Маріупольський державний університет

Кафедра Математичних методів та системного аналізу

ЗАТВЕРДЖУЮ
Завідувач кафедри ММСА
_____ Т.В. Шабельник
«__» _____ 20__р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

НДПП 1.2.16_«Захист інформації в комп'ютерних системах та мережах»
(шифр і назва навчальної дисципліни)

спеціальність 125 – Кібербезпека
(шифр і назва спеціальності)

спеціалізація кібербезпека
(назва спеціалізації)

факультет економіко-правовий
(назва факультету)

2020-2021 рік

Робоча програма ___Захист інформації в комп'ютерних системах та мережах___ для студентів
(назва навчальної дисципліни)
за напрямом підготовки 125 - Кібербезпека

Розробник:
Гранкін Д.В. кандидат фізико-математичних наук, доцент
(вказати авторів, їхні посади, наукові ступені та вчені звання)

Робоча програма затверджена на засіданні кафедри_математичних методів та системного аналізу_____

Протокол від "27" серпня 2020 року № 1

Завідувач кафедри _____математичних методів та системного аналізу_____

_____(Шабельник Т.В.)
(прізвище та ініціали)

"27" серпня 2020 року

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td><td>заочна форма навчання</td></tr>
<tr><td rowspan="2">Кількість кредитів – 8</td><td>Галузь знань
12 Інформаційні технології
(шифр і назва)</td><td colspan="2" rowspan="2">Нормативна</td></tr>
<tr><td>Напрям підготовки
125 Кібербезпека
(шифр і назва)</td></tr>
<tr><td>Модулів – 1</td><td rowspan="6">Спеціальність (професійне спрямування):
_____</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td>Змістових модулів – 3</td><td colspan="2">4-й</td></tr>
<tr><td>Індивідуальне науково-дослідне завдання вирішення типових завдань за темами змістовних модулів

(назва)</td><td colspan="2">Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин - 240</td><td colspan="2">7-й</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td rowspan="13">Тижневих годин для денної форми навчання:
аудиторних – 3
самостійної роботи студента – 11</td><td rowspan="13">Освітньо-кваліфікаційний рівень: бакалавр</td><td>28</td><td>8</td></tr>
<tr><td colspan="2">Практичні, семінарські</td></tr>
<tr><td></td><td></td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>22</td><td>4</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>190</td><td>228</td></tr>
<tr><td colspan="2">Індивідуальні завдання: год.</td></tr>
<tr><td></td><td></td></tr>
<tr><td colspan="2">Вид контролю:</td></tr>
<tr><td colspan="2">екзамен</td></tr>
</table>

Примітка:
Співвідношення кількості годин аудиторних занять до самостійної і індивідуальної роботи становить:
для денної форми навчання – 26%,
для заочної форми навчання – 5%.

2. Мета та завдання навчальної дисципліни

Мета вивчення курсу: закласти термінологічний фундамент, навчити студентів правильно проводити аналіз погроз інформаційній безпеці, основним методам, принципам, алгоритмам захисту інформації в комп'ютерних системах та мережах з урахуванням сучасного стану та прогнозу розвитку методів, систем та засобів здійснення погроз зі сторони потенційних порушників.

Завдання курсу:

- полягає у формуванні теоретичних знань та практичних умінь у сфері інформаційної та кібернетичної безпеки та набуття **наступних компетентностей**:

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.
КЗ 2. Знання та розуміння предметної області та розуміння професії.
КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.
КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.
КФ 1. Здатність використовувати державні та міжнародні стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.
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 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.
КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та /або кібербезпекою.
КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.
КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та /або кібербезпеки.
КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та /або кібербезпеки.
КФ 13. Здатність розробляти програмне забезпечення із застосуванням різних парадигм програмування
КФ 14. Здатність застосовувати в професійній діяльності базові знання в області фундаментальних та прикладних наук.
КФ 16. Здатність прогнозувати, виявляти та оцінювати можливі загрози інформаційному простору держави та дестабілізуючі чинники.

