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

Емблема кафедри (за наявності) штучного інтелекту

БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ

Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни

Рівень вищої освіти	***Перший (бакалаврський)***
Галузь знань	*12 Інформаційні технології*
Спеціальність	*122 Комп'ютерні науки*
Освітня програма	*Системи і методи штучного інтелекту*
Статус дисципліни	*Нормативна*
Форма навчання	*очна(денна)/дистанційна/змішана*
Рік підготовки, семестр	*4 курс, осінній семестр*
Обсяг дисципліни	*3.5 кредитів ЄКТС*
Семестровий контроль/ контрольні заходи	*Залік*
Розклад занять	
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	Лектор: *доктор технічних наук, професор Мухін Вадим Євгенійович, v_mukhin@i.ua, (067)5087684* Лабораторні: *доктор технічних наук, професор Мухін Вадим Євгенійович, v_mukhin@i.ua, (067)5087684*
Розміщення курсу	*https://drive.google.com/drive/u/0/ /folders/1XAchCgUycJ1OplIy8COEChSVGYK0j3EJ?usp=sharing*

Програма навчальної дисципліни

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

1.1. Опис навчальної дисципліни

Навчальна дисципліна "Безпека інформаційних систем" призначений для вивчення методів та засобів управління доступом до носіїв інформації та баз даних, сучасних стандартів та засобів шифрування для побудови комплексних систем захисту комп'ютерних систем та мереж від вторгнень. Навчальна дисципліна призначена для вивчення методів проектування та прийомів настроювання програмно-технічних засобів захисту операційних систем, які забезпечують створення високо захищених розподілених комп'ютерних систем. Дисципліна передбачає наступні компетенції:

ЗК 2 Здатність застосовувати знання у практичних ситуаціях;

ФК 14 Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури.

Також за результатами будуть отримані наступні програмні результати:
ПР15 Розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних.

1.2. Мета и завдання навчальної дисципліни

Метою навчальної дисципліни є формування у студентів компетентностей.

ЗДАТНІСТЬ:

- аналізу завдань та нормативно-правової бази захисту інформації в автоматизованих системах, методів та засобів управління доступом та розмежування прав користувачів до інформації, прийомів створення й настоювання відповідного програмно-технічного забезпечення для захисту інформаційних ресурсів систем;
- застосування стандартних засобів та алгоритмів побудови програмно-технічного забезпечення для криптографічного захисту особливо важливої інформації та формування необхідної ключової бази шифрування.
- застосування методів та прийомів вирішення аналітичних завдань генерації великий простих чисел, розрахунку ключів та крипостійкості сучасних симетричних й асиметричних систем шифрування та визначення їх базових характеристик.
- застосування методів та протоколів для створення чи ефективного використання засобів ідентифікації та аутентифікації користувачів та їх програм у відкритих каналах зв'язку при організації мереж контрольованої безпечної переді даних.
- застосування механізмів й прийомів розробки та налагодження окремих підсистем попередження вторгнень та комплексів програм для захисту інформації обмеженого доступу в мережах підтримки інформаційних та Web-технологій.

1.3. Результати вивчення навчальної дисципліни

Після засвоєння навчальної дисципліни студенти мають продемонструвати такі результати навчання:

ЗНАННЯ:

- основні концепції створення доказово достатніх систем захисту інформації,
- моделі Adept-50, Белла-Ла-Падули 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, алгоритмів DES, 3-DES, SHA, SSL, RSA, El-Gamal та інших,
- 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 (місце в структурно-логічній схемі навчання за відповідною освітньою програмою)

Міждисциплінарні зв'язки: Навчальна дисципліна відноситься до циклу загальної (базової) підготовки. Дисципліні передують наступні курси: „Дискретна математика", „Архітектура комп'ютерів", "Операційні системи", "Програмування та алгоритмічні мови", "Чисельні методи", "Об'єктно-орієнтоване програмування"; "Операційні системи", "Комп'ютерні системи".

