Національний технічний університет України
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Кафедра програмного забезпечення комп'ютерних систем

БЕЗПЕКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Робоча програма навчальної дисципліни (Силабус)

1. Реквізити навчальної дисципліни

Рівень вищої освіти	***Перший (бакалаврський)***
Галузь знань	*12 Інформаційні технології*
Спеціальність	*121 Інженерія програмного забезпечення*
Освітня програма	*Інженерія програмного забезпечення мультимедійних та інформаційно-пошукових систем*
Статус дисципліни	*Нормативна*
Форма навчання	*Очна (денна)*
Рік підготовки, семестр	*4 рік підготовки, 7 семестр*
Обсяг дисципліни	*Лекції: 36 год., лабораторні роботи: 18 год., самостійна робота: 66 год.*
Семестровий контроль/ контрольні заходи	*Екзамен, модульна контрольна робота, календарний контроль*
Розклад занять	*Згідно розкладу на осінній семестр поточного навчального року (http://roz.kpi.ua/*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	*Лектор: к.т.н., доцент, Цуркан В. В., v.v.tsurkan@gmail.com* *Лабораторні роботи: к.т.н., доцент, Цуркан В.В., v.v.tsurkan@gmail.com*
Розміщення курсу	Google classroom: https://classroom.google.com/

2. Програма навчальної дисципліни

3. Опис навчальної дисципліни, її мета, предмет вивчання та результати навчання

Вивчення дисципліни «Безпека програмного забезпечення» дозволяє сформувати у здобувачів освіти компетенції, необхідні для розв'язання практичних задач професійної діяльності, пов'язаної із розробленням програмного забезпечення у аспекті його безпеки (насамперед конфіденційності, цілісності, доступності).

***Метою** вивчення дисципліни «Безпека програмного забезпечення» є формування у здобувачів освіти здатностей самостійно розробляти програмне забезпечення шляхом визначення і реалізування вимог його безпеки (насамперед конфіденційності, цілісності, доступності).*

***Предметом** дисципліни «Безпека програмного забезпечення» є методи моделювання загроз безпеці програмного забезпечення.*

*Вивчення дисципліни «Безпека програмного забезпечення» формує у здобувачів освіти **фахові компетентності (ФК)**, необхідні для розв'язання практичних задач професійної діяльності, пов'язаної з розробленням, вдосконаленням та експлуатуванням програмного забезпечення:*
***ФК01** Здатність ідентифікувати, класифікувати та формулювати вимоги до програмного забезпечення, зокрема, вимоги забезпечення його безпеки.*

ФК03 *Здатність проєктувати архітектуру програмного забезпечення, моделювати процеси функціонування окремих підсистем і модулів.*
ФК06 *Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки (в тому числі кібербезпеки).*
ФК08 *Здатність застосовувати фундаментальні і міждисциплінарні знання для успішного розв'язання завдань інженерії програмного забезпечення.*
ФК14 *Здатність до алгоритмічного та логічного мислення.*
ФК17 *Здатність розробляти програмне забезпечення інформаційно-пошукових систем.*
ФК19 *Здатність розробляти програмне забезпечення мультимедійних та мульсемедійних систем.*

Вивчення дисципліни «Безпека програмного забезпечення» сприяє формуванню у студентів наступних ***програмних результатів навчання*** *(ПРН) за освітньою програмою:*
ПРН01 *Аналізувати, цілеспрямовано шукати і вибирати необхідні для вирішення професійних завдань інформаційно-довідникові ресурси і знання з урахуванням сучасних досягнень науки і техніки.*
ПРН18 *Знати та вміти застосовувати інформаційні технології обробки, зберігання та передачі даних.*
ПРН21 *Знати засоби, аналізувати, вибирати, кваліфіковано застосовувати засоби забезпечення інформаційної безпеки (в тому числі кібербезпеки) і цілісності даних відповідно до розв'язуваних прикладних завдань та створюваних програмних систем.*
ПРН38 *Вміти застосовувати технології програмування для розроблення програмного забезпечення мультимедійних та інформаційно-пошукових систем.*

4. Пререквізити та постреквізити дисципліни (місце в структурно-логічній схемі навчання за відповідною освітньою програмою)

Успішному вивченню дисципліни «Безпека програмного забезпечення» передує вивчення дисциплін «Компоненти програмної інженерії», «Основи програмування», «Бази даних», «Програмування» навчального плану підготовки бакалаврів за спеціальністю 121 Інженерія програмного забезпечення.

