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

Кафедра інформатики та
програмної інженерії

БЕЗПЕКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни

Рівень вищої освіти	***Перший (бакалаврський)***
Галузь знань	*12 Інформаційні технології*
Спеціальність	*121 Інженерія програмного забезпечення*
Освітня програма	*Інженерія програмного забезпечення комп'ютерних систем*
Статус дисципліни	*Нормативна (цикл професійної підготовки)*
Форма навчання	*Очна (денна)*
Рік підготовки, семестр	*4 курс, осінній семестр*
Обсяг дисципліни	*4 кредити/120 годин*
Семестровий контроль/ контрольні заходи	*Екзамен, МКР*
Розклад занять	*http://rozklad.kpi.ua/Schedules/ScheduleGroupSelection.aspx*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	*доцент каф. ІПІ, к.т.н., доцент Курченко О.А.*
Розміщення курсу	*https://campus.kpi.ua*

Програма навчальної дисципліни

1. Опис навчальної дисципліни, її мета, предмет вивчення та результати навчання

Силабус освітнього компонента «Безпека програмного забезпечення» складено відповідно до освітніх програм підготовки бакалаврів «Інженерія програмного забезпечення комп'ютерних систем», «Інженерія програмного інформаційних комп'ютерних систем» за спеціальністю 121 «Інженерія програмного забезпечення» першого (бакалаврського) рівня вищої освіти галузі знань 12 Інформаційні технології.

Метою навчальної дисципліни*є формування та закріплення у студентів наступних фахових компетентностей:*

- *ФК01 Здатність ідентифікувати, класифікувати та формулювати вимоги до програмного забезпечення..*
- *ФК03 Здатність розробляти архітектури, модулі та компоненти програмних систем.*
- *ФК06 Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки (в тому числі кібербезпеки).*
- *ФК07 Володіння знаннями про інформаційні моделі даних, здатність створюватипрограмне забезпечення для зберігання, видобування та опрацювання даних.*
- *ФК14 Здатність до алгоритмічного та логічного мислення.*

Метою вивчення кредитного модуля є надбання студентом практичних навичок проектування та програмування при створені комплексних систем чи спеціальних апаратно-програмних підсистем захисту інформації від несанкціонованого доступу на основі:

- *вміння формалізувати та використати нормативно-правову базу захисту інформації в автоматизованих системах, методи та засоби управління доступом для розмежування прав користувачів до інформації з обмеженим доступом,*
- *засвоювання стандартних засобів та алгоритмів шифрування для побудови програмно-технічного забезпечення криптографічного захисту особливо важливої інформації та формування необхідної ключової бази шифрування.*
- *вміння вирішення аналітичних завдань генерації великий простих чисел, розрахунку ключів та крипостійкості сучасних симетричних й асиметричних систем шифрування та визначення їх базових характеристик.*
- *придбання прийомів створення й настоювання відповідного програмно-технічного забезпечення для захисту інформаційних ресурсів автоматизованих систем.*

***Предмет навчальної дисципліни** - методи та засоби управління доступом до носіїв інформації та баз даних, сучасні стандарти та засоби шифрування для побудови комплексних систем захисту комп'ютерних систем та мереж від вторгнень. Кредитний модуль призначений для вивчення методів проектування та прийомів настроювання програмно-технічних засобів захисту операційних систем, які забезпечують створення високо захищених розподілених комп'ютерних систем.*

Програмні результати навчання, на формування та покращення яких спрямована дисципліна:

- *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, 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.*

Знання:

основні концепції створення доказово достатніх систем захисту інформації, моделі Adept, Белла-Лападули та інші, існуючі механізми реалізації моделей захисту, які впроваджуються в різних операційних системах на основі „мандатних списків" та „списків доступу", шляхи реалізації принципів „розширення прав доступу" та „мінімальних привілеїв", стандарти, алгоритми та режими реалізації криптографічного захисту інформації, методи та засоби формування ключів шифрування, протоколи та етапи аутентифікації суб'єктів та повідомлень у відкритих каналах зв'язку, протоколи проведення конференцій та відкритих замовлень, структуру та характеристики електронних платіжних систем та пластикових платіжних карток, вимоги відомих стандартів щодо класифікації та критеріїв захищеності комп'ютерних систем від несанкціонованого доступу до інформації у напрямках конфіденційності, цілісності, доступності, контрольованості.

