МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
МАТЕМАТИЧНИЙ ФАКУЛЬТЕТ
КАФЕДРА ПРОГРАМНОЇ ІНЖЕНЕРІЇ

ЗАТВЕРДЖУЮ

Декан математичного факультету

_____ С.І. Гоменюк
(підпис) (ініціали та прізвище)

«_____»_____2021 р.

КІБЕРВІЙНИ ТА КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
підготовки бакалавра

Спеціальності:	**Освітні програми:**
081 Право	правознавство
051 Економіка	економічна кібернетика, міжнародна економіка, управління персоналом та економіка праці
071 Облік і оподаткування	облік і аудит
072 Фінанси, банківська справа та страхування	фінанси і кредит
073 Менеджмент	менеджмент
075 Маркетинг	маркетинг
076 Підприємництво, торгівля та біржова діяльність	соціологія
054 Соціологія	політологія
052 Політологія	соціальна педагогіка
231 Соціальна робота	психологія
053 Психологія	інформаційні системи та технології
126 Інформаційні системи та технології	мова і література, переклад: анг., нім., фр., ісп. мови
035 Філологія	програмна інженерія
121 Інженерія програмного забезпечення	біологія
091 Біологія	
(шифр, назва спеціальності)	(назва програми)

Укладач: Горбенко В.І., кандидат фізико-математичних наук, доцент, доцент кафедри програмної інженерії

Обговорено та ухвалено
на засіданні кафедри програмної інженерії
Протокол № від “ ” _____ 2021 р.
Завідувач кафедри

_____ А.О. Лісняк
(підпис) (ініціали, прізвище)

Ухвалено науково-методичною радою
математичного факультету
Протокол № від “ ” _____ 2021 р.
Голова науково-методичної ради
математичного факультету

_____ О.С. Пшенична
(підпис) (ініціали, прізвище)

Погоджено
з навчально-методичним відділом

_____ _____
(підпис) (ініціали, прізвище)

2021 рік

1. Опис навчальної дисципліни

<table>
<tr><th>1</th><th>2</th><th colspan="2">3</th></tr>
<tr><td rowspan="2">Галузь знань, спеціальність, освітня програма
рівень вищої освіти</td><td rowspan="2">Нормативні показники для планування і розподілу дисципліни на змістові модулі</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>очна (денна) форма здобуття освіти</td><td>заочна (дистанційна) форма здобуття освіти</td></tr>
<tr><td rowspan="2">Галузь знань
01 Освіта/Педагогіка
03 Гуманітарні науки
05 Соціальні та поведінкові науки
07 Управління та адміністрування
08 Право
09 Біологія
10 Природничі науки
11 Математика та статистика
12 Інформаційні технології
23 Соціальна робота</td><td rowspan="2">Кількість кредитів – 3</td><td colspan="2">Вибіркова</td></tr>
<tr><td colspan="2">Блок дисциплін вільного вибору студента в межах Університету</td></tr>
<tr><td rowspan="2">Спеціальність
081 Право
051 Економіка
071 Облік і оподаткування
072 Фінанси, банківська справа та страхування
073 Менеджмент
075 Маркетинг
076 Підприємництво, торгівля та біржова діяльність
054 Соціологія
052 Політологія
231 Соціальна робота
053 Психологія
126 Інформаційні системи та технології
035 Філологія
121 Інженерія програмного забезпечення
091 Біологія</td><td rowspan="2">Загальна кількість годин – 90</td><td colspan="2">Семестр:</td></tr>
<tr><td>4-й</td><td>4-й</td></tr>
<tr><td rowspan="8">Освітньо-професійна програма
правознавство
економічна кібернетика, міжнародна економіка, управління персоналом та економіка праці
облік і аудит
фінанси і кредит
менеджмент
маркетинг
соціологія
політологія
соціальна педагогіка
психологія
інформаційні системи та технології
мова і література, переклад: анг., нім., фр., ісп. мови
програмна інженерія
біологія</td><td rowspan="8">Змістових модулів – 4</td><td colspan="2">Лекції</td></tr>
<tr><td>28 год.</td><td>–</td></tr>
<tr><td colspan="2">Практичні, семінарські</td></tr>
<tr><td>–</td><td>–</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>62 год.</td><td>–</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td colspan="2"></td></tr>
<tr><td>Рівень вищої освіти:
бакалаврський</td><td>Кількість поточних контрольних заходів – 8</td><td colspan="2">Вид підсумкового семестрового контролю:
залік</td></tr>
</table>

