

**КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ НАУК ТА КІБЕРНЕТИКИ
КАФЕДРА ІНТЕЛЕКТУАЛЬНИХ ПРОГРАМНИХ СИСТЕМ**

«ЗАТВЕРДЖУЮ»

Заступник декана
з навчальної роботи

_____ Кашпур О.Ф.

«__» _____ 2019 року

**РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
АКТУАЛЬНІ ПИТАННЯ ЗАХИСТУ
ІНФОРМАЦІЇ
для студентів**

галузь знань	12 Інформаційні технології
спеціальність	121 Інженерія програмного забезпечення
освітній рівень	магістр
освітня програма	Програмне забезпечення систем
спеціалізація	Програмне забезпечення систем
вид дисципліни	вибіркова

Форма навчання	денна
Навчальний рік	2019/2020
Семестр	4
Кількість кредитів ECTS	5
Мова викладання, навчання та оцінювання	українська
Форма заключного контролю	іспит

Викладач: **к. ф.-м. н., асистент Ходзінський О.М.** (лекції).

Пролонговано: на 20__/20__ н. р. _____ (_____) «__» __ 20__ р.

на 20__/20__ н. р. _____ (_____) «__» __ 20__ р.

Розробник: Ходзінський Олександр Миколайович к. ф.-м. н., с. н. с., асистент кафедри інтелектуальних програмних систем.

ЗАТВЕРДЖЕНО

Завідувач кафедри інтелектуальних програмних систем

_____ О.І. Провотар

Протокол № __ від «__» _____ 2019 р.

Схвалено науково-методичною комісією факультету комп'ютерних наук та кібернетики

Протокол від «__» _____ 2019 року №__

Голова науково-методичної комісії _____ Л.Л. Омельчук

«__» _____ 2019 року

Затверджено вченою радою факультету комп'ютерних наук та кібернетики

Протокол від «__» _____ 2019 року №__

Голова вченої ради факультету _____ А.В. Анісімов

1. Мета дисципліни – засвоєння знань про сучасні розробки в галузі інформаційної безпеки програмних систем.

2. Попередні вимоги до опанування або вибору навчальної дисципліни. Для успішного вивчення дисципліни «Актуальні проблеми захисту інформації» студенти повинні відповідати наступним вимогам:

1. **Знати:** основні поняття з базового курсу «Дискретна математика», Курсу «Математичні основи захисту інформації».
2. **Вміти:** проектувати і досліджувати алгоритми розв'язування задач, пов'язаних з контролем доступу до інформації.
3. **Володіти навичками:** використання персональної комп'ютерної техніки.

Для засвоєння курсу необхідні знання дискретної математики, алгебри, теорії алгоритмів, програмування. Студент повинен знати основи теорії множин, булевих функцій, основи загальної алгебри, основи математичної логіки і теорії алгоритмів.

3. Анотація навчальної дисципліни. Навчальна дисципліна «Актуальні проблеми захисту інформації» є складовою освітньо-наукової програми підготовки фахівців за другим (магістерським) рівнем вищої освіти у галузі знань 12 Інформаційні технології за спеціальністю 121 Інженерія програмного забезпечення в рамках освітньо-наукової програми «Програмне забезпечення систем».

Дана дисципліна є навчальною дисципліною вільного вибору студентів в рамках блоку спеціалізації «Програмне забезпечення систем». Викладається у **2 семестрі в обсязі – 150 год. (5 кредитів ECTS)**, зокрема: лекції – 34 год., самостійна робота – 114 год., консультації – 2 год. В курсі передбачено 2 змістовні частини та 2 контрольні роботи. Завершується дисципліна – **іспитом**.

Предмет навчальної дисципліни включає в себе розгляд прикладів застосування методів захисту інформації в різних областях людської діяльності. В результаті вивчення навчальної дисципліни студенти повинні:

знати: основні загрози витоку та пошкодження інформації в інформаційних системах та методи боротьби з цими загрозами;

вміти: визначати типи загроз підбирати відповідні способи їх попередження та усунення.

Навчальна дисципліна «Актуальні проблеми захисту інформації» є логічним продовженням нормативного курсу «Математичні основи захисту інформації», «Теоретичні основи та методи розробки інформаційних систем», «Алгебро-автоматні методи проектування програмного забезпечення».

4. Завдання (навчальні цілі). Основними завданнями дисципліни «Актуальні проблеми захисту інформації» є набуття знань, умінь та навичок (компетентностей) на рівні новітніх досягнень в області захисту інформації відповідно до освітньої кваліфікації магістр з інженерії програмного забезпечення за спеціалізацію «Інтелектуальні програмні системи». Зокрема, розвивати:

- Здатність до абстрактного мислення, аналізу та синтезу (ЗК-1).
- Здатність проведення теоретичних та прикладних досліджень на відповідному рівні (ЗК-3).
- Здатність аналізувати предметні області, формувати, аналізувати та моделювати вимоги до програмного забезпечення (СК-1).