Дисципліною забезпечуються наступні курси: "Автоматизоване проектування комп'ютерних систем", "Комп'ютерні мережі", "Аналіз і управління великими сховищами даних".

3. Зміст навчальної дисципліни

Розділ 1. Вступ.

Тема 1.1 Проблеми захисту інформації в комп'ютерних системах і мережах (КСМ). Поняття несанкціонованого доступу (НСД), вразливості КСМ, загрози вторгнення, каналу витоку інформації.

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. Поняття інформації з обмеженим доступом та системи захисту. Основні напрямки і засоби захисту інформації в КСМ.

Тема 2.2 Моделі систем доказово достатнього захисту інформації. Концептуальна модель Adept-50. Поняття об'єкта і категорії. Модель Деннінга. Поняття домену безпеки. Модель Лендвера. Поняття периметра відповідальності.

Тема 2.3 Матрична модель системи захисту Белла і Ла-Падули. Поняття суб'єкта, вектору прав та диспетчера доступу. Розширення прав доступу.

Тема 2.4. Модель системи моніторингу безпеки КСМ. Поняття фактору загрози та статистичної аномалії. Вектор індикації аномалій.

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 VAX/VMS.

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. Шифр „скитала". Задачі дешифрування та криптоаналіза.

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 за Шенноном. Засоби максимізації ентропії.

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

Тема 6.3 Федеральний стандарт шифрування Data Encryption 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. Приклади.

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

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. Поняття майстер – ключа та змінного - ключа. Протоколи встановлення зв'язку.

Тема 9.2 Встановлення „довіри" суб'єктів на основі асиметричних систем шифрування. Поняття сертифікату відкритого ключа. Протоколи встановлення зв'язку.

Тема 9.3 Встановлення цілісності повідомлень на основі симетричних та асиметричних систем шифрування. Поняття сигнатури повідомлення та 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. Класифікація платіжних карток. 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. Функції майстер-ключа, системного, клієнтського, торгово-касового та сесійного ключів.

Тема 10.4 Електронна торгівля на базі технології Е-бізнеса. Безпека електронних платежів через мережу Інтернет. Протоколи SSL та SET. Ієрархія підписів в довірчих відносинах.

4. Навчальні матеріали та ресурси

4.1. Базова література

1.Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. – К.: BHV, 2009. – 608 с.

2. Остапов С.Е., Валь Л.О. Основи криптографії: навчальний посібник. Чернівці: Книги–XXI, 2008. – 188с.

3. Захист інформації в автоматизованих системах управління : навчальний посібник / Уклад. І. А. Пількевич, Н. М. Лобанчикова, К. В. Молодецька. – Житомир : Вид-во ЖДУ ім. І. Франка, 2015. – 226 с.

4. Логінова Н. І. правовий захист інформації : навчальний посібник / Н. І. Логінова, Р. Р. Дробожур. – Одеса : Фенікс, 2015. – 264 с.

5. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби : посібник / [В. Л. Бурячок, С. В. Толюпа, В. В. Семко та ін.]. – К. : ДУТ-КНУ, 2016. – 178 с

4.2. Допоміжна література

1. Вербіцький О.В. Вступ до криптології. – Львів, НТЛ, 1998. – 248 с.
2. Хорошев В. Базова модель експертної системи оцінки безпеки інформації в комп'ютерних системах. Сб. Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні, вып.3, 2001. с. 86-90.
3. 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.
4. 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.
5. Weissman C. Security Controls in the ADEPT-50 Time Sharing System. // Proceedings AFIPS, FJCC. – 1969. – v. 35. – pp. 119-133.
6. Hartson R., Hsiao D. Full protection specification in the semantic model for database protection languages. // Proceedings Annual Conference ACM. – Houston, New York. – 1976. – pp. 90-95.
7. Harrison M. A.. Russo W. L. Protection in Operating Systems. // Communications of the ACM. – 1976. – v. 19, № 8. – pp. 461-471.