Уміння:

виконати заключні етапи проектування при створенні чи модифікації підсистем захисту інформації від несанкціонованого доступу та попередження вторгнень в комп'ютерні системи, врахувати вимоги до паролів та оцінки базових характеристик систем парольного захисту, написати комплекс програм дискретного управління доступом до інформації на носіях чи сайті, визначити оцінки складності програмної чи апаратної реалізації симетричних та асиметричних алгоритмів криптографічного захисту, оцінити крипостійкості алгоритмів, застосувати методи та алгоритми формування цифрових підписів та сертифікатів ключів, розробити графічний інтерфейс адміністратора безпеки,

виконати налагодження програм захисту інформації, організувати їх розміщення та виконання на робочий станції та в комп'ютерній мережі.

2. Пререквізити та постреквізити дисципліни

Для успішного засвоєння дисципліни студентубажано володіти освітніми компонентами: «Основи програмування», «Дискретна математика», «Системне програмування», «Структури даних та алгоритми», «Компонентиінженерії програмного забезпечення», «Операційні системи», «Комп'ютерні мережі».

Компетенції, знання та уміння, одержані в процесі вивчення освітнього компонента можуть бути використані для подальшого вивчення освітніх компонентів: «Переддипломна практика», «Дипломне проектування».

3. Зміст навчальної дисципліни

Розділ 1. Вступ

Тема 1.1 Проблеми захисту інформації в комп'ютерних системах і мережах (КСМ).
Тема 1.2 Основні напрямки загроз НСД та канали витоку інформації з КСМ. Цілі, суб'єкти та схеми активних та пасивних вторгнень

Розділ 2. Комплексний підхід до створення систем захисту інформації в комп'ютерних системах.

Тема 2.1 Нормативно-правова база захисту інформації. Основні напрямки і засоби захисту інформації в КСМ.
Тема 2.2 Моделі систем доказово достатнього захисту інформації. Концептуальні моделі Adept. Деннінга, Лендвера.
Тема 2.3 Матрична модель системи захисту Белла і Ла-Падули. Поняття суб'єкта, вектора прав та диспетчера доступу. Розширення прав доступу.
Тема 2.4. Модель системи моніторингу безпеки КСМ. Поняття фактора загрози та статистичної аномалії.

Розділ 3. Ідентифікація суб'єктів та управління доступом на основі парольної системи.

Тема 3.1 Ідентифікація користувачів на основі системи паролів. Вимоги до паролів. Схема зберігання паролів в ОС Unix.
Тема 3.2 Аналіз характеристик системи простих паролів. Формула Андерсона.Приклади.
Тема 3.3 Модифікації системи паролів. Підтвердження прав доступу на основі процедури однобічного та двобічного „рукостискання".
Тема 3.4 Log-журнали: реєстраційний та операційний. Моніторинг безпеки на основі ведення журналів в ОС Unix та Windows

Розділ 4. Дискретне розмежування доступу суб'єктів к інформації в обмеженій матричній моделі системи захисту.

Тема 4.1 Списки доступу та формування категорій користувачів. Наслідування прав. Замки, ключі та умови доступу в ОС.
Тема 4.2 Мандатні списки та реалізація принципу „мінімальних привілей". Мандатний доступ в ОС Unix.

Розділ 5. До комп'ютерні підходи щодо криптографічного захисту інформації з обмеженим доступом.

Тема 5.1 Шифрування на основі одно та багато алфавітних підстановок. Поняття шифру і таємного ключа. Шифр Цезаря
Тема 5.2 Шифрування на основі перестановок. Задачі дешифрування та криптоаналізу
Тема 5.3 Біграмні шифри. Шифр Віжинера та квадрати Уітстона. Шифрувальні машини

Тема 5.4 Потокові шифри з необмеженою довжиною ключа. Шифрування „гамуванням”.

Розділ 6. Симетричне шифрування в системах зв’язку з відкритими комунікаціями.

Тема 6.1 Організація передач даних в секретних системах по Шеннону. Засоби максимізації ентропії.

Тема 6.2 Шифрування на основі чередування перестановок та підстановок. Система Люціфер.

