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

Кафедра комп'ютерних наук, інформаційних технологій та прикладної математики

«ЗАТВЕРДЖУЮ»
Проректор з навчально-виховної роботи
Галина ЄВСЄЄВА

«01» 09 2021 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
			VIII
Всього годин за навчальним планом, з них:	120	4	120
Аудиторні заняття, у т.ч:	46		46
лекції	30		30
лабораторні роботи			
практичні заняття	16		16
Самостійна робота, у т.ч:	74		74
підготовка до аудиторних занять	20		20
підготовка до контрольних заходів	14		14
виконання курсового проекту або роботи			
опрацювання розділів програми, які	10		10

не викладаються на лекціях			
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 «Інформатика», «Операційні системи», «Архітектура та проектування програмного забезпечення», «Комп'ютерні мережі».

Постреквізити дисципліни. Вивчення дисципліни забезпечує формування у фахівців знання основних понять і методів, які використовуються для виконання кваліфікаційних робіт.

Компетентності:

Інтегральна компетентність

ІК. *Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі* комп'ютерних наук або у процесі навчання, що передбачає застосування теорій та методів комп'ютерних наук, 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.

4. СТРУКТУРА (ТЕМАТИЧНИЙ ПЛАН) ДИСЦИПЛІНИ

Назва змістових модулів і тем	Кількість годин, у тому числі				
	усього	л	п	лаб	с/р
Семестр VIII					
Змістовий модуль 1. Вступ, Криптографія					
Вступ. Основні види і джерела атак на	15	4	4		7

інформацію.					
Криптографія. Симметричні криптоалгоритми	18	6	4		8
Асиметричні криптоалгоритми.	14	6			8
Разом за змістовим модулем 1	47	16	8		23
Змістовий модуль 2. Мережева безпека, ПЗ					
Мережева безпека.	15	4	4		7
ПЗ та інформаційна безпека.	13	4	2		7
Комплексна система безпеки.	15	6	2		7
Разом за змістовим модулем 2	43	14	8		21
Підготовка до екзамену	30				30
Усього годин	120	30	16		74

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

№ занять	Тема занять	Кількість годин
1-2	Базові алгоритми шифрування.	4
3-4	Розробка блок-схем базових алгоритмів шифрування.	4
5-8	Розробка програм алгоритмів шифрування.	8
	Усього годин	16

7. ТЕМИ ЛАБОРАТОРНИХ ЗАНЯТЬ

Лабораторні заняття навчальним планом не передбачені.

8. САМОСТІЙНА РОБОТА

№ п/п	Вид роботи / Назва теми	Кількість годин
1	Підготовка до аудиторних занять	20
2	Підготовка до контрольних заходів	14
3	*Опрацювання розділів програми, які не викладаються на лекціях* - Скремблери, симетричні криптоалгоритми. - 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

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

10. ПОРЯДОК ТА КРИТЕРІЇ ОЦІНЮВАННЯ

Змістовий модуль 1. Вступ, Криптографія.

№ п/п	Вид навчальної роботи студента	Максимальна кількість балів
1	Відвідування лекцій	16 *(2 бали × 8 лекцій)*
2	Виконання практичних робот: 1. Базові алгоритми шифрування. 2. *Розробка блок-схем базових алгоритмів шифрування.*	 30 30
3	Контрольна робота	24 (12 балів × 2 питання)
	Разом	100

Змістовий модуль 2. Мережева безпека, ПЗ.

№ п/п	Вид навчальної роботи студента	Максимальна кількість балів
1	Відвідування лекцій	14 (2 бали × 7 лекцій)
2	Виконання практичних робіт: 1. Розробка програм алгоритмів шифрування.	 30
3	Контрольна робота	56 (28 балів × 2 питання)
	Разом	100

Критерії оцінювання практичних робот

Максимальна кількість балів за виконання однієї практичної роботи – 30.

Кількість балів «30» – ставиться, якщо студент у відведений час повністю виконав обсяг робіт згідно з передбаченим варіантом. Розв'язання задач виконано послідовно відповідно до методичних вказівок, отримано правильні результати. Робота оформлена охайно.

Кількість балів «20–29» – ставиться, якщо студент у відведений час повністю виконав обсяг робіт згідно з передбаченим варіантом. Розв'язання задач виконано послідовно відповідно до методичних вказівок, отримано в цілому правильні результати, однак мають місце помилки, пов'язанні з помилками у побудові блок-схем або написанні коду програми, робота оформлена не досить охайно.

Кількість балів «10–19» – ставиться, якщо студент у відведений час не повністю виконав обсяг робіт згідно з передбаченим варіантом. Розв'язання задач виконано відповідно до методичних вказівок, отримано результати, однак мають місце помилки, пов'язанні з помилками у написанні коду програми або помилки, пов'язанні з викладанням теоретичного матеріалу (невірне використання термінології, помилки в поясненнях), робота оформлена неохайно.

Кількість балів «0–9» – ставиться, якщо студент у відведений час не повністю виконав обсяг робіт згідно з передбаченим варіантом, при розв'язанні задач мають місце помилки, пов'язанні з помилками у побудові блок-схем, написанні коду програми та помилки, пов'язанні з викладанням теоретичного матеріалу (невірне використання термінології, помилки в поясненнях), робота оформлена неохайно.

Критерії оцінювання контрольної роботи

Контрольна робота складається з 2 запитань. Максимальна кількість балів за відповідь на 1 запитання першого змістового модуля –12, а другого змістового модуля – 28.