8. Spier M. J. A Model Implementation for protective domains. // International Journal on Computer Information Science. – 1973. – v. 2, № 3. – pp. 201-229.
9. Bell D. E., LaPadula L. J. Secure computer systems: mathematical foundations and model. // M74-244, The MITRE Corp., Bedford, Mass.- May 1973.
10. Bell D. E. Secure computer systems: a refinement of the mathematical model. // Springfield, The MITRE Corp. – 1974. – Report № 2574, pp. 75
11. Graham R. M., Denning P. J. Protection – Principles and Practice. // Proceedings AFIPS. – 1972. – v.40, pp. 417-429.
12. Denning D. E. A Lattice Model of Secure Information Flow. // Communications of the ACM. –1976. – v. 19, № 5. – pp. 236-243
13. Landwehr C., Heitmeyer C., McLean J. A security model for military message systems. // ACM Trans. on Computer Systems. – 1984. – V. 2, № 3. – pp. 198-222.
14. Комплексні системи захисту інформації: проектування, впровадження, супровід. Збірник лекцій [Електронний ресурс] / Гребенніков В.В. // 2015 - Режим доступу: http://www.cryptohistory.ru/for students/ 03-KSZI
15. Операційна система «OpenBSD, шифр BBOS» [Електронний ресурс] / Кампанія «ATMNIS» // 2012 - Режим доступу: http://www.atmnis.com/files/user files/BBOS overview.pdf
16. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. НД ТЗІ 3.7-003-05 [Електронний ресурс] / Нормативна база Держспецзв'язку // 2015 - Режим доступу:http://www.dstszi.gov.ua/dstszi/control/uk/ publish/article?art id=46074
17. Стратегія національної безпеки України (затверджена Указом Президента України від 26 травня 2015 року № 287/2015) 7. Закон України "Про національну безпеку (2018) 8. Стратегія кібербезпеки України" (Введено в дію Указом Президента України від 15 березня 2016 року №96/2016)
18. НД ТЗІ 1.6-004-2013 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що становить державну таємницю.
19. Information Security Handbook for Network Beginners. National Center of Incident Readiness and Strategy for Cybersecurity (NISC) ver. 2.11e

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

5.1. Структура навчальної дисципліни

Назви розділів і тем	Кількість годин				
	Всього	У тому числі			
		Лекції	Практичні (семінар-ські)	Лабора-торні	СРС
Розділ 1. Вступ	**4**	**2**			**2**
Тема 1.1 Проблеми захисту інформації в		1			1

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		1			1
Розділ 2. Комплексний підхід до створення систем захисту інформації в комп’ютерних системах.	**8**	**4**			**4**
Тема 2.1 Нормативно-правова база захисту інформації. Основні напрямки і засоби захисту інформації в КСМ.		1			1
Тема 2.2 Моделі систем доказово достатнього захисту інформації. Концептуальні моделі Adept-50,. Деннінга, Лендвера.		1			1
Тема 2.3 Матрична модель системи захисту Белла і Ла-Падули. Поняття суб’єкта, вектору прав та диспетчера доступу. Розширення прав доступу.		1			1
Тема 2.4. Модель системи моніторингу безпеки КСМ. Поняття фактору загрози та статистичної аномалії.		1			1
Розділ 3. Ідентифікація суб’єктів та управління доступом на основі парольної системи.	**20**	**4**		**12**	**4**
Тема 3.1 Ідентифікація користувачів на основі системи паролів. Вимоги		1		4	1

