Міжнародний гуманітарний університет
Факультет права та економіки
Кафедра кримінального права, процесу та криміналістики

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
Основи кібербезпеки

Галузь знань 26 «Цивільна безпека»
Спеціальність 262 «Правоохоронна діяльність»
Назва освітньої програми Правоохоронна діяльність
Рівень вищої освіти перший (бакалаврський) рівень

Розробники і викладачі *(зазначаються розробники і викладачі, які викладають дисципліну - посада, наук. ступінь, вчене звання, П.І.Б.)*	**Контактний тел.**	**E-mail**
викладач Слатвінська В.М.	067-122-39-12	kafedraKPPK@i.ua

1. АНОТАЦІЯ ДО КУРСУ

Предметом вивчення є кібербезпека - запобігання несанкціонованому доступу, використанню, розкриттю, спотворенню, зміні, дослідженню, записи або знищенню інформації в інформаційно-комунікаційних системах різного рівня.

Метою навчальної дисципліни «Основи кібербезпеки» є ознайомлення студентами з міжнародними стандартами та практиками кібербезпеки, тактикою та стратегію нападу і захисту для інформаційно-комунікаційних систем різного масштабу і призначення, інструментальними засобами аудиту вторгнень, нападу і захисту для інформаційно-комунікаційних систем різного масштабу і призначення. процедурами аудита джерел загроз та уразливостей, заходами та засобами захисту даних.

Передумови для вивчення дисципліни (*наприклад, перелік дисциплін, які мають бути вивчені раніше, тощо*) Даний курс підґрунтям для засвоєння та удосконалення знань отриманих при вивчені дисциплін «Інформаційне забезпечення професійної діяльності», «Комп'ютерна криміналістика».

2. ОЧІКУВАНІ КОМПЕТЕНТНОСТІ, ЯКІ ПЛАНУЄТЬСЯ СФОРМУВАТИ ТА ДОСЯГНЕННЯ ПРОГРАМНИХ РЕЗУЛЬТАТІВ

У процесі реалізації програми дисципліни «Основи кібербезпеки» формуються наступні компетентності із передбачених освітньою програмою:

Інтегральна компетентність

Здатність вирішувати складні спеціалізовані задачі та практичні проблеми у сфері правоохоронної діяльності або у процесі навчання, що передбачає застосування певних теорій та методів правоохоронної діяльності і характеризується комплексністю та невизначеністю умов.

Загальні компетентності (ЗК)

ЗК1. Здатність застосовувати знання у практичних ситуаціях.

ЗК2. Знання та розуміння предметної області та розуміння професійної діяльності.

ЗК4. Здатність використовувати інформаційні та комунікаційні технології.

ЗК5. Здатність вчитися і оволодівати сучасними знаннями.

Спеціальні (фахові) компетентності

СК3. Здатність професійно оперувати категоріально-понятійним апаратом права і правоохоронної діяльності.

СК4. Здатність до критичного та системного аналізу правових явищ і застосування набутих знань та навичок у професійній діяльності.

СК5. Здатність самостійно збирати та критично опрацьовувати, аналізувати та узагальнювати правову інформацію з різних джерел.

СК6. Здатність аналізувати та систематизувати одержані результати, формулювати аргументовані висновки та рекомендації.

СК9. Здатність ефективно застосовувати сучасні техніку і технології захисту людини, матеріальних цінностей і суспільних відносин від проявів криміногенної обстановки та обґрунтовувати вибір засобів та систем захисту людини і суспільних відносин.

СК12. Здатність систематизувати закономірності злочинності, визначати особу злочинця, причини і умови злочинності та її окремих видів, реалізовувати напрями і заходи її запобігання.

СК18. Здатність забезпечувати кібербезпеку, економічну та інформаційну безпеку держави, об’єктів критичної інфраструктури.

Навчальна дисципліна Основи кібербезпеки забезпечує досягнення **програмних результатів навчання (РН)**, передбачених освітньою програмою:

РН1. Розуміти історичний, економічний, технологічний і культурний контексти розвитку правоохоронної діяльності.

РН3. Збирати необхідну інформацію з різних джерел, аналізувати і оцінювати її.

РН14. Здійснювати пошук та аналіз новітньої інформації у сфері правоохоронної діяльності, мати навички саморозвитку та самоосвіти протягом життя, підвищення професійної майстерності, вивчення та використання передового досвіду у сфері правоохоронної діяльності.