У результаті вивчення навчальної дисципліни студент повинен

знати:

- принципи комп'ютерної та мережевої безпеки;
- типові загрози і вразливості веб-додатків;
- принципи роботи засобів забезпечення безпеки (корпоративні антивіруси, WAF, системи виявлення вторгнень тощо);
- UNIX-подібні системи на рівні користувача;
- операційну систему Linux на рівні адміністратора;
- навички ручного і автоматизованого тестування безпеки веб-додатків;
- підходи до проведення тестування на проникнення;
- підходи до організації компенсуючих заходів щодо захисту інформаційних систем.

вміти:

- виконувати налаштування і здійснювати управління підсистемами безпеки;
- складати скрипти по оптимізації управління системами безпеки;
- управляти інфраструктурою надання доступів;
- аналізувати лог-файли і журнали подій;
- забезпечувати інформаційну безпеку і захист даних;
- виконувати моніторинг та контроль функціонування засобів забезпечення інформаційної безпеки;
- аналізувати інциденти інформаційної безпеки і приймати рішення за результатами аналізу;
- вносити зміни до настройки засобів забезпечення безпечної міжмережевої взаємодії при виявленні ознак атаки.

Місце навчальної дисципліни в освітній програмі: ОК 28

Передумови для вивчення дисципліни: Архітектура комп'ютерних систем, Комп'ютерні мережі, Основи криптографічного захисту інформації, Прикладна криптологія.

Результати навчання:
РН2 - організувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;
РН14 - 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-телекомунікаційних технологій;
РН 19 - застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;
РН 27 - вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах;
РН 36 - виявляти небезпечні сигнали технічних засобів;
РН 37 - вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації;
РН 38 - інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації;
РН 40 - інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації.

3. Програма навчальної дисципліни

Змістовий модуль 1. Інформаційна безпека: сутність, поняття, схема забезпечення.

Тема 1. Моделі безпеки та нормативно-правове регулювання інформаційної безпеки.
Модель безпеки CIA (Confidentiality, Integrity, and Availability), інші категорії моделі безпеки. Нормативно-правове регулювання інформаційної безпеки. Типи міжнародних організацій в сфері інформаційної безпеки. Закон України № 80/94-ВР «Про захист інформації в інформаційно-телекомунікаційних системах».

Тема 2. Загальні принципи та методи забезпечення інформаційної безпеки.
Вивчення принципів і специфічних методів забезпечення інформаційної безпеки. Принципи побудови системи інформаційної безпеки. Системний підхід до захисту інформації.

Тема 3. Уразливість даних та протидія витоку інформації.
Поняття уразливості і витоку інформації. Види уразливості. Сутність криптографічних методів забезпечення інформаційної безпеки. Організаційно-адміністративні заходи забезпечення комп'ютерної безпеки. Принципи забезпечення інформаційної безпеки на основі інженерно-технічного забезпечення. Дії і події, що порушують інформаційну безпеку. Основні види каналів витоку інформації. Шляхи несанкціонованого доступу до інформації. Стратегія і тактика зловмисника при несанкціонованому доступі.

Тема 4. Способи практичної реалізації механізмів захисту інформації.
Шкідливе програмне забезпечення (malware), його види. Організація конфіденційного діловодства. Структура і функції служби інформаційної безпеки компанії. Забезпечення інформаційної без-

пеки автоматизованих банківських систем. Інформаційна безпека електронної комерції. Електронний цифровий підпис та особливості його застосування. Інформаційна безпека користувачів мобільних пристроїв. Протоколи мережевого доступу AAA (Authentication, Authorization, Accounting).

Змістовий модуль 2. Технології взаємодії між інформаційними системами та UNIX-подібні системи.

Тема 5. Основні поняття і концепції UNIX-подібних систем.
UNIX-подібні системи: історія, основні особливості та області використання. Базові команди і утиліти Linux. Розмежування прав доступу в UNIX-подібній системі.

Тема 6. Основи програмування на shell. Створення скриптів для моніторингу і управління процесами в UNIX-подібній системі.
Командні інтерпретатори, їх різновиди та відмінності. Оболонки (shells). Конвеєри і перенаправлення вводу-виводу. Налаштування shell. Взаємодія shell-скриптів з користувачем. Умовні оператори, цикли в програмах на shell. Створення функцій у програмах на shell. Процеси і їх ідентифікатори. Взаємодія процесів в UNIX-подібній системі.