Тема 6.3 Федеральний стандарт шифрування DataEncryption Standard. (DES). Загальна схема та функція маскування з ключовими словами.

Тема 6.4 Блок управління ключами в DES. Алгоритм 3-DES та чотири режими реалізації криптографічного захисту на основі DES.

Розділ 7. Асиметричні системи шифрування на основі відкритих та таємних ключів.

Тема 7.1 Нове направлення в криптографії по Діффі і Хелману. Незворотні функції в шифруванні. Три схеми та задачі криптозахисту.

Тема 7.2 Система RSA. Модулярна арифметика. Алгоритм швидкого дискретного потенціювання. Процесор - акселератор RSA.

Тема 7.3. Проблема генерації великих простих чисел (ВПЧ). Тест Рабіна та мала теорема Ферма. Перевірки на простоту.

Тема 7.4. Схеми та алгоритми розрахунків ключів для системи RSA. Класичний та розширений алгоритми Евкліда. Приклади

Контрольна робота з розділів 2 - 7

Розділ 8. Підвищення крипостійкості в асиметричних системах шифрування.

Тема 8.1 Оцінки криптостійкості алгоритму RSA. Порівняння з схемами DES та 3-DES. Приклади

Тема 8.2 Система шифрування Ель-Гамаля. Схеми та алгоритми розрахунків ключів для системи Ель-Гамаля. Приклади шифрування та дешифрування

Розділ 9. Аутентифікація суб’єктів та встановлення „довірчого” зв’язку в розподілених системах та мережах.

Тема 9.1 Встановлення „довіри” суб’єктів на основі симетричних систем шифрування. Протоколи встановлення зв’язку.

Тема 9.2. Встановлення „довіри” суб’єктів на основі асиметричних систем шифрування. Поняття сертифікату відкритого ключа.

Тема 9.3 Встановлення цілісності повідомлень на основі симетричних та асиметричних систем шифрування. Поняття цифрового підпису.

Тема 9.4 Організація „довірчого” зв’язку в протоколах „відкритих замовлень”. Поняття електронних чеку та квитанції.

Розділ 10. Системи електронних платежів. Засоби підвищення „довіри” віртуальних відносин.

Тема 10.1 Пластикові картки як база для організації електронних платежів. Банки – емітенти та банки – еквайєри.

Тема 10.2 Структура системи електронних платежів. POS- термінали. Функції та організація процесінгового центру.

Тема 10.3 Багато рівнева організація формування та використання ключів шифрування.

Тема 10.4 Електронна торгівля на базі технології Е-бізнеса. Протоколи SSL та SET. Ієрархія підписів в довірчих відносинах.

4. Навчальні матеріали та ресурси

Основна література

1. Відеозаписи з курсу лекцій за 2021-2022 навчальний рік. https://bbb.comsys.kpi.ua/b/art-ulj-mrk-ayr Access Code: 12096

2. Волокита А.М., Іваніщев Б.В.. Безпека програм і даних: Теорія та практикум. Рекомендовано Методичною радою КПІ ім. Ігоря Сікорського як навчальний посібник для здобувачів ступеня бакалавра за спеціальністю 121 Інженерія програмного забезпечення. Гриф надано Методичною радою КПІ ім. Ігоря Сікорського (протокол № 1 від 02.09.2022 р.) за поданням Вченої ради Факультету інформатики та обчислювальної техніки (протокол № 11 від 11.07.2022 р.). Оновлено. https://comsys.kpi.ua/metodichni-vkazannya-po-disciplinam

3. Дем'яненко, В. А. Безпека програм та даних [Електронний ресурс] : навч. посіб. до лаб. практикуму / В. А. Дем'яненко, Ю. А. Кузнецова. – Харків : Нац. аерокосм. ун-т ім. М. Є. Жуковського «Харків. авіац. ін-т», 2021. – 95 с. http://dspace.library.khai.edu/xmlui/handle/123456789/798

4. Безпека програм та даних [Текст] : Навчальний посібник / Сенів М.М., Яковина В.С. Львівська політехніка, 2018 р. - 256 с.

Додаткова література

5. Вербіцький О.В. Вступ до криптології. – Львів, НТЛ, 1998. – 248 с.