2. Мета та завдання навчальної дисципліни

Метою вивчення навчальної дисципліни «Кібервійни та кібербезпека в сучасному світі» є оволодіння цілісним уявленням про використання сучасних інформаційних технологій для створення та застосування специфічного типу зброї у політичній та конкурентній боротьбі, протистоянні держав, а також про проблеми та шляхи досягнення кібербезпеки.

Основні **завдання** вивчення дисципліни «Кібервійни та кібербезпека в сучасному світі»:

- ознайомитися з об’єктами кібервійни та принципами її ведення;
- навчитися розрізняти кібервійну та кібершахрайство, дії кіберзброї та інструментів хакерського шантажу;
- навчитися аналізувати здатність підприємства/установи щодо створення необхідних умов для практичної реалізації протидії кібератакам і кіберінцидентам;
- навчитися виявляти появу загроз з боку кіберпростору;
- навчитися визначати вимоги щодо забезпечення кібербезпеки на підприємстві або в установі;
- навчитися визначати потенційні об’єкти кібератак на підприємстві або в установі;
- орієнтуватися у засобах кіберзахисту та навчитися визначати шляхи покращення кібербезпеки.

Міждисциплінарні зв’язки. Вивчення навчальної дисципліни «Кібервійни та кібербезпека в сучасному світі» передбачає використання досягнень наступних дисциплін:

1. Історії України – при дослідженні впливу зовнішніх чинників на становлення та розвиток незалежності держави, формування зовнішньої політики та міжнародну діяльність.

2. Права і свободи людини та громадянина в Україні – при вивченні впливу кібервійні та кіберзагроз на права та свободи громадян, політики уряду України щодо кіберзахисту та кібербезпеки.

3. Програма навчальної дисципліни

Змістовий модуль 1. Кіберпростір та кібервійна

Загальні поняття кібервійни. Кіберпростір і кібербезпека. Класифікація кібервійн. Об’єкти кібервійн. Об’єкти впливу в інформаційному та кіберпросторі. Реагування на кібернетичні втручання і загрози. Класифікація кібернетичних втручань і загроз. Джерела інцидентів, об’єкти та результати їхнього впливу. Заходи при порушенні кібербезпеки компанії.

Змістовий модуль 2. Кіберзброя та кібератаки

Кібернетичні потужності та кіберзброя. Кібератака та її операційні аспекти. Кіберармії світу. Фахівці кібервійни. Особливості реалізації кібератак. Мета, об’єкт та суб’єкт кібератаки. Типи та властивості кібератаки. Механізми формування кібератаки. Типи впливу кібератак. Типи кіберзброї, її засоби та застосування. Характеристики наступальної та оборонної кіберзброї. Характеристика кібератак та кібероперацій. Методи та моделі кібернападу та кіберзахисту. Способи та методи ведення розвідки ІТ-систем.

Змістовий модуль 3. Кібербезпека та кіберзахист

Кібербезпека. Кіберзахист. Стратегія кібербезпеки України. Загрози щодо компонент ІС. Методи забезпечення інформаційної безпеки. Складові інформаційної безпеки. Проблеми забезпечення кібербезпеки. Сутність кібербезпеки. Моніторинг кібернетичних втручань і загроз. Безпека державних інформаційних ресурсів. Надійність кіберінфраструктури. Роль вітчизняних виробників програмного та апаратного забезпечення. Реалізація механізмів партнерства держави, бізнесу й громадян у сфері кібербезпеки. Удосконалення національного нормативно-правового та понятійно-термінологічного апарату кібербезпеки.

Змістовий модуль 4. Кібермир та миротворча діяльність у кіберпросторі

Військові стратегії в інформаційному середовищі. Інформаційна війна. Миротворча діяльність у кіберпросторі. Міжнародне співробітництво у сфері кібербезпеки. Співпраця з НАТО та країнами-партнерами у сфері кіберзахисту. Організаційно-правові норми міжнародної взаємодії у процесі боротьби з кіберзлочинністю і кібертероризмом. Міжнародні експертні центри з питань кібербезпеки. Взаємодопомога в технічних і методологічних аспектах кібербезпеки.