РН18. Застосовувати штатне озброєння підрозділу (вогнепальну зброю, спеціальні засоби, засоби фізичної сили); інформаційні системи, інформаційні технології, технології захисту даних, методи обробки, накопичення та оцінювання інформації, інформаційно-аналітичної роботи, бази даних (в тому числі міжвідомчі та міжнародні), оперативні та оперативно-технічні засоби, здійснення оперативно-розшукової діяльності.

РН21. Організовувати заходи щодо режиму секретності та захисту інформації.

РН1. Розуміти історичний, економічний, технологічний і культурний контексти розвитку правоохоронної діяльності.

Заплановані результати навчання за навчальною дисципліною

Знання:

1) поняття та типи загроз в кібербезпеці

2) аналіз та оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки

3) методику виявлення, ідентифікації, аналізу та реагування на інциденти кібербезпеки;

4) загрози кібербезпеки в Україні;

5) загрози кібербезпека в ЄС.

Уміння:

1) забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки;

2) впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки;

3) аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки;

4) застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів;

5) впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки;

6) вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів з інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної/або кібербезпеки.

3. ОБСЯГ ТА ОЗНАКИ КУРСУ

Загалом		**Вид заняття** (денне відділення / заочне відділення)			**Ознаки курсу**		
ЄКТС	**годин**	**Лекційні заняття**	**Практичні заняття**	**Самостійна робота**	**Курс, (рік навчання)**	**Семестр**	**Обов'язкова / вибіркова**
4	120	14 / 10	14 / 8	92 / 78	3	6 / 8	Вибіркова

4. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви змістових модулів і тем	Кількість годин							
	денна форма				Заочна форма			
	усього	у тому числі			усього	у тому числі		
		лекц.	прак	сам. роб.		лекц.	прак	сам. роб.
Тема 1. Сутність та зміст понять у сфері кібербезпеки. Практики самозахисту в мережі	16	2	2	12	16		-	14
Тема 2. Інформаційна безпека та комп'ютерні протоколи	16	2	2	12	16	2	2	14
Тема 3. Хакерське: типи хакерів та методи кіберзламів	16	2	2	12	16	-	2	14
Тема 4. Хакерські атаки та їх види: боти ботнети Дос ДДос фішинг брутфорс	18	2	2	12	18	2	2	14
Тема 5. Програми шкідники: віруси хробаки, трояни	18	2	2	14	18	2	2	14
Тема 6. Методи захисту систем та протидії кібератакам	18	2	2	14	18	2	-	16
Тема 7. Інструменти кіберзахисту: антивіруси, брандмауери, шифрування, біометрія, ідентифікація	18	2	2	14	18	2	-	16
Усього годин	**120**	**14**	**14**	**92**	**120**	**10**	**8**	**102**
ПІДСУМКОВИЙ КОНТРОЛЬ - ЗАЛІК								

5. ТЕХНІЧНЕ Й ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ / ОБЛАДНАННЯ

Студенти отримують теми та питання курсу, основну і додаткову літературу, рекомендації, завдання та оцінки за їх виконання як традиційним шляхом, так і з використанням університетської платформи он-лайн навчання на базі Moodle. Окрім того, практичні навички у пошуку та аналізу інформації за курсом, з оформлення індивідуальних завдань, тощо, студенти отримують, користуючись університетськими комп'ютерними класами та бібліотекою. Технічне забезпечення: Kali Linux - дистрибутив Debian-похідних Linux, призначений для цифрової криміналістики і тестування на проникнення

6. ПИТАННЯ ДО ПРАКТИЧНИХ ЗАНЯТЬ

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
1	**Тема 1. Забезпечення конфіденціальної роботи користувача в ОС** 1. Найпоширеніші методи викрадення інформації (зламу паролів). 2. Стадії зламу отримання ключів та паролів. Ознаки можливого злому комп'ютера та його зараження шкідливими програмами. 3. Рекомендації з безпеки Вашого комп'ютера. Виявлення шкідливих програм зі шкідливими функціями, які беруть участь в атаках.	2	-
2	**Тема 2. Основні міжнародні стандарти і практики кібербезпеки** 1. Уразливості, загрози, kill-chain. 2. Категоріальні системи Common Weakness Enumeration (CWE),	2	2

