ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет програмування та комп'ютерних і телекомунікаційних систем
Кафедра кібербезпеки та комп'ютерних систем і мереж

ЗАТВЕРДЖУЮ
Декан ФПКТС
_____ Савенко О.С.
«___» _____ 2021 р.

СИЛАБУС

Навчальна дисципліна: **"Програмні і програмно-апаратні засоби захисту інформаційних систем від несанкціонованого доступу"**

Освітньо-професійна програма: **Кібербезпека**

Рівень вищої освіти: **перший (бакалаврський)**

Загальна інформація

Позиція	Зміст інформації
Викладач(і)	Муляр Ігор Володимирович
Профайл викладача	http://ksm.khnu.km.ua/sklad-kafedry/
E-mail викладача(ів)	betsmen555@gmail.com
Контактний телефон	+3 8 0679381544
Сторінка дисципліни в ІСУ	https://msn.khnu.km.ua/course/view.php?id=6540
Сторінки інтернет-ресурсів для онлайн занять	ZOOM: https://us04web.zoom.us/j/5011940672 * пароль у викладача, старости групи і на сторінці дисципліни в ІСУ
Навчальний рік, семестр	2020-2021, семестр IV (зимово-весняний)
Розклад занять	Лекції: понеділок, 3 пара (чисельник), онлайн Лабораторні роботи: четвер, 1-2 пара (чисельник), 1-113
Консультації	Очні: вівторок, 6-а пара, 1-103 Онлайн: за необхідністю та попередньою домовленістю

Характеристика дисципліни

Форма навчання	Курс	Семестр	Загальне навантаження		Кількість годин						Курсовий проект	Курсова робота	Форма семестрового контролю	
					Аудиторні заняття				Індивідуальна робота студента	Самостійна робота студента				
			Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття					Залік	Іспит
Д	2	4	5	150	54	18	36	-	-	96	-	-	+	-

Анотація дисципліни

Дисципліна “Програмні і програмно-апаратні засоби захисту інформаційних систем від несанкціонованого доступу” - одна з спеціальних профілюючих дисциплін професійної підготовки бакалаврів зі спеціальності „Кібербезпека”, орієнтована на систематизацію інформації про сучасний стан програмних і програмно-апаратних засобів захисту інформаційних систем від несанкціонованого доступу, формування комплексу базових знань і практичних навичок з розробки і використання сучасних методів створення систем захисту інформаційних ресурсів, методів захисту від несанкціонованого доступу до програм, способів протидії несанкціонованому копіюванню, використанню, статичному вивченню та динамічному дослідженню захищених програм, необхідних при вивченні подальших дисциплін і в професійній діяльності.

При викладанні дисципліни використовуються наступні форми (методи) навчання: пояснювально-ілюстративні, практичні, продуктивні, тренінгові, застосування інформаційно-комп’ютерних технологій (MS CryptoAPI, антивірусне ПЗ, апаратні ключі захисту тощо).

Пререквізити: мережеві операційні системи.

Кореквізити: комплексні системи захисту інформації: проєктування, впровадження, супровід; проєктно-технологічна практика.

Мета і завдання дисципліни

Мета дисципліни. Формування знань та розуміння предметної області і професійних навиків на основі вивчення передового досвіду, сучасних підходів, методів та програмних і програмно-апаратних засобів захисту інформаційних систем від несанкціонованого доступу.

Предмет дисципліни. Методи та програмні і програмно-апаратні засоби захисту інформаційних систем від несанкціонованого доступу.

Завдання дисципліни. Вивчення і набуття практичних навичок використання передового досвіду і сучасних підходів, методів, програмних та програмно-апаратних засобів захисту інформаційних систем; основних понять щодо програмного та програмно-апаратного захисту програм та інформації; ідентифікації та аутентифікації користувачів комп’ютерних систем; засобів і методів обмеження доступу до програм, несанкціонованого копіювання, захисту програмних засобів від дослідження.

компетентності:

КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах/

КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.

результати навчання:

РН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами, та давати оцінку результативності якості прийнятих рішень.

РН 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.

РН 18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.

РН 20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.

РН 23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

РН 31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.
РН 41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.
РН 48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.
РН 50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).
РН 53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз.

Студент, який успішно завершив вивчення дисципліни, повинен: *використовувати* програмні та програмно-апаратні комплекси засобів захисту інформаційних ресурсів інформації в інформаційно-телекомунікаційних (автоматизованих) системах, сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій, *вирішувати* задачі аналізу програмного коду на наявність можливих загроз, завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами, та *давати оцінку* результативності якості прийнятих рішень, *забезпечувати* функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах, функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); використовувати інформаційно-комунікаційні технології, сучасні методи і моделі інформаційної безпеки та/або кібербезпеки, застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем, *реалізовувати* заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; *забезпечувати* захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах, з метою реалізації встановленої політики інформаційної та/або кібербезпеки, *підтримувати* працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; *використовувати* програмні та програмно-апаратні комплекси засобів захисту для забезпечення неперервності процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур; *застосовувати* методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності, *виконувати* впровадження та підтримку систем виявлення вторгнень.

