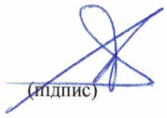
Міністерство освіти і науки України
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»

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

ЗАТВЕРДЖУЮ

Керівник проектної групи



(підпис) В.С.Харченко
(ініціали та прізвище)

«30» 08 2019 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 2019 рік

Робоча програма Захист інформації в інформаційно-комунікаційних системах

для студентів за спеціальністю 125 «Кібербезпека "

освітньою програмою " Безпека інформаційних та комунікаційних систем "

«28» 08 2019 р., – 14 с.

Розробник: Боярчук А.В., доцент, к.т.н.
(прізвище та ініціали, посада, науковий ступінь та вчене звання) (підпис)

Пєвнєв В.Я., доцент, к.т.н.
(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 2019 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 – 13,5</td><td rowspan="14">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>Цикл 2.3. Дисципліни вільного вибору студента</td></tr>
<tr><td>Кількість модулів –</td><td>Навчальний рік</td></tr>
<tr><td>Кількість змістових модулів –</td><td>2019/ 2020</td></tr>
<tr><td>Індивідуальне завдання курсовий проект, РГР</td><td>Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин
денна – 128 / 405</td><td>7,8-й</td></tr>
<tr><td>Лекції</td></tr>
<tr><td rowspan="6">Кількість тижневих годин для денної форми навчання:
аудиторних – 5(4) год.
самостійної роботи студента – 9(11) год.</td><td>56 годин</td></tr>
<tr><td>Практичні, семінарські</td></tr>
<tr><td>16 годин</td></tr>
<tr><td>Лабораторні</td></tr>
<tr><td>56 годин</td></tr>
<tr><td>Самостійна робота</td></tr>
<tr><td>277 годин</td><td>Вид контролю</td></tr>
<tr><td></td><td>модульний контроль, іспит</td></tr>
</table>

2. Мета та завдання навчальної дисципліни

Мета – ознайомлення тих, хто навчається, з методологією, основними напрямами, методами і алгоритмами реалізації функцій захисту інформації при побудові та адмініструванні баз даних, від руйнівних програм в інформаційних та комунікаційних системах, а також придбанні навичок розробці та використання стегонографічних алгоритмів щодо забезпечення захисту інформації.

Завдання – вивчення типів і видів атак на бази даних, принципів конфігурування реляційних баз даних, принципів організації фізичної структури зберігання даних у базі даних, принципів побудови руйнівних програм, методів протидії їм, а також базових положень щодо реалізації комплексної системи захисту інформації від руйнівних програм в установі (підприємстві), принципів та використання стеганографічних методів захисту інформації.

Результати навчання: в результаті вивчення дисципліни студенти повинні бути здатними до завдань забезпечення захисту інформації в комп'ютерних системах, побудови баз даних різного типу та методам захисту інформації під час використання та збереження.

Міждисциплінарні зв'язки: дисципліна базується на деяких поняттях дисциплін «Алгоритми та методи обчислювань», «Дискретна математика», «Теорія інформації та кодування», «Теорія ймовірностей та математична статистика», «Архітектура комп'ютерів», «Комп'ютерні системи», «Моделі та структури даних», «Прикладна криптологія», «Системи технічного захисту інформації».

Дисципліна «Захист інформації в інформаційно-комунікаційних системах» є підґрунтям для 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.

Змістовий модуль 3. *Захист операційних систем та додатків*

Тема 6. *Захист програм та даних*

Руйнуючі програмні засоби (РПЗ). Типи РПЗ. Тенденції розвитку РПЗ. Методи захисту від РПЗ. Недоліки існуючих засобів захисту від РПЗ

Типи шкідливого ПЗ. Класифікація шкідливих програм. Принципи створення та аналізу троянських програм. Життєвий цикл вірусу. Принципи створення та аналізу вірусів.

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.

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

Операційна система iOS. Операційна система Android. Операційна система Windows Phone. Операційна система BlackBerry.

Організація контролю доступу в ОС. Руткіти та шпигунські програми. Інструменти, що використовуються 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

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. Засоби захисту захист 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.

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.

4. Структура навчальної дисципліни

Назва змістовного модуля і тем	Кількість годин				
	Усього	У тому числі			
		л	п	лаб.	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	22	4		3	14
Модульний контроль				1	
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	42	8		7	26
Модульний контроль				1	
Разом за змістовим модулем 2	83	16		16	51
Модуль 2					
Курсовий проєкт	60		16		44
Усього годин	**225**	**32**	**16**	**32**	**145**
Модуль 3					
Змістовий модуль 3. Захист операційних систем та додатків					
Тема 6. Захист програм та даних	28	4		4	20
Тема 7. Захист операційних систем	30	4		3	22
Модульний контроль				1	
Разом за змістовим модулем 3	58	8		8	42
Змістовий модуль 4. Захист інформації при передачі даних					
Тема 8. Захист в системах передачі даних та системах зв'язку	64	8		7	48
Модульний контроль				1	
Разом за змістовим модулем 4	64	8		8	48
Змістовий модуль 5. Стеганографічні системи					
Тема 9. Загальні відомості	12	2			10
Тема 10. Використання стеганографічних систем	46	6		7	32
Модульний контроль				1	
Разом за змістовим модулем 5	58	8		8	42
Усього годин	**180**	**24**		**24**	**132**
Всього	**405**	**56**	**16**	**56**	**277**