до паролів. Схема зберігання паролів в ОС Unix.					
Тема 3.2 Аналіз характеристик системи простих паролів. Формула Андерсона. Приклади.		1		2	1
Тема 3.3 Модифікації системи паролів. Підтвердження прав доступу на основі процедури однобічного та двобічного „рукости-скання”.		1		4	1
Тема 3.4 Log-журнали: реєстраційний та операційний. Моніторинг безпеки на основі ведення журналів в ОС Unix та Windows		1		2	1
Розділ 4. Дискретне розмежування доступу суб’єктів к інформації в обмеженій матричній моделі системи захисту.	**4**	**2**			**2**
Тема 4.1 Списки доступу та формування категорій користувачів. Наслідування прав. Замки, ключі та умови доступу в ОС VAX/VMS.		1			1
Тема 4.2 Мандатні списки та реалізація принципу „мінімальних привілей”. Мандатний доступ в ОС Unix.		1			1
Розділ 5. До комп’ютерні підходи щодо криптографічного захисту інформації з обмеженим доступом.	**6**	**4**			**2**

Тема 5.1 Шифрування на основі одно та багато алфавітних підстановок. Поняття шифру і таємного ключа. Шифр Цезаря		1			
Тема 5.2 Шифрування на основі перестановок. Задачі дешифрування та криптоаналізу		1			1
Тема 5.3 Біграмні шифри. Шифр Віжинера та квадрати Уітстона. Шифрувальні машини		1			
Тема 5.4 Потокові шифри з необмеженою довжиною ключа. Шифрування „гамуванням”.		1			1
Розділ 6. Симетричне шифрування в системах зв’язку з відкритими комунікаціями.	**12**	**4**		**4**	**4**
Тема 6.1 Організація передач даних в секретних системах по Шеннону. Засоби максимізації ентропії.		1			1
Тема 6.2 Шифрування на основі чередування перестановок та підстановок. Система Люціфер.		1			1
Тема 6.3 Федеральний стандарт шифрування Data Encryption Standard. (DES). Загальна схема та функція маскування з ключовими словами.		1		2	1
Тема 6.4 Блок управління ключами в DES. Алгоритм 3-DES та чотири режими реалізації		1		2	1

криптографічного захисту на основі DES.					
Розділ 7. Асиметричні системи шифрування на основі відкритих та таємних ключів.	**26**	**6**		**14**	**6**
Тема 7.1 Нове направлення в криптографії по Діффі і Хелману. Незворотні функції в шифруванні. Три схеми та задачі криптозахисту.		1		2	2
Тема 7.2 Система RSA. Модулярна арифметика. Алгоритм швидкого дискретного потенцюювання. Процесор - акселератор RSA.		1		4	2
Тема 7.3. Проблема генерації великих простих чисел (ВПЧ). Тест Рабіна та мала теорема Ферма. Перевірки на простоту.		2		4	1
Тема 7.4. Схеми та алгоритми розрахунків ключів для системи RSA. Класичний та розширений алгоритми Евкліда. Приклади		2		4	1
Контрольна робота з розділів 2 - 7	**2**	**1**			**1**
Розділ 8. Підвищення крипостійкості в асиметричних системах шифрування.	**6**	**3**			**3**
Тема 8.1 Оцінки криптостійкості алгоритму RSA.		1			2

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		2			1
Розділ 9. Аутентифікація суб'єктів та встановлення „довірчого" зв'язку в розподілених системах та мережах.	**16**	**4**		**6**	**6**
Тема 9.1 Встановлення „довіри" суб'єктів на основі симетричних систем шифрування. Протоколи встановлення зв'язку.		1		2	1
Тема 9.2. Встановлення „довіри" суб'єктів на основі асиметричних систем шифрування. Поняття сертифікату відкритого ключа.		1		2	2
Тема 9.3 Встановлення цілісності повідомлень на основі симетричних та асиметричних систем шифрування. Поняття цифрового підпису.		1		2	1
Тема 9.4 Організація „довірчого" зв'язку в протоколах „відкритих замовлень". Поняття електронних чеку та квитанції.		1			2
Розділ 10. Системи електронних платежів. Засоби підвищення „довіри" віртуальних відносин.	**8**	**2**			**6**