6. Національний стандарт ТЗІ України НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в компютерних системах від несанкціонованного доступу. Чинний з 01.07.1999 р.

7. Національний стандарт ТЗІ України НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищенності оброблювальної інформації від несанкціоновіанного доступу. Чинний з 01.07.1999 р.

8. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги;

9. ДСТУ ISO/IEC TS 27008:2019 Інформаційні технології. Методи захисту. Настанова щодо оцінювання захисту інформаційної безпеки;

10. ДСТУ ISO/IEC 27018:2019 Інформаційні технології. Методи захисту. Кодекс усталеної практики для захисту персональної ідентифікаційної інформації (PII) у загальнодоступних хмарах, що діють як процесори PII.

11. Weissman C. Security Controls in the ADEPT-50 Time Sharing System. // Proceedings AFIPS, FJCC. – 2010. – v. 35. – pp. 119-133.

12. Hartson R., Hsiao D. Full protection specification in the semantic model for database protection languages. // Proceedings Annual Conference ACM. – Houston, New York. – 2014. – pp. 90-95.

13. Harrison M. A.. Russo W. L. Protection in Operating Systems. // Communications of the ACM. – 2014. – v. 19, № 8. – pp. 461-471.

14. Spier M. J. A Model Implementation for protective domains. // International Journal on Computer Information Science. – 2021. – v. 2, № 3. – pp. 201-229.

15. Bell D. E., LaPadula L. J. Secure computer systems: mathematical foundations and model. // M74-244, The MITRE Corp., Bedford, Mass.- May 1999.

16. Bell D. E. Secure computer systems: a refinement of the mathematical model. // Springfield, The MITRE Corp. – 2018. – Report № 2574, pp. 75

17. Graham R. M., Denning P. J. Protection – Principles and Practice. // Proceedings AFIPS. – 2018. – v.40, pp. 417-429.

18. Denning D. E. A Lattice Model of Secure Information Flow. // Communications of the ACM. –2011. – v. 19, № 5. – pp. 236-243

19. *Landwehr C., Heitmeyer C., McLean J. A security model for military message systems. // ACM Trans. on Computer Systems. – 2017. – V. 2, № 3. – pp. 198-222.*

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

Лекційні заняття

№	*Назва теми лекції та перелік основних питань (перелік дидактичних засобів, посилання на інформаційні джерела)*
1	***Розділ 1. Вступ.*** ***Лекція 1. Проблеми захисту інформації в комп'ютерних системах і мережах (КСМ).*** *Основні питання: Поняття несанкціонованого доступу (НСД), вразливості КСМ, загрози вторгнення, каналу витоку інформації. Основні напрямки загроз НСД та канали витоку інформації з КСМ. Цілі, суб'єкти та схеми активних та пасивних вторгнень.* *Відеозапис лекції:https://bbb.comsys.kpi.ua/b/art-ulj-mrk-ayr Access Code: 12096*
2	***Розділ 2. Комплексний підхід до створення систем захисту інформації в комп'ютерних системах.*** ***Лекція 2. Нормативно-правова база захисту інформації.*** *Основні питання:Поняття інформації з обмеженим доступом та системи захисту. Основні напрямки і засоби захисту інформації в КСМ. Моделі систем доказово достатнього захисту інформації. КонцептуальнамодельAdept. Поняття об'єкта і категорії. Модель Деннінга. Поняття домену безпеки. Модель Лендвера. Поняття периметра відповідальності.* *Відеозапис лекції:https://bbb.comsys.kpi.ua/b/art-ulj-mrk-ayr Access Code: 12096*
3	***Лекція 3. Матрична модель системи захисту Белла і Ла-Падули.*** *Основні питання:Поняття суб'єкта, вектора прав та диспетчера доступу. Розширення прав доступу. Модель системи моніторингу безпеки КСМ. Поняття фактора загрози та статистичної аномалії. Вектор індикації аномалій.* *Відеозапис лекції:https://bbb.comsys.kpi.ua/b/art-ulj-mrk-ayr Access Code: 12096*
4	***Розділ 3. Ідентифікація суб'єктів та управління доступом на основі парольної системи.*** ***Лекція 4. Ідентифікація користувачів на основі системи паролів.*** *Основні питання:Вимоги до паролів. Схема зберігання паролів в ОС Unix. Аналіз характеристик системи простих паролів. Формула Андерсона. Приклади.* *Відеозапис лекції:https://bbb.comsys.kpi.ua/b/art-ulj-mrk-ayr Access Code: 12096*
5	***Лекція 5. Модифікації системи паролів.*** *Основні питання:Підтвердження прав доступу на основі процедури однобічного та двобічного „рукопожаття". Log-журнали: реєстраційний та операційний. Моніторинг безпеки на основі ведення журналів в ОС Unix та Windows.* *Відеозапис лекції:https://bbb.comsys.kpi.ua/b/art-ulj-mrk-ayr Access Code: 12096*
6	***Розділ 4. Дискретне розмежування доступу суб'єктів к інформації в обмеженій матричній моделі системи захисту.*** ***Лекція 6. Списки доступу та формування категорій користувачів.*** *Основні питання:Наслідування прав. Замки, ключі та умови доступу в ОС. Мандатні списки та реалізація принципу „мінімальних привілей". Мандатний доступ в ОС Unix.* *Відеозапис лекції:https://bbb.comsys.kpi.ua/b/art-ulj-mrk-ayr Access Code: 12096*
7	***Розділ 5. До комп'ютерні підходи щодо криптографічного захисту інформації з обмеженим доступом.***