Тема 7. Файлові підсистеми UNIX-подібного оточення.
Сучасні файлові підсистеми, що використовуються у UNIX-подібних системах та їх особливості. Робота з таблицями розділів MBR і GPT. Відновлення таблиць розділів в разі збоїв. Пошук у файловій системі і в текстовому файлі. Утиліти find і grep.

Тема 8. Налаштування і використання мережевих комунікацій в UNIX-подібних системах.
Багаторівневий підхід до організації мережевих взаємодій. Засоби налаштування мережевої підсистеми Linux. Доступ до локальної мережі засобами Linux. Команди налаштування протоколу IP. Постійні мережеві конфігурації (на прикладі Debian/GNU Linux). Базова діагностика мережевих підключень. Транспортний і прикладний рівні моделі мережевої взаємодії. Налаштування деяких мережевих служб в Debian/GNU Linux. Маршрутизація в Linux. Забезпечення доступу до мережі Інтернет.

Змістовий модуль 3. Прикладні аспекти захисту інформації.

Тема 9. Маніпуляції з локальними даними: виявлення скритих або видалених даних, їх відновлення та шифрування.
Комп'ютерна криміналістика (форензіка): вирішувані завдання і методи. Відновлення даних. Утиліти TestDisk, PhotoRec, Extundelete, Foremost. Симетричні алгоритми шифрування даних. Асиметричні алгоритми шифрування даних. Шифрування даних. PGP / GPG: можливості та особливості програмного забезпечення. Шифрування даних. TrueCrypt: можливості, особливості, нюанси програми. Специфікація шифрування диску / блочного пристрою LUCKS/dm-crypt (Linux Unified Key Setup).

Тема 10. Підходи до забезпечення інформаційної безпеки у мережі.
Призначення, цілі, опис ідентифікатора MAC. Засоби отримання MAC-адреси стороннього пристрою. Мотивація зловмисника при отриманні MAC-адреси чужого пристрою. Статичний і динамічний IP-адреси. Метод сканування протоколів IP. Основні методи сканування Nmap. Призначення, цілі, опис Honeypot. Способи виявлення Honeypot. Недоліки Honeypot. Проблеми, які можуть виникнути при його використанні. RPC-сервіси. Цілі RPC-сканування. Важливість інформації щодо активності та розміщення таких сервісів. Балансування навантаження (load balancing). Методи балансування навантаження на веб-сервер. DoS / DDoS-атаки. Чотири основні класи атак, що відповідають рівням моделі ISO OSI. Виявлення ознак DDoS-атаки. Основні способи захисту від DDoS-атак. Брандмауер: призначення. Принцип роботи Netfilter. Таблиці брандмауера Netfilter, їх призначення.

4. 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	с.р.		л	п	лаб	інд	с.р
1	2	3	4	5	6	7	8	9	10	11	12	13
Змістовний модуль 1. Інформаційна безпека: сутність, поняття, схема забезпечення.												
Тема 1. Моделі безпеки та нормативно-правове регулювання інформаційної безпеки.	20	1				19	22.5	0.5				22
Тема 2. Загальні принципи та методи забезпечення інформаційної безпеки.	20	1				19	22.5	0.5				22
Тема 3. Уразливість даних та протидія витоку інформації.	20	1				19	22.5	0.5				22
Тема 4. Способи практичної реалізації механізмів захисту інформації.	20	1				19	22.5	0.5				22
Разом за модулем 1	80	4				76	90	2				88
Змістовий модуль 2. Технології взаємодії між інформаційними системами та UNIX-подібні системи.												
Тема 5. Основні поняття і концепції UNIX-подібних систем.	27	4		4		19	24.5	1		0.5		23
Тема 6. Основи програмування на shell. Створення скриптів для моніторингу і управляння процесами в UNIX-подібній системі.	25	4		2		19	24.5	1		0.5		23
Тема 7. Файлові підсистеми UNIX-подібного оточення.	27	4		4		19	24.5	1		0.5		23
Тема 8. Налаштування і використання мережевих комунікацій в UNIX-подібних системах.	27	4		4		19	24.5	1		0.5		23
Разом за модулем 2	106	16		14		76	98	4		2		92
Змістовий модуль 3. Прикладні аспекти захисту інформації.												
Тема 9. Маніпуляції з локальними даними: виявлення скритих або видалених даних, їх відновлення та шифрування.	27	4		4		19	26	1		1		24
Тема 10. Підходи до забезпечення інформаційної безпеки у мережі.	27	4		4		19	26	1		1		24
Разом за модулем 3	54	8		8		38	52	2		2		48
Усього годин	**240**	**28**		**22**		**190**	**240**	**8**		**4**		**228**

5. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Вивчення базових команд Linux.	2
2	Розмежування прав доступу.	2

3	Файлові підсистеми.	4
4	Відновлення даних.	2
5	Шифрування даних.	2
6	Honeypot, Nmap.	4
7	LAN, веб-сервер з CMS.	4
8	Тестування навантаження веб-сервера.	2
	Усього	22

6. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Забезпечення цілісності та доступності даних. Raid, LVM.	19
2	Робота з пісочницями та файловими антивірусами. Sandbox.	19
3	Захист від спаму. Антиспам (ASSP).	19
4	Управління інформаційною безпекою та подіями безпеки. SIEM.	19
5	Налаштування веб-серверу на UNIX-подібній системі.	19
6	DDoS-атаки – основні особливості їх організації та захисту від них.	19
7	Мережеві системи виявлення та запобігання вторгнень. NIPS/NIDS: Snort.	19
8	Правила брандмауера. Створення правил для брандмауера утилітою Iptables.	19
9	Міжмережеві екрани WAF (Web Application Firewall).	19
10	Пісочниця (sandbox). Принцип роботи. Приклади використання. Переваги та недоліки пісочниць. Альтернативи використанню пісочниць.	19
	Усього	190

7. Методи навчання: лекції, лабораторні заняття, самостійне вивчення деяких теоретичних питань, самостійна робота студентів з виконанням практичних завдань, захист лабораторних робіт.

8. Критерії оцінювання

Критерії поточного оцінювання знань студентів.

Усний виступ та виконання письмового завдання, тестування	Критерії оцінювання
5	В повному обсязі володіє навчальним матеріалом, вільно самостійно та аргументовано його викладає під час усних виступів та письмових відповідей, глибоко та всебічно розкриває зміст теоретичних питань та практичних завдань, використовуючи при цьому обов'язкову та додаткову літературу. Правильно вирішив усі тестові завдання.
4	Достатньо повно володіє навчальним матеріалом, обґрунтовано його викладає під час усних виступів та письмових відповідей, в основному розкриває зміст теоретичних питань та практичних завдань, використовуючи при цьому обов'язкову літературу. Але при викладанні деяких питань не вистачає достатньої глибини та аргументації, допускаються при цьому окремі несуттєві неточності та незначні помилки. Правильно вирішив більшість тестових завдань.
3	В цілому володіє навчальним матеріалом викладає його основний зміст під час усних виступів та письмових відповідей, але без глибокого всебічного аналізу, обґрунтування та аргументації, без використання необхідної

	літератури допускаючи при цьому окремі суттєві неточності та помилки. Правильно вирішив половину тестових завдань.
2	Не в повному обсязі володіє навчальним матеріалом. Фрагментарно, поверхово (без аргументації обґрунтування) викладає його під час усних виступів та письмових відповідей, недостатньо розкриває зміст теоретичних питань та практичних завдань, допускаючи при цьому суттєві неточності, правильно вирішив меншість тестових завдань.
1	Частково володіє навчальним матеріалом не в змозі викласти зміст більшості питань теми під час усних виступів та письмових відповідей, допускаючи при цьому суттєві помилки. Правильно вирішив окремі тестові завдання.

Доповнення виступу*:*

2 бали – отримують студенти, які глибоко володіють матеріалом, чітко визначили його зміст; зробили глибокий системний аналіз змісту виступу, виявили нові ідеї та положення, що не були розглянуті, але суттєво впливають на зміст доповіді, надали власні аргументи щодо основних положень даної теми.