Тема 10.1 Пластикові картки як база для організації електронних платежів. Банки – емітенти та банки – еквайєри.		1			1
Тема 10.2 Структура системи електронних платежів. POS- термінали. Функції та організація процесінгового центру.		1			1
Тема 10.3 Багато рівнева організація формування та використання ключів шифрування.					2
Тема 10.4 Електронна торгівля на базі технології Е-бізнеса. Протоколи SSL та SET. Ієрархія підписів в довірчих відносинах.					2
РГР з розділів 1-8	26				26
Підготовка до екзамену	12				12
Екзамен	4				4
Всього в семестрі:	**154**	**36**	**-**	**36**	**82**

5.2. Лекційні заняття

№ з/п	Назва теми лекції та перелік основних питань *(перелік дидактичних засобів, завдання на СРС з посиланням на літературу)*
1	**Проблеми захисту інформації в комп'ютерних системах і мережах (КСМ)**. 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. [1, с.56-57 ; 2, с. 63-68]
2	**Нормативно-правова база захисту інформації.** Поняття інформації з обмеженим доступом та системи захисту. Основні напрямки і засоби захисту інформації в КСМ. Моделі систем доказово достатнього захисту інформації. Концептуальна модель Adept-50. Поняття об'єкта і категорії. Модель Деннінга. Поняття домену безпеки. Модель Лендвера. Поняття периметра відповідальності. [3, с. 31-33 ; 2, с. 53-54, 74-77, 121-122]

3	**Матрична модель системи захисту Белла і Ла-Падули.** Поняття суб'єкта, вектора прав та диспетчера доступу. Розширення прав доступу. Модель системи моніторингу безпеки КСМ. Поняття фактору загрози та статистичної аномалії. Вектор індикації аномалій. [1, с.78-84, 58-62 ; 2, с. 69-73, 90-92, 117-120]
4	**Ідентифікація користувачів на основі системи паролів.** Вимоги до паролів. Схема зберігання паролів в ОС Unix. Аналіз характеристик системи простих паролів. Формула Андерсона. Приклади. [1, с 65-70. ; 2, с. 104-107].
5	**Модифікації системи паролів.** Підтвердження прав доступу на основі процедури однобічного та двобічного „рукостискання". Log-журнали: реєстраційний та операційний. Моніторинг безпеки на основі ведення журналів в ОС Unix та Windows. [1, с. 71-72 ; 2, с. 108-112].
6	**Списки доступу та формування категорій користувачів.** Наслідування прав. Замки, ключі та умови доступу в ОС VAX/VMS. Мандатні списки та реалізація принципу „мінімальних привілей". Мандатний доступ в ОС Unix. [1, с117-123. ; 2, с. 134-138].
7	**Шифрування на основі одно та багато алфавітних підстановок.** Поняття шифру і таємного ключа. Шифр Цезаря. Шифрування на основі перестановок. Шифр „скитала". Задачі дешифрування та криптоаналізу. [1, с.78-84, 58-62 ; 2, с. 69-73, 90-92, 117-120].
8	**Біграмні шифри.** Шифр Віжинера та квадрати Уітстона. Шифрувальні машини. Потокові шифри з необмеженою довжиною ключа. Шифрування „гамуванням". [3, с. 31-33 ; 2, с. 53-54, 74-77, 121-122].
9	**Організація передач даних в секретних системах по Шеннону.** Засоби максимізації ентропії. Шифрування на основі чередування перестановок та підстановок. Система Люціфер. [1, с 65-70. ; 2, с. 104-107].
10	**Федеральний стандарт шифрування Data Encryption Standard. (DES).** 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. [1, с. 71-72 ; 2, с. 108-112].
11	**Нове направлення в криптографії по Діффі і Хелману.** Незворотні функції в шифруванні. Три схеми та задачі криптозахисту. Система RSA. Модулярна арифметика. Алгоритм швидкого дискретного потенціювання. Процесор - акселератор RSA. [1, с117-123. ; 2, с. 134-138].
12	**Проблема генерації великих простих чисел (ВПЧ).** Тест Рабіна та мала теорема Ферма. Перевірки на простоту. Приклади. [1, с.71-72 ; 2, с. 108-112].
13	**Схеми та алгоритми розрахунків ключів для системи RSA.** Класичний та розширений алгоритми Евкліда. Приклади. [1, 134-136с.].
14	**Оцінки криптостійкості алгоритму RSA.** Порівняння з схемами DES та 3-DES. Приклади. [1, с.78-84, 58-62 ; 2, с. 69-73, 90-92, 117-120].
15	**Система шифрування Ель-Гамаля.** Схеми та алгоритми розрахунків ключів для системи Ель-Гамаля. Приклади шифрування та дешифрування.. [3, с. 31-33 ; 2, с. 53-54, 74-77, 121-122].