	Лекція 7. Шифрування на основі одно та багато алфавітних підстановок. *Основні питання:Поняття шифру і таємного ключа. Шифр Цезаря. Шифрування на основі перестановок. Шифр „скитала”. Задачі дешифрування та криптоаналізу.* *Відеозапис лекції:https://bbb.comsys.kpi.ua/b/art-ulj-mrk-ayr Access Code: 12096*
8	***Лекція 8. Біграмні шифри.*** *Основні питання:Шифр Віжинера та квадрати Уітстона. Шифрувальні машини. Потокові шифри з необмеженою довжиною ключа. Шифрування „гамуванням”.* *Відеозапис лекції:https://bbb.comsys.kpi.ua/b/art-ulj-mrk-ayr Access Code: 12096*
9	***Розділ 6. Симетричне шифрування в системах зв’язку з відкритими комунікаціями.*** ***Лекція 9. Організація передач даних в секретних системах по Шеннону.*** *Основні питання:Засоби максимізації ентропії. Шифрування на основі чередування перестановок та підстановок. Система Люціфер.* *Відеозапис лекції:https://bbb.comsys.kpi.ua/b/art-ulj-mrk-ayr Access Code: 12096*
10	***Лекція 10. Федеральний стандарт шифрування DataEncryption Standard. (DES).*** *Основні питання:Загальна схема та функція маскування з ключовими словами. Блок управління ключами в DES. Алгоритм 3-DES та чотири режими реалізації криптографічного захисту на основі DES.* *Відеозапис лекції:https://bbb.comsys.kpi.ua/b/art-ulj-mrk-ayr Access Code: 12096*
11	***Розділ 7. Асиметричні системи шифрування на основі відкритих та таємних ключів.*** ***Лекція 11. Нове направлення в криптографії по Діффі і Хелману.*** *Основні питання:Незворотні функції в шифруванні. Три схеми та задачі криптозахисту. Система RSA. Модулярна арифметика. Алгоритм швидкого дискретного потенціювання. Процесор - акселератор RSA.* *Відеозапис лекції:https://bbb.comsys.kpi.ua/b/art-ulj-mrk-ayr Access Code: 12096*
12	***Лекція 12. Проблема генерації великих простих чисел (ВПЧ).*** *Основні питання:Тест Рабіна та мала теорема Ферма. Перевірки на простоту. Приклади.* *Відеозапис лекції:https://bbb.comsys.kpi.ua/b/art-ulj-mrk-ayr Access Code: 12096*
13	***Лекція 13. Схеми та алгоритми розрахунків ключів для системи RSA.*** *Основні питання:Класичний та розширений алгоритми Евкліда. Приклади.* *Відеозапис лекції:https://bbb.comsys.kpi.ua/b/art-ulj-mrk-ayr Access Code: 12096*
14	***Розділ 8. Підвищення крипостійкості в асиметричних системах шифрування.*** ***Лекція 14. Оцінки криптостійкості алгоритму RSA.*** *Основні питання:Порівняння з схемами DES та 3-DES. Приклади.* *Відеозапис лекції:https://bbb.comsys.kpi.ua/b/art-ulj-mrk-ayr Access Code: 12096*
15	***Лекція 15. Система шифрування Ель-Гамаля.*** *Основні питання:Схеми та алгоритми розрахунків ключів для системи Ель-Гамаля. Приклади шифрування та дешифрування.* *Відеозапис лекції:https://bbb.comsys.kpi.ua/b/art-ulj-mrk-ayr Access Code: 12096*
16	***Розділ 9. Аутентифікація суб’єктів та встановлення «довірчого» зв’язку в розподілених системах та мережах.*** ***Лекція 16. Встановлення «довіри» суб’єктів на основі симетричних систем шифрування.*** *Основні питання: Поняття майстер – ключа та змінного - ключа. Протоколи встановлення зв’язку. Встановлення «довіри» суб’єктів на основі асиметричних систем*