	3. бази даних Common Vulnerability Enumeration (CVE), 4. фреймворк MITRE, стандарт PCI DSS, ISO 27001.		
3	**Тема 3. Хакерське: типи хакерів та методи кіберзламів** 1. Встановлення програми Wireshark. 2. Збір та аналіз даних протоколу ICMP	2	2
4	**Тема 4. Хакерські атаки та їх види: боти ботнети Дос ДДос фішинг брутфорс** 1. Перехоплення, ідентифікація і аналіз трафіку 2. Системи захисту інформації та виявлення атак	2	2
5	**Тема 5. Програми шкідники: віруси хробаки трояни** 1. Види інформації, яка може стати об'єктом злочинних посягань. 2. Методика виявлення, ідентифікації, аналізу та реагування на інциденти кібербезпеки	2	2
6	**Тема 6. Методи захисту систем та протидії кібератакам** 1. Типи атак на інформаційні системи. Технології антивірусів та цілісності системи 2.Технології аудиту, моніторингу та менеджменту 3.Персональні дані і GDPR	2	-
7	**Тема 7. Інструменти кіберзахисту: антивіруси брандмаузери шифрування біометрія ідентифікація** 1. Конфіденційність особистої інформації. Міжнародні і національні стандарти і специфікації в області інформаційної безпеки. 2. Системи захисту інформації в провідних світових компаніях. Практика компанії IBM в області захисту. Практика компанії Cisco Systems в розробці політики розвитку мереж безпеки. Практика компанії Microsoft в області інформаційної безпеки.	2	-
	Всього	**14**	**8**

7. САМОСТІЙНА РОБОТА

До самостійної роботи студентів щодо вивчення дисципліни «Основи кібербезпеки» включаються:

1. Знайомство з науковою та навчальною літературою відповідно зазначених у програмі тем.
2. Опрацювання лекційного матеріалу.
3. Підготовка до практичних занять.
4. Консультації з викладачем протягом семестру.
5. Самостійне опрацювання окремих питань навчальної дисципліни.
6. Підготовка та виконання індивідуальних завдань у вигляді есе, рефератів тощо.
7. Підготовка до підсумкового контролю.

Тематика та питання до самостійної підготовки та індивідуальних завдань

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
1	**Тема 1. Аудит загроз серверних систем Debian GNU Linux** 1. Кіберпростір, кібербезпека та кібертероризм: поняття і визначення. 2. Поняття та види кіберзлочинів. 3. Заходи України із забезпечення кібербезпеки національної інфосфери та протидії проявам кіберзлочинності.	12	14
2	**Тема 2. Фреймворк MITRE ATT & CK** 1. Законодавство в даній області низки країн (США, Австралія, Китай і ряд інших). Питання судового переслідування. 2. Конфіденційність особистої інформації. Міжнародні і національні стандарти і специфікації в області інформаційної безпеки. 3. Проблеми взаємодії слідчого з оперативними та інформаційно-аналітичними підрозділами Національної поліції України	12	14
3	**Тема 3. Розгортання системи CALDERA** 1. Окремі аспекти інформаційно-аналітичного забезпечення правоохоронної діяльності 2. Правове регулювання основних термінів щодо систем обробки інформації у сфері забезпечення кібербезпеки в Україні 3. Освітні заходи превенції кіберзлочинності в Україні	12	14
4	**Тема 4. Моделювання загроз за концепціями cyber kill chain / diamond model** 1. Хмарний шлюз інтернет-безпеки cisco umbrella 2. Використання систем відеоспостереження, як джерела доказової інформації 3. Вдосконалення біометричних інформаційних систем ідентифікації осіб як чинник у протидії торгівлі людьми	12	14
5	**Тема 5. Моделювання загроз за концепціями cyber kill chain / матрици дій** 1. Інформаційно-аналітична діяльність як запорука підвищення ефективності роботи Національної поліції у протидії злочинності 2. Проблеми кваліфікації та криміналізації фішингу 3. Кібербезпека та інтелектуальна власність: питання правового забезпечення	14	14
6	**Тема 6. Комп'ютерна форензіка.** 1. Вимоги до кібербезпеки елементів телекомунікації 2. Методи і технології управління визначенням ідентичності 3. Проблеми підготовки іт-фахівців в Україні	14	16
7	**Тема 7. Вимоги до кібербезпеки елементів телекомунікації** 1. Поняття, види та форми кіберрозвідки	14	16

	2. Принципи кіберрозвідки 3. Засоби і способи кіберрозвідки		
	Всього	**92**	**102**