Тематичний і календарний план вивчення дисципліни

Номер тижня	Номер теми	Тема лекції*	Тема лабораторної роботи**	Самостійна робота студента		
				Зміст	Години	Література
1	2	3	4	5	6	7
1	1	**Предмет і задачі дисципліни. Використання засобів захисту від несанкціонованого доступу (НСД).** Предмет і задачі дисципліни. Задачі протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах. Базові функції захисту від НСД. Загальна характеристика і класифікація заходів і засобів захисту інформації від несанкціонованого доступу. Реалізація заходів з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах. Аналіз сучасного програмно-апаратного забезпечення захисту від несанкціонованого доступу.	ЛР1. Організація захисту інформації від несанкціонованого доступу в автоматизованих системах класу «1» із застосуванням програмного засобу ЛОЗА™-1**.**	Опрацювання теоретичного матеріалу, підготовка до виконання ЛР1.	5	[1] с.131-143; [2] с.19-38, 328-343, с.500-515; [3] с.163-178; [4] с.60-66; [8] с.2-44; [10] с.64-84; [19-22].

2	1			Опрацювання теоретичного матеріалу, підготовка до захисту ЛР1.	5	[1] с.112-131, 164-192 ; [3] с.188-192; [10] с.64-84; [22]; [23].
3	1	**Програмні і програмно-апаратні системи інформаційної безпеки.** Архітектура та загальні особливості операційних центрів безпеки (SOC). Система управління інформаційною безпекою (SIM). Система управління подіями безпеки (SEM). Система збору та кореляції подій безпеки(SIEM). Фукціональність систем. Приклади використання. Журналювання даних і генерації звітів. IBM Security QRadar SIEM**.** Система запобігання витоку конфіденційної інформації (DLP). Лінгвістичні та статистичні механізми визначення ступеня конфіденційності документа**.**	ЛР2. Застосування ЛОЗА™-1 як засобу неперервного автоматизованого ведення журналів реєстрації подій та інцидентів.	Опрацювання теоретичного матеріалу, підготовка до виконання ЛР2.	5	[3] с.188-192; [22]; [23].
4	1			Опрацювання теоретичного матеріалу, підготовка до захисту ЛР2.	6	[3] с.188-192; [22]; [23].
5	2	**Методи та засоби захисту програмного забезпечення та інформації.** Мета і доцільність використання систем захисту (СЗ). Завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами. Вимоги до	ЛР3. Робота з засобами відновлення та стирання даних, програм та носіїв інформації.	Опрацювання теоретичного матеріалу, підготовка до виконання ЛР3.	5	[1] с.112-131; [2] с.473-499, с.510-515; [4] с.138-145; [6] с.13-25; [7] с.6-12; [19-22].

		систем захисту від несанкціонованого копіювання. Класифікація СЗ ПЗ. Пакувальники/шифратори. Системи захисту від несанкціонованого копіювання. Системи захисту від несанкціонованого доступу. Основні алгоритми захисту програмного забезпечення. Показники застосовності та критерії оцінювання СЗ ПЗ. Основні вимоги до розробки систем захисту ПЗ. Розповсюджені типи захистів та їх недоліки.				
6	2			Опрацювання теоретичного матеріалу, підготовка до захисту ЛР3.	5	[2] с.492-495. [8] с 277-283, с. 387-391.
7	2	**Методи та засоби дослідження програмного коду виконуваних файлів на наявність можливих загроз.** Задачі аналізу програмного коду на наявність можливих загроз Загальні відомості про компілятори і декомпілятори. Інструменти для статичного дослідження Методи аналізу програм із допомогою HEX-редакторів, дизасемблерів та відладчиків. Основні методи протидії дизасемблюванню програм. Захист програм шляхом обфускації.	ЛР4. Використання програмно-апаратного комплексу Sentinel LDK для захисту інформаційних ресурсів шляхом створення апаратних ключів.	Опрацювання теоретичного матеріалу, підготовка до виконання ЛР4.	5	[2] с.488-491; [5] с.154-194, с.328-372; [6] с.33-71; [7] с.13-40, с.53-74.
8	2			Опрацювання теоретичного матеріалу,	8	[1] с.201-235; [3] с.205-209; [9] с. 117-129.