	шифрування. Поняття сертифікату відкритого ключа. Протоколи встановлення зв'язку. *Відеозапис лекції:https://bbb.comsys.kpi.ua/b/art-ulj-mrk-ayr Access Code: 12096*
17	***Лекція 17. Встановлення цілісності повідомлень на основі симетричних та асиметричних систем шифрування.*** *Основні питання:Поняття сигнатури повідомлення та цифрового підпису. Організація „довірчого" зв'язку в протоколах „відкритих замовлень". Поняття електронних чеку та квитанції.* *Відеозапис лекції:https://bbb.comsys.kpi.ua/b/art-ulj-mrk-ayr Access Code: 12096*
18	***Розділ 10. Системи електронних платежів. Засоби підвищення «довіри» віртуальних відносин.*** ***Лекція 18. Електронна торгівля.*** *Основні питання: Протоколи безпеки. Ієрархія підписів в довірчих відносинах.* *Відеозапис лекції:https://bbb.comsys.kpi.ua/b/art-ulj-mrk-ayr Access Code: 12096*

Контрольні роботи

Метою контрольних робіт є закріплення та перевірка теоретичних знань із освітнього компонента, набуття студентами практичних навичок самостійного вирішення задач та складанні та компіляції програм.

Контрольна робота КР1 виконується після вивчення розділів 1 - 5.

Контрольна робота КР2 виконується після вивчення розділів 6 - 10.

Лабораторні роботи

Метою проведення циклу лабораторних робіт є набуття студентами необхідних практичних навиків розробки та дослідження макетних зразків підсистем захисту інформації, які являють собою втілення ефективних підходів та алгоритмів створення комплексної системи захисту інформації від несанкціонованого доступу, дослідження характеристик необхідних структур даних, розробки та налагодження окремих компонентів інтерфейсу консолі адміністратора безпеки.

Лабораторна робота включає:

- *постановку вхідної задачі,*
- *теоретичні відомості з методів та засобів рішення задачі,*
- *аналіз математичного та алгоритмічного забезпечення,*
- *обґрунтування вибору програмних засобів дослідження,*
- *розробку структурної схеми взаємодії підсистем захисту,*
- *результати виконання покрокової верифікації алгоритмів,*
- *результати виконання модельних експериментів,*
- *інтерпретація результатів моделювання та висновки,*
- *лістинг програми.*