Отримані при засвоєнні дисципліни «Безпека програмного забезпечення» теоретичні знання та практичні уміння забезпечують успішне виконання курсових проєктів та дипломних проєктів за спеціальністю 121 Інженерія програмного забезпечення.

5. Зміст навчальної дисципліни

Дисципліна «Безпека програмного забезпечення» передбачає вивчення таких тем:

Тема 1. Вступ до безпеки програмного забезпечення

Тема 2. Методи моделювання загроз безпеці програмного забезпечення

Модульна контрольна робота

Екзамен

6. Навчальні матеріали та ресурси

Базова література

1. Безпека програмного середовища. Електронний кампус НТУУ «КПІ ім. Ігоря Сікорського». Матерали з дисципліни «Безпека програмного середовища». – Доступ зареєстрованим студентам.

Додаткова література:

2. Shostack A. Threat Modeling: Designing for Security. Indianapolis: John Wiley & Sons, 2014. 590 p.

3. Tarandach I., Coles M. J. Threat Modeling. A Practical Guide for Development Teams. Sebastopol: O'Reilly Media, 2020, 201 p.

4. Threat Modeling. URL: https://owasp.org/www-community/Threat_Modeling (accessed on: 01.06.2022).

5. Common Vulnerability Scoring System v3.1: Specification Document. URL: https://www.first.org/cvss/v3.1/specification-document (accessed on: 01.06.2022).

6. LINDDUN framework. URL: https://www.linddun.org/linddun (accessed on: 01.06.2022).

7. ISO/IEC 27005:2018. Information technology. Security techniques. Information security risk management. [Valid from 2018-06-10]. URL: https://www.iso.org/standard/75281.html (accessed on: 01.06.2022).

8. MITER ATT&CK. URL: https://attack.mitre.org/ (accessed on: 01.06.2022).

9. Threat Modeling Manifesto. URL: https://www.threatmodelingmanifesto.org/ (accessed on: 01.06.2022).

10. Threat Modeling. URL: https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling (accessed on: 01.06.2022).

11. Threat Modeling. Process. URL: https://owasp.org/www-community/Threat_ Modeling_Process (accessed on: 01.06.2022).

12. Create a threat model using data-flow diagram elements. URL: https://docs.microsoft.com/en-us/learn/modules/tm-create-a-threat-model-using-foundational-data-flow-diagram-elements/ (accessed on: 01.06.2022).

13. ISO/IEC 27000:2018. Information technology. Security techniques. Information security management systems. Overview and vocabulary. [Valid from 2018-02-07]. URL: https://www.iso.org/standard/73906.html (accessed on: 01.06.2022).

14. DREAD Threat Modeling: An Introduction to Qualitative Risk Analysis. URL: https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/dread-threat-modeling-intro/ (accessed on: 01.06.2022).

15. Schneier B. Attack Trees. URL: https://www.schneier.com/academic/archives/1999/12/attack_trees.html (accessed on: 01.06.2022).

16. An Alternative: Attack Trees. URL: https://www.oreilly.com/library/view/building-secure-servers/0596002173/ch01s03.html (accessed on: 01.06.2022)

17. Common Vulnerability Scoring System v3.1: Examples. URL: https://www.first.org/cvss/v3.1/examples (accessed on: 01.06.2022).