7. ВИДИ ТА МЕТОДИ КОНТРОЛЮ

Робоча програма навчальної дисципліни передбачає наступні види та методи контролю:

Види контролю	**Складові оцінювання**
поточний контроль, який здійснюється у ході: проведення практичних занять, виконання індивідуального завдання; проведення консультацій та відпрацювань.	**50%**
підсумковий контроль, який здійснюється у ході проведення іспиту (заліку).	**50%**

Методи діагностики знань (контролю)	фронтальне опитування; наукова доповідь, реферати, усне повідомлення, індивідуальне опитування; робота у групах; ділова гра, розв`язання ситуаційних завдань, кейсів, практичних завдань, залік

1-34 (2)	F		

Питання до заліку

1. У чому полягає проблема «кібербезпеки»?
2. Дайте визначення «кібербезпеки».
3. Перерахуйте компоненти кібербезпеки і їх визначення.
4. Яким чином взаємопов'язані між собою складові кібербезпеки? Наведіть власні приклади.
5. Перерахуйте рівні формування режиму кібербезпеки.
6. Перерахуйте основні документи по «кібербезпеки».
7. Які види вимог включає стандарт ISO / IEC 15408?
8. Дайте характеристику складових «кібербезпеки» стосовно до обчислювальних мереж.
9. Перерахуйте основні механізми безпеки.
10. Що розуміється під адмініструванням коштів безпеки?
11. Класи захищеності міжмережевих екранів.
12. Зміст адміністративного рівня забезпечення «кібербезпеки».
13. Дайте визначення політики безпеки.
14. Які характерні риси комп'ютерних вірусів?
15. Дайте визначення програмного вірусу.
16. Який вид вірусів найбільш розповсюджуваний в розподілених обчислювальних мережах? Чому?

17. Перерахуйте класифікаційні ознаки комп'ютерних вірусів.
18. У чому особливості резидентних вірусів?
19. Перерахуйте деструктивні можливості комп'ютерних вірусів.
20. Поясніть самошифрування і поліморфічность як властивості комп'ютерних вірусів.
21. Перерахуйте види «вірусоподібних» програм.
22. Поясніть механізм функціонування «троянської програми» (логічної бомби).
23. Поясніть поняття «сканування на льоту» і «сканування за запитом».
24. Перерахуйте види антивірусних програм.
25. Характеризуйте антивірусні сканери.
26. У чому особливості евристичних сканерів?
27. Які фактори визначають якість антивірусної програми?
28. Перерахуйте найбільш поширені шляхи зараження комп'ютерів вірусами.
29. Перерахуйте основні правила захисту від комп'ютерних вірусів, одержуваних з обчислювальних мереж.
30. Характерні риси макровірусу.
31. Як перевірити систему на наявність макровірусу?
32. Чи є наявність прихованих аркушів в Excel ознакою зараження макровірусів?
33. У чому полягають особливості забезпечення «кібербезпеки» комп'ютерних мереж?
34. Дайте визначення поняття «віддалена загроза».
35. У чому полягає специфіка методів і засобів захисту комп'ютерних мереж?
36. Поясніть поняття «глобальна мережева атака», наведіть приклади.
37. Які протоколи утворюють модель TCP / IP?
38. Який протокол забезпечує перетворення логічних мережевих адрес в апаратні?
39. Проведіть порівняльну характеристику моделей передачі даних TCP / IP і OSI / ISO.
40. На якому рівні моделі OSI / ISO реалізується сервіс безпеки «неспростовності» (згідно «Загальним критеріям»)?
41. Для чого призначений DNS-сервер?
42. Перерахуйте класи віддалених загроз.
43. Як класифікуються віддалені загрози «за характером впливу»?
44. Охарактеризуйте віддалені загрози «по ланцюгу впливу».
45. Чи може пасивна загроза привести до порушення цілісності інформації?
46. Дайте визначення типової віддаленої атаки.
47. Що є метою зловмисників при «аналізі мережевого трафіку»?
48. Назвіть причини успіху віддаленої атаки «помилковий об'єкт».
49. Що таке "сірі" IP-адреси і чим вони відрізняються від "білих"?
50. Назвіть основні рівні моделі OSI.
51. Що розуміється під ідентифікацією й аутентифікації користувача?
52. Перерахуйте можливі ідентифікатори при реалізації механізмів ідентифікації і аутентифікації.
53. Що таке «електронний ключ»?
54. Який з видів аутентифікації (стійка аутентифікація або постійна аутентифікація) більш надійний?