16	**Встановлення „довіри” суб’єктів на основі симетричних систем шифрування.** 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. [1, с 65-70. ; 2, с. 104-107].
17	**Встановлення цілісності повідомлень на основі симетричних та аси-метричних систем шифрування.** Поняття сигнатури повідомлення та циф-рового підпису. Організація „довірчого” зв’язку в протоколах „відкритих за-мовлень”. Поняття електронних чеку та квитанції.[1, с. 71-72 ; 2, с. 108-112].
18	**Оцінки криптостійкості алгоритму RSA.** Порівняння з схемами DES та 3-DES. Приклади. Структура системи електронних платежів. POS- термінали. Функції та організація процесінгового центру. [1, с.78-84, 58-62 ; 2, с. 69-73, 90-92, 117-120].

5.3. Лабораторні заняття

Метою проведення циклу лабораторних робіт є придбання 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 під ОС Linux, Windows, FreeBSD з застосуванням мов Java, C, C++, Python для дослідження механізмів захисту в автоматизованих системах різного призначення.

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,
- інтерпретація результатів та висновки,
- листінг програми.
- результати виконання модельних експериментів
- інтерпретація результатів моделювання та висновки,
- листінг програми.

№ з/п	Назва лабораторної роботи	Кількість ауд. годин
1	Розробка та дослідження програмної підсистеми дискретного управління доступом до окремого носія інформації з складною структурою каталогів.	2
2	Програмування та дослідження підсистеми ідентифікації користувачів на основі простих паролів з контролем вимог та супроводженням журналів.	2

3	Програмування та дослідження підсистеми аутентифікації користувачів під час роботи з використанням „питань-відповідей” та таємних функцій.	2
4	Програмування та дослідження підсистеми моніторингу для виявлення аномалій та небезпечних подій щодо інформації, яка захищається.	2
5	Розробка програмного макету для дослідження та покрокової верифікації алгоритмів генерації великих простих чисел з формуванням бази даних ВПЧ**.**	2
6	Розробка програмного макету для дослідження та покрокової верифікації RSA - підсистеми управління ключами, шифрування та дешифрування повідомлень**.**	2
7	Розробка програмного макету для дослідження та покрокової верифікації RSA - підсистеми управління ключами, шифрування та дешифрування повідомлень**.**	2
8	Розробка програмного макету для дослідження та покрокової верифікації DES - підсистеми формування сигнатур, шифрування та дешифрування повідомлень.	2