				підготовка до тестування і до захисту ЛР4.		
9	3	**Програмні і програмно-апаратні засоби ідентифікації та аутентифікації користувачів.** Ідентифікація користувачів. Аутентифікація користувачів. Протоколи ідентифікації та аутентифікації. Технічні засоби ідентифікації і аутентифікації. Носії ключової інформації (флеш пам'ять, електронні ключі, SMART-карти, пристрої Touch-Memory). Електронні ключі.	Тестування. ЛР5. Побудова системи захисту інформаційних ресурсів шляхом створення програмно-цифрових ліцензійних ключів засобами Sentinel LDK та їх дистанційне адміністрування.	Опрацювання теоретичного матеріалу, підготовка до виконання ЛР5, підготовка до тестування	5	[1] с.143-164; [2] с.272-325; [3] с.188-192; [11] с. 225-227.
10	3			Опрацювання теоретичного матеріалу, підготовка до захисту ЛР5.	5	[1] с.201-235; [9] с. 117-129, с. 151-160.
11	3	**Електронний цифровий підпис як засіб захисту від несанкціонованого доступу.** Електронний цифровий підпис. Сертифіковані ключі, стандарт X.509. Сфери застосування інфраструктури відкритих ключів та цифрових сертифікатів. Особливості програми Ciphermail для захищеного обміну e-mail.	ЛР6. Дослідження структури виконуваних файлів на наявність можливих загроз в програмному коді.	Опрацювання теоретичного матеріалу, підготовка до виконання ЛР6	5	[3] с.205-209; [8] с. 311-324; [9] с. 117-129, с. 151-162.
12	3			Опрацювання теоретичного матеріалу, підготовка до захисту ЛР6.	5	[5] с.154-236, с.328-372; [6] с.33-71; [7] с.13-40.
13	3	**Засоби захисту від щкідливого програмного забезпечення. Антивірусні комплекси.** Типи шкідливого ПЗ.	ЛР7. Дослідження ліцензійних та безкоштовних засобів захисту від шкідливого програмного забезпечення.	Опрацювання теоретичного матеріалу, підготовка до виконання ЛР7.	5	[1] с.276-301; [3] с.98-201; [5] с.239-282; [8] с.72-110, с.354-393.

		Класифікація шкідливих програм. Принципи створення та аналізу троянських програм. Життєвий цикл вірусу. Принципи створення та аналізу вірусів. Спеціальне програмне забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телеко мунікаційних системах. Протидія і виявлення троянських програм, черв'яків та вірусів. Основи роботи антивірусних програм. Сигнатурний аналіз. Евристичні аналізатори. Поведінкові блокатори. Протидія шкідливому коду. Шкідливе ПЗ для мобільних пристроїв. Етапи забезпечення антивірусного захисту. Концепція антивірусної безпеки. Політика антивірусної безпеки. Антивірусні комплекси. Особливості ESET Secure Business. Структура та алгоритми роботи антивірусних комплексів.				
14	3			Опрацювання теоретичного матеріалу, підготовка до захисту ЛР7.	5	[1] с.271-300; [3] с.198-201.
15	3	**Засоби захисту інформації від руйнуючих програмних впливів і руйнуючих кодів в інформаційно-телек омунікаційних системах.** Забезпечення функціонування спеціального програмного забезпечення, Формат файлів PE-програм і	ЛР8 Використання компонентів криптографічного захисту бібліотеки CRYPTOAPI для забезпечення необхідного рівня захищеності інформації.	Опрацювання теоретичного матеріалу, підготовка до виконання ЛР8.	5	[1] с.276-301; [5] с.194-236; [7] с.13-39.

		його використання для файлових вірусів. Імпорт об'єктів. Функціонування вірусів.				
16	3			Опрацювання теоретичного матеріалу, підготовка до захисту ЛР8.	6	[1] с.201-235; [3] с.205-209; [8] с. 311-324; [9] с. 151-160.
17	3	**Засоби виявлення атак і протидії несанкціонованому доступу.** няття систем виявлення атак. Заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телеко мунікаційних (автоматизованих) системах. Система виявлення мережевих вторгнень (NIDS). Функції систем виявлення атак. IDS. IDM. Аналіз сигнатур. Статистичний аналіз. Контроль цілісності системами виявлення атак. Методи зміни мережевого середовища. Оцінка вірогідності атак. Види систем виявлення атак.	Тестування.	Опрацювання теоретичного матеріалу, підготовка до тестування.	6	[2] с.371-380; [3] с.193-195; [4] с.25-95; [8] с. 234-249; [11] с.210-225.
18	3		Підсумкове заняття	Опрацювання теоретичного матеріалу.	5	[2] с.371-380; [3] с.193-195; [4] с.25-95; [8] с. 234-249; [11] с. 210-225

Умовні позначення: ЛР – лабораторна робота

* лекції проводяться по 2 години раз на два тижні.