4. Структура навчальної дисципліни

Змістовий модуль	Усього годин	Аудиторні (контактні) години			Самостійна робота, год		Система накопичення балів		
		Усього годин	Лекційні заняття, год				Теор. зав-ня, к-ть балів	Практ. зав-ня, к-ть балів	Усього балів
			о/д ф.	з/дист ф.	о/д ф.	з/дист ф.			
1	**2**	**3**	**4**	**5**	**8**	**9**	**10**	**11**	**12**
1	14	6	6		8		15		15
2	16	8	8		8		15		15
3	14	6	6		8		15		15
4	16	8	8		8		15		15
Усього за змістові модулі	60	28	28		32		60	0	60
Підсумковий семестровий контроль **залік**	30				30		20	20	40
Загалом	**90**						**100**		

5. Теми лекційних занять

№ змістового модуля	Назва теми	Кількість годин	
		о/д ф.	з/дист ф.
1	**2**	**3**	**4**
1	1. Загальні поняття кібервійни	2	
	2. Класифікація кібервійн	2	
	3. Об’єкти кібервійн	2	
2	4. Кібернетичні потужності та кіберзброя	2	
	5. Кібератака та її операційні аспекти	2	

	6. Кіберармії світу	2	
	7. Фахівці кібервійни	2	
3	8. Кібербезпека	2	
	9. Кіберзахист	2	
	10. Стратегія кібербезпеки України	2	
4	11. Військові стратегії в інформаційному середовищі	2	
	12. Інформаційна війна	2	
	13. Миротворча діяльність у кіберпросторі	2	
	14. Міжнародне співробітництво у сфері кібербезпеки	2	
Разом		**28**	–

6. Види і зміст поточних контрольних заходів

№ змістового модуля	Вид поточного контрольного заходу	Зміст поточного контрольного заходу	Критерії оцінювання	Усього балів
1	**2**	**3**	**4**	**5**
1	Тест 1	Тестування з теоретичних питань змістового модулю	Тестові питання оцінюються з урахуванням вагових коефіцієнтів. Кількість питань у тесті – 10. Правильна відповідь оцінюється у 0,7 бали.	7
	Тест 2	Тестування з теоретичних питань змістового модулю	Тестові питання оцінюються з урахуванням вагових коефіцієнтів. Кількість питань у тесті – 10. Правильна відповідь оцінюється у 0,8 бали.	8
Усього за ЗМ 1 контр. заходів	**2**			**15**
2	Тест 3	Тестування з теоретичних питань змістового модулю	Тестові питання оцінюються з урахуванням вагових коефіцієнтів. Кількість питань у тесті – 10. Правильна відповідь оцінюється у 0,7 бали.	7
	Тест 4	Тестування з теоретичних питань змістового модулю	Тестові питання оцінюються з урахуванням вагових коефіцієнтів. Кількість питань у тесті – 10. Правильна відповідь оцінюється у 0,8 бали.	8
Усього за ЗМ 2 контр. заходів	**2**			**15**
3	Тест 5	Тестування з теоретичних питань змістового модулю	Тестові питання оцінюються з урахуванням вагових коефіцієнтів. Кількість питань у тесті – 10. Правильна відповідь оцінюється у 0,7 бали.	7
	Тест 6	Тестування з теоретичних питань змістового модулю	Тестові питання оцінюються з урахуванням вагових коефіцієнтів. Кількість питань у тесті – 10. Правильна відповідь оцінюється у 0,8 бали.	8
Усього за ЗМ 3 контр. заходів	**2**			**15**
4	Тест 7	Тестування з теоретичних питань змістового модулю	Тестові питання оцінюються з урахуванням вагових коефіцієнтів. Кількість питань у	7

			тесті – 10. Правильна відповідь оцінюється у 0,7 бали.	
	Тест 8	Тестування з теоретичних питань змістового модулю	Тестові питання оцінюються з урахуванням вагових коефіцієнтів. Кількість питань у тесті – 10. Правильна відповідь оцінюється у 0,8 бали.	8
