ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«ПРИДНІПРОВСЬКА ДЕРЖАВНА АКАДЕМІЯ БУДІВНИЦТВА ТА АРХІТЕКТУРИ»

Кафедра комп'ютерних наук, інформаційних технологій та прикладної математики

«ЗАТВЕРДЖУЮ»
Проректор з науково-педагогічної
та навчальної роботи
_____ Р. Б. Папірник

«_01_» _____ 2020 року

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
Технології захисту інформації

спеціальність	122 «Комп'ютерні науки»
освітньо-професійна програма	«Комп'ютерні науки»
освітній ступінь	бакалавр
форма навчання	денна
розробник	Ільєв Ілля Маркович

1. АНОТАЦІЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Навчальна дисципліна «Технології захисту інформації» є нормативною компонентою циклу загальної підготовки бакалаврів за спеціальністю 122 «Комп'ютерні науки». Викладання дисципліни забезпечує формування у фахівців комплексу професійних знань, вмінь та навичок розробки захищених веб-додатків. Знання основ захисту систем передачі даних, навички адміністрування мережі.

2. ЗМІСТ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

	Години	Кредити	Семестр
			VII
Всього годин за навчальним планом, з них:	105	3,5	105
Аудиторні заняття, у т.ч:	46		46
лекції	30		30
лабораторні роботи	16		16
практичні заняття			
Самостійна робота, у т.ч:	59		59
підготовка до аудиторних занять	15		15
підготовка до контрольних заходів	4		4
виконання курсового проекту або роботи			
опрацювання розділів програми, які не викладаються на лекціях	10		10
підготовка до екзамену	30		30
Форма підсумкового контролю			Екзамен

3. СТИСЛИЙ ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Мета дисципліни - формування у студентів системи теоретичних знань і придбання практичних умінь і навичок з теоретичної бази знань в області автоматизації розробки захищених веб-додатків з доступом до баз даних, так і практичних навичок ефективного їх використання; розвиток вміння впроваджувати системи інтелектуальної обробки даних в задачах системного аналізу і управління, та системах підтримки прийняття рішень; формування навичок в області управління IT-проектами, проведення стратегічного аналізу, управління якістю та вартістю в IT-проектах.

Завдання дисципліни - формування уявлення про концепції, принципи і моделях, вивчення теоретичних основ та одержання практичних навичок на прикладі деяких інструментальних програмних систем; оволодіння основними прийомами й придбання практичних навичок застосування технічних і програмних засобів. Навчити студента методиці самостійної роботи при підготовці до занять та підсумкового контролю знань.

Пререквізити дисципліни. Система знань, що формується на базі знань наступних дисциплін «Архітектура та проектування програмного забезпечення», «Комп'ютерні мережі».

Постреквізити дисципліни. Знання з даної дисципліни використовуються при вивченні наступних дисциплін циклу професійної підготовки «Технології комп'ютерного проектування», «Веб-технології та веб-дизайн», а також в подальшій професійній діяльності.

Компетентності.

Інтегральна компетентність:

Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у сфері комп'ютерних наук або у процесі навчання, що передбачає застосування теорій та методів інформаційних технологій і характеризується комплексністю та невизначеністю умов.

Загальні компетентності:

ЗК-3. Знання та розуміння предметної області та розуміння професійної діяльності.

ЗК-6. Здатність вчитися і оволодівати сучасними знаннями.

ЗК-7. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

Спеціальні компетентності:

СК-1. Здатність до математичного та логічного мислення, формулювання та досліджування математичних моделей, зокрема дискретних математичних моделей, обґрунтовування вибору методів і підходів для розв'язування теоретичних і прикладних задач в галузі комп'ютерних наук, інтерпретування отриманих результатів.

СК-4. Здатність опанувати сучасні технології математичного моделювання об'єктів, процесів і явищ, розробляти обчислювальні моделі та алгоритми чисельного розв'язання задач математичного моделювання з урахуванням похибок наближеного чисельного розв'язання професійних задач.
СК-14. Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти та експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури.