- Здатність проектувати програмне забезпечення, включаючи проведення моделювання його архітектури, поведінки та процесів функціонування окремих підсистем і модулів (СК-3).
- Вміння планувати і проводити наукові дослідження, готувати результати наукових робіт з інженерії програмного забезпечення до оприлюднення (СК-9).
- Здатність до алгоритмічного та логічного мислення (СК-11.1).

5. Результати навчання за дисципліною.

Результат навчання (1. знати; 2. вміти; 3. комунікація; 4. автономність та відповідальність)		Форми (та/або методи і технології) викладання і навчання	Методи оцінювання та пороговий критерій оцінювання (за необхідності)	Відсоток у підсумковій оцінці з дисципліни
Код	Результат навчання			
РН1.1	Знати основні області використання інформаційних систем.	Лекції.	Контрольна робота № 1, іспит.	15%
РН1.2	Знати основні типи загроз в інформаційних системах.	Лекції.	Контрольні роботи № 1, №2, іспит.	20%
РН1.3	Знати основні сучасні методи контролю доступу до інформації в програмних системах.	Лекції.	Контрольна робота № 2, іспит.	15%
РН2.1	Вміти застосовувати на практиці методи забезпечення інформаційної безпеки в інформаційних системах.	Лекції.	Контрольні роботи № 1, №2, іспит.	24%
РН3.1	Погодження проектних рішень в колективі, користуючись методами аналізу загроз інформаційній безпеці та способами їх усунення.	Лекції.	Іспит.	10%
РН4.1	Самостійно використовувати тестування для пошуку помилок в системі, що розробляється.	Лекції.	Іспит.	8%
РН4.2	Відповідально ставитися до виконуваних робіт, нести відповідальність за їх якість.	Лекції.	Іспит.	8%

6. Співвідношення результатів навчання дисципліни із програмними результатами навчання.

Програмні результати навчання	Результати навчання дисципліни						
	РН1.1	РН1.2	РН1.3	РН2.1	РН3.1	РН4.1	РН4.2
ПРН-1. Знати і системно застосовувати методи аналізу та моделювання прикладної області, виявлення інформаційних потреб і збору вихідних даних для проектування програмного забезпечення.	+	+					
ПРН-3. Знати і застосовувати базові концепції і методології моделювання інформаційних процесів.				+			
ПРН-8. Проводити аналітичне дослідження параметрів функціонування програмних систем для їх валідації та верифікації, а також проводити аналіз обраних методів, засобів автоматизованого проектування та реалізації програмного забезпечення.					+	+	
ПРН-14. Пояснити, аналізувати, цілеспрямовано шукати і обирати необхідні для вирішення фахових наукових і прикладних задач інформаційно-довідкові та науково-технічні ресурси і джерела знань з урахуванням сучасних досягнень науки і техніки.	+	+	+				
ПРН-15.1. Знати та кваліфіковано застосовувати засоби забезпечення інформаційної безпеки і цілісності даних відповідно до створюваних програмних систем.							+

7. Схема формування оцінки.

7.1 Форми оцінювання студентів.

Семестрове оцінювання:

1. Контрольна робота 1: РН1.1, РН1.2, РН2.1 – **30 балів/15 балів.**
2. Контрольна робота 2: РН1.2, РН1.3, РН2.1 – **30 балів/15 балів.**

Підсумкове оцінювання (у формі іспиту):

- Максимальна кількість балів які можуть бути отримані студентом: 40 балів/24 бали.
- Результати навчання які будуть оцінюватись: РН1.1, РН1.2, РН1.3.
- Форма проведення і види завдань: письмова робота.
- Види завдань 4 письмових завдання.

Критерії оцінювання на іспиті.

Завдання	Тема завдання	Максимальний відсоток від 40 балів	Всього відсотків
Завдання 1-4	Задача на знання типів інформаційних загроз та методів їх попередження і усунення.	По 25%	100%

			100%
--	--	--	-------------

Студенти не допускаються до іспиту, якщо під час семестру вони набрали менше ніж 20 балів та/або не виконали хоча б 70% передбачених планом лабораторних робіт.

Питання для підготовки до іспиту.