** лабораторні роботи проводяться раз у два тижні по 4 години

Політика дисципліни

Організація освітнього процесу з дисципліни відповідає вимогам положень про організаційне і навчально- методичне забезпечення освітнього процесу, освітній програмі та навчальному плану. Студент зобов'язаний відвідувати лекції і лабораторні роботи згідно з розкладом, не запізнюватися на заняття, контрольні точки виконувати відповідно до графіка. Пропущену лабораторну роботу студент зобов'язаний опрацювати самостійно у повному обсязі і відзвітувати перед викладачем не пізніше, ніж за тиждень до чергової атестації. До лабораторних робіт студент має підготуватися за відповідною темою і проявляти активність. Набутті особою знання з дисципліни або її окремих розділів у неформальній освіті зараховуються відповідно до Положення про порядок перезарахування результатів навчання та визначення академічної різниці у ХНУ https://www.khnu.km.ua/root/files/01/10/03/006.pdf.

Оцінювання результатів навчання студентів

Оцінювання академічних досягнень студента здійснюється відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ». Кожний вид роботи з дисципліни оцінюється за інституційною чотирибальною шкалою. Семестрова підсумкова оцінка визначається як середньозважена з усіх видів навчальної роботи, виконаних і зданих позитивно з урахуванням коефіцієнта вагомості. Вагові коефіцієнти змінюються залежно від структури дисципліни і важливості окремих видів її робіт.

Структурування дисципліни за видами робіт і оцінювання результатів навчання студентів у семестрі за ваговими коефіцієнтами

Аудиторна робота		**Контрольні заходи**		**Підсумковий контрольний захід**
Вид заняття	Лабораторна робота	Тестовий контроль 1	Тестовий контроль 2	Залік за рейтингом
Тема	Т 1-3	Т 1-2	Т3	
Ваговий коефіцієнт	0,8	0,10	0,10	

Оцінювання лабораторних робіт. Оцінка, яка виставляється за лабораторне заняття, складається з таких елементів: усне опитування студентів перед допуском до виконання лабораторної роботи; знання теоретичного матеріалу з теми; якість оформлення протоколу і графічної частини; вільне володіння студентом спеціальною термінологією і уміння професійно обґрунтувати прийняті конструктивні рішення; своєчасний захист лабораторної роботи.

Термін захисту звіту з лабораторної роботи вважається своєчасним, якщо студент захистив її в день виконання або на наступному після виконання роботи занятті. Пропущене лабораторне заняття студент зобов'язаний відпрацювати в лабораторіях кафедри у встановлений викладачем термін з реєстрацією у відповідному журналі кафедри, але не пізніше, ніж за два тижні до кінця теоретичних занять у семестрі.

Оцінку за лабораторне заняття викладач оголошує одразу після захисту звіту з лабораторної роботи і проставляє в електронний журнал дисципліни.

Оцінювання тестових завдань. Тематичний тест для кожного студента складається з п'ятнадцяти тестових завдань, кожне з яких оцінюється одним балом. Максимальна сума балів, яку може набрати студент, складає 15.

Відповідність набраних балів за тестове завдання оцінці, що виставляється студенту

Сума балів за тестове завдання	1–5	6–10	11–13	14–15
Оцінка за 4-ри бальною шкалою	2	3	4	5

На тестування відводиться 15 хвилин (для закритої форми тестів – по одній хвилині на кожне завдання). Правильні відповіді студент записує у талоні відповідей. При цьому усі графи

для відповідей мають бути заповнені цифрами, що відповідають правильним, на погляд студента, відповідям. Через 15 хвилин студенти здають викладачу завдання з талонами відповідей.

Тестування студент може також пройти і в он-лайн режимі в модульному середовищі для навчання MOODLE.

Оцінку за тестування викладач проставляє в електронний журнал дисципліни.

Засвоєння студентом теоретичного матеріалу з дисципліни оцінюється за наведеними в таблиці критеріями оцінювання знань.

