати навчання і не готовий до професійної діяльності після закінчення університету без повторного вивчення даної дисципліни.

При виставленні оцінки враховуються результати навчальної роботи студента протягом семестру.

Академічна доброчесність: Політика щодо академічної доброчесності учасників освітнього процесу формується на основі дотримання принципів академічної доброчесності з урахуванням норм Положення про академічну доброчесність в ДВНЗ «Ужгородський національний університет, затвердженого

вченою радою університету від 23.02.2017 р., протокол № 3, https://www.uzhnu.edu.ua/uk/infocentre/get/12223.

Правила перезарахування кредитів у випадку мобільності: Політика щодо перезарахування кредитів ЄКТС у випадку мобільності формується з урахуванням норм Положення про порядок визнання (перезарахування) кредитів ЄКТС для учасників програм академічної мобільності у Державному вищому навчальному закладі «Ужгородський національний університет», затвердженого вченою радою університету від 30.05.2019 р., протокол № 6, https://www.uzhnu.edu.ua/uk/infocentre/get/21266.

Правила визнання результатів навчання, отриманих у неформальній та/або інформальній освіті: Політика щодо визнання результатів навчання, отриманих у неформальній та/або інформальній освіті, формується з урахуванням норм Положення про порядок визнання в Державному вищому навчальному закладі «Ужгородський національний університет» результатів навчання, здобутих протягом неформальної та / або інформальної освіти, затвердженого вченою радою університету від 18.12.2023 р., протокол № 11, https://www.uzhnu.edu.ua/uk/infocentre/get/69166.

6. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

6.1. Зміст навчальної дисципліни

Змістовий модуль 1. Інженерія безпечного програмного забезпечення та базові технології інформаційної безпеки

Тема 1. Сучасні засади програмних технологій інформаційної безпеки. Еволюція програмних засобів захисту інформації. Принципи конфіденційності, цілісності, доступності, автентичності, підзвітності та кіберстійкості. Підходи Secure by Design, Secure by Default і Privacy by Design.

Тема 2. Безпечний життєвий цикл програмного забезпечення та управління програмою безпеки. Інтеграція вимог безпеки в процеси аналізу, проєктування, розроблення, тестування, розгортання, супроводу та виведення програмного продукту з експлуатації. NIST SSDF, OWASP SAMM, політики, ролі, метрики та рівні зрілості процесів.

Тема 3. Моделювання загроз і ризик-орієнтоване проєктування захищених систем. Ідентифікація активів, поверхні атаки, суб'єктів загроз і сценаріїв зловживання. Діаграми потоків даних, межі довіри, STRIDE та інші методи моделювання загроз. Формування і пріоритизація вимог інформаційної безпеки.

Тема 4. Програмні технології ідентифікації, автентифікації та керування доступом. Багатофакторна автентифікація, керування ідентичностями та привілейованим доступом, федерація ідентичностей, OAuth 2.0 та OpenID Connect. Моделі RBAC і ABAC, принцип найменших привілеїв та архітектура Zero Trust.

Тема 5. Криптографічні сервіси та програмне керування ключами, секретами і довірою. Застосування криптографічних примітивів і протоколів у програмних системах. PKI, TLS, цифрові підписи, сертифікати, KMS і HSM. Життєвий цикл ключів і секретів, криптографічна гнучкість та підготовка до постквантової міграції.

Тема 6. Безпечне програмування, захист застосунків та API. Типові класи вразливостей веб-, мобільних і API-орієнтованих систем. Безпечна робота з даними, пам'яттю, сесіями та помилками. OWASP Top 10 і OWASP API Security Top 10, аналіз коду, SAST, DAST, IAST, фаззинг та перевірка вимог безпеки.

Змістовий модуль 2. DevSecOps, захист програмних екосистем та новітні технології інформаційної безпеки

Тема 7. DevSecOps і автоматизація безпеки у конвеєрах CI/CD. Вбудовування контролів безпеки в планування, розроблення, складання, тестування та розгортання. Security gates, policy as code, infrastructure as code, захищені середовища розроблення, керування секретами, автоматичне сканування та безпечне розгортання.

Тема 8. Безпека ланцюга постачання програмного забезпечення та компонентів з відкритим кодом. Керування залежностями і сторонніми компонентами, Software Composition Analysis, оцінювання CVE/CWE та ліцензійних ризиків. SBOM, походження артефактів, цифрове підписування, захист систем складання, відтворювані збірки та рівні довіри SLSA.