55. Що входить до складу криптосистеми?
56. Як реалізуються симетричний і асиметричний методи шифрування?
57. Що таке електронний цифровий підпис?
58. Перерахуйте методи розмежування доступу.
59. На чому заснований механізм реєстрації?
60. Які події, пов'язані з безпекою, підлягають реєстрації?
61. Чим відрізняються механізми реєстрації та аудиту?
62. Які етапи передбачають механізми реєстрації та аудиту?
63. У чому полягає принцип міжмережевого екранування?
64. Принцип функціонування міжмережевих екранів з фільтрацією пакетів.
65. Які сервіси безпеки включає технологія віртуальних приватних мереж?
66. Чому при використанні технології VPN IP-адреси внутрішньої мережі недоступні зовнішньої мережі?
67. Чим визначається політика безпеки віртуальної приватної мережі?
68. Опишіть структуру мережі Фейстеля
69. У чому полягає роль замін і перестановок в шифрі DES?
70. Назвіть слабкі сторони режиму шифрування ECB, як вони виправлені в режимі CBC?
71. Опишіть операцію розшифрування в режимі CFB.
72. У чому полягають завдання факторизації і визначення квадратичного вирахування? Розмістіть ці проблеми в порядке збільшення складності.
73. Опишіть алгоритм асиметричного шифрування RSA.
74. Коректно чи наступне висловлювання: «Злом алгоритму шифрування RSA еквівалентний розкладанню на множники модуля шифрування».
75. Порівняйте алгоритми RSA і Ель-Гамаля з точки зору можливості використання для постановки і верифікації ЕЦП.
76. Як з використанням електронного цифрового підпису вирішується завдання аутентифікації?
77. Чим хеш-функції відрізняються від блокових шифрів?
78. Опишіть алгоритм цифрового підпису DSA і поясніть, як в ньому забезпечується стійкість.
79. Що собою являє проблема розподілу ключів?
80. Які дії виконує центр сертифікації ключів?
81. Чому в сертифікат ключа включають термін його дії?
82. Перший етап злому: пасивний і активний збір інформації
83. Другий етап злому: сканування системи
84. Третій етап злому: отримання доступу
85. Четвертий етап злому: закріплення в системі
86. П'ятий етап злому: приховування слідів перебування
87. Короткий огляд вразливостей Wi-Fi
88. Бездротові мережі - загрози для WEP
89. Бездротові мережі - загрози для WPA
90. Бездротові мережі - загрози для Bluetooth

91. Атаки на веб-додатки:-файли
92. Атаки на веб-додатки: Міжсайтовий скриптинг (XSS)
93. Атаки на веб-додатки: Включення локальних або віддалених файлів
94. Атаки на веб-додатки: SQL-ін'єкції

8. ОЦІНЮВАННЯ ПОТОЧНОЇ, САМОСТІЙНОЇ ТА ІНДИВІДУАЛЬНОЇ РОБОТИ СТУДЕНТІВ З ПІДСУМКОВИМ КОНТРОЛЕМ У ФОРМІ ЕКЗАМЕНУ/ ЗАЛІКУ

Денна форма навчання			
Поточний контроль			
Види роботи	**Планові терміни виконання**	**Форми контролю та звітності**	**Максимальний відсоток оцінювання**
Систематичність і активність роботи на семінарських (практичних) заняттях			
1.1. Підготовка до практичних занять	Відповідно до робочої програми та розкладу занять	Перевірка обсягу та якості засвоєного матеріалу під час практичних занять	**25**
Виконання завдань для самостійного опрацювання			
1.2. Підготовка програмного матеріалу (тем, питань), що виноситься на самостійне вивчення	-//-	Розгляд відповідного матеріалу під час аудиторних занять або ІКР[1], перевірка конспектів навчальних текстів тощо	**10**
Виконання індивідуальних завдань (науково-дослідна робота студента)			
1.3. Підготовка реферату (есе) за заданою тематикою	Відповідно до розкладу занять і графіку ІКР	Обговорення (захист) матеріалів реферату (есе)	**10**
1.4. Інші види індивідуальних завдань, в т.ч. підготовка наукових публікацій, участь у роботі круглих столів, конференцій тощо.	-//-	Обговорення результатів проведеної роботи під час аудиторних занять або ІКР, наукових конференцій та круглих столів.	**5**
Разом балів за поточний контроль			**50**
Підсумковий контроль залік			**50**
Всього балів			**100**
Заочна форма навчання			
Поточний контроль			