Критерії оцінювання знань студентів

Оцінка за інституційною шкалою	Узагальнений критерій
1	*2*
Відмінно	Студент глибоко і у повному обсязі опанував зміст навчального матеріалу, легко в ньому орієнтується і вміло використовує понятійний апарат; уміє пов'язувати теорію з практикою, вирішувати практичні завдання, впевнено висловлювати і обґрунтовувати свої судження. Відмінна оцінка передбачає, логічний виклад відповіді державною мовою (в усній або у письмовій формі), демонструє якісне оформлення роботи і володіння спеціальними інструментами. Студент не вагається при видозміні запитання, вміє робити детальні та узагальнюючі висновки. При відповіді допустив дві-три несуттєві похибки.
Добре	Студент виявив повне засвоєння навчального матеріалу, володіє понятійним апаратом і фаховою термінологією, орієнтується у вивченому матеріалі; свідомо використовує теоретичні знання для вирішення практичних задач; виклад відповіді грамотний, але у змісті і формі відповіді можуть мати місце окремі неточності, нечіткі формулювання закономірностей тощо. Відповідь студента будується на основі самостійного мислення. Студент у відповіді допустив дві–три несуттєві помилки.
Задовільно	Студент виявив знання основного програмного матеріалу в обсязі, необхідному для подальшого навчання та практичної діяльності за професією, справляється з виконанням практичних завдань, передбачених програмою. Як правило, відповідь студента будується на рівні репродуктивного мислення, студент має слабкі знання структури курсу, допускає неточності і суттєві помилки у відповіді, вагається при відповіді на видозмінене запитання. Разом з тим, набув навичок, необхідних для виконання нескладних практичних завдань, які відповідають мінімальним критеріям оцінювання і володіє знаннями, що дозволяють йому під керівництвом викладача усунути неточності у відповіді.
Незадовільно	Студент виявив розрізнені, безсистемні знання, не вміє виділяти головне і другорядне, допускається помилок у визначенні понять, перекручує їх зміст, хаотично і невпевнено викладає матеріал, не може використовувати знання при вирішенні практичних завдань. Як правило, оцінка "незадовільно" виставляється студенту, який не може продовжити навчання без додаткової роботи з вивчення дисципліни.

Якщо студент отримав негативну оцінку за певним видом робіт, то він має перездати її в установленому порядку, але обов'язково до терміну наступного контролю.

У випадку, коли студент не виконав індивідуальний план з дисципліни у заплановані терміни без поважних причин, то під час відпрацювання заборгованості при позитивній відповіді йому виставляється оцінка „задовільно”.

Студент, який у встановлені терміни не виконав індивідуальний план поточної роботи з дисципліни повністю або частково, до здачі підсумкового контрольного заходу не допускається.

Залік вважається зданим при отриманні студентом за зведеними результатами поточного контролю підсумкової оцінки з дисципліни від 3,00 до 5,00 балів. При цьому за вітчизняною шкалою ставиться оцінка за двобальною шкалою, а за шкалою ECTS – оцінка, що відповідає набраній студентом кількості балів.

Підсумкова семестрова оцінка за інституційною шкалою і шкалою ЄКТС встановлюється в автоматизованому режимі після внесення викладачем усіх оцінок до електронного журналу.

Співвідношення вітчизняної шкали оцінювання і шкали оцінювання ЄКТС

Оцінка ЄКТС	**Інституційна інтервальна шкала балів**	**Інституційна оцінка, критерії оцінювання**		
A	4,75–5,00	5	Зараховано	***Відмінно*** – глибоке і повне опанування навчального матеріалу і виявлення відповідних умінь та навиків
B	4,25–4,74	4		***Добре*** – повне знання навчального матеріалу з кількома незначними помилками
C	3,75–4,24	4		***Добре*** – в загальному правильна відповідь з двома-трьома суттєвими помилками
D	3,25–3,74	3		***Задовільно*** – неповне опанування програмного матеріалу, але достатнє для практичної діяльності за професією
E	3,00–3,24	3		***Задовільно*** – неповне опанування програмного матеріалу, що задовольняє мінімальні критерії оцінювання
FX	2,00–2,99	2	Незарахо-вано	***Незадовільно*** – безсистемність одержаних знань і неможливість продовжити навчання без додаткових знань з дисципліни
F	0,00–1,99	2		***Незадовільно*** – необхідна серйозна подальша робота і повторне вивчення дисципліни