Тема 9. Захист хмарно-нативних, контейнерних і розподілених програмних систем. Моделі спільної відповідальності у хмарі. Безпека контейнерів, Kubernetes, мікросервісів і serverless-застосунків. Керування конфігураціями, ідентичностями робочих навантажень, мережевими політиками, ізоляцією, секретами та образами.

Тема 10. Програмні засоби моніторингу, керування вразливостями та реагування на інциденти. Безпекове журналювання, телеметрія та спостережуваність. IDS/IPS, EDR/XDR, SIEM і SOAR, кореляція подій, аналітика ризиків та підтримка прийняття рішень. Виявлення вразливостей, пріоритизація виправлень, координація розкриття і реагування на інциденти.

Тема 11. Інженерія приватності та програмні технології захисту даних. Класифікація і життєвий цикл даних, мінімізація та контроль цільового використання. Шифрування, токенізація, маскування, DLP і керування згодою. Моделювання загроз приватності та технології підвищення конфіденційності (PETs).

Тема 12. Безпека програмних систем зі штучним інтелектом і новітні напрями розвитку. Загрози для даних, моделей, конвеєрів машинного навчання та генеративного ШІ. Prompt injection, отруєння даних, витік інформації, атаки на ланцюг постачання моделей і ризики використання ШІ-асистентів програмування. Безпечний життєвий цикл AI/ML-систем, оцінювання, моніторинг і дослідницькі перспективи.

6.2. Структура навчальної дисципліни

Назви тем	Денна форма				Заочна форма			
	усього	у тому числі			усього	у тому числі		
		л	прак	с.р.		л	прак	с.р.
1	2	3	4	5	6	7	8	9
Тема 1. Сучасні засади програмних технологій інформаційної безпеки.	7	2	0	5	8	1	0	7
Тема 2. Безпечний життєвий цикл програмного забезпечення та управління програмою безпеки.	7	2	0	5	8	1	0	7
Тема 3. Моделювання загроз і ризик-	6	2	0	4	8	1	0	7

Назви тем	Денна форма				Заочна форма			
	усього	у тому числі			усього	у тому числі		
		л	прак	с.р.		л	прак	с.р.
1	2	3	4	5	6	7	8	9
орієнтоване проєктування захищених систем.								
Тема 4. Програмні технології ідентифікації, автентифікації та керування доступом.	9	2	2	5	7	1	1	5
Тема 5. Криптографічні сервіси та програмне керування ключами, секретами і довірою.	9	2	2	5	7	1	1	5
Тема 6. Безпечне програмування, захист застосунків та API.	8	2	2	4	8	1	0	7
Тема 7. DevSecOps і автоматизація безпеки у конвеєрах CI/CD.	7	2	0	5	8	1	0	7
Тема 8. Безпека ланцюга постачання програмного забезпечення та компонентів з відкритим кодом.	9	2	2	5	8	1	0	7
Тема 9. Захист хмарно-нативних, контейнерних і розподілених програмних систем.	8	2	2	4	7	0	0	7
Тема 10. Програмні засоби моніторингу, керування вразливостями та реагування на інциденти.	8	2	2	4	7	0	0	7
Тема 11. Інженерія приватності та програмні технології захисту даних.	6	1	1	4	7	0	0	7
Тема 12. Безпека програмних систем зі штучним інтелектом і новітні напрями розвитку.	6	1	1	4	7	0	0	7
Всього	**90**	**22**	**14**	**54**	**90**	**8**	**2**	**80**

6.3. Теми практичних занять

№ з/п	Назва теми	Денна	Заочна
1	Практична робота №1, етап 1. Формалізація активів, загроз	2	1