6. Самостійна робота здобувача вищої освіти

№ з/п	Назви тем і питань, що виноситься на самостійне опрацювання та посилання на навчальну літературу	Кількість годин СРС
1	Провести порівняльний аналіз параметрів каналів витоку інформації [1, с.56-57 ; 2, с. 63-68]	6
2	Дослідити структури моделей Adept-50 і Деннінга. [3, с. 31 - 33 ; 2, с. 53-54, 74-77, 121-122].	6
3	Дослідити структури моделей Белла і Ла-Падули. [1, с.78-84, 58-62 ; 2, с. 69-73, 90-92, 117-120].	6
4	Особливості реалізації процедури паролів в ОС Unix. [1, с 65-70. ; 2, с. 104-107].	6
5	Провести аналіз засобів моніторингу безпеки на основі ведення журналів в ОС Unix та Windows. [1, с. 71-72 ; 2, с. 108-112].	6
6	Дослідити особливості побудови мандатних списків та принципу „мінімальних привілей”. [1, с117-123; 2, с. 134-138].	6
7	Розробити алгоритм реалізації шифрування на основі перестановок. [1, с.78-84, 58-62 ; 2, с. 69-73, 90-92, 117-120].	6
8	Розробити алгоритм реалізації потокового шифрування з необмеженою довжиною ключа на основі перестановок. [3, с. 31-33 ; 2, с. 53-54, 74-77, 121-122].	4
9	Розробити алгоритм реалізації шифрування на основі чередування перестановок та підстановок[1, с 65-70. ; 2, с. 104-107].	4

10	Розробити алгоритм реалізації блоку управління ключами в DES. [1, с. 71-72 ; 2, с. 108-112].	4
11	Розробити структуру процесору шифрування за системою RSA. [1, с117-123. ; 2, с. 134-138].	4
12	Розробити алгоритм реалізації генерації великих простих чисел (ВПЧ). [1, с. 71-72 ; 2, с. 108-112].	4
13	Розробити алгоритм реалізації розрахунків ключів для системи RSA. [1, 134-136с.]	4
14	Провести порівняльний аналіз криптостійкості алгоритмів RSA та DES. [1, с.78-84, 58-62 ; 2, с. 69-73, 90-92, 117-120]	4
15	Розробити алгоритм реалізації шифрування Ель-Гамаля. [3, с. 31-33 ; 2, с. 53-54, 74-77, 121-122].	4
16	Провести порівняльний аналіз протоколів встановлення зв'язку. та встановлення „довіри" суб'єктів на основі асиметричних систем шифрування [1, с 65-70. ; 2, с. 104-107]	4
17	Розробити алгоритм реалізації встановлення цілісності повідомлень на основі симетричних та асиметричних систем шифрування. [1, с. 71-72 ; 2, с. 108-112].	4
18	Розробити структурну схеми підтримки системи електронних платежів. [1, с.78-84, 58-62 ; 2, с. 69-73, 90-92, 117-120].	4

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

Застосовуються наступні вимоги до здобувачів:

- відвідування занять, як лекцій, так і лабораторних є обов'язковим;
- враховується активність на лекціях;
- лабораторні роботи повинні бути захищені персонально і в чітко визначені терміни;
- застосовується політика щодо академічної доброчесності, всі лабораторні роботи повинні бути виконані персонально з можливою перевіркою на плагіат
- додатково можуть застосовуватись інші вимоги, що не суперечать законодавству України та нормативним документам Університету.

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

Поточний контроль: експрес-опитування, опитування за темою заняття, МКР
Календарний контроль: провадиться двічі на семестр як моніторинг поточного стану виконання вимог Силабусу.
Семестровий контроль: залік
Умови допуску до семестрового контролю: зарахування усіх лабораторних робіт та семестровий рейтинг не менше ніж 30 балів.

Рейтинг студента з дисципліни складається з балів, що отримуються за наступне:

1. Дві відповіді при лекційному опитуванні змісту попередньої лекції.

2. Виконання 1-ї контрольної роботи.

Система рейтингових (вагових) балів та критерії оцінювання

1. Поточний контроль засвоєння лекційного матеріалу

Ваговий бал - 2. Максимальна кількість балів на всіх лекціях дорівнює 2 бали *9 = 18 балів.

2. Виконання контрольної роботи.

Ваговий бал – 42 (максимально можливий).

Штрафні бали за:

- відсутність на лекції або лабораторному занятті без поважної причини - 1 бал.

Умови позитивної проміжної атестації

Календарна атестація студентів (на 8 та 14 тижнях семестру) проводиться викладачем за значенням поточного рейтингу студента на час атестації. Для отримання "зараховано" з першої проміжної атестації (8-ий тиждень) студент повинен мати не менше ніж 25 балів. Для отримання "зараховано" з другої проміжної атестації (14-ий тиждень) повинен мати не менше ніж 50 балів.

