Міністерство освіти і науки України
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»

Кафедра комп'ютерних систем, мереж і кібербезпеки (№ 503)

ЗАТВЕРДЖУЮ

Гарант освітньої програми

_____ О. О. Ілляшенко
(підпис) (ініціали та прізвище)

«31» ___серпня_____ 2021 р.

РОБОЧА ПРОГРАМА ОБОВ'ЯЗКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Захист інформації в інформаційно-комунікаційних системах

(назва навчальної дисципліни)

Галузь знань: 12 Інформаційні технології
(шифр і найменування галузі знань)

Спеціальність: 125 Кібербезпека
(код та найменування спеціальності)

Освітня програма: " Безпека інформаційних та комунікаційних систем "
(найменування освітньої програми)

Рівень вищої освіти: перший (бакалаврський)

Харків 2021 рік

Розробник: Пєвнєв В. Я., доцент, д.т.н., доцент
(прізвище та ініціали, посада, науковий ступінь та вчене звання) (підпис)

Робочу програму розглянуто на засіданні кафедри «Комп'ютерних систем, мереж і кібербезпеки»
(назва кафедри)

Протокол № 1 від «30» 08 2021 р.

Завідувач кафедри д.т.н., професор В. С. Харченко
(науковий ступінь та вчене звання) (підпис) (ініціали та прізвище)

1. Опис навчальної дисципліни

<table>
<tr><td>Найменування показників</td><td>Галузь знань, спеціальність, освітня програма, рівень вищої освіти</td><td>Характеристика навчальної дисципліни
(денна форма навчання)</td></tr>
<tr><td>Кількість кредитів – 11,5</td><td rowspan="11">Галузь знань
12 "Інформаційні технології"
(шифр та найменування)

Спеціальність
125 Кібербезпека
(код та найменування)

Освітня програма
" Безпека інформаційних та комунікаційних систем "
(найменування)

Рівень вищої освіти:

перший (бакалаврський)</td><td>Обов’язкова</td></tr>
<tr><td>Кількість модулів – 6</td><td>Навчальний рік</td></tr>
<tr><td>Кількість змістових модулів –5</td><td>2021/ 2022</td></tr>
<tr><td>Індивідуальне завдання - 2</td><td>Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин
денна – 124 / 221</td><td>7, 8-й</td></tr>
<tr><td>Лекції</td></tr>
<tr><td rowspan="6">Кількість тижневих годин для денної форми навчання:
аудиторних –
7 сем. - 4 год;
8 сем. - 5 год
самостійної роботи студента –
7 сем. – 6,3 год;
8 сем. – 10 год.</td><td>68 годин</td></tr>
<tr><td>Практичні, семінарські</td></tr>
<tr><td>56 годин</td></tr>
<tr><td>Лабораторні</td></tr>
<tr><td></td></tr>
<tr><td>Самостійна робота</td></tr>
<tr><td>221 годин</td></tr>
<tr><td>Вид контролю</td></tr>
<tr><td>модульний контроль, іспит</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної роботи становить для денної форми навчання – 64/101.

[1)] Аудиторне навантаження може бути зменшене або збільшене на одну годину в залежності від розкладу занять.

2. Мета та завдання навчальної дисципліни

Мета вивчення: здатність аналізувати методологію створення, основні напрями, методи, алгоритми реалізації функцій захисту інформації в інформаційно-комунікаційних системах, засоби забезпечення основних вимог інформаційної безпеки..

Завдання: знати сучасні міжнародні та вітчизняні стандарти з інформаційної безпеки; знати загальні аспекти проблематики в галузі інформаційної безпеки, а також тенденції і перспективи створення механізмів захисту інформації та засобів подолання цих механізмів; розуміти властивостіі інформаційних ресурсів та технологій, як об'єктів кібербезпеки, та вміння здійснювати класифікацію загроз безпеці інформаційних ресурсів, класифікацію та ранжирування джерел загроз і уразливостей безпеці, застосовуючи системний підхід та знання основ теорії інформаційної безпеки; розуміти принципи і методи теорії захищених систем, основних механізми захисту, які реалізовані в сучасних операційних системах та системах управління базами даних, видів і прийомів використання шкідливого програмного забезпечення та методів його нейтралізації.