1. Класифікація платіжних карток. Основні відмінності карток з магнітною смугою та смарт-карток.
2. Захист секретної інформації платіжних карток. Алгоритми Луна та IBM 3624 PIN offset.
3. Захист секретної інформації платіжних карток. Алгоритми Visa PVV та генерації CVV-коду.
4. Різновиди шахрайства з банківськими картками та заходи щодо їх запобігання.
5. Додаткові рівні безпеки операцій з платіжними картками. Технології DCV та 3DSecure.
6. Поняття системи «Клієнт-банк». Схема виконання платежу в системі «Клієнт-банк».
7. Класифікація систем «Клієнт-банк».
8. Засоби захисту транзакцій в системі клієнт-банк.
9. Різновиди атак на систему клієнт-банк.
10. Захист від атак на систему клієнт-банк.
11. Дайте формальне визначення терміну БПЛА, та його класифікацію.
12. Назвіть основні проблеми захисту передачі комунікаційних сигналів до БПЛА.
13. Які є стандарти захисту передачі даних для БПЛА.
14. Які є цивільні напрями застосування БПЛА
15. Які є методи захисту каналу передачі даних БПЛА
16. Біометрія. Ідентифікація особи. Роль ока в ідентифікації
17. Сканування сітківки. Переваги та недоліки
18. Історія розвитку сканування сітківки
19. Фази процесу розпізнавання сітківки
20. Порівняння сканування сітківки та райдужної оболонки ока
21. Структура даних «блокчейн» – ідея та недоліки.
22. Поняття консенсусу. Види консенсусу. PoW, BFT (PoS) консенсуси.
23. Порівняння PoW і PoS консенсусів, недоліки.
24. Bitcoin blockchain. Історія, реалізація, вид консенсусу, спосіб добичі ресурсу.
25. Ethereum blockchain. Історія, реалізація, вид консенсусу, спосіб добичі ресурсу.
26. Які класи алгоритмів застосовують при порівнянні відбитків пальців?
27. Які є недоліки методу ідентифікації за відбитками пальців?
28. Забезпечення біометричних пристроїв та їх технічна реалізація.
29. Що впливає на процес ідентифікації за відбитками пальців?
30. Як визначаються мініатюри на відбитках?

7.2 Організація оцінювання.

Терміни проведення форм оцінювання:

1. Контрольна робота 1: до 2 тижня семестру.
2. Контрольна робота 2: до 4 тижня семестру.

Студент має право на одне перескладання кожної контрольної роботи із можливістю отримання максимально 80% початково визначених за цю контрольну роботу балів. Термін перескладання визначається викладачем.

У випадку відсутності студента з поважних причин відпрацювання та перездачі контрольних робіт здійснюються у відповідності до „Положення про порядок оцінювання знань студентів при кредитно-модульній системі організації навчального процесу” від 1 жовтня 2010 року.

У разі неякісного виконання лабораторної роботи, викладач має право не зарахувати лабораторну роботу, або знизити за неї бали.

Студент має право здавати лабораторні роботи після закінчення визначеного для них терміну, але з втратою одного балу за кожен тиждень, який пройшов з моменту закінчення терміну її здачі.

7.3 Шкала відповідності оцінок.

Відмінно / Excellent	90-100
Добре / Good	75-89
Задовільно / Satisfactory	60-74
Незадовільно / Fail	0-59

1. Структура навчальної дисципліни. Тематичний план лекцій.

№ лекції	Назва лекції	Кількість годин	
		Лекції	Самостійна робота
Частина 1. Захист інформації у платіжних системах.			
1	Тема 1. Платіжні картки та їх різновиди.	2	8
2	Тема 2. Захист секретної інформації платіжних карток.	2	8
3-4	Тема 3. Різновиди шахрайства з банківськими картками та заходи щодо їх запобігання.	4	8
5	Тема 4. Додаткові рівні безпеки операцій з платіжними картками.	2	8
6-7	Тема 5. Основні положення клієнт-банку. Класифікація.	4	8
8	Тема 6. Різновиди атак на систему клієнт-банк.	2	8
Контрольна робота № 1			2
Всього по частині 1		16	50
Частина 2. Захист інформації у кібер-фізичних та криптосистемах.			
9-11	Тема 7. Захист інформації при керуванні БПЛА. Класифікація і призначення БПЛА. Методи локалізації за допомогою радіозв'язку. Алгоритми планування шляху покриття. Реалізація безпеки передачі командних сигналів до БПЛА.	6	20
12-14	Тема 8. Біометрія. Ідентифікація за біологічними характеристиками. Будова ока. Сітківка. Сканування сітківки. Історія та особливості. Відкриті бази даних, де зібрані знімки сітківки, серед яких DRIVE , STARE та VARIA .	6	22
15-17	Тема 9. Криптогроші. Ознайомлення з технологією	6	20

	«блокчейн» на прикладі конкретної розробки.		
Контрольна робота № 2			2
Всього по частині 2	18		64
Консультація	2		
ВСЬОГО	34		114

Загальний обсяг годин – **150** год., у тому числі:

Лекції – **34** год.

Самостійна робота – **114** год.

Консультації – **2** год.

Теми, винесені на самостійне вивчення.