До іспиту допускаються студенти, у яких зараховані всі лабораторні роботи, а також значення R > 30 (30% від R).

Розрахунок шкали (R) рейтингу:

Сума вагових балів контрольних заходів протягом семестру складає:

R=18+42= 60 балів.

Атестація проводиться за поточним рейтингом студента. Якщо поточний рейтинг складає не менше 50% від максимально можливого на цей момент, студент вважається атестованим.

Всі студенти повинні з'явитись на залік незалежно від набраного рейтингу. Оцінку на заліку студенти отримують згідно таблиці:

R	Оцінка ECTS	Оцінка традиційна
95...100	A	Відмінно
85..94	B	Добре
75...84	C	Добре
65...74	D	Задовільно
60...64	E	Задовільно
R < 60	FX	Незадовільно
R < 30	F	Недопущений

Якщо студент отримав за рейтингом R< 30 балів (менш ніж 30% від R) і по початку заліку виконав необхідну додаткову роботу (підвищив свій рейтинг), то він допускається до заліку.

Ваговий бал за залік R складає **40 балів** і одержується за наступне:

1. Відповідь на 2 теоретичні питання оцінюються максимально в 20 балів по 10 балів за кожну вірну відповідь.

2. Відповідь на 2 практичних питання оцінюється максимально в 20 бали по 10 балів за кожну вірну відповідь.

9. Додаткова інформація з дисципліни (освітнього компонента)

Перелік основних питань, які виносяться на семестровий контроль:

1. Проблеми захисту інформації та периметр відповідальності механізмів захисту в комп'ютерних системах та мережах.

2. Основні напрямки загроз та каналів витоку інформації в комп'ютерних системах та мережах.

3. Моделі систем захисту інформації в конституційному суді. Модель Белла та Ла-Падула та її впровадження в комп'ютерних системах.

4. Основні напрями захисту інформації та безпеки комп'ютерних систем.

5. Моніторинг моделі комп'ютерної системи на основі алгоритму найбільших статистичних аномалій (АНСА).

6. Ідентифікація користувача на основі системи простих паролів.

7. Модифікація системи простих паролів.

8. Реєстраційні та операційні журнали та їх роль у системах захисту інформації.

9. Шифрування на основі одно-абеткових підстановок. Шифр Цезаря.

10. Федеральний стандарт США для симетричних систем шифрування.

11. Асиметричні системи шифрування на основі відкритих та закритих ключів. Алгоритм Аль-Гамала.

12. Асиметричні системи шифрування на основі відкритих та закритих ключів. Алгоритм RSA.

13. Цифрові підписи та протоколи аутентифікації для симетричних систем шифрування.

14. Протоколи аутентифікації суб'єктів та встановлення комунікації в мережах на основі використання лише закритих ключів.

15. Встановлення справжності суб’єктів у мережах на основі використання алгоритму шифрування RSA.

16. Аутентифікація суб'єктів у мережах за допомогою відкритих ключів.

17. Підтвердження справжності повідомлень у мережах на основі використання цифрових підписів.

18. Управління ключами шифрування у захисті POS-терміналів та банкоматів у режимі реального часу та в режимі он-лайн.

19. Узагальнена структура електронної платіжної системи

20. Вимоги щодо захисту суб’єктів від несанкціонованого доступу відповідно до критеріїв доступності та спостережності

21. Загальні підходи та методи забезпечення безпеки комп'ютерних систем

Робочу програму навчальної дисципліни (силабус):

Складено завідуючий кафедрою системного проектування, доктор технічних наук, професор Мухін Вадим Євгенійович

Ухвалено кафедрою штучного інтелекту (протокол № ___ від _____)

Погоджено Методичною комісією НН ІПСА (протокол № ___ від _____)