[1] Індивідуально-консультативна робота викладача зі студентами

Види самостійної роботи	Планові терміни виконання	Форми контролю та звітності	Максимальний відсоток оцінювання
Систематичність і активність роботи під час аудиторних занять			
1.1. Підготовка до аудиторних занять	Відповідно до розкладу	Перевірка обсягу та якості засвоєного матеріалу під час аудиторних занять	**15**
За виконання контрольних робіт (завдань)			
1.2. Підготовка контрольних робіт	-//-	Перевірка контрольних робіт (завдань)	**15**
Виконання завдань для самостійного опрацювання			
1.3. Підготовка програмного матеріалу (тем, питань), що виноситься на самостійне вивчення	-//-	Розгляд відповідного матеріалу під час аудиторних занять або ІКР[2], перевірка конспектів навчальних текстів тощо	**10**
Виконання індивідуальних завдань (науково-дослідна робота студента)			
2.1. Підготовка реферату (есе) за заданою тематикою	Відповідно до графіку ІКР	Обговорення (захист) матеріалів реферату (есе) під час ІКР	**5**
2.3. Інші види індивідуальних завдань, в т.ч. підготовка наукових публікацій, участь у роботі круглих столів, конференцій тощо.	-//-	Обговорення результатів проведеної роботи під час ІКР, наукових конференцій та круглих столів.	**5**
Разом балів за поточний контроль			**50**
Підсумковий контроль залік			**50**
Всього балів підсумкової оцінки			**100**

Таблиця відповідності результатів контролю знань за різними шкалами

100-бальною шкалою	Шкала за ECTS	За національною шкалою	
		екзамен	залік
90-100 (10-12)	A	Відмінно	зараховано
82-89 (8-9)	B	Добре	
74-81(6-7)	C		
64-73 (5)	D	Задовільно	
60-63 (4)	E		
35-59 (3)	Fx	незадовільно	не зараховано

[2] Індивідуально-консультативна робота викладача зі студентами

8. КРИТЕРІЇ ПІДСУМКОВОЇ ОЦІНКИ ЗНАНЬ СТУДЕНТІВ
(для іспиту / заліку)

Рівень знань оцінюється:

- «відмінно» / «зараховано» A - від 90 до 100 балів. Студент виявляє особливі творчі здібності, вміє самостійно знаходити та опрацьовувати необхідну інформацію, демонструє знання матеріалу, проводить узагальнення і висновки. Був присутній на лекціях та семінарських заняттях, під час яких давав вичерпні, обґрунтовані, теоретично і практично правильні відповіді, має конспект з виконаними завданнями до самостійної роботи, презентував реферат (есе) за заданою тематикою, проявляє активність і творчість у науково-дослідній роботі;

- «добре» / «зараховано» B - від 82 до 89 балів. Студент володіє знаннями матеріалу, але допускає незначні помилки у формуванні термінів, категорій, проте за допомогою викладача швидко орієнтується і знаходить правильні відповіді. Був присутній на лекціях та семінарських заняттях, має конспект з виконаними завданнями до самостійної роботи, презентував реферат (есе) за заданою тематикою, проявляє активність і творчість у науково-дослідній роботі;

- «добре» / «зараховано» C - від 74 до 81 балів. Студент відтворює значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень, з допомогою викладача може аналізувати навчальний матеріал, але дає недостатньо обґрунтовані, невичерпні відповіді, допускає помилки. При цьому враховується наявність конспекту з виконаними завданнями до самостійної роботи, реферату та активність у науково-дослідній роботі;

- «задовільно» / «зараховано» D - від 64 до 73 балів. Студент був присутній не на всіх лекціях та семінарських заняттях, володіє навчальним матеріалом на середньому рівні, допускає помилки, серед яких є значна кількість суттєвих. При цьому враховується наявність конспекту з виконаними завданнями до самостійної роботи, рефератів (есе);

- «задовільно» / «зараховано» E - від 60 до 63 балів. Студент був присутній не на всіх лекціях та семінарських заняттях, володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні, на всі запитання дає необґрунтовані, невичерпні відповіді, допускає помилки, має неповний конспект з завданнями до самостійної роботи.