18. IEC 31010:2019. Risk management. Risk assessment techniques. [Valid from 2019-06-17]. URL: https://www.iso.org/standard/72140.html (accessed on: 01.06.2022).

19. Finding Cyber Threats with ATT&CK™-Based Analytics. URL: https://www.mitre.org/sites/default/files/2021-11/16-3713-finding-cyber-threats-with-attack-based-analytics.pdf (accessed on: 01.06.2022).

Використати для опанування практичних умінь дисципліни. Матеріали знаходяться у вільному доступі в Інтернеті.

7. Навчальний контент

8. Методика опанування навчальної дисципліни (освітнього компонента)

№ з/п	*Тип навчального заняття*	*Опис навчального заняття*
Тема 1. Вступ до безпеки програмного забезпечення		
1	*Лекція 1. Зміст курсу, вступ до безпеки програмного забезпечення*	*Огляд змісту курсу. Поняття безпеки програмного забезпечення. Властивості конфіденційності, цілісності, доступності. Життєвий цикл розроблення безпечного програмного забезпечення. Підходи до визначення вимог безпеки програмного забезпечення* *Завдання на СРС: п. 6 № 1.*
2	*Лекція 2. Моделювання загроз безпеці програмного забезпечення*	*Поняття моделювання загроз безпеці програмного забезпечення. Процес моделювання загроз безпеці програмного забезпечення. Етапи моделювання загроз безпеці програмного забезпечення. Декомпозиціювання програмного забезпечення у аспекті загроз.* *Завдання на СРС: п. 6 № 2.*
3	*Лабораторна робота 1. Декомпозиціювання програмного забезпечення у аспекті загроз*	*Завдання: декомпозиціювати програмне забезпечення у аспекті загроз.* *Завдання на СРС: п. 6 № 3.*
Тема 2. Методи моделювання загроз безпеці програмного забезпечення		
4	*Лекція 3. Метод моделювання загроз безпеці програмного забезпечення на основі діаграми потоку даних*	*Поняття і характеристика діаграми потоку даних. Особливості використання діаграми потоку для моделювання загроз безпеці програмного забезпечення. Елементи діаграми потоку даних. Процес побудови діаграми потоку даних.* *Завдання на СРС:. п. 6 № 4.*
5	*Лекція 4. Етапи побудови діаграми потоку даних*	*Правила побудови діаграми потоку даних. Визначення процесів програмного забезпечення. Визначення сховищ даних програмного забезпечення. Визначення сутностей програмного забезпечення. Визначення потоків даних і меж довіри між елементами програмного забезпечення.* *Завдання на СРС: п. 6 № 5.*
6	*Лабораторна робота 2. Створення моделі загроз безпеці програмного забезпечення на основі діаграми потоку даних*	*Завдання: створити модель загроз безпеці програмного забезпечення на основі діаграми потоку даних.* *Завдання на СРС: п. 6 № 6.*

