Сумський державний педагогічний університет імені А.С. Макаренка
Фізико-математичний факультет

Кафедра інформатики

ЗАТВЕРДЖУЮ
Декан фізико-математичного факультету
_____ Каленик М.В.
«_31_» _серпня_ 2021 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ТЕХНОЛОГІЯ ЗАХИСТУ ДАНИХ

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
«_31_» _серпня_ 2021 р.
Голова: Одінцова О.О., к. ф-м. н, доц.
_____

Суми – 2021

Розробники:

Мулеса Павло Павлович – кандидат технічних наук, доцент

Робоча програма розглянута і схвалена на засіданні кафедри інформатики

Протокол № 11 від «29» червня 2021 р.

Завідувач кафедри

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

Опис навчальної дисципліни

Найменування показників	Освітній ступінь	Характеристика навчальної дисципліни
		денна форма навчання
Кількість кредитів – **3**	Бакалавр	Вибіркова
		Рік підготовки
		4
		Семестр
Загальна кількість годин – **120**		**7**
		Лекції
		18
		Практичні, семінарські
		Лабораторні
		18
		Самостійна робота
		54
		Консультації
		Вид контролю: **залік**

1. Мета вивчення навчальної дисципліни

Мета – отримання теоретичних знань про програмні загрози ПК

Завдання – ознайомлення з різновидами шкідливого програмного забезпечення, та способами боротьби з ними.

В результаті вивчення даного курсу студент повинен

знати:

– історію розвитку комп'ютерної техніки, операційних систем, шкідливого програмного забезпечення, засобів протидії та їх класифікувати.

– ефективно налаштовувати роботу операційної системи та прикладного програмного забезпечення.

вміти:

- захищати ПК від шкідливого програмного забезпечення,
- протидіяти різним класам ШПЗ,
- виконувати процедури, що забезпечують безпеку даних на ПК;

2. 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.

К-сть балів	**Критерії оцінювання навчальних досягнень студента**
90–100	Студент у повному обсязі володіє навчальним матеріалом, глибоко та всебічно розкриває зміст теоретичних питань, вільно самостійно та аргументовано користується теоретичними знаннями та отриманим практичним досвідом під час усних виступів; застосовує набуті знання при виконанні лабораторних завдань, може пояснити хід розв'язання задачі, аргументувати його ефективність;

К-сть балів	Критерії оцінювання навчальних досягнень студента
	демонструє результати виконання всіх видів навчальної роботи, передбачених робочою програмою
82–89	Студент володіє навчальним матеріалом, обґрунтовано його викладає під час усних виступів та письмових відповідей, здатний теоретично обґрунтовувати обрані шляхи розв'язання завдань, успішно виконує лабораторні роботи з використанням спеціалізованих джерел; при викладенні окремих питань допускає несуттєві неточності та\або незначні помилки; демонструє результати виконання всіх видів навчальної роботи, передбачених робочою програмою.
74–81	Студент в цілому володіє навчальним матеріалом, викладає його основний зміст під час усних виступів та письмових відповідей, але без глибокого всебічного аналізу, обґрунтування та аргументації, здатний критично оцінювати джерела, проте у відповідях припускається помилок, які після вказівки здатний усунути; демонструє результати виконання всіх видів навчальної роботи, передбачених робочою програмою.
64–73	Студент володіє матеріалом лекцій, але не може навести власних прикладів, не може пояснити процес виконання лабораторної роботи, аргументувати алгоритм вирішення завдань; ситуативно здатний розв'язувати поставлені завдання, успішно виконує завдання за зразком, проте без аргументації та обґрунтування відповідає на запитання, недостатньо володіє теоретичними основами теми; лабораторні роботи виконує з суттєвими неточностями та\ або помилками; лабораторних робіт виконує та захищає понад 66%.
60–63	Ситуативно володіє матеріалом лекцій, але не виявляє бажання розширювати чи поглиблювати власні знання; орієнтується в основних поняттях, але відчуває труднощі у наведенні прикладів, аргументації положень, поясненні процесів та функціоналу програмних засобів; ситуативно здатний до критичного аналізу та пошуку потрібних джерел; демонструє результати виконання не менше половини від всіх видів навчальної роботи, передбачених робочою програмою.
35–59	Студент не володіє теоретичним матеріалом. Виконання практичних завдань викликають значні труднощі; неправильно вибирає відповідний програмний засіб для опрацювання даних; демонструє результати виконання менше половини від всіх видів навчальної роботи, передбачених робочою програмою.
1–34	Студент не володіє теоретичним матеріалом з дисципліни. Допускає принципові помилки, не може пояснити алгоритм розв'язування типових практичних завдань.

Розподіл балів

Поточне тестування та самостійна робота								Колоквіум	Тести	Сума
Т 1	Т 2	Т 3	Т 4	Т 5	Т 6	Т 7	Т 8	35	25	100
5	5	5	5	5	5	5	5			

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**

3. Засоби діагностики результатів навчання

1. Поточний контроль – фронтальне опитування, виконання практичних завдань.
2. Модульний контроль – колоквіум.
3. Підсумковий контроль – залік, виконання тестових завдань.

Оцінка успішності студента з спеціально програмного забезпечення для захисту операційних систем є рейтинговою і виставляється за стобальною шкалою з урахуванням оцінок засвоєння окремих модулів.

4. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

4.1. Зміст навчальної дисципліни

Тема1: Історія розвитку ОС та ШПЗ.
Тема2: Загальна характеристика загроз безпеці ПК.
Тема3: Шкідливе програмне забезпечення.
Тема4: Шкідливі мережеві технології.
Тема5: Потенційні цілі та способи їх захисту.
Тема6: Способи протидії ШПЗ.
Тема7: Методи протидії шкідливим мережевим технологіям.
Тема8: Процедури що забезпечують безпеку даних.

4.2. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин											
	Денна форма						Заочна форма					
	Усього	у тому числі					Усього	у тому числі				
		л	п	лаб	інд	ср		л	п	лаб	інд	ср
Змістовий модуль 1. Державне управління та організація охорони праці.												
Тема1: Історія розвитку ОС та ШПЗ.	10	2	2	-	-	6						
Тема2: Загальна характеристика загроз безпеці ПК.	10	2	2	-	-	6						
Тема3: Шкідливе програмне забезпечення.	10	2	2	-	-	6						
Тема4: Шкідливі мережеві технології.	10	2	2	-	-	6						
Тема5: Потенційні цілі та способи їх заисту.	10	2	2	-	-	6						
Тема6: Способи протидії ШПЗ.	18	4	4	-	-	10						
Тема7: Методи протидії шкідливим мережевим технологіям.	12	2	2	-	-	8						
Тема8: Процедури що забезпечують безпеку даних.	10	2	2	-	-	6						
Усього годин	90	18	18	-	-	54						

4.3. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1.	Історія розвитку ОС та ШПЗ.	2
2.	Загальна характеристика загроз безпеці ПК.	2
3.	Шкідливе програмне забезпечення.	2
4.	Шкідливі мережеві технології.	2
5.	Потенційні цілі та способи їх заисту.	2
6.	Способи протидії ШПЗ.	2
7.	Методи протидії шкідливим мережевим технологіям.	2
8.	Процедури що забезпечують безпеку даних.	2
9.	Колоквіум	2
	Разом	18

5. РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

Основна література

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. Рекомендовано до друку вченою радою Київського університету імені Бориса. – 2021. – 320 с.
4. 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
5. Вишня В. Б. Основи інформаційної безпеки : навч. посіб. / В.Б. Вишня, О.С. Гавриш, Е.В. Рижков. Дніпро: ДДУВС, 2020. 128 с. https://er.dduvs.in.ua/handle/123456789/4206
6. 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
7. 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.
8. Заплотинський, Б.А. Основи інформаційної безпеки / Б. А. Заплотинський. — Київ : КІВіП НУ “ОЮА”, 2017. — 128 с.
9. Захист інформації в комп’ютерних системах: підручник / В. Д. Козюра, В.О. Хорошко, М. Є. Шелест, Ю. М Ткач, О.О.Балюнов. – Ніжин: ФОП Лук’яненко В.В., ТПК «Орхідея», 2020. – 236с. http://ir.stu.cn.ua/handle/123456789/19248?locale-attribute=ru
10. Захист інформації в комп'ютерних системах та мережах : навч. посібник / С. Г. Семенов [та ін.] ; Нац. техн. ун-т "Харків. політехн. ін-т". – Харків : НТУ "ХПІ", 2014. – 251 с. http://repository.kpi.kharkov.ua/handle/KhPI-Press/37596
11. Кібербезпека: сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсеєв, О.Г. Король. Львів: «Новий Світ-2000», 2020. 678 с. http://ns2000.com.ua/wp-content/uploads/2019/11/Kiberbezpeka-suchasni-tekhnolohii-zakhystu.pdf

12. Кібергігієна. Кібербезпека. Безпека держави : матеріали наукових семінарів (Київ, 27 листопада 2020 р.) / відп. ред. А. М. Десятко. – Київ : Київ. нац. торг.-екон. ун-т, 2020. – 101 с. https://knute.edu.ua/file/MjExMzA=/d8e24930571c0d91476be247343bb902.pdf
13. Лужецький В. А., Кожухівський А. Д,, Войтович О. П. Основи інформаційної безпеки: навчальний посібник. Вінниця: ВНТУ. 2013. 221 с.
14. 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.
15. Остапов С. Е., Євсеєв С. П., Король О.Г.. «Кібербезпека : сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів». – Львів: «Новий Світ- 2000», 2020 . – 678 с.
16. 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.
17. ISO 15408-1: 2005. Інформаційні технології. Методи захисту. Критерії оцінки для інформаційних технологій. Частина 1. Вступ і загальна модель.
18. ISO 15408-2: 2005. Інформаційні технології. Методи захисту. Критерії оцінки для інформаційних технологій. Частина 2. Функціональні вимоги безпеки.
19. ISO 15408-3: 2005. Інформаційні технології. Методи захисту. Критерії оцінки для інформаційних технологій. Частина 3. Вимоги до забезпечення захисту.
20. ISO 17799: 2005. Інформаційні технології. Методи захисту. Практичні рекомендації з управління інформаційної безпеки

Інформаційні ресурси в мережі Інтернет

1. The Web We Want (Інтернет, який ми хочемо) Доступно з електронного джерела: http://www.webwewant.eu/documents/10180/973204/Handbook_teachers_lesson_plans_all_UA.pdf/87b2bd1c-bcab-4701-8017-19dff1887003