‘Сумський державний педагогічний університет імені А. С. Макаренка

Фізико-математичний факультет

ЗАТВЕРДЖУЮ
Декан фізико-математичного факультету
_____ Каленик М. В.
«23» вересня 2020 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ЗАХИСТ ІНФОРМАЦІЇ

Перший (бакалаврський) рівень

галузь знань **Інформаційні технології**

спеціальність **122 Комп’ютерні науки**

освітньо-професійна програма **Комп'ютерні науки**

мова навчання **українська**

Погоджено науково-методичною комісією фізико-математичного факультету
«23» вересня 2020 р.
Голова
Одінцова О.О., к.фіз.-мат.наук, доц.

Суми – 2020

Розробник:

Дегтярьова Н.В. – кандидат педагогічних наук, доцент

Робоча програма розглянута і схвалена на засіданні кафедри інформатики

Протокол № 11 від «23» червня 2020 р.

Завідувач кафедри

Семеніхіна О.В., доктор педагогічних наук, професор _____

Опис навчальної дисципліни

Найменування показників	Освітній ступінь	Характеристика навчальної дисципліни	
		денна форма навчання	**Заочна форма навчання**
Кількість кредитів – 3	Бакалавр	Обов'язкова	
		Рік підготовки:	
		4-й	
		Семестр	
Загальна кількість годин - 90		7-й	
		Лекції	
		10 год.	год.
		Практичні, семінарські	
		год.	год.
		Лабораторні	
		16 год.	год.
		Самостійна робота	
		62 год.	год.
		Консультації:	
		2 год.	год.
		Вид контролю: іспит	

1. Мета вивчення навчальної дисципліни

Метою вивчення дисципліни є формування у майбутніх бакалаврів комп'ютерних наук професійної компетентності через розвиток у них здатності застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури

2. Передумови для вивчення дисципліни

Перелік дисциплін, які мають бути вивчені раніше: основи ІКТ, основи програмування.

3. Результати навчання за дисципліною

Результати навчання за дисципліною узгоджуються з вимогами Стандарту спеціальності 122 і впливають на розвиток:

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 інформаційних технологій і характеризується комплексністю та невизначеністю умов;

ЗК1. Здатність до абстрактного мислення, аналізу та синтезу;

ЗК2. Здатність застосовувати знання у практичних ситуаціях;

ЗК3. Знання та розуміння предметної області та розуміння професійної діяльності;

ЗК4. Здатність спілкуватися державною мовою як усно, так і письмово

ЗК5. Здатність спілкуватися іноземною мовою

ЗК6. Здатність вчитися і оволодівати сучасними знаннями;

ЗК7. Здатність до пошуку, оброблення й аналізу інформації з різних джерел;

ЗК8. Здатність генерувати нові ідеї (креативність);

ЗК9. Здатність працювати в команді;

ЗК11. Здатність приймати обґрунтовані рішення;

ЗК12. Здатність оцінювати та забезпечувати якість виконуваних робіт;

ЗК13. Здатність діяти на основі етичних міркувань;

ЗК14. Здатність реалізувати свої права і обов’язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні;

СК12. Здатність забезпечити організацію обчислювальних процесів в інформаційних системах різного призначення з урахуванням архітектури, конфігурування, показників результативності функціонування операційних систем і системного програмного забезпечення.

СК14. Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об’єктів критичної інформаційної інфраструктури

СК15. Здатність до аналізу та функціонального моделювання бізнес-процесів, побудови та практичного застосування функціональних моделей організаційно-економічних і виробничо-технічних систем, методів оцінювання ризиків їх проектування

ПР1. Застосовувати знання основних форм і законів абстрактно-логічного мислення, основ методології наукового пізнання, форм і методів вилучення, аналізу, обробки та синтезу інформації в предметній області комп'ютерних наук.