7	*Лекція 5. Метод моделювання загроз безпеці програмного забезпечення STRIDE*	*Характеристика методу STRIDE. Атрибути методу STRIDE: спуфінг, фальсифікування, відмова, розкриття інформації, відмова в обслуговуванні, підвищення привілеїв. Процес моделювання загроз безпеці програмного забезпечення за методом STRIDE.* *Завдання на СРС:. п. 6 № 7.*
8	*Лекція 6. Етапи моделювання загроз безпеці програмного забезпечення за методом STRIDE*	*Визначення загрози спуфінгу. Визначення загрози фальсифікування. Визначення загрози відмови. Визначення загрози розкриття інформації. Визначення загрози відмови в обслуговуванні. Визначення загрози підвищення привілеїв. Визначення вимог безпеки програмного забезпечення.* *Завдання на СРС:. п. 6 № 8.*
9	*Лабораторна робота 3. Створення моделі загроз безпеці програмного забезпечення за методом STRIDE*	*Завдання: створити модель загроз безпеці програмного забезпечення за методом STRIDE.* *Завдання на СРС: п. 6 № 9.*
10	*Лекція 7. Метод моделювання загроз безпеці програмного забезпечення DREAD*	*Характеристика методу DREAD. Шкали оцінювання загроз методом DREAD. Обирання шкали оцінювання загроз методом DREAD. Процес моделювання загроз безпеці програмного забезпечення за методом DREAD.* *Завдання на СРС: п. 6 № 10.*
11	*Лекція 8. Етапи моделювання загроз безпеці програмного забезпечення за методом DREAD*	*Визначення загроз безпеці програмного забезпечення. Визначення шкали оцінювання загроз безпеці програмного забезпечення. Оцінювання загроз безпеці програмного забезпечення. Ранжування загроз безпеці програмного забезпечення. Визначення вимог безпеки програмного забезпечення.* *Завдання на СРС: п.6 № 11.*
12	*Лабораторна робота 4. Створення моделі загроз безпеці програмного забезпечення за методом DREAD*	*Завдання: створити модель загроз безпеці програмного забезпечення за методом DREAD.* *Завдання на СРС: п.6 №12.*
13	*Лекція 9. Моделювання загроз безпеці програмного забезпечення методом створення дерева атак*	*Характеристика методу створення дерева атак. Способи використання дерева атак. Обирання способу використання дерева атак. Процес моделювання загроз безпеці програмного забезпечення методом створення дерева атак.* *Завдання на СРС: п. 6 № 13.*
14	*Лекція 10. Етапи моделювання загроз безпеці програмного забезпечення методом створення дерева атак*	*Обрання способу представлення дерева атак. Створення кореневого вузла дерева атак. Створення підвузлів кореневого вузла дерева атак. Перевіряння повноти створеного дерева*

		атак. Обрізання створеного дерева атак. Перевіряння створеного дерева атак. *Завдання на СРС: п. 6 № 14.*
15	*Лабораторна робота 5. Створення моделі загроз безпеці програмного забезпечення методом дерева атак*	*Завдання: створити модель загроз безпеці програмного забезпечення за методом дерева атак.* *Завдання на СРС: п.6 № 15.*
16	*Лекція 11. Метод оцінювання серйозності вразливостей програмного забезпечення*	*Характеристика методу оцінювання серйозності вразливостей. Метрики оцінювання серйозності вразливостей. Вектор-рядок оцінювання серйозності вразливостей. Калькулятор оцінювання серйозності вразливостей.* *Завдання на СРС: п. 6 № 16.*
17	*Лекція 12. Етапи методу оцінювання серйозності вразливостей програмного забезпечення*	*Визначення базових метрик. Визначення часових метрик. Визначення метрик середовища користувача. Визначення рівняння оцінювання серйозності вразливостей програмного забезпечення. Використання калькулятора оцінювання серйозності вразливостей програмного забезпечення.* *Завдання на СРС: п. 6 № 17.*
18	*Лабораторна робота 6. Оцінювання уразливостей програмного забезпечення за стандартом CVSS*	*Завдання: оцінити вразливості програмного забезпечення за стандартом CVSS.* *Завдання на СРС: п.6 № 18.*
19	*Лекція 13. Моделювання загроз безпеці програмного забезпечення методом LINDDUN*	*Характеристика методу LINDDUN. Категорії загроз за методом LINDDUN. Побудова моделі загроз безпеці програмного забезпечення. Виявлення загроз приватності програмного забезпечення. Керування загрозами приватності програмного забезпечення.* *Завдання на СРС: п. 6 № 19.*
20	*Лекція 14. Виявлення загроз приватності програмного забезпечення методом LINDDUN*	*Побудова моделі програмного забезпечення. Зіставлення елементів діаграми потоку даних стосовно категорій загроз приватності. Виявлення та документування загроз приватності.* *Завдання на СРС: п. 6 № 20.*
21	*Модульна контрольна робота. Реалізування вимог безпеки програмного забезпечення*	*Завдання: реалізувати вимоги безпеки програмного забезпечення.* *Завдання на СРС: п.6 № 21.*
22	*Лекція 15. Методи оцінювання ризиків безпеки програмного забезпечення*	*Різновиди методів оцінювання ризиків безпеки програмного забезпечення. Критерії обирання методів оцінювання ризиків безпеки програмного забезпечення. Підходи до обирання методів*