№	*Перелік лабораторних робіт.*
1	***Лабораторна робота 1.*** *Розробка та дослідження програмної підсистеми дискретного управління доступом до окремого носія інформації з складною структурою каталогів.*
2	***Лабораторна робота 2.1.*** *Програмування та дослідження підсистеми ідентифікації користувачів на основі простих паролів з контролем вимог та супроводженням журналів.* ***Лабораторна робота 2.2.*** *Програмування та дослідження підсистеми аутентифікації користувачів під час роботи з використанням „питань-відповідей” та таємних функцій.*
3	***Лабораторна робота 3.1.*** *Програмування та дослідження підсистеми моніторингу для виявлення аномалій та небезпечних подій щодо інформації, яка захищається.* ***Лабораторна робота 3.2.*** *Розробка програмного макету для дослідження та покрокової веріфікації алгоритму швидкого дискретного потенціювання та інших операцій з довільною довжиною операндів.*
4	***Лабораторна робота 4.*** *Розробка програмного макету для дослідження та покрокової верифікації алгоритмів генерації великих простих чисел з формуванням бази даних ВПЧ.*
5	***Лабораторна робота 5.*** *Розробка програмного макету для дослідження та покрокової верифікації RSA - підсистеми управління ключами, шифрування та дешифрування повідомлень.*
6	***Лабораторна робота 6.*** *Розробка програмного макету для дослідження та покрокової верифікації DES - підсистеми формування сигнатур, шифрування та дешифрування повідомлень.*
7	***Розрахунково-графічна робота (Лабораторна робота 7).*** *Розробка програмного макету згідно індивідуального завдання. Використання засобів штучного інтелекту для задачі моніторингу безпеки, удосконалення програмних компонентів з ЛР1-6. Виконання експериментальних досліджень, оформлення відповідно до спрощеної структури наукових праць.*

Самостійна робота студента

№ з/п	*Вид самостійної роботи*	*Кількість годин СРС*
1	*Підготовка та виконання лабораторних робіт*	*40*
2	*Підготовка до МКР. Опрацювання лекційного матеріалу і додаткових джерел.*	*6*
3	*Виконання РГР*	*20*
	Всього годин СРС	*66*

Політика та контроль

6. Політика навчальної дисципліни (освітнього компонента)

При зарахування та оцінювання лабораторних робот беруться до уваги наступні чинники:

- *Повнота виконання завдання на лабораторну роботу за індивідуальним варіантом;*
- *Своєчасність виконання лабораторної роботи згідно графіку;*
- *Самостійність виконання лабораторної роботи та відсутність ознак плагіату;*
- *Відповіді на питання щодо змісту лабораторної роботи під час її захисту.*

При оцінюванні контрольних робіт до уваги приймаються:

- *Правильність та повнота виконання завдань;*

- *Кількість виконаних завдань в умовах обмеженого часу;*
- *Самостійність виконання завдань та відсутність ознак плагіату;*
- *Кількість спроб виконання контрольних.*

Для підготовки до контрольних студенти отримують перелік теоретичних питань та зміст типових задач, які будуть у завданнях на контрольних.

При першої та другої атестації (календарного контролю) до уваги приймається кількість лабораторних робіт та контрольних робіт зарахованих на час проведення атестації.

Політика щодо академічної доброчесності: Кодекс честі Національного технічного університету України «Київський політехнічний інститут» https://kpi.ua/files/honorcode.pdf встановлює загальні моральні принципи, правила етичної поведінки осіб та передбачає політику академічної доброчесності.

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

Поточний контроль: *вправи на лекційних заняттях, тестування, виконання РГР, МКР, виконання та захист лабораторних робіт.*

Календарний контроль: *провадиться двічі на семестр як моніторинг поточного стану виконання вимог силабусу.*

Семестровий контроль: *екзамен.*

Умови допуску до семестрового контролю: *виконані та захищені лабораторні роботи, МКР (або курси на дистанційній платформі Курсера і т.д.)*

Таблиця відповідності рейтингових балів оцінкам за університетською шкалою:

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

Загальна рейтингова оцінка студента після завершення семестру складається з балів, отриманих за:

- виконання та захист лабораторних робіт (ЛР1-ЛР6);

- виконання розрахунково-графічної роботи (ЛР7);

- виконання модульної контрольної роботи (МКР);

Лабораторні роботи

Ваговий бал. *Лабораторні роботи ЛР1-6 мають ваговий бал 10. Заплановано самостійне виконання шести лабораторних робіт і розрахунково-графічної роботи (за вибором).Теми лабораторних робіт узгоджені у часі та за змістом з темами лекцій. Виконання лабораторних робіт у повному обсязі дозволяє набути практичних навичок програмування систем безпеки. До кожної ЛР викладачем ставляться індивідуальні практичні завдання, які виконуються особисто кожним студентом. Також для отримання додаткових балів студент може виконати розширене додаткове завдання.*

Критерії оцінювання: *Базовий варіант 6 балів, з захистом додаткового практичного завдання до 10 балів.*

Розрахунково-графічна робота

Ваговий бал. *Розрахунково-графічна робота(ЛР 7) має ваговий бал 20.*

Заплановано самостійне виконання розрахунково-графічної роботи. Виконання ЛР7 передбачає творче осмислення попередніх робіт ЛР1-6, і удосконалення однієї з програмних компонентів, які використовувались в ЛР1-6 (за вибором студента).Звіт з ЛР7 включає в себе звіти з ЛР1-6, опис модифікацій, порівняльні експерименти, і список літератури з посиланням на власний репозиторій git.