Питання для самоконтролю студентів

1. Вимоги із захисту службової інформації від несанкціонованого доступу.
2. Загальна характеристика і класифікація заходів і засобів захисту інформації від несанкціонованого доступу.
3. Технічні засоби захисту інформації від їх витоку.
4. Програмні засоби захисту інформації від несанкціонованого доступу
5. Шкідливі ПЗ.
6. Засоби захисту від комп'ютерних вірусів та їх особливості.
7. Шкідливе ПЗ для мобільних пристроїв.
8. DLP-системи.
9. Контекстний контроль в DLP-системі.
10. Тематична фільтрація в DLP-системі.
11. Засоби «Батьківського контролю», як елементи захисту неповнолітніх від шкідливого контенту.
12. Засоби блокування реклами як елементи захисту від небажаного контенту.
13. Засоби відновлення програм, даних та носіїв інформації.
14. SIEM – системи.
15. Основні сучасні комп'ютерні віруси: види, будова, особливості дії.
16. Основи роботи антивірусних програм.
17. Антивірусні програми: типи, властивості, особливості застосування.
18. Криптографічні методи захисту інформації: технологія, особливості застосування.
19. Основні сучасні програмно-апаратні заходи забезпечення безпеки інформації.
20. Методи захисту від вірусів: види, переваги та недоліки.
21. Основні принципи захисту інформації від несанкціонованого доступу.
22. Основні вимоги до розробки засобів захисту ПЗ.
23. Програми-дебагери (налагоджувачі) і їх використання для зламу програм.
24. Програми-декомпілятори з різних мов програмування
25. Пакувальники-шифрувальники програмного забезпечення, їх негативні та позитивні сторони.
26. Захист від несанкціонованого доступу програмного забезпечення за допомогою парольного захисту, його позитивні і негативні сторони.
27. Засоби подолання захистів програмного забезпечення шляхом копіювання областей ОЗП, відновлення вилучених файлів.
28. Засоби подолання захистів програмного забезпечення: файлові оболонки, програми пошуку файлів та послідовностей у них, засоби побітового копіювання, програми-монітори файлових систем, монітори системних файлів, програми-монітори виклику підпрограм.
29. Можливості використання завантажувального запису для захисту програмного забезпечення.
30. Засоби динамічного аналізу алгоритмів захисту програм.
31. Засоби статичного дослідження алгоритмів захисту програм.
32. Захист програмного забезпечення від дизасемлювання шляхом маніпулювання з EXE-заголовками.
33. Поняття обфускації програм. Мета обфускації та її види.
34. Основні програмні засоби для здійснення динамічного дослідження програм
35. Поняття про ідентифікацію користувача та її особливості. Основні принципи та методи аутентифікації.
36. Технічні засоби ідентифікації і аутентифікації.
37. Носії ключової інформації (флеш пам'ять, електронні ключі, SMART-карти, пристрої Touch-Memory).
38. IDS – системи.
39. IDM – системи.
40. Електронний цифровий підпис *(digital signature)* у захисті програмних продуктів.
41. Захист від несанкціонованого доступу програмного забезпечення шляхом програмно-апаратних засобів за допомогою електронного ключа, його позитивні і негативні сторони.

42. Заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
43. Цифрові підписи як перспективна технологія захисту інформації.
44. Забезпечення функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.
45. Спеціальне програмне забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.
46. Різновиди методів подання, зберігання, передачі та обробки інформації та аналіз їх незахищеності від стороннього втручання.
47. Уразливість інформації та сучасний погляд на її захист від несанкціонованого доступу.
48. Засоби захисту ПЗ від несанкціонованого копіювання.
49. Перетворення та захист інформації при накопичуванні та передачі адресатам.
50. Збереження захищеної інформації.

Методичне забезпечення

Навчальний процес з дисципліни “Програмні і програмно-апаратні засоби захисту інформаційних систем від несанкціонованого доступу” повністю і в достатній кількості забезпечений необхідною навчально-методичною літературою, розміщеною в електронному варіанті в модульному середовищі.