Заплановані результати навчання:

РН-1. Здобувати систематичні знання в галузі комп'ютерних наук, аналізувати проблеми з точки зору сучасних наукових парадигм, осмислювати і робити обґрунтовані висновки з наукової і навчальної літератури та результатів експериментів
РН-2. Реалізовувати засвоєні поняття, концепції, теорії та методи в інтелектуальній і практичній діяльності в галузі комп'ютерних наук, осмислювати зміст і послідовність застосування способів виконання дій, узагальнювати і систематизувати результати робіт.
РН-14. Використовувати формальні моделі алгоритмів та обчислюваних функцій, встановлювати розв'язність, часткову розв'язність та нерозв'язність алгоритмічних проблем, проектувати, розробляти та аналізувати алгоритми , оцінювання їх ефективності та складності.
РН-24. Розв'язувати питання адміністрування, ефективного застосування, безпеки, діагностування, відновлення, моніторингу й оптимізації роботи комп'ютерів, операційних систем і системних ресурсів комп'ютерних систем.
РН-26. Зберігати конфіденційність, цілісність та доступність інформації, забезпечувати автентичність, відстежуваність та надійність інформації в умовах неповноти та невизначеність вихідних даних, багатокритеріальності професійних задач.

У результаті вивчення навчальної дисципліни студент повинен
знати:

- фундаментальні концепції і принципи проектування програмного забезпечення з доступом до баз даних, на яких базуються сучасні технології створення програмних комплексів;
- етапи проектування та експлуатації систем;
- життєвий цикл програмного забезпечення; програмні продукти, які застосовуються для проектування програмного забезпечення та бази даних;
- тестування програмного забезпечення та впровадження його у експлуатаційний процес;

вміти:

- використовувати засоби фреймворку як при проектуванні, так і при реалізації додатків з доступом до баз даних;
- відлагоджувати скрипти в браузері;
- проектувати інтелектуальні, інформаційні, інформаційно-пошукові системи;
- застосовувати сучасні інформаційні технології при вирішенні задач системного аналізу.

Методи навчання:

- словесні: лекції (вступна, тематичні, оглядові, підсумкова). Проведення лекційних занять включає викладання теоретичного матеріалу, оглядові лекції з використанням опорного конспекту, лекції візуалізації з використанням мультимедійних технологій;
- практичні: робота над індивідуальними завданнями на комп'ютерах, робота в групах;

Форми навчання: фронтальні, групові, аудиторні, позааудиторні.

4. СТРУКТУРА (ТЕМАТИЧНИЙ ПЛАН) ДИСЦИПЛІНИ

Назва змістових модулів і тем	Кількість годин, у тому числі				
	усього	л	п	лаб	с/р
Змістовий модуль 1. Вступ, Кріптографія					
Вступ. Основні види і джерела атак на інформацію.	12	4		4	4
Криптографія. Симметричні криптоалгоритми	16	6		4	6
Асиметричні криптоалгоритми.	12	6			6
Разом за змістовим модулем 1	40	16		8	16

Змістовий модуль 2. Мережева безпека, ПЗ					
Мережева безпека.	15	4		8	3
ПЗ та інформаційна безпека.	9	4			5
Комплексна система безпеки.	11	6			5
Разом за змістовим модулем 2	35	14		8	13
Підготовка до екзамену	30				30
Разом з дисципліни	105	30		16	59

5. ЛЕКЦІЙНИЙ КУРС

№ занять	Тема занять	Кількість годин
1,2	**Вступ. Основні види і джерела атак на інформацію.** Сучасна ситуація в області інформаційної безпеки. Категорії інформаційної безпеки, Абстрактні моделі захисту інформації. Огляд найбільш поширених методів «злому».	4
3-5	**Криптографія.** Класифікація криптоалгоритмів, Симетричні криптоалгоритми, скремблера, блокові шифри, мережа Фейштеля. Симетричні криптосистеми, архівація, генератори випадкових і псевдовипадкових послідовностей, архівація, хешування паролів, транспортний кодування.	6
6-8	**Асиметричні криптоалгоритми.** Асиметричні криптосистеми. Алгоритм RSA, технології цифрових підписів. Механізм поширення відкритих ключем.	6
9,10	**Мережева безпека**. мережеві компоненти які атакують. Рівні мережевих атак згідно моделі OSI.	4
11,12	**ПЗ та інформаційна безпека**. Огляд ПЗ, помилки, які призводять до можливості атак на інформацію, основні положення по розробці ПЗ.	4
13-15	**Комплексна система безпеки.** Класифікація інформаційних об'єктів, політика ролей, Політика інформаційної безпеки, методи забезпечення безвідмовності.	6
	Усього годин	30

6. ТЕМИ ПРАКТИЧНИХ ЗАНЯТЬ

Практичні заняття навчальним планом не передбачені.