Змістовий модуль 1.

Кількість балів «12» – ставиться студенту за повну, змістовну, логічну, послідовну, правильну відповідь у письмово-графічній формі на питання контрольної роботи.

Кількість балів «8–11» – ставиться студенту за логічну, послідовну, загалом правильну відповідь в письмово-графічній формі на питання контрольної роботи. Але окремі пункти відповідей не повністю розкривають суть питання і мають незначні помилки при написанні коду програми.

Кількість балів «4–7» – ставиться студенту за відповідь в письмово-графічній формі на питання контрольної роботи, в якій не повністю розкривається суть поставлених питань. У розв'язанні задач наявні суттєві помилки, що свідчать про недостатнє засвоєння студентом теоретичного та практичного матеріалу. Представлена відповідь має фрагментарний характер, слабо пов'язана з суттю поставленого питання, оформлена недбало і не дає повного уявлення про правильність кінцевих результатів.

Кількість балів «0–3» – ставиться студенту за відсутність конкретної відповіді в письмово-графічній формі на питання контрольної роботи. Відповідь носить поверхневий безсистемний характер, відсутня теоретична база у висвітлені поставленого питання, наявні грубі помилки, що свідчить про відсутність у студента мінімуму знань з дисципліни.

Змістовий модуль 2.

Кількість балів «28» – ставиться студенту за повну, змістовну, логічну, послідовну, правильну відповідь у письмово-графічній формі на питання контрольної роботи.

Кількість балів «17–27» – ставиться студенту за логічну, послідовну, загалом правильну відповідь в письмово-графічній формі на питання контрольної роботи. Але окремі пункти відповідей не повністю розкривають суть питання і мають незначні помилки при написанні коду програми.

Кількість балів «6–16» – ставиться студенту за відповідь в письмово-графічній формі на питання контрольної роботи, в якій не повністю розкривається суть поставлених питань. У розв'язанні задач наявні суттєві помилки, що свідчать про недостатнє засвоєння студентом теоретичного та практичного матеріалу. Представлена відповідь має фрагментарний характер, слабо пов'язана з суттю поставленого питання, оформлена недбало і не дає повного уявлення про правильність кінцевих результатів.

Кількість балів «0–5» – ставиться студенту за відсутність конкретної відповіді в письмово-графічній формі на питання контрольної роботи. Відповідь носить поверхневий

безсистемний характер, відсутня теоретична база у висвітлені поставленого питання, наявні грубі помилки, що свідчить про відсутність у студента мінімуму знань з дисципліни.

Критерії оцінювання знань студентів на екзамені

Максимальна кількість балів на екзамені – 100 балів.

В екзаменаційному білеті 4 питання.

Максимальна кількість балів за відповідь на кожне питання – 25.

24–25 балів – ставиться за змістовну, логічну, послідовну, правильну відповідь в письмовій формі на питання екзаменаційного білета. При цьому повністю розкриті усі пункти питання, відповідь охайно оформлено.

16–23 балів – ставиться за відповідь в письмовій формі на питання екзаменаційного білета при порушенні послідовного викладення матеріалу, окремі підпункти питання розкриті не в повному обсязі, мають місце незначні помилки при написанні коду програми.

11–15 балів – ставиться за відповідь в письмовій формі на питання екзаменаційного білета, якщо студент надав поверхневу відповідь на питання екзаменаційного білета. Допущені суттєві помилки, що свідчать про недостатнє засвоєння студентом теоретичного та практичного матеріалу, відсутня логічна послідовність відповіді.

1–10 балів – ставиться студенту при відсутності конкретної відповіді в письмово-графічній формі на екзаменаційне питання. Відповідь носить поверхневий безсистемний характер, відсутня теоретична база у висвітлені поставленого питання, наявні грубі помилки, що свідчить про відсутність у студента відповідних теоретичних та практичних знань.

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

11. ПОЛІТИКА КУРСУ

Порядок зарахування пропущених занять:

- пропущена лекція відпрацьовується підготовкою конспекту відповідно до теми пропущеного заняття та його захистом;
- пропущені практичні 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.

12. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Лагун А.Е. Криптографічні системи та протоколи: навч. посібник. Львів : Вид-во *Львів. політехніки, 2013.* - 96 с.
2. 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.
3. Столлингс В. Криптография и защита сетей: принципы и практика. М.: Издательский дом «Вильямс», 2001. – 672с
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. 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.
2. Антонюк А.О. Основи захисту інформації в автоматизованих системах: Навч. посібник. – К. : Видавничий дім «КМ Академія», 2003. - 244 с.
3. В.Зима, А.Молдовян, Н.Молдовян. Безопасность глобальных сетевых технологий. СПб.: БХВ-Петербург, 2000.
4. Лукацкий А.В. Обнаружение атак. – СПб.: БХВ-Петербург, 2003. – 608.
5. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации.– К.: Издательство Юниор, 2003. – 504 с.
6. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства. – М.: ДМК Пресс, 2008.
7. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. – К.: *ТИД ДС, 2001.* - 688 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 _____ (Ілля ІЛЬСВ)
(підпис)

Гарант освітньої програми _____ (Наталя ВЕЛЬМАГІНА)
(підпис)

Силабус затверджено на засіданні кафедри
комп`ютерних наук, інформаційних технологій та прикладної математики
Протокол від « 30 » 08 2021 року № 1