Компетентності, які набуваються:

- здатність застосовувати знання у практичних ситуаціях;
- знання та розуміння предметної області та розуміння професії;
- здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово;
- вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням;
- здатність до пошуку, оброблення та аналізу інформації;
- здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки;
- здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки;
- здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класів та походження;
- здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.);
- здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку;
- здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпеки;
- здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки;

- здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

Очікувані результати навчання:

- застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації;
- організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;
- використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;
- аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;
- адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат;
- критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності;
- готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки;
- впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки;
- виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем;
- виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах;
- розробляти моделі загроз та порушника;
- аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних;
- вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень;
- використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій;
- використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів;
- застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;
- забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах;

- вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах;
- здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем;
- застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем;
- вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки;
- приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації;
- забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах;
- вирішувати задачі аналізу програмного коду на наявність можливих загроз.

Пререквізити: дисципліна базується на деяких поняттях дисциплін «Дискретна математика», «Теорія інформації та кодування», «Прикладна криптологія», «Теоретичні основи криптології», «Інформаційно-комунікаційні системи», «Організація баз даних», «Операційні системи», «Технології проектування комп'ютерних систем», «Антивірусний захист», «Безпека операційних систем», «Апаратні та програмні засоби захисту інформації».

Кореквізити є підґрунтям для «Комплексні системи захисту інформації: проектування, впровадження, супровід», курсового та дипломного проектування.

3. Програма навчальної дисципліни

Модуль 1.

Змістовий модуль 1. ***Організація та безпека баз даних***

Тема 1. ***Характеристики та види атак на баз даних***

Інструменти для підключення до SQL-сервера та роботи з SQL, Прості SQL – ін’єкції, Сліпі SQL ін’єкції, Out-of-band SQL- ін’єкції, Способи виконання SQL-ін’єкцій, Причини виникнення вразливостей, пов’язаних з SQL-ін’єкціями, Захист від SQL-ін’єкцій, Інструменти для автоматичного пошуку вразливостей, пов’язаних з SQL-ін’єкціями. Вразливості веб-серверів та веб-застосувань. Види атак на веб-сервер. Використання помилок у конфігурації. Атаки на парольний захист веб-сервера. Атаки з розділенням HTTP запитів/відповідей та подібні. Атака отруєння кеша. Атака людина посередині.

Тема 2. ***Принципи конфігурування реляційних баз даних***

Статичне хешування. Відкрита адресація. Пов'язана область переповнення. Багаторазове хешування. Динамічне хешування. Обмеження, властиві методу хешування. Перевірка і призначення повноважень і уявлень

даних користувачів. Захист бази даних. Визначення терміна «адміністрування та захист даних (баз даних)». Процеси управління групи адміністратора БД. Перелік функцій групи адміністратора БД.

Тема 3. ***Транзакції та підтримка цілісності бази даних***

Поняття цілісності бази даних. Умови цілісності. Обробка транзакцій. Властивості транзакцій. Модель ANSI / ISO. Призначення і використання журналу транзакцій. Відкат і відновлення. Типи конфліктів. Зниклі поновлення. Читання «брудних» даних. Рядки-примари. Захвати та блокування. Data mining. Системи OLAP. Стандарт SQL3. Стандарт ODMG93.

Змістовний модуль 2. ***Антивірусний захист***

Тема 4. ***Загальні відомості щодо вірусів***

Характеристика сучасного стану проблематики забезпечення антивірусного захисту інформації в інформаційних та комунікаційних системах. Поняття шкідливої програми. Види шкідливих програм. Визначення комп'ютерного вірусу. Життєвий цикл вірусу. Ознаки зараження комп'ютера вірусами. Класифікація комп'ютерних вірусів. Завантажувальні віруси. Файлові віруси. Реплікатори. Макровіруси Основні види троянських програм і їх можливості. Мережеві віруси. Основні деструктивні дії, що виконуються вірусами і черв'яками. Мережеві черв'яки. Поштові черв'яки. IRC-черв'яки. P2P черв'яки. IM-черв'яки. Запуск EXE-програми Класифікація EXE-вірусів. Віруси, які заміщають програмний код. Віруси-супутники. Інфікування методом створення COM-файлу супутника. Віруси, впроваджуються в програму. Спосіб зараження EXE-файлів. Впровадження способом зрушення. Впровадження способом перенесення. Програмна реалізація вірусів. Алгоритм дії вірусів. Основні демаскуючи признаки.