Рекомендована література

Основна

№	Назва	Режим доступу
1.	Бурячок В. Л. Основи інформаційної та кібернетичної безпеки: навчальний посібник / В. Л. Бурячок, Р. В. Киричок, П. М. Складанний – К., 2018. – 320 с.	http://elibrary.kubg.edu.ua/id/eprint/27370/1/V_Buriachok_Posibnik_2019_FITU.pdf
2.	Інформаційна безпека: навчальний посібник / [Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв та ін.]; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого. – Львів: Видавництво Львівської політехніки, 2019. – 580 с.	https://drive.google.com/file/d/1jACvCh2O4duJOYA3uLUID8cdVf2EFSWU/view?usp=sharing
3.	Даник Ю.Г. Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. – [Видання друге, перероб. та доп.]. – Одеса.: ОНАЗ ім. О.С. Попова, 2019. − 320 с.	https://metod.onat.edu.ua/download/686
4.	Інформаційна безпека держави: навчальний посібник/ В.І. Гур’єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова. – Ніжин: ФОП Лук’яненко В.В. ТПК «Орхідея», 2018. – 166 с.	http://ir.stu.cn.ua/bitstream/handle/123456789/19246/Інформ.%20безпека%20держ.%20New%20booklet%201.pdf?sequence=1&isAllowed=y
5.	Learning Malware Analysis. Explore the concepts, tools, and techniques to analyze and investigate Windows malware Security / Edited by Monnappa K A. – Packt Publishing Ltd, 2018. – 500 p.	https://www.pdfdrive.com/learning-malware-analysis-explore-the-concepts-tools-and-techniques-to-analyze-and-investigate-windows-malware-d176269731.html
6.	Каплун В. А. Захист програмного забезпечення : лабораторний практикум / В. А. Каплун, О. В. Дмитришин, Ю. В. Баришев – Вінниця : ВНТУ, 2015. – 72 с.	https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/14332/Захист%20програмного%20забезпечення.%20Лабораторний%20практикум.%202015.pdf?sequence=1&isAllowed=y
7.	Каплун, В. А. Захист програмного забезпечення. Частина 2 : навчальний посібник / В. А. Каплун, О. В. Дмитришин, Ю. В. Баришев – Вінниця : ВНТУ, 2014. – 105 с.	https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/14257/Kaplun-6678619f16033b998a0c233b1e652488.pdf?sequence=1&isAllowed=y
8.	Fundamentals of Information Systems Security / Editors : David Kim, Michael G. Solomon. – Burlington, Massachusetts : Jones & Bartlett Learning, 2018. – 548 p.	https://www.pdfdrive.com/fundamentals-of-information-systems-security-d186521700.html
9.	Технології захисту інформації [Електронний ресурс] / Ю. А. Тарнавський; – Електронні текстові дані (1 файл: 2,04 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2018. – 162 с.	https://ela.kpi.ua/bitstream/123456789/23896/1/TZI_book.pdf
10.	Основи інформаційної безпеки. Конспект лекцій / Б.А. Заплотинський. – КІВіП НУ “ОЮА”, 2017. – 128 с.	http://dspace.onua.edu.ua/bitstream/handle/11300/11111/ОІБ%20конспект%20лекцій.pdf?sequence=1&isAllowed=y
11.	Організація захисту інформації з обмеженим доступом : підручник / А.М. Гуз**,** І.П. Касперський, С.О.Князєв та ін. – К.: Нац. акад., СБУ, 2018. –252 с.	http://zacon.at.ua/load/0-0-0-66-20

12.	Еременко, В.Т. Программно-аппаратные средства защиты информации: учебное пособие для высшего профессионального образования / В.Т.Еременко, А.П. Фисун. – Орел: ФГБОУ ВПО «Госуниверситет – УНПК», 2015. – 165 с.	https://www.pdfdrive.com/Еременко-В-Т-Программно-аппаратные-средства-защиты-информации-e187927195.html

Додаткова

13.	Эриксон Д. Хакинг: искусство эксплойта / Эриксон Джон. – [2-е изд.] – СПб.: Питер, 2010. – 512 с.	https://drive.google.com/file/d/1BzAbi0jWjpSNHeAOblZ9-g5foaM9EHoT/view?usp=sharing
14.	Організаційно-правові основи захисту службової інформації: навч. посіб. /1. П. Касперський, С. 0. Князєв, О. І. Матяш та ін. – Київ : Нац. акад. СБУ, 2017. – 120 с.	http://zacon.at.ua/_ld/0/72__17.pdf
15.	Методичні рекомендації до лабораторних робіт з дисципліни «Безпека програмного забезпечення комп'ютерних систем» / В.Г. Бабенко, Т.В. Миронюк, Т.А. Стабецька – Черкаси : ЧДТУ, 2018. – 42 с.	https://er.chdtu.edu.ua/bitstream/ChSTU/78/1/Метод_реком_БПЗКС-2017.pdf
16.	Методичні вказівки для лабораторних робіт з дисципліни «Захист інформації у комп'ютерних системах» / Р.О. Жаровський. – Тернопіль : ТНТУ, 2019. – 68 с.	http://elartu.tntu.edu.ua/bitstream/lib/29277/1/%21%21_Lab_print_zahust_2019%20123.pdf
17.	Information Security. Foundations, technologies and applications / Editors : Ali Ismail Awad, Michael Fairhurst. – The Institution of Engineering and Technology, 2018. – 418 p.	https://www.pdfdrive.com/information-security-foundations-technologies-and-applications-d187541495.html
18.	НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого. – Чинний від 28 квітня 1999 р. – Київ : ДСТСЗІ СБ, 1999. – [21] с.	https://tzi.com.ua/downloads/1.1-002-99.pdf
19.	НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. – Чинний від 28 квітня 1999 р. – Київ : ДСТСЗІ СБ, 1999. – [23] с.	https://tzi.com.ua/downloads/1.1-003-99.pdf
20.	НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. – Чинний від 28 квітня 1999 р. – Київ : ДСТСЗІ СБ, 1999. – [67] с.	https://tzi.com.ua/downloads/2.5-004-99.pdf
21.	НД ТЗІ 2.5-008-2002. Вимоги із захисту службової інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2. – Чинний від 13 грудня 2002р. – Київ : ДСТСЗІ СБ, 1999. – [29] с.	https://tzi.ua/assets/files/НД-ТЗІ-2.5-008-2002.pdf
22.	ЛОЗА-1-4.І3.03.1. Інструкція системного адміністратора - Київ : ТОВ НДІ "Автопром", 2020 – [22] с.	http://avtoprom.kiev.ua/avtoprom/sites/default/files/LOZA-1_4_SysAdmin.pdf
23.	Микитишин А. Г. Комплексна безпека інформаційних мережевих систем: навчальний посібник / А.Г. Микитишин, М.М. Митник, П.Д. Стухляк. .– Тернопіль: ТНТУ, 2016. – 255 с	http://elartu.tntu.edu.ua/handle/123456789/18299
24.	Муляр, І.В. Метод надання доступу до сервісів однорангової розподіленої хмарної системи / І. В. Муляр, А. С. Сівак // Вимірювальна та обчислювальна техніка в технологічних процесах. – 2019. – №1. – С. 65-73.	http://elar.khnu.km.ua/jspui/handle/123456789/8246
25.	Муляр І.В. Динамічні показники оцінки рівня функціональної безпеки інформаційної системи ./ С.В.Ленков, В.М.Джулій, І.В. Муляр -Сучасна спеціальна техніка. Науково практичний журнал. – ДНДІ МВС України, 2016. – Вип. №2(45). – С.59-66	http://nbuv.gov.ua/UJRN/sstt_2016_2_11
26.	Shevchenko S. Analysis and research of the characteristics of standardized in ukraine antivirus software / S. Shevchenko, P. Skladannyi, M. Martseniuk // Кібербезпека: освіта, наука, техніка, Київ, 2019. – Вип. 4 (4). – с. 62-71	https://csecurity.kubg.edu.ua/index.php/journal/article/view/82
27.	Nizovtsev Yu. The usage of antivirus software in forensic expertise against malicious software means / Yu. Nizovtsev, O. Yakovlev // Scientific journal of the National Academy of Public Prosecutor of Ukraine, 2017. – № 4(16). – P. 161–169	http://www.chasopysnapu.gp.gov.ua/chasopys/ua/pdf/4-2017/nizovcev.pdf

28.	Інформаційна безпека держави : підручник / [В.М. Петрик, М.М. Присяжнюк, Д.С. Мельник та ін.]; в 2 т. - Т.1. / за аг. ред.. В.В. Остроухова. – К. : ДНУ «Книжкова палата Україна», 2016. – 264 с	https://mil.univ.kiev.ua/files/7_50255454.pdf
29.	Kali Linux. Тестирование на проникновение и безопасность / П. Шива, З. Алекс, Х. Теди и др. – СПб.: Питер, 2020. – 448 с.	https://drive.google.com/drive/folders/0AOwk3E6vGowtUk9PVA
30.	Методи і алгоритми захисту інформаційних ресурсів комп'ютерних систем : навч. посіб. / В. М. Джулій, Ю. П. Кльоц, І. В. Муляр, В. М. Чешун. Хмельницький : ХНУ, 2021. 174 с.	https://drive.google.com/file/d/1-ZmFMuTkL5VnBgh1bXNfD6nODchxWI4U/view?usp=sharing
31.	Захист від прихованих загроз в середовищі хмарних обчислень / І. В. Муляр, О. В. Мірошниченко, А. В. Краснік, Л. В. Солодєва // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – Київ : ВІКНУ, 2018. – Вип. 59. – С. 115-126.	http://elar.khnu.km.ua/jspui/handle/123456789/6986
32.	Метод предикативної ідентифікації процесів для захисту від прихованих загроз в середовищі хмарних обчислень / С. В. Лєнков, В. М. Джулій, О. В. Селюков, І. В. Муляр // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – 2017. – Вип. 55. – С. 145–154.	http://nbuv.gov.ua/UJRN/Znpviknu_2017_55_19

Інформаційні ресурси

Електронний університет:

1. Модульне середовище для навчання MOODLE (розміщені усі необхідні матеріали з дисципліни, в тому числі завдання для поточного та семестрового контролю знань) Доступ до ресурсу: https://msn.khnu.km.ua/course/view.php?id=6540

2. Електронна бібліотека університету. Доступ до ресурсу: http://lib.khnu.km.ua/asp/php_f/p1age_lib.php.

Розробник _____ к.т.н., доцент _____ І.І. Муляр
Підпис | Вчений ступінь, звання | Ініціали, прізвище викладача(ів)

Погоджено

Гарант освітньої програми _____ к.т.н., доцент _____ В.М. Чешун
Підпис | Вчений ступінь, звання | Ініціали, прізвище

Зав. кафедри кібербезпеки та комп'ютерних систем і мереж _____ к.т.н., доцент _____ Ю.П. Кльоц
Підпис | Вчений ступінь, звання | Ініціали, прізвище