		оцінювання ризиків безпеки програмного забезпечення. *Завдання на СРС: п. 6 № 22.*
23	*Лекція 16. Оцінювання ризиків інформаційної безпеки методом «Матриця "Наслідки – вірогідність"»*	*Характеристика методу оцінювання ризиків. Шкали оцінювання ризиків. Обирання шкали оцінювання ризиків. Критерії прийнятності ризиків. Етапи використання методу оцінювання ризиків.* *Завдання на СРС: п. 6 № 23.*
24	*Лабораторна робота 7. Демонстрування реалізованих вимог безпеки програмного забезпечення*	*Завдання: продемонструвати реалізовані вимоги безпеки програмного забезпечення.* *Завдання на СРС: п. 6 № 24.*
25	*Лекція 17. База знань MITRE ATT&CK про тактики та техніки порушника безпеки програмного забезпечення*	*Структура бази знань MITRE ATT&CK. Матриця MITRE ATT&CK. Категорії структурування знань про тактики та техніки порушника: підприємство, мобільні пристрої, промислові системи керування.* *Завдання на СРС: п. 6 № 25.*
26	*Лекція 18. Створення моделі загроз безпеці програмного забезпечення на основі бази знань MITRE ATT&CK*	*Визначення поведінки порушника. Встановлення даних для визначення поведінки порушника. Визначення аналітики на основі встановлених даних для визначення поведінки порушника. Визначення вірогідних сценаріїв дій порушника. Оцінювання вірогідних дій порушника.* *Завдання на СРС: п. 6 № 26.*

9. Самостійна робота студента/аспіранта

Дисципліна «Безпека програмного забезпечення» ґрунтується на самостійних підготовках до аудиторних занять на теоретичні та практичні теми.

№ з/п	*Назва теми, що виноситься на самостійне опрацювання*	*Кількість годин*	*Література*
1	*Підготовка до лекції 1*	*1*	*1; 2; 3; 4; 9–11*
2	*Підготовка до лекції 2*	*1*	*1; 2; 3; 4; 9–11*
3	*Підготовка до лабораторної роботи 1*	*2*	*1; 2; 3; 4; 9–11*
4	*Підготовка до лекції 3*	*1*	*1; 2; 3; 4; 9–11*
5	*Підготовка до лекції 4*	*1*	*1; 2; 3; 4; 9–11*
6	*Підготовка до лабораторної роботи 2*	*2*	*1; 2; 3; 4; 9–11*
7	*Підготовка до лекції 5*	*1*	*1; 2; 3; 4; 9–11; 13*
8	*Підготовка до лекції 6*	*1*	*1; 2; 3; 4; 9–11; 13*
9	*Підготовка до лабораторної роботи 3*	*2*	*1; 2; 3; 4; 9–11; 13*
10	*Підготовка до лекції 7*	*1*	*1; 2; 3; 4; 9–11; 14*