7. ТЕМИ ЛАБОРАТОРНИХ ЗАНЯТЬ

№ занять	Тема занять	Кількість годин
1-3	Базові алгоритми шифрування.	4
4-5	Розробка блок-схем базових алгоритмів шифрування.	4
6-8	Розробка програм алгоритмів шифрування.	8
	Усього годин	16

8. САМОСТІЙНА РОБОТА

№ п/п	Вид роботи / Назва теми	Кількість годин
1	Підготовка до аудиторних занять	15
2	Підготовка до контрольних заходів	4
3	Опрацювання розділів програми, які не викладаються на лекціях - Скремблери, симетричні криплоалгоритми. - Алгоритм стиснення Лемпеля-Зива. - Алгоритм RSA. - Обмін ключами по алгоритму Диффи-Хеллмана. - Атака «відмова в сервісі (DoS)».	10 2 2 2 2 2
4	Підготовка до екзамену	30

9. МЕТОДИ КОНТРОЛЮ

Основними методами контролю знань студентів є усний, письмовий і графічний методи, а також методи самоконтролю та самооцінки.

10. ПОРЯДОК ТА КРИТЕРІЇ ОЦІНЮВАННЯ

Контроль успішності студента здійснюється за допомогою 100-бальної системи оцінювання, що має відповідні оцінки в національній шкалі ECTS.

Змістовий модуль 1. Вступ. Криптографія.

Лабораторна робота (максимальна кількість балів – 100 за кожну):
№1 «Базові алгоритми шифрування»
№2 «Розробка блок-схем базових алгоритмів шифрування»
Виконання лабораторної роботи та її оформлення – 60 балів;
Відповідь на теоретичне питання №1, №2 при захисті контрольної роботи (максимальна кількість балів на одне питання – 20 балів) – 40 балів:

- правильна відповідь на питання – 20 балів;
- здебільшого правильна відповідь на питання, але потребує деяких уточнень щодо принципів роботи різних типів алгоритмів шифрування – 16 – 19 балів;
- відповідь на питання повна, сутність розкрита, але із незначними помилками (помилки в формулюваннях термінів, використанні відповідних блоків) – 6 – 15 балів;
- відповідь на питання неповна, але із значними помилками (неправильно названі методи шифрування, помилки при побудові блок-схем) 1 – 5 балів;
- неправильна відповідь, або немає відповіді – 0 балів.

Підсумкова оцінка зі змістового модуля 1 складається як середня оцінка за лабораторні роботи змістового модуля 1.

Змістовий модуль 2. Мережева безпека, ПЗ.

Лабораторна робота (максимальна кількість балів – 100):
№3 «Розробка програм алгоритмів шифрування»
Виконання лабораторної роботи та її оформлення – 60 балів;
Виконання лабораторної роботи та її оформлення – 60 балів;
Відповідь на теоретичне питання №1, №2 при захисті контрольної роботи (максимальна кількість балів на одне питання – 20 балів) – 40 балів:

- правильна відповідь на питання – 20 балів;
- здебільшого правильна відповідь на питання, але потребує деяких уточнень щодо принципів написання програми – 16 – 19 балів;
- відповідь на питання повна, сутність розкрита, але із незначними помилками (програма не повністю відповідає алгоритму) – 6 – 15 балів;
- відповідь на питання неповна, із значними помилками (помилки в програмі, невідповідність програм до блок-схем) 1 – 5 балів;
- неправильна відповідь, або немає відповіді – 0 балів.

Підсумкова оцінка зі змістового модуля 2 складається як оцінка за лабораторну роботу змістового модуля 2.

Критерії оцінювання знань студентів на екзамені

Екзамен (максимальна кількість балів – **100**):

– відповідь на теоретичні питання (максимальна кількість балів на одне питання - 25 балів): 50 балів:

- правильна відповідь на питання 25 балів;
- робота виконана повністю, розрахунки виконані послідовно, але виконання завдання потребує деяких уточнень (щодо принципів роботи різних типів алгоритмів шифрування) 19 – 24 балів;
- відповідь на питання повна, сутність розкрита, але із незначними помилками (помилки в формулюваннях термінів, використанні відповідних блоків) – 9 – 18 балів;
- відповідь на питання неповна, із значними помилками (неправильно названі методи шифрування, помилки при побудові блок-схем) 1 - 8 балів;
- неправильна відповідь або немає відповіді 0 балів.