- «незадовільно з можливістю повторного складання» / «не зараховано» FX – від 35 до 59 балів. Студент володіє матеріалом на рівні окремих фрагментів, що становлять незначну частину навчального матеріалу.

- «незадовільно з обов'язковим повторним вивченням дисципліни» / «не зараховано» F – від 0 до 34 балів. Студент не володіє навчальним матеріалом.

11. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Заплотинський Б.А. Основи інформаційної безпеки. Конспект лекцій. КІВіП НУ “ОЮА”, кафедра інформаційно-аналітичної та інноваційної діяльності, 2017. 128 с.
2. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. Humanitarian vision. 2016. Vol. 2, Num. 1. С. 27-32.
3. Доктрина інформаційної безпеки України : Указ Президента України від 25.02.2017 р. № 47/2017. *Офіційний вісник Президента України. 2017*. № 5. С. 15. Ст. 102.
4. Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII
5. Стратегія кібербезпеки України : Указ Президента України від 15.03.2016 р. № 96/2016. *Офіційний вісник України*. 2016. № 23. С. 69. Ст. 899.
6. Кібербезпека та системи захисту інформації: виклики сьогодення: збірник матеріалів круглого столу, м. Маріуполь, 26 жовтня2017 р. / Маріупольський державний університет; Кафедра математичних методів та системного аналізу; уклад. Тимофєєва І. Б. Маріуполь.: МДУ, 2017. 104 с.
7. Лісовська Ю.П. Кібербезпека: ризики та заходи: навч. посібник. Київ: Видавничий дім «Кондор», 2019. 272 с.
8. Василенко М.Д., Новіков В.П., Рачук В.О., Слатвінська В.М. Кібербезпека в проявах ризиків у період пандемії: стан та генеза. *Вісник Черкаського державного технологічного університету*. 2020. Вип. 3. С. 30-39. DOI: 10.24025/2306-4412.3.2020.214774.
9. 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.

Допоміжна

1. Конахович Г. Ф., Прогонов Д. О., Пузиренко О. Ю. Комп'ютерна стеганографічна обробка й аналіз мультимедійних даних. К. : «Центр навчальної літератури», 2018. 558 с.
2. ДСТУ ISO/IEC 27032:2016 (ISO/IEC 27032:2012, IDT) Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки
3. ДСТУ ISO/IEC 27005:2015 (ISO/IEC 27005:2011, IDT) Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки
4. Слатвінська В.М. Різновиди кібератак на судні в контексті управління кібербезпекою. Пріоритетні напрями розвитку науки та техніки: Матеріали LXII Міжнародної інтернет-конференції (м. Чернігів, 1 березня 2021 р.). 2021. С. 125-128.
5. Василенко М.Д., Рачук В.О., Слатвінська В.М. Шкідливі програми в контексті розуміння комп’ютерної вірусології та техніко-правової змагальності: міждисциплінарне дослідження. Наукові праці Національного університету «Одеська юридична академія». 2021. Т. 28. С. 28-36.
6. Василенко М.Д. Підвищення стану кібербезпеки інформаційно-комунікаційних систем: якість в контексті удосконалення інформаційного законодавства. Юридичний вісник. Одеса : ВД «Гельветика». 2018. № 3. С. 17-34.
7. Василенко М.Д. Якість кібербезпеки інформаційно-комунікаційних систем (ІКС) та деякі законодавчі питання щодо її підвищення. Юридичний вісник. Одеса : ВД «Гельветика». 2018. № 4. С. 35-41.
8. Василенко М.Д. Кібербезпека та захист персональних даних в ЄС: проблеми цифрового суспільства. Наукові праці Національного університету «ОЮА». Т. 23. Одеса: 2019. С. 34-48.
9. Василенко М.Д. Безпека комп’ютерних систем в контексті законодавства та запобігання кіберзагроз // Юридичний вісник. – О. : ВД «Гельветика». 2019. № 2. С. 70-76.