11	*Підготовка до лекції 8*	*1*	*1; 2; 3; 4; 9–11; 14*
12	*Підготовка до лабораторної роботи 4*	*2*	*1; 2; 3; 4; 9–11; 14*
13	*Підготовка до лекції 9*	*1*	*1; 2; 3; 4; 9–11; 15; 16*
14	*Підготовка до лекції 10*	*1*	*1; 2; 3; 4; 9–11; 15; 16*
15	*Підготовка до лабораторної роботи 5*	*2*	*1; 2; 3; 4; 9–11; 15; 16*
16	*Підготовка до лекції 11*	*1*	*1; 2; 3; 4; 5; 9–11; 17*
17	*Підготовка до лекції 12*	*1*	*1; 2; 3; 4; 5; 9–11; 17*
18	*Підготовка до лабораторної роботи 6*	*2*	*1; 2; 3; 4; 5; 9–11; 17*
19	*Підготовка до лекції 13*	*1*	*1; 2; 3; 4; 6; 9–11*
20	*Підготовка до лекції 14*	*1*	*1; 2; 3; 4; 6; 9–11*
21	*Підготовка до модульної контрольної роботи*	*4*	*1; 2; 3; 4; 9–16*
22	*Підготовка до лекції 15*	*1*	*1; 2; 3; 4; 7; 9–11; 18*
23	*Підготовка до лекції 16*	*1*	*1; 2; 3; 4; 7; 9–11; 18*
24	*Підготовка до лабораторної роботи 7*	*2*	*1; 2; 3; 4; 9–16*
25	*Підготовка до лекції 17*	*1*	*1; 2; 3; 4; 8–11; 19*
26	*Підготовка до лекції 18*	*1*	*1; 2; 3; 4; 8–11; 19*
27	*Підготовка до екзамену*	*30*	*1-19*

10. Політика та контроль

11. Політика навчальної дисципліни (освітнього компонента)

Відвідування лекційних занять є обов'язковим.

Відвідування занять лабораторних робіт може бути епізодичним та за потреби консультації/захисту лабораторних робіт.

Правила поведінки на заняттях: активність, повага до присутніх, відключення телефонів.

Дотримання політики академічної доброчесності.

Правила захисту лабораторних робіт: роботи повинні бути виконані відповідно до поставлених завдань та згідно з обраним студентом варіантом.

12. Види контролю та рейтингова система оцінювання результатів навчання (РСО)

Протягом семестру студенти виконують 7 лабораторних робіт. ***Максимальна кількість балів*** *за кожну лабораторну роботу: 5 балів.*

Бали нараховуються за якість виконання і захист лабораторних робіт: 0-5 балів.

Критерії оцінювання якості виконання і захисту:
5 балів – робота виконана якісно, в повному обсязі, відповіді повні, добре аргументовані;
4 бали – робота виконана якісно, в повному обсязі, але має недоліки, відповіді з незначними помилками;
3 бали – робота виконана достатньо якісно, в повному обсязі, але містить суттєві недоліки, відповіді зі суттєвими помилками;

0 балів – робота виконана не якісно, не в повному обсязі, відповідей або немає, або невірні.

Максимальна кількість балів за виконання та захист лабораторних робіт:
5 балів × 7 лабораторних робіт = 35 балів.

Завданням ***модульної контрольної роботи*** є реалізування вимог безпеки програмного забезпечення*. Відповідь оцінюється 15 балами.*

Критерії оцінювання модульної контрольної роботи:
14–15 балів – відповідь вірна, повна, добре аргументована;
12–13 балів – в цілому відповідь вірна, але має недоліки;
9–11 балів – у відповіді є суттєві помилки;
0 балів – немає відповіді або відповідь невірна.

Максимальна кількість балів за модульну контрольну роботу:
15 балів × 1 завдання = 15 балів.

Рейтингова шкала з дисципліни дорівнює:
$R = R_C = R_{лабор.\ робіт} + R_{МКР} + R_{екзамен} = 35$ *балів + 15 балів + 50 балів = 100 балів.*

Календарний контроль: проводиться двічі на семестр як моніторинг поточного стану виконання вимог силабусу.
На першій атестації (8-й тиждень) студент отримує «Зараховано», якщо його поточний рейтинг не менше 10 балів (50 % від максимальної кількості балів, яку може отримати студент до першої атестації).
На другій атестації (14-й тиждень) студент отримує «Зараховано», якщо його поточний рейтинг не менше 20 балів (50 % від максимальної кількості балів, яку може отримати студент до другої атестації).