ПР15 Застосовувати знання методології та CASE-засобів проектування складних систем, методів структурного аналізу систем, об'єктно-орієнтованої методології проектування при розробці і дослідженні функціональних моделей організаційно-економічних і виробничо-технічних систем

ПР16 Розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп’ютерних мереж в умовах неповноти та невизначеності вихідних даних

ПР17 Виконувати паралельні та розподілені обчислення, застосовувати чисельні методи та алгоритми для паралельних структур, мови паралельного програмування при розробці та експлуатації паралельного та розподіленого програмного забезпечення

4. Критерії оцінювання результатів навчання

Викладання курсу ґрунтується на принципах академічної доброчесності, що передбачає: самостійне виконання навчальних завдань, завдань поточного і підсумкового контролю результатів навчання; посилання на джерела інформації у разі використання ідей, тверджень, відомостей; дотримання норм законодавства про авторське право.

Шкала ЄКТС	Критерії оцінювання навчальних досягнень здобувача
A	Здобувач має системні, дієві знання, виявляє неординарні творчі здібності у навчальній діяльності, використовує широкий арсенал засобів доказів своєї думки, розв'язує складні проблемні завдання захисту інформації, схильний до системно-наукового аналізу захисту інформації; уміє ставити і розв'язувати проблеми захисту інформації, самостійно здобувати і використовувати інформацію, виявляє власне ставлення до неї, виконує науково-дослідну роботу, логічно та творчо викладає матеріал в усній та письмовій формі; розвиває свої здібності й нахили; використовує Інтернет
B	Здобувач вільно володіє вивченим матеріалом, застосовує знання у дещо змінених ситуаціях, вміє аналізувати і систематизувати інформацію щодо захисту інформації, робить аналітичні висновки, використовує загальновідомі докази у власній аргументації, чітко тлумачить поняття зі сфери захисту інформації, нормативних документів, може самостійно опрацювати матеріал, виконує прості творчі завдання; має сформовані типові навички

C	Знання студента досить повні, він вільно застосовує вивчений матеріал у стандартних ситуаціях, вміє аналізувати впровадження захисту інформації, робити висновки; відповідь його повна, логічна, обґрунтована, однак із деякими неточностями; вміє самостійно працювати
D	Здобувач розуміє основні положення навчального матеріалу, може поверхово аналізувати захист інформації, робить певні висновки; відповідь може бути правильною, проте недостатньо осмисленою, самостійно відтворює більшу частину матеріалу; вміє застосовувати знання під час розв'язування завдань за алгоритмом, користуватися додатковими джерелами
E	Здобувач володіє початковими знаннями, знає близько половини навчального матеріалу, здатний відтворити його відповідно до тексту підручника або пояснень викладача, провести за зразком дії; слабо орієнтується у поняттях, визначеннях, самостійне опрацювання навчального матеріалу викликає значні труднощі
F	Здобувач намагається аналізувати на основі побутових знань і навичок; виявляє окремі властивості, спроби виконання вправ, дій репродуктивного характеру, за допомогою викладача робить дії за готовим алгоритмом
FX	Здобувач мало усвідомлює мету навчально-пізнавальної діяльності, робить спробу знайти способи дій, розповісти суть заданого, проте відповідає лише за допомогою викладача на рівні «так» чи «ні», може самостійно знайти в підручнику відповідь

Розподіл балів

Поточний контроль							Разом	Сума
Т 1	Т 2	Т 3	Т 4	Т 5	Т 6	Т 7		
Поточний контроль							35	100
5	5	5	5	5	5	5		
Контроль самостійної роботи							40	
5	5	5	10	5	5	5		
Іспит							25	
25								

Шкала оцінювання: національна та ECTS

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою
		для екзамену, заліку, курсового проекту (роботи), практики
90 – 100	**A**	**відмінно**
82 - 89	**B**	**добре**
74 - 81	**C**	
64 - 73	**D**	**задовільно**
60 - 63	**E**	
35-59	**FX**	**незадовільно з можливістю повторного складання**
1 - 34	**F**	**незадовільно з обов’язковим повторним вивченням дисципліни**

5. Засоби діагностики результатів навчання

Об’єктами поточного контролю знань здобувачів є:

– систематичність роботи на лабораторних заняттях;

– активність роботи на лабораторних заняттях;
– виконання практичних завдань;
– виконання завдань для самостійного опрацювання;
– виконання контрольних завдань.

Поточний контроль здійснюється шляхом прийняття виконаних завдань та робіт на лабораторних заняттях.