10. Василенко М.Д. Кібербезпека в ЄС та країнах-членах: генезис та проблеми її підвищення. *Інформаційна безпека людини, суспільства, держави*. К.: СБУ, 2019. № 3. С. 57-69.
11. Василенко М.Д. Кібербезпека розумних міст: соціальні аспекти, ризики деанонімізації і доксінгу. Науково-технічний зб. «Комунальне господарство міст». Серія: технічні науки та архітектура. Харків, 2020. Вип.6 (159). С. 181-190.
12. Слатвінська В. М. Особливості навчання правоохоронців основам кібербезпеки. Науково-педагогічне стажування Прикладні науково-технічні дослідження: європейський досвід і напрями розвитку (м. Прага, Чеська Республіка, 13 вересня – 24 жовтня 2021 року). 2021. 63-65.
13. Бойко В. Д., Василенко М. Д., Слатвінська В. М. Версіонування файлової системи для боротьби з програмами-вимагачами. VIII Міжнародна науково-технічна конференція "Інформатика, управління та штучний інтелект (ІУШІ-2021)". (м. Харків, 16 – 19 листопада 2021 р). Харків: НТУ "ХПІ". 2021. С. 9.
14. Слатвінська В.М., Федченко О.І. SMS-Bomber як інструмент кібершахрайства. VIII Всеукраїнська мультидисциплінарна конференція «Чорноморські наукові студії» 24 черв+ня 2022 Одеса МГУ. 2022. С. 127-129. URL: http://www.sci-notes.mgu.od.ua/archive/v36_1/2022_Chornomorski.pdf
15. Слатвінська В.М., Рябчук А.Р. Різновид DoS-атак і DDoS-атак. VIII Всеукраїнська мультидисциплінарна конференція «Чорноморські наукові студії» 24 червня 2022 Одеса МГУ. 2022. С. 109-111. URL: http://www.sci-notes.mgu.od.ua/archive/v36_1/2022_Chornomorski.pdf
16. Слатвінська В.М., Вяткіна А.Є. Стратегія інформаційної безпеки від Microsoft. VIII Всеукраїнська мультидисциплінарна конференція «Чорноморські наукові студії» 24 червня 2022 Одеса МГУ. 2022. С. 26-29. URL: http://www.sci-notes.mgu.od.ua/archive/v36_1/2022_Chornomorski.pdf
17. Boyko V.D., Vasylenko M.D., Slatvinska V.M. Linked list systems for system logs protection from cyberattacks. Conference proceedings of the VI International Scientific-Practical Conference "Information Technologies in Education, Science and Technology" (ITEST-2022), (Cherkasy, June 23-25, 2022). Cherkasy: ChSTU, 2022. P. 81-82. URL: https://knsa.chdtu.edu.ua/wp-content/uploads/2022/08/%D0%97%D0%B1%D1%96%D1%80%D0%BD%D0%B8%D0%BA_%D1%82%D0%B5%D0%B7_%D0%86%D0%A2%D0%9E%D0%9D%D0%A2-2022_01_08.pdf
18. Василенко М. Д. Соціальна інженерія як зброя хакінгу з підвищеним ризиком / М. Д. Василенко, В. М. Слатвінська // Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття» (до 25-річчя Національного університету «Одеська юридична академія» та 175-річчя Одеської школи права) : у 2 т. : матеріали Міжнар.наук.-практ. конф. (м. Одеса, 17 червня 2022 р.) / за загальною редакцією С. В. Ківалова. – Одеса : Видавничий дім «Гельветика», 2022. – Т. 1. – С. 729-731. URL: http://dspace.onua.edu.ua/handle/11300/19773

Інформаційні ресурси

1. Офіційний портал Верховної Ради України (законодавство): веб-сайт. URL: https://www.rada.gov.ua/ (дата звернення: 30.06.2022).
2. Сайт Державна служба спеціального зв'язку та захисту інформації України URL: www.dsszzi.gov.ua. (дата звернення: 30.06.2022).
3. Державний науково-дослідний експертно-криміналістичний центр URL: https://mvs.gov.ua/ua/structure/Derzhavnij-naukovo-dosl%D1%96dnij-ekspertno-krim%D1%96nal%D1%96stichnij-tsentr.htm/ (дата звернення: 30.06.2022)
4. Українська антивірусна лабораторія. / Єдиний український розробник інноваційних технологій кіберзахисту https://zillya.ua/antivirusnalaboratoriya (дата звернення: 30.06.2022)
5. Національна бібліотека України імені В. І. Вернадського URL: http://www.nbuv.gov.ua/ (дата звернення: 30.06.2022)
6. Офіційний вісник України URL: https://zakon.rada.gov.ua/laws/main/b19 (дата звернення: 30.06.2022)
7. Сайт Міжнародного гуманітарного університету URL: https://mgu.edu.ua/ (дата звернення: 30.06.2022)