1 бал отримують студенти, які виклали матеріал з обговорюваної теми, що доповнює зміст виступу, поглиблює знання з цієї теми та висловили власну думку.

Суттєві запитання до доповідачів*:*

2 бали отримують студенти, які своїм запитанням до виступаючого суттєво і конструктивно можуть доповнити хід обговорення теми.

1 бал отримують студенти, які у своєму запитанні до виступаючого вимагають додаткової інформації з ключових проблем теми, що розглядається.

Експрес-контроль*:*

2 бали нараховуються студентам, які вільно володіють усім навчальним матеріалом, орієнтуються в темі та аргументовано висловлюють свої думки.

1 бал отримують студенти, які частково володіють матеріалом та можуть окреслити лише деякі проблеми теми.

Складання словника основних термінів**,** що визначені програмою курсу (за темами):

Програмою курсу визначено перелік ключових термінів, що розкривають зміст кожної теми. Студентам пропонується скласти словник основних термінів з конкретної теми на останніх сторінках опорного конспекту лекцій.

2 бали нараховуються студентам, які не лише склали повний перелік визначених термінів з конкретної теми, а й можуть вільно розтлумачити їх зміст.

1 бал нараховуються студентам, які склали неповний перелік визначених термінів з конкретної теми і не можуть їх розтлумачити без конспекту.

Ведення опорного конспекту лекції*:*

2 бали нараховуються студентам, які в повному обсязі самостійно і творчо опрацювали всі питання лекції і вільно володіють її змістом.

1 бал нараховується студентам, які опрацювали лише окремі питання лекції і не достатньо вільно володіють її змістом.

Підготовка творчих завдань (есе, дайджест):

2 бали отримують студенти, які можуть виокремити з різних джерел основні положення, структурно об’єднати їх, коротко проаналізувати кожне з них та зробити ґрунтовні узагальнюючі висновки.

1 бал отримують студенти, які в цілому правильно виокремили основні положення кожного з джерел, але не зробили їх відповідного аналізу та узагальнюючих висновків.

Ведення конспекту першоджерел.

2 бали отримують студенти, які опрацювали всю необхідну обов’язкову літературу, засвоїли її основні теоретичні положення, вміють їх пояснити і розтлумачити.

1 бал отримують студенти, котрі опрацювали не всю необхідну літературу, не завжди розуміють її вихідні теоретичні положення, поверхово їх пояснюють.

Підсумковий модульний контроль знань студентів.
Критерії підсумкового модульного оцінювання знань студентів

Письмова контрольна робота або тестування	Критерії оцінювання
21-25	В повному обсязі володіє навчальним матеріалом, вільно самостійно та аргументовано його викладає під час усних виступів та письмових відповідей, глибоко та всебічно розкриває зміст теоретичних питань та практичних завдань, використовуючи при цьому обов'язкову та додаткову літературу. Правильно вирішив усі тестові завдання.
17-21	Достатньо повно володіє навчальним матеріалом, обґрунтовано його викладає під час усних виступів та письмових відповідей, в основному розкриває зміст теоретичних питань та практичних завдань, використовуючи при цьому обов'язкову літературу. Але при викладанні деяких питань не вистачає достатньої глибини та аргументації, допускаються при цьому окремі несуттєві неточності та незначні помилки. Правильно вирішив більшість тестових завдань.
14-17	В цілому володіє навчальним матеріалом викладає його основний зміст під час усних виступів та письмових відповідей, але без глибокого всебічного аналізу, обґрунтування та аргументації, без використання необхідної літератури допускаючи при цьому окремі суттєві неточності та помилки. Правильно вирішив половину тестових завдань.
10-14	Не в повному обсязі володіє навчальним матеріалом. Фрагментарно, поверхово (без аргументації та обґрунтування) викладає його під час усних виступів та письмових відповідей, недостатньо розкриває зміст теоретичних питань та практичних завдань, допускаючи при цьому суттєві неточності, правильно вирішив меншість тестових завдань.
10	Частково володіє навчальним матеріалом не в змозі викласти зміст більшості питань теми під час усних виступів та письмових відповідей, допускаючи при цьому суттєві помилки. Правильно вирішив окремі тестові завдання.
0	Не володіє навчальним матеріалом та не в змозі його викласти, не розуміє змісту теоретичних питань та практичних завдань. Не вирішив жодного тестового завдання.