– виконання практичних завдань максимальна кількість балів: 50 балів;

- правильне виконання завдання, розрахунки виконані без помилок, проведено аналіз результатів 50 балів;
- робота виконана повністю, розрахунки виконані послідовно, але виконання завдання потребує деяких уточнень (щодо пояснення принципів написання програми)40 – 49 балів;
- робота виконана повністю, але аналіз результатів недостатній (сутність розкрита, але програма не повністю відповідає алгоритму) 30 – 39 балів;
- виконання завдання повне, сутність розкрита, але із незначними помилками (програма працює з деякими помилками) 20 -29 балів;
- виконання завдання повне, але зі значними помилками (помилки в створенні блок-схеми і відповідні помилки у програмі) 10 - 19 балів;
- виконання завдання неповне, із значними помилками (помилки в програмі, невідповідність програм до блок-схем) 1 – 9 балів;
- неправильне виконання завдання або немає розв'язання 0 балів.

Підсумкова оцінка з дисципліни визначається як середньоарифметичне між оцінками змістових модулів 1 і 2 та екзамену.

11. ПОЛІТИКА КУРСУ

Порядок зарахування пропущених занять:

- пропущена лекція відпрацьовується підготовкою реферату відповідно до теми пропущеного заняття та його захистом;
- пропущені лабораторні заняття відпрацьовуються студентами виконанням відповідної практичної роботи самостійно та її захистом.

Зміни в нарахуванні балів у випадках несвоєчасного виконання завдань не відбувається.

Дотримання академічної доброчесності студента передбачає:

- самостійне та добросовісне виконання завдань, в тому числі поточного та підсумкового контролю;
- відповідальне ставлення до своїх обов'язків;
- повага до честі й гідності інших осіб;
- посилання на джерела інформації у разі запозичення ідей, розробок, тверджень, відомостей;
- використання при виконанні завдань лише перевірених та достовірних джерел інформації.

За порушення академічної доброчесності студент може бути притягнутий до академічної відповідальності (повторне проходження оцінювання).

Також неприятливим у навчальній діяльності студентів є академічний плагіат, самоплагіат, фальсифікація та інші види академічної нечесності. Перевірці на академічний плагіат підлягають кваліфікаційні роботи студентів.

12 РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Столлингс В. Криптография и защита сетей: принципы и практика. М.: Издательский дом «Вильямс», 2001. – 672с
2. Лагун А.Е. Криптографічні системи та протоколи: навч. посібник. Львів : Вид-во Львів. політехніки, 2013. - 96 с.
3. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства. – М.: ДМК Пресс, 2008.
4. Мамаев М., Петренко С. Технологии защиты информации в Интернете. Специальный справочник. СПб.: Питер, 2002.
5. Безопасность и резильентность систем и сетей. Практикум / И.В. Жуковицкий, Д.А. Остапец, С.А. Разгонов, А.П. Заец – Под ред. Жуковицкого И.В. – Харьков: Национальный аэрокосмический университет имени Н.Е. Жуковского «ХАИ». – 2017. – 131 с.

Допоміжна

1. В.Зима, А.Молдовян, Н.Молдовян. Безопасность глобальных сетевых технологий. СПб.: БХВ-Петербург, 2000.
2. Лукацкий А.В. Обнаружение атак. – СПб.: БХВ-Петербург, 2003. – 608.
3. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации.– К.: Издательство Юниор, 2003. – 504 с.
4. Архипов О.Є., Луценко В.М., Худяков В.О. Захист інформації в телекомунікаційних мережах та системах зв'язку: Навч. – метод. посіб. – К.: ІВЦ «Видавництво «Політехніка», 2003. – 40с.
5. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. – К.: ТИД ДС, 2001. - 688 с.

6. Вертузаєв М.С., Юрченко О.М. Захист інформації в комп'ютерних системах від несанкціонованого доступу: Навч. посібник – К. : Вид-во Європ. ун-ту, 2001. - 321 с.
7. Антонюк А.О. Основи захисту інформації в автоматизованих системах: Навч. посібник. – К. : Видавничий дім «КМ Академія», 2003. - 244 с.

13. INTERNET-РЕСУРСИ

1. Доменна система імен – Вікіпедія (http://uk.wikipedia.org/wiki/DNS).
2. Ruby on Rails Tutorial (http://russian.railstutorial.org/chapters/beginning).
3. Apache – Вікіпедія (http://uk.wikipedia.org/wiki/Apache).
4. MVC – Вікіпедія (http://uk.wikipedia.org/wiki/MVC).

Розробник _____ (підпис) (І. М. Ільєв)

Гарант освітньої програми _____ (підпис) (Н. О. Вельмагіна)

Силабус затверджено на засіданні кафедри
комп'ютерних наук, інформаційних технологій та прикладної математики

Протокол від « 31 » серпня 2020 року № 2