	та вхідної моделі оцінювання ризиків та інцидентів безпеки мережевих й інформаційних систем об’єктів критичної інфраструктури. Побудова моделі загроз із визначенням захищуваних активів, меж довіри, потенційних порушників, векторів атак, вразливостей і можливих сценаріїв порушення інформаційної безпеки.		
2	Практична робота №1, етап 2. Фазифікація вхідних даних, розрахунок коефіцієнтів інциденту, агрегування оцінок і визначення рівня ризику за активами. Розроблення шкал оцінювання, функцій належності та правил прийняття рішень, а також перевірка чутливості моделі до зміни вхідних параметрів.	2	0
3	Практична робота №1, етап 3. Реалізація програмної системи підтримки прийняття рішень, розрахунок фінансових збитків, агрегованих оцінок Y та Y(Z), формування рекомендацій щодо зниження ризику і підготовка звіту. Реалізація валідації вхідних даних, розмежування доступу, журналювання подій, безпечного оброблення помилок, тестування та верифікації результатів.	2	0
4	Практична робота №2, етап 1. Побудова програмної моделі вхідних даних, фазифікація та нормування критеріїв керованості систем для забезпечення інформаційної безпеки. Формування системи показників конфіденційності, цілісності, доступності, автентичності, підзвітності та кіберстійкості програмної системи.	2	1
5	Практична робота №2, етап 2. Реалізація сценарних згорток M_1–M_4 і проєктування тренду рівня керованості процесами у системі. Моделювання сценаріїв нормального функціонування, деградації, відмов, виникнення інцидентів інформаційної безпеки та реалізації кібератак.	2	0
6	Практична робота №2, етап 3. Оцінювання режимів функціонування C_1–C_8, дефазифікація, визначення безпечного стану системи, тестування та візуалізація результатів. Проведення функціонального тестування і тестування безпеки, перевірка стійкості моделі, аналіз помилкових і граничних сценаріїв, формування програмної документації та рекомендацій щодо підвищення рівня інформаційної безпеки.	4	0
	Загальна кількість	**14**	**2**

Результатом виконання кожної практичної роботи є працездатний програмний прототип, вихідний код, набір тестових даних, опис моделі загроз і вимог безпеки, результати тестування та верифікації, структурна схема програмної системи, інструкція користувача і висновки щодо можливостей практичного застосування розробленої технології.

6.4. Самостійна робота

№ з/п	Назва теми	Денна	Заочна
1	Тема 1. Сучасні засади програмних технологій інформаційної безпеки.	5	7
2	Тема 2. Безпечний життєвий цикл програмного забезпечення та управління програмою безпеки.	5	7
3	Тема 3. Моделювання загроз і ризик-орієнтоване проєктування захищених систем.	4	7
4	Тема 4. Програмні технології ідентифікації, автентифікації та керування доступом.	5	5
5	Тема 5. Криптографічні сервіси та програмне керування ключами, секретами і довірою.	5	5
6	Тема 6. Безпечне програмування, захист застосунків та API.	4	7
7	Тема 7. DevSecOps і автоматизація безпеки у конвеєрах CI/CD.	5	7
8	Тема 8. Безпека ланцюга постачання програмного забезпечення та компонентів з відкритим кодом.	5	7
9	Тема 9. Захист хмарно-нативних, контейнерних і розподілених програмних систем.	4	7
10	Тема 10. Програмні засоби моніторингу, керування вразливостями та реагування на інциденти.	4	7
11	Тема 11. Інженерія приватності та програмні технології захисту даних.	4	7
12	Тема 12. Безпека програмних систем зі штучним інтелектом і новітні напрями розвитку.	4	7
	Загальна кількість	**54**	**80**

7. ІНСТРУМЕНТИ, ОБЛАДНАННЯ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ВИКОРИСТАННЯ ЯКИХ ПЕРЕДБАЧАЄ НАВЧАЛЬНА ДИСЦИПЛІНА

Для вивчення дисципліни використовуються персональні комп'ютери з доступом до мережі Інтернет, мультимедійне обладнання, операційні системи Windows, Linux або macOS, середовища програмування, системи керування версіями, бази даних, засоби тестування, аналізу коду, мережевого трафіку та виявлення вразливостей.

Можуть застосовуватися Visual Studio Code, Git, GitHub, Docker, Postman, Wireshark, OWASP ZAP, Python та інші програмні засоби або їх аналоги, необхідні для розроблення, тестування, верифікації та візуалізації програмних прототипів.

Допускається використання безкоштовного, відкритого, академічного та хмарного програмного забезпечення.

8. РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

Основна література

1. ISO/IEC 27001:2022. *Information security, cybersecurity and privacy protection — Information security management systems — Requirements.* 3rd ed. Geneva: International Organization for Standardization, 2022.
2. ISO/IEC 27005:2022. *Information security, cybersecurity and privacy protection — Guidance on managing information security risks.* 4th ed. Geneva: International Organization for Standardization, 2022.
3. ISO/IEC 27034-1:2011. *Information technology — Security techniques — Application security — Part 1: Overview and concepts.* 1st ed. Geneva: International Organization for Standardization, 2011.
4. ISO/IEC/IEEE 12207:2026. *Systems and software engineering — Software life cycle processes.* 2nd ed. Geneva: International Organization for Standardization, 2026.
5. Pascoe C., Quinn S., Scarfone K. *The NIST Cybersecurity Framework (CSF) 2.0.* NIST CSWP 29. Gaithersburg, MD: National Institute of Standards and Technology, 2024. DOI: 10.6028/NIST.CSWP.29.
6. Scarfone K., Souppaya M., Dodson D. *Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities.* NIST SP 800-218. Gaithersburg, MD: National Institute of Standards and Technology, 2022. DOI: 10.6028/NIST.SP.800-218.
7. Ross R., Winstead M., McEvilley M. *Engineering Trustworthy Secure Systems.* NIST SP 800-160, Vol. 1, Rev. 1. Gaithersburg, MD: National Institute of Standards and Technology, 2022. DOI: 10.6028/NIST.SP.800-160v1r1.
8. Nelson A., Rekhi S., Souppaya M., Scarfone K. *Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile.* NIST SP 800-61, Rev. 3. Gaithersburg, MD: National Institute of Standards and Technology, 2025. DOI: 10.6028/NIST.SP.800-61r3.