5. Теми семінарських занять

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

6. Теми практичних занять

№ з/п	Назва теми	Кількість годин
		Денна форма навчання
1	*Курсове проектування*	16
	Разом	16

7. Теми лабораторних 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	Дослідження можливості використання описаних вразливостей для вбудовування в вірусний код	4
6	Дослідження можливості виявлення вірусної активності вбудованими засобами ОС.	4
7	Дослідження можливості виявлення вірусної активності на локальному комп’ютеру.	
8	Дослідження можливості виявлення вірусних програм за допомогою командного рядку	3
9	Дослідження ефективності атак на парольний захист	4
10	Дослідження атаки типа «переповнення буферу» та методів протидії.	3
11	Дослідження алгоритмів завадостійкого кодування	4
12	Дослідження методів м’якого кодування	3
13	Дослідження можливостей розміщення повідомлення у текстовому файлі та цифрового водяного знаку	4
14	Дослідження можливостей розміщення повідомлення у графічному та аудіо файлах	3
	Разом	58

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	Курсове проєктування	44
5	Загальні відомості щодо вірусів	25
6	Антивірусні засоби захисту інформації	26
7	Захист програм та даних	20
8	Захист операційних систем	22
9	Захист в системах передачі даних та системах зв'язку	48
10	Загальні відомості про стеганографічні системи	10
11	Використання стеганографічних систем	32
	Разом	**277**

9. Індивідуальні завдання

№ з/п	Назва теми	Кількість годин
1	*Курсовий проект*	60

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

12.1. Розподіл балів, які отримують студенти (кількісні критерії оцінювання)

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Змістовний модуль 1			
Робота на лекціях	0…1	10	0…10
Виконання і захист лабораторних (практичних) робіт	0...6	5	0...30
Модульний контроль	0…25	1	0…25
Змістовний модуль 2			
Робота на лекціях	0…1	6	0…6
Виконання і захист лабораторних (практичних) робіт	0...6	3	0...18
Модульний контроль	0…25	1	0…25
Виконання і захист РР	0…10	1	0…10
Усього за семестр			**0…100**
Змістовний модуль 3			
Робота на лекціях	0…1	4	0…4
Виконання і захист лабораторних (практичних) робіт	0...6	2	0...12
Модульний контроль	0…15	1	0…15
Змістовний модуль 4			
Робота на лекціях	0…1	4	0…4
Виконання і захист лабораторних (практичних) робіт	0...6	2	0...12
Модульний контроль	0…15	1	0…15
Змістовний модуль 5			
Робота на лекціях	0…1	4	0…4
Виконання і захист лабораторних (практичних) робіт	0...6	3	0...12
Модульний контроль	0…15	1	0…15
Виконання і захист РР	0…10	1	0…10
Усього за семестр			**0…100**

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

Білет для іспиту/заліку складається з двох теоретичних питання (0…30 балів за кожне питання) та одно практичне завдання (0…40 балів).

12.2. Якісні критерії оцінювання

Необхідний обсяг знань для одержання позитивної оцінки.
Студент повинен знати:

- загальні аспекти проблематики в галузі інформаційної безпеки (сучасний стан задач та проблем, загрози та види руйнівних програм та атаки на інформаційні та комунікаційні системи, вимоги до їх захищеності);
- встановлену політику інформаційної та/або кібербезпеки.
- методи функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.);
- методи забезпечування захисту інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки;
- характеристику методів реалізації основних функцій системи захисту інформації;
- принципи відновлювання штатного функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класів та походження;
- методи забезпечення автентичності користувачів комп'ютерної мережі.
- характеристику методів реалізації основних функцій системи управління ключовими структурами;
- методи забезпечення скритності передачі інформації;
- принципи побудови комплексної системи захисту інформації установи (підпрємства).

Необхідний обсяг вмінь для одержання позитивної оцінки.
Студент повинен вміти:

- забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-комунікаційних системах
- вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах;
- вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки;
- вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки

- забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах
- вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-комунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень;
- виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах;
- впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.

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
83-89	добре	
75-82		
68-74	задовільно	
60-67		
01-59	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання

13. Методичне забезпечення

1. Презентації лекцій
2. Керівництво до лабораторних 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.
3. Конахович Г. Ф., Пузыренко А. Ю. Компьютерная стеганография. Теория и практика. К.: МК-Пресс, 2006. 288 с.
4. Грибунин В. Г., Оков И. Н., Туринцев И. В. Цифровая стеганография. М.: Солон-Пресс, 2002. 272 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. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. М.: Техносфера, 2006. 320 с.
5. Ачилов Р. Построение защищенных корпоративных сетей. М.: ДМК Пресс, 2013. 250 с.
6. Есин В.И., Кузнецов А.А., Сорока Л.С. Безопасность информационных систем и технологий. Х.: ООО «ЭДЭНА», 2010. : 656 с.
7. 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/