Контроль самостійної роботи здобувачів з дисципліни передбачається на основі застосування наступних форм:

– перевірка здатності самостійно працювати над засвоєнням основних тем та питань дисципліни;

– перевірка конспектів лекцій за темами курсу, що виносяться на самостійне опрацювання;

– перевірка завдань, що самостійно виконуються здобувачами при підготовці до лабораторних занять

Підсумковий контроль проводиться у формі письмового іспиту.

6. Програма навчальної дисципліни

6.1. Інформаційний зміст навчальної дисципліни

Тема 1. Теоретичні аспекти захисту інформації. Види, джерела та носії інформації, що захищається. Концептуальні засади захисту інформації. Аналіз і оцінка загроз інформаційній безпеці. Політика безпеки та управління ризиками. Класифікація та основні характеристики технічних каналів витоку інформації.

Тема 2. Кібербезпека в умовах розгортання четвертої промислової революції. Процедура обрання раціонального варіанта реагування на кібернетичні втручання і загрози. Методи та засоби протидії соціотехнічним атакам і захисту від них: переваги та недоліки.

Тема 3. Рівні протидії загрозам інформаційній безпеці. Законодавчий рівень забезпечення протидії загрозам інформаційній безпеці. Адміністративний та процедурний рівні забезпечення протидії загрозам інформаційній безпеці. Програмно-технічний рівень протидії загрозам інформаційній безпеці та політика безпеки.

Тема 4. Методи та засоби захисту інформації. Канали несанкціонованого доступу до інформації. Методи та засоби протидії соціотехнічним атакам і захисту від них: переваги та недоліки. Засоби та заходи фізичного захисту інформації з обмеженим доступом. Засоби та заходи технічного захисту інформації з обмеженим доступом.

Тема 5. Засоби безпеки систем управління баз даних. Концептуальні питання побудови рівнів захисту систем управління базами даних. Основні вимоги до підсистеми безпеки баз даних. Найпростіша модель безпеки баз даних. Перевірка повноважень. Перевірка автентичності. Модель багаторівневої безпеки баз даних. Безпечні середовища розподілених баз даних. Мови безпечних баз даних

Тема 6. Криптографічні методи захисту та перетворення інформації. Стандарти на створення систем захисту даних. Основні вимоги до криптографічних систем. Класифікація криптографічних атак. Застосування різноманітних технік шифрувань. Загальна класифікація криптографічних алгоритмів шифрування. Методи перестановки і заміни. Реалізація алгоритмів шифрування. Симетрична (таємна) методологія. Асиметрична (відкрита) методологія. Загальні принципи утворення блокових симетричних шифрів. Переваги та недоліки блокових шифрів. Загальні принципи

побудови симетричних алгоритмів. Основні відомості та принципи побудови асиметричних алгоритмів. Криптографічні протоколи. Цифровий підпис. Хеш-функції та вимоги до них. Керування ключами. Протоколи, пов'язані з підписами. Протоколи узгодження ключа.

Тема 7. Особливості організації та функціонування команд (груп) CERT/CSIRT. Характеристика діяльності груп CERT/CSIRT. Етапи створення груп CERT/CSIRT. Сервіси, що надаються групами реагування на інциденти інформаційної безпеки. Обробка інцидентів інформаційної безпеки групами CERT/CSIR. Документаційне забезпечення процесу управління інцидентами інформаційної безпеки.

6.2. Структура та обсяг навчальної дисципліни

Назви розділів і тем	**Кількість годин**											
	Денна форма						**Заочна форма**					
	Усього	**у тому числі**					**Усього**	**у тому числі**				
		Лекції	**Практ.**	**Лабор.**	**Конс.**	**Самост.р**		**Лекції**	**Практ.**	**Лабор.**	**Конс.**	**Самост. робота**
Розділ 1. Робота з РНР												
Тема 1. Теоретичні аспекти захисту інформації	12	2		2		8						
Тема 2. Кібербезпека в умовах розгортання четвертої промислової революції	12	2		2		8						
Тема 3. Рівні протидії загрозам інформаційній безпеці	12	2		2		8						
Тема 4. Методи та засоби захисту інформації	12	2		2		8						
Тема 5. Засоби безпеки систем управління баз даних	14	2		2		10						
Тема 6. Криптографічні методи захисту та перетворення інформації	12			2		10						
Тема 7. Особливості організації та функціонування команд (груп) CERT/CSIRT	16			4	2	10						
Всього	90	10		16	2	62						