Тема 5. ***Антивірусні засоби захисту інформації***

Класифікація антивірусних програм. Програми-детектори. Програми-доктора (фаги). Програми-ревізори. Програми-фільтри. Програми-вакцини (іммунізатори). Технологія багаторівневої розподіленої системи захисту. Регламентація проведення робіт. Застосування програмних засобів захисту. Використання спеціальних апаратних засобів. Технологічна схема захисту. Вхідний контроль нових програм. Сегментація інформації на магнітному диску. Захист операційної системи від зараження. Систематичний контроль цілісності інформації. Інтегрований програмний комплекс Каталог детекторів. Програма-пастка вірусів. Програма для вакцинації. База даних про віруси і їх характеристиках. Резидентні засоби захисту. Пошук вірусів. Сигнатурний аналіз. Евристичний аналіз. Робота з командного рядка. Робота з диспетчером команд. Класифікація антивірусів. Призначення антивірусних програм. Принципи побудови антивірусних програм. Побудова баз вірусів. Порядок роботи з антивірусними програмами. Експериментальні дослідження сучасних антивірусних програм. Порівняльна характеристика сучасних антивірусних програм.

Модуль 2.

Індивідуальне завдання

Модуль 3.

Змістовий модуль 3. ***Захист операційних систем та додатків***

Тема 6. ***Захист програм та даних***

Руйнуючі програмні засоби (РПЗ). Типи РПЗ. Тенденції розвитку та методи захисту від РПЗ. Недоліки існуючих засобів захисту від РПЗ. Класифікація шкідливих програм. Принципи створення та аналізу троянських програм.

Протидія і виявлення троянських програм, черв'яків. Основи роботи антивірусних програм. Протидія шкідливому коду. Захист програмного забезпечення. Ідентифікація програм та захист авторських прав

Тема 7. ***Захист операційних систем***

Механізми захисту операційних систем Підсистема безпеки операційної системи та виконувані нею функції. Реалізація підсистем безпеки у найбільш розповсюджених операційних системах. Критерії захищеності операційних систем. Операційні системі iOS, Android, Windows Phone, BlackBerry.

Організація контролю доступу в ОС. Руткіти та шпигунські програми. Інструменти для здійснення атак на операційні системи. Атака на парольний захист. Протидія атакам на операційні системи

Переповнення буферу. Поняття стеку та купи. Функції стеку викликів. Сегментація пам'яті. Причини виникнення переповнення буферу. Захист від переповнення буферу. Запобігання виконання даних

Модуль 4

Змістовий модуль 4. ***Захист інформації при передачі даних***

Тема 8. ***Захист в системах передачі даних та системах зв'язку***

Методи та технології захисту інформації в системах передачі даних та системах зв'язку. Організаційні засади забезпечення захисту інформації

Типи атак на систему передачі даних. Механізми захисту від атак. Отримання інформації про організацію, її мережу, вузли та сервіси з відкритих джерел. Способи протидії пасивному збору інформації. Засоби активного сбору інформації про систему передачі даних. Пошук вразливостей та інструменти сканування вузлів систем передачі даних та систем зв'язку на вразливості. Оцінка захищеності інформації в системах передачі даних та системах зв'язку.

Механізми захисту від збору інформації, сканування та проникнення. Системи виявлення вторгнень та системи запобігання вторгненням.

Модуль 5

Змістовий модуль 5. ***Стеганографічні системи***

Тема 9. ***Загальні відомості про стеганографічні системи***

Місце стеганографічних систем у сфері кібербезпеки. Терміни та визначення. Принципи побудови стеганографії. Структурна схема та математична модель типової стегосистеми. Протоколи. Методи приховування інформації. Класифікація методів стеганографії. Класична стеганографія.

Комп'ютерна стеганографія. Цифрова стеганографія. Мережева стеганографія. Цифрові водяні знаки

Тема 10. ***Використання стеганографічних систем***

Технологічна схема захисту. Приховування інформації в тексті. Методи довільного інтервалу. Синтаксичні та семантичні методи. Приховування даних в нерухомих зображеннях. Приховування даних в просторової області. Метод заміни найменш значущого біта. Метод псевдовипадкового інтервалу. Метод блокового приховування. метод квантування зображення. Приховування даних в частотної області зображення. Метод Коха і Жао. Метод Хсу і Ву. Метод Фрідріх. Методи розширення спектру. Статистичні методи. Структурні методи. Приховування даних в ауді сигналах. Кодування найменш значущих біт. Метод фазового кодування. Метод розширення спектра. Приховування даних з використанням луна - сигналу.

Модуль 6.