1. Класифікація платіжних карток.
2. Основні відмінності карток з магнітною смугою та смарт-карток.
3. Алгоритми Луна та IBM 3624 PIN offset.
4. Алгоритми Visa PVV та генерації CVV-коду.
5. Різновиди шахрайства з банківськими картками та заходи щодо їх запобігання.
6. Додаткові рівні безпеки операцій з платіжними картками.
7. Технології DCV та 3DSecure.
8. Поняття системи «Клієнт-банк».
9. Схема виконання платежу в системі «Клієнт-банк».
10. Класифікація систем «Клієнт-банк».
11. Засоби захисту транзакцій в системі клієнт-банк.
12. Різновиди атак на систему клієнт-банк. Захист від атак на систему клієнт-банк.
13. Сканування сітківки. Історія розвитку сканування сітківки. Фази процесу розпізнавання сітківки. Порівняння сканування сітківки та райдужної оболонки ока.
14. Розібратися в документі «Керівництво користувача програмним продуктом Aeneas Sanctum (wallet app) v1.1.0 for (Windows 10)»
15. Використовуючи навчальні матеріали (https://dev.px4.io/en/apps/hello_sky.html, <https://dev.px4.io/en/simulation/>) виконати наступні завдання:
 1. Симулювати на схемі ArduPlane v 2.76 льотну фігуру Acro
 2. Симулювати на схемі ArduPlane v 2.76 льотну фігуру Alt Hold
 3. Симулювати на схемі ArduPlane v 2.76 льотну фігуру AutoTune
 4. Симулювати на схемі ArduCopter v 3.0.1 Quad льотну фігуру Brake
 5. Симулювати на схемі ArduCopter v 3.0.1 Quad льотну фігуру Circle
 6. Симулювати на схемі ArduCopter v 3.0.1 Quad льотну фігуру Drift

9. Рекомендовані джерела.

Основні:

1. «Історія впровадження платіжних карток».
http://dengi.polnaya.info/platezhnye_sistemy/evoluciya_deneg/
2. Стандарти ISO7810, ISO7811-2, ISO7811-6.
3. «Cryptographic properties of the CVV».
https://ctcrypt.ru/files/files/2017/02_Ahmetzyanova_Alekseev_Karpunin_Smyshlyaev.pdf

4. «ТОП-5 схем воровства денег с банковских карт»
<https://finance.rambler.ru/money/38969868-eksperty-sostavili-top-5-shem-vorovstva-deneg-s-bankovskih-kart/?updated>
5. «Платежные карты: Бизнес-энциклопедия» <https://coollib.com/b/188439/read#t43>
6. Сітківка – Wikipedia [online]. <https://uk.wikipedia.org/wiki/Сітківка19>
7. Rahib HA, Altunkaya K. Neural network based biometric personal identification with fast iris segmentation. International Journal of Control Automation and Systems 2009; Volume 7. No.1.
8. JDN 2/11 (2011). «Точка зору Великої Британії на безпілотні авіаційні системи» (The UK approach to unmanned aircraft systems). Публікація МО Великої Британії Joint Doctrine Note 2/11, dated 30 March 2011. (англ.)
9. DOD-USRM-2013 (2013). «Інтегрована дорожня карта щодо систем без людини на борту на 2013 – 2038 фінансові рр.» (Unmanned Systems Integrated Roadmap FY2013 – 2038). Публікація Департаменту оборони США. (англ.)
10. Bitcoin: A Peer-to-Peer Electronic Cash System Satoshi Nakamoto
11. Блокчейн. Как это работает и что ждет нас завтра Артем Генкин, Алексей Михеев, Альпина Паблицер, 2018.

Додаткові:

1. Панасенко С. Алгоритмы шифрования. Специальный справочник. – СПб: БХВ-Петербург, 2009 – 576 с.
2. Алешко Р.А., Гурьев А.Т. Структурное моделирование взаимосвязей дешифровочных признаков спутниковых снимков и таксационных параметров лесных насаждений // Труды СПИИРАН. Вып. 29 (2013). С. 180-189.
3. Р.А. Алешко, А.Т. Гурьев, К.В. Шошина, В.С. Щеников Разработка методики визуализации и обработки геопространственных данных // Научная визуализация. – 2015. – №1. – С. 20-29.
4. Земор Ж. Курс криптографии. – М: Регулярная и хаотическая динамика, Институт компьютерных исследований, 2006 – 256 с.
5. The Age of Cryptocurrency: How Bitcoin and the Blockchain Are Challenging the Global Economic Order Paul Vigna, Michael Casey, 2014.
6. Blockchain: The Simple Guide to Everything You Need to Know Jacob William, 2016
7. Bitcoin Basics: 101 Questions and Answers Eric Sammons, 2015.
8. Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World (Don Tapscott, Alex Tapscott).
9. Ethereum Builder's Guide.
10. Decentralized Applications (Siraj Raval).
11. Roger Wattenhofer. «The Science of the Blockchain».