Критерії оцінювання: *Базовий варіант 12 балів, з захистом додаткового практичного завдання до 20 балів.*

Модульні контрольні роботи

Ваговий бал. *Дві контрольні роботи мають ваговий бал по 10.*

Заплановано виконання двох модульних контрольних робіт (КР1, КР2) виконується протягом календарного контролю (завдання видаються за тиждень до початку календарного контролю). За погодженням зі студентами терміни виконання КР1 і КР2 можуть бути подовжені. Також можливе поєднання КР1 і КР2 в одну розширену роботу МКР.

Критерії оцінювання: *У завданнях до КР1 і КР2 розписані бали за відповідні питання. Питання, на які відповідати, студент обирає самостійно.*

Додаткові (бонусні) бали

Передбачені додаткові бали за активність на лекції (1 бал), за виконання розширених додаткових завдань до ЛР1-7 (2 бали), участь в хакатонах, рішення олімпіадних задач з програмування і інша діяльність (бали погоджується зі студентами індивідуально). Максимальний бонусний бал 10. За погодженням зі студрадою можливий розіграш «призових балів» на день факультету з використанням генераторів псевдовипадкових чисел.

Штрафні бали

Штрафні бали не передбачені. Якщо студент не виконує додаткові завдання до ЛР1-7, то буде зараховано мінімальний бал за відповідну ЛР (табл.1).

Календарний контроль

Календарний контроль базується на поточній рейтинговій оцінці. Умовою позитивної атестації є значення поточного рейтингу студента не менше 30% від максимально можливого на час атестації. Бал, необхідний для отримання позитивного календарного контролю доводиться до відома студентів викладачем не пізніше ніж за 2 тижні до початку календарного контролю.

Форма семестрового контролю. Екзамен.

Семестровий рейтинг студента складається з балів, які він отримує за види робіт відповідно.

Оцінювання окремих видів навчальної роботи студента(у балах)

Вид навчальної роботи	*Всьогозавидоморботи*
ВиконаннятазахистлабораторнихробітЛР1-6	*36..60*
Виконання та захист РГР (ЛР7)	*12..20*
ВиконанняКР1	*6..10*
ВиконанняКР2	*6..10*
Рейтинг за семестр	*60-100*

Необхідною умовою допуску студента до екзамену автоматом є його індивідуальний семестровий рейтинг, не менший, ніж 60 балів та виконані ЛР1-6. При невиконанні згаданих вимог студент до екзамену не допускається. Для підвищення оцінки дозволяється переписувати КР1, КР2 і перездавати ЛР1-6, ЛР7.

8. Додаткова інформація з дисципліни (освітнього компонента)

В рамках вивчення дисципліни «Безпека програмного забезпечення» допускається зарахування балів, одержаних в результаті дистанційних курсів на платформі "Coursera", за умови попереднього погодження програми даного курсу з викладачем та за умови отримання офіційного сертифікату (якщо це можливо безкоштовно). Бали за курси, в яких є тільки тестові завдання, зараховуються у кількості годин не менше 60, та з балом 55 (замість ЛР1-ЛР7). Таким чином, максимальний бал обмежується 75 (з урахування контрольних робіт). Якщо в курсах є практична частина, то звіти з практичних частин можуть бути зараховані в якості лабораторних робіт, в такому випадку максимальний бал обмежується 100.

Робочу програму навчальної дисципліни (силабус):

Складено к.т.н., доцент Курченко О.А.

Ухвалено кафедрою інформатики та програмної інженерії (протокол № 16 від 29.05.2024 р.)

Погоджено Методичною комісією факультету (протокол № 10 від 21.06.2024 р.)