6.3 Теми лабораторних занять

№ з/п	Назва теми	Кількість годин	
		Денна форма	Заочна форма
1	Механізми захисту операційних систем	2	
2	Побудова моделі порушника та моделі загроз в інформаційній системі	2	
3	Механізми безпеки баз даних	2	
4	Шифри перестановки. Матричний шифр	2	
5	Шифрування даних за допомогою спеціальних програм та утиліт	2	
6	Пошук вразливостей у вихідних текстах програмного	2	

	забезпечення, що написані на мові високого рівня		
7	Механізми захисту додатків	4	
	Разом	16	

7. Рекомендовані джерела інформації

1. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Посібник]. / В. Л. Бурячок, С.В.Толюпа, В.В.Семко, Л.В.Бурячок, П.М.Складанний Н.В. Лукова-Чуйко/ – К. : ДУТ - КНУ, 2016. – 178 с.
2. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Підручник]. / В. Л. Бурячок, Г.М.Гулак, В.Б. Толубко. К. : ТОВ «СІК ГРУП УКРАЇНА», 2015. – 449 с.
3. Бурячок, В.Л. Інформаційна та кібербезпека: соціотехнічний аспект : Підручник [Електронний ресурс] / [В.Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа], заг. ред. д-ра техн. наук, професора В.Б. Толубка. – К.: ДУТ, 2015. – 288 с. http://www.dut.edu.ua/uploads/p_303_79299367.pdf
4. Електронне урядування та електронна демократія: навч. посіб.: у 15 ч. / за заг. ред. А.І. Семенченка, В.М. Дрешпака. – К., 2017. Частина 13: Захист інформації в системах електронного урядування / [О.М. Хошаба]. – К.: ФОП Москаленко О. М., 2017. 72 с. https://onat.edu.ua/wp-content/uploads/2018/05/Part_013_Feb_2018.pdf
5. Жаровський, Р. О. Конспект лекцій з дисципліни "Захист інформації у комп'ютерних системах": для студ. денної та заочної форми навчання / Р. О. Жаровський. — Тернопіль : ТНТУ ім. І. Пулюя, 2019. — 268 с.
6. Заплотинський, Б.А. Основи інформаційної безпеки / Б. А. Заплотинський. — Київ : КІІВіП НУ “ОЮА”, 2017. — 128 с.
7. Інформаційна безпека. За заг. ред. Ю. Я. Бобала, І. В. Горбатого. 2019. 680 с.
8. Лизанчук, В.В. Інформаційна безпека України: теорія і практика [Текст] : підручник / В. В. Лизанчук. — Львів : Львівський нац. ун-т ім. І. Франка, 2017. — 728 с.
9. Лужецький В. А., Кожухівський А. Д,, Войтович О. П. Основи інформаційної безпеки: навчальний посібник. Вінниця: ВНТУ. 2013. 221 с.
10. Макаренко ЄА.,Рижков М.М., Ожеван М.А., Кучмій О.П., Фролова О.М. Міжнародна інформаційна безпека: теорія і практика. Підручник. – К. : Центр вільної преси, 2016. 418 с.
11. Правові засади інформаційної безпеки України: монографія / П. Д. Біленчук, Л. В. Борисова, І. М. Неклонський., В. О. Собина; за ред. П. Д. Біленчука. Харків: 2018. 289 с.

Додаткові:

12. ISO 15408-1: 2005. Інформаційні технології. Методи захисту. Критерії оцінки для інформаційних технологій. Частина 1. Вступ і загальна модель.
13. ISO 15408-2: 2005. Інформаційні технології. Методи захисту. Критерії оцінки для інформаційних технологій. Частина 2. Функціональні вимоги безпеки.
14. ISO 15408-3: 2005. Інформаційні технології. Методи захисту. Критерії оцінки для інформаційних технологій. Частина 3. Вимоги до забезпечення захисту.
15. ISO 17799: 2005. Інформаційні технології. Методи захисту. Практичні рекомендації з управління інформаційної безпеки

8. Інструменти, обладнання та програмне забезпечення, використання яких передбачає навчальна дисципліна

Мультимедійна аудиторія, комп’ютерний клас