Індивідуальне завдання

4. Структура навчальної дисципліни

Назва змістовного модуля і тем	Кількість годин				
	Усього	У тому числі			
		л	лаб	п.	с. р.
1	2	3	4	5	6
Модуль 1					
Змістовий модуль 1. Організація та безпека баз даних					
Тема 1. Характеристики та види атак на бази даних	34	6		8	20
Тема 2. Принципи конфігурування реляційних баз даних	26	6		4	16
Тема 3. Транзакції та підтримка цілісності бази даних. Модульний контроль	22	4		3	14
Разом за змістовим модулем 1	82	16		16	50
Змістовний модуль 2. Антивірусний захист					
Тема 4. Загальні відомості щодо вірусів	41	8		8	25
Тема 5. Антивірусні засоби захисту інформації. Модульний контроль	42	8		7	20
Разом за змістовим модулем 2	83	16		16	45
Модуль 2					
Індивідуальне завдання	6				6
Всього за семестр	**165**	**32**		**32**	**101**
Модуль 3					
Змістовий модуль 3. Захист операційних систем та додатків					
Тема 6. Захист програм та даних	30	6		4	20
Тема 7. Захист операційних систем. Модульний контроль	29	6		3	20
Разом за змістовим модулем3	60	12		8	40
Модуль 4					
Змістовий модуль4.Захист інформації при передачі даних					
Тема 8. Захист в системах передачі даних та системах зв'язку. Модульний контроль	57	10		7	40
Разом за змістовим модулем 4	58	10		8	40
Модуль 5					
Змістовий модуль 5.Стеганографічні системи					
Тема 9. Загальні відомості	14	4			10
Тема 10. Використання стеганографічних систем. Модульний контроль	47	10		7	24
Разом за змістовим модулем 5	61	14		8	34
Модуль 6					
Індивідуальне завдання	6				6
Всього за семестр	**180**	**36**		**24**	**120**
Всього	**345**	**68**		**56**	**221**

5. Теми семінарських занять

№ з/п	Назва теми	Кількість годин	
		Денна форма навчання	Заочна форма навчання
1	*Не передбачено*		
	Разом		

6. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
		Денна форма навчання
1	*Не передбачено*	
	Разом	

7. Теми практичних занять

№ з/п	Назва теми	Кількість годин
		Денна форма навчання
1	Функціонування та запобігання SQL-ін‘єкціям	4
2	Дослідження вразливостей веб- сервера	4
3	Робота з процедурами	4
4	Механізми виконання транзакцій	3
5	Можливості використання описаних вразливостей для вбудовування в вірусний код	4
6	Можливості виявлення вірусної активності вбудованими засобами ОС.	4
7	Можливості виявлення вірусної активності на локальному комп’ютеру.	4
8	Можливості виявлення вірусних програм за допомогою командного рядку	3
9	Ефективність атак на парольний захист	4
10	Атаки типа «переповнення буферу» та методів протидії.	3
11	Алгоритми завадостійкого кодування	4
12	Методи м’якого кодування	3
13	Можливості розміщення повідомлення у текстовому файлі та цифрового водяного знаку	4
14	Можливості розміщення повідомлення у графічному та аудіо файлах	3
	Разом	51

8. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Характеристики та види атак на бази даних	20
2	Принципи конфігурування реляційних баз даних	16
3	Транзакції та підтримка цілісності бази даних	14
4	Загальні відомості щодо вірусів	25
5	Антивірусні засоби захисту інформації	26
6	Виконання розрахунко-графічної роботи.	6
7	Захист програм та даних	20
8	Захист операційних систем	20
9	Захист в системах передачі даних та системах зв’язку	40
10	Загальні відомості про стеганографічні системи	10
11	Використання стеганографічних систем	24
12	Виконання розрахунково-графічної роботи.	6
	Разом	**221**

9. Індивідуальні завдання

№ з/п	Назва теми	Кількість годин
1	Розрахунково-графічна робота за темою 5	6
2	Розрахунково-графічна робота за темою 10	6
3	**Разом**	**Разом**

10. Методи навчання

Проведення аудиторних лекцій, практичних занять, консультацій, а також самостійна робота студентів за матеріалами, опублікованими кафедрою.

11. Методи контролю

Проведення поточного контролю, письмового модульного контролю, підсумковий контроль у вигляді іспиту.