Семестровий контроль: екзамен
Умови допуску до семестрового контролю:
Необхідною умовою допуску студента до екзамену є семестровий рейтинг (R_C) не менше 30 балів. Після складання екзамену виставляється оцінка відповідно до таблиці (Таблиця відповідності рейтингових балів оцінкам за університетською шкалою).

Завдання на екзаменаційну роботу складається з 3 питань – 2 теоретичних та 1 практичних. Відповідь на кожне теоретичне запитання оцінюється 15 балами, а відповідь на практичне запитання оцінюється 20 балами.

Критерії оцінювання теоретичного запитання:
14–15 балів – відповідь вірна, повна, добре аргументована;
11–13 балів – в цілому відповідь вірна, але має недоліки;
5–10 балів – у відповіді є суттєві помилки;
0 балів – немає відповіді або відповідь невірна.

Критерії оцінювання практичного запитання:
17–20 балів – відповідь вірна, повна, добре аргументована;
12–16 балів – в цілому відповідь вірна, але має недоліки;
5–11 балів – у відповіді є суттєві помилки;
0 балів – немає відповіді або відповідь невірна.

Таблиця відповідності рейтингових балів оцінкам за університетською шкалою:

Кількість балів	*Оцінка*
100-95	Відмінно
94-85	Дуже добре
84-75	Добре
74-65	Задовільно

64-60	Достатньо
Менше 60	Незадовільно
Не виконані умови допуску	Не допущено

13. Додаткова інформація з дисципліни (освітнього компонента)

Перелік питань, які виносяться на семестровий контроль, наведено у Додатку 1.

Робочу програму навчальної дисципліни (силабус):

Складено к.т.н., доцент Цуркан В.В.

Ухвалено кафедрою ПЗКС (протокол № 12 від 26.04.2023 р.)

Погоджено Методичною комісією факультету прикладної математики (протокол № 10 від 26.05.2023 р.)

Додаток 1. Перелік питань, які виносяться на семестровий контроль

1. Охарактеризувати поняття безпеки програмного забезпечення.
2. Охарактеризувати властивості конфіденційності, цілісності, доступності даних програмного забезпечення.
3. Охарактеризувати життєвий цикл розроблення безпечного програмного забезпечення.
4. Охарактеризувати підходи до визначення вимог безпеки програмного забезпечення.
5. Охарактеризувати поняття моделювання загроз безпеці програмного забезпечення.
6. Охарактеризувати процес моделювання загроз безпеці програмного забезпечення.
7. Охарактеризувати етапи моделювання загроз безпеці програмного забезпечення.
8. Охарактеризувати декомпозиціювання програмного забезпечення у аспекті загроз.
9. Охарактеризувати метод моделювання загроз безпеці програмного забезпечення на основі діаграми потоку даних.
10. Охарактеризувати метод моделювання загроз безпеці програмного забезпечення STRIDE.
11. Охарактеризувати метод моделювання загроз безпеці програмного забезпечення DREAD.
12. Охарактеризувати моделювання загроз безпеці програмного забезпечення методом створення дерева атак.
13. Охарактеризувати метод оцінювання серйозності вразливостей програмного забезпечення.
14. Охарактеризувати метрики серйозності вразливостей програмного забезпечення.
15. Охарактеризувати моделювання загроз безпеці програмного забезпечення методом LINDDUN.
16. Охарактеризувати підходи до обирання методів оцінювання ризиків безпеки програмного забезпечення.
17. Охарактеризувати оцінювання ризиків інформаційної безпеки методом «Матриця "Наслідки – вірогідність"».
18. Охарактеризувати створення моделі загроз безпеці програмного забезпечення на основі бази знань MITRE ATT&CK.
19. Охарактеризувати визначення аналітики поведінки порушника безпеки програмного забезпечення на основі бази знань MITRE ATT&CK.
20. Охарактеризувати визначення вірогідних сценаріїв дій порушника безпеки програмного забезпечення на основі бази знань MITRE ATT&CK.