9. OWASP Foundation. *OWASP Application Security Verification Standard.* Version 5.0.0. OWASP Foundation, 2025.
10. Anderson R. *Security Engineering: A Guide to Building Dependable Distributed Systems.* 3rd ed. Hoboken, NJ: Wiley, 2020. 1232 p. DOI: 10.1002/9781119644682.
11. Shostack A. *Threat Modeling: Designing for Security.* Indianapolis, IN: John Wiley & Sons, 2014. 624 p. ISBN 978-1-118-80999-0.
12. Kohnfelder L. *Designing Secure Software: A Guide for Developers.* San Francisco, CA: No Starch Press, 2021. 312 p. ISBN 978-1-7185-0192-8.
13. McGraw G. *Software Security: Building Security In.* Boston, MA: Addison-Wesley Professional, 2006. ISBN 978-0-321-35670-3.
14. Zimmermann H.-J. *Fuzzy Set Theory—and Its Applications.* 4th ed. Dordrecht: Springer, 2001. 514 p. DOI: 10.1007/978-94-010-0646-0.
15. Pedrycz W., Gomide F. *Fuzzy Systems Engineering: Toward Human-Centric Computing.* Hoboken, NJ: Wiley-IEEE Press, 2007. 560 p. DOI: 10.1002/9780470168967.
16. Kahraman C., ed. *Fuzzy Multi-Criteria Decision Making: Theory and Applications with Recent Developments.* New York, NY: Springer, 2008. 590 p. DOI: 10.1007/978-0-387-76813-7.

Допоміжна література

17. Joint Task Force Transformation Initiative. *Guide for Conducting Risk Assessments.* NIST SP 800-30, Rev. 1. Gaithersburg, MD: National Institute of Standards and Technology, 2012. DOI: 10.6028/NIST.SP.800-30r1.
18. Joint Task Force. *Security and Privacy Controls for Information Systems and Organizations.* NIST SP 800-53, Rev. 5. Gaithersburg, MD: National Institute of Standards and Technology, 2020; Release 5.2.0, 2025. DOI: 10.6028/NIST.SP.800-53r5.
19. OWASP Foundation. *Software Assurance Maturity Model — OWASP SAMM.* Version 2.0. OWASP Foundation, 2020. Офіційна сторінка випуску OWASP SAMM 2.0.
20. Cybersecurity and Infrastructure Security Agency. *Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software.* Washington, DC: CISA, 2023. Офіційна інформація CISA про документ.
21. MITRE. *2025 CWE Top 25 Most Dangerous Software Weaknesses.* Common Weakness Enumeration, 2025. Офіційний перелік CWE Top 25.
22. Zadeh L. A. Fuzzy Sets. *Information and Control.* 1965. Vol. 8, No. 3. P. 338–353. DOI: 10.1016/S0019-9958(65)90241-X.
23. Polishchuk V., Kelemen M., Włoch I., Polishchuk A., Sharkadi M., Mlavets Y. Conceptual Model of Presentation of Fuzzy Knowledge. *CEUR Workshop Proceedings.* 2021. Vol. 3018. P. 1–12. Повний текст статті.
24. Polishchuk V., Kelemen M., Kelemen M. Jr. Methodology for Determining the Level of Process Control in Complex Systems Taking into Account Risk-Oriented Factors from Safe Time to Pandemics. *CEUR Workshop Proceedings.* 2021. Vol. 2864. P. 419–433. Повний текст статті.
25. Gavurova B., Kelemen M., Polishchuk V. Expert Model of Risk Assessment for the Selected Components of Smart City Concept: From Safe Time to Pandemics as COVID-19. *Socio-Economic Planning Sciences.* 2022. Vol. 82. Article 101253. DOI: 10.1016/j.seps.2022.101253.