9. Засоби оцінювання

Поточний контроль знань ЗВО здійснюється за допомогою тестів, опитувань по темам, захисту звітів про виконання лабораторних робіт. Модульний контроль здійснюється із застосуванням тестів або письмової контрольної роботи. Підсумковий контроль здійснюється у формі екзамену.

Завданням поточного контролю знань ЗВО є перевірка розуміння та запам'ятовування певного теоретичного матеріалу, умінь самостійної роботи зі спеціальною літературою, набуття практичних навичок роботи з ПК і окремими програмними засобами, вміння пояснити і захистити свою роботу.

10. Розподіл балів, які отримують студенти

Поточне тестування та самостійна робота													Сума (в балах)		
Змістовий модуль №1					Змістовий модуль №2					Змістовий модуль №3					
Т1	Т2	Т3	Т4	Тест	Т5	Т6	Т7	Т8	Тест	Т9	Т10	Тест	мод. контроль	екзамен	всього
2	2	2	2	2	5	5	5	5	5	5	5	5	50	50	100

Т1, Т2, ... – змістові теми

Шкала оцінювання: національна та ECTS

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	для заліку
90 – 100	**A**	відмінно	зараховано
82-89	**B**	добре	
74-81	**C**		
64-73	**D**	задовільно	
60-63	**E**		
35-59	**FX**	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
0-34	**F**	незадовільно з обов'язковим повторним вивченням дисципліни	не зараховано з обов'язковим повторним вивченням дисципліни

11. Рекомендовані джерела інформації

Основні:

1. 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.
2. 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.
3. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.
4. Захист інформації в автоматизованих системах управління: навч. посібник / Уклад. І.А. Пількевич, Н.М. Лобанчикова, К.В. Молодецька. – Житомир: Вид-во ЖДУ ім. І. Франка, 2015. – 226 с.
5. Інформаційна безпека України: теорія і практика : підручник / В.В. Лизанчук. – Львів : ЛНУ імені Івана Франка, 2017. – 728 с.
6. Криворучко О.В. Захист систем електронних комунікацій: навч.посіб./ В.О. Хорошко, О.В. Криворучко, М.М. Браіловський та ін. – Київ: Київ. нац. торг.-екон. ун-т, 2019. – 164 с..
7. Телекомунікаційні системи передавання інформації. Методи кодування [Текст] : навч. посібник / Р. А. Бурачок, М. М. Климаш, Б. В. Коваль. – Львів : Вид-во Львів. політехніки, 2015. – 476 с.
8. Інформаційна безпека : навчальний посібник / Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв, С. С. Войтусік, А. Я. Горпенюк, О. А. Нємкова, І. М. Журавель, Б. М. Березюк, Є. І. Яковенко, В. І. Отенко, І. Я. Тишик ; 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.

Додаткові:

1. ДСТУ 3396.2–97. Захист інформації. Технічний захист інформації. Терміни та визначення. – К. : Укр. НДІССІ, 1997. – 11 с.
2. ДСТУ 4145–2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка. – К. : Держстандарт України, 2002. – 40 с.
3. НД ТЗІ 1.1-003-99: Термінологія в області захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБУ № 22 від 28.04.1999. ДСТСЗІ СБУ. – К., 1999. – 34 с.
4. НД ТЗІ 2.5-004-99: Критерії оцінки захищеності інформації у комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБУ № 22 від 28.04.1999. ДСТСЗІ СБУ. – К., 1999. – 34 с.
5. НД ТЗІ 2.5-005-99: Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБУ № 22 від 28.04.1999. ДСТСЗІ СБУ. – К., 1999. – 34 с.

6. . НД ТЗІ 3.7-001-99: Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі. Затверджено наказом ДСТСЗІ СБУ № 22 від 28.04.1999 р. ДСТСЗІ СБУ. – К., 1999. – 34 с.

7. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 18.04.2006, – К. : Урядовий кур'єр. – 2006. № 73 – 74.

8. Про інформацію : Закон України від 03.04.1997. – К. : Урядовий кур’єр. – 1997. – № 62.