12. Критерії оцінювання та розподіл балів, які отримують студенти

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Змістовний модуль 1			
Робота на лекціях	0…1	8	0…8
Виконання і захист практичних робіт	0...5	4	0...20
Модульний контроль	0…17	1	0…17
Змістовний модуль 2			
Робота на лекціях	0…1	8	0…8
Виконання і захист практичних робіт	0...5	4	0...20
Модульний контроль	0…17	1	0…17
Виконання і захист РГР	0…10	1	0…10
Усього за семестр			**0…100**
Змістовний модуль 3			
Робота на лекціях	0…1	6	0…6
Виконання і захист практичних робіт	0...5	4	0...20
Модульний контроль	0…10	1	0…12
Змістовний модуль 4			
Робота на лекціях	0…1	5	0…5
Виконання і захист практичних робіт	0...5	2	0..10
Модульний контроль	0…10	1	0…10
Змістовний модуль 5			
Робота на лекціях	0…1	7	0…7
Виконання і захист практичних робіт	0...5	2	0...10
Модульний контроль	0…10	1	0…10
Виконання і захист РГР	0…10	1	0…10
Усього за семестр			**0…100**

Контроль знань при проведенні занять оцінюється за такими шкалами:
активність на лекції під час відповідей на питання:
- активна робота на лекції - 1 бал;
виконання і захист практичних робіт:
- при виконанні всіх вимог завдань методик на роботи - 5 бали;
- незначні недоліки при відповіді на питання при захисті результатів роботи за змістом досліджуваної теми - 4 бали;

- неповні відповіді на питання при захисті результатів роботи за змістом досліджуваної теми - 3 бали;
- неповні відповіді на питання за змістом і результатами роботи - 2 бала;
- недооформлені результати роботи і неповні відповіді на питання за змістом результатів роботи -1бал;
- якщо робота не виконана і не захищена - 0 балів.

На модульний контроль виносяться всі пройдені за контрольований період теми, які включаються в варіанти завдань, що містять по 17 або 10 питанн (по всім темам та видам занять). Максимальна кількість балів за кожне питання - 1.

Семестровий контроль у вигляді іспиту проводиться у разі відмови студента від балів поточного тестування й за наявності допуску до іспиту. Під час складання семестрового іспиту студент має можливість отримати максимум 100 балів.

Білет для іспиту складається з двох теоретичних та одного практичного запитань, максимальна кількість за кожне із запитань, складає за теоретичними питаннями 30 балів, за практичнім - 40 балів.

Критерії оцінювання роботи студента протягом семестру

Задовільно (60-74). Показати мінімум знань та умінь. Захистити не менше 80% від усіх завдань практичних занять. Уміти використовувати правові та нормативні документи, вітчизняних та міжнародних стандартів для проведення наукових робіт та робіт щодо забезпечення захисту інформації.

Добре (75-89). Твердо знати необхідний обсяг знань для одержання позитивної оцінки, захистити не менше 90% завдань практичних занять. Уміти використовувати сучасні методи теоретичних та експериментальних досліджень для організації захисту інформації. Мати необхідний обсяг вмінь для одержання позитивної оцінки.

Відмінно (90-100). Здати всі контрольні точки з оцінкою «відмінно». Досконально знати всі теми та уміти їх застосовувати. Уміти організувати й виконувати роботи з забезпечення захисту інформації.

Шкала оцінювання: бальна і традиційна

Сума балів за всі види навчальної діяльності	Оцінка за національною шкалою	
	для екзамену, курсового проекту (роботи), практики	для заліку
90-100	відмінно	зараховано
75-89	добре	
60-74	задовільно	
01-59	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання

13. Методичне забезпечення

1. Тексти лекцій
2. Презентації лекцій
3. Керівництво до практичних робіт

14. Рекомендована література

Базова

1. Проскурин В. Г. Защита программ и данных: учеб. пособие М.: Издательский центр «Академия», 2012. 208 с.
2. Проскурин, В.Г. Защита в операционных системах [Электронный ресурс]: учеб. пособие для вузов. М.: Горячая линия – Телеком, 2014. 193 с.

Допоміжна

1. Столлингс В. Современные компьютерные сети. Спб.: Питер, 2003. 783 с.
2. Бирюков А.А. Информационная безопасность: защита и нападение. М.: ДМК Пресс, 2012. 474 с.
3. Скляров Д. Искусство защиты и взлома информации. Спб.: БХВ-Петербург, 2004. 288 с.
4. Разрушающие программные воздействия: Учебно-методическое пособие. под ред. М.А. Иванова. М.: НИЯУ МИФИ, 2011. 328 с.

15. Інформаційні ресурси

1. http://www.solon-press/ ru
2. http://bookash.pro/ru/s/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D1%8B%D0%B5+%D0%B2%D0%B8%D1%80%D1%83%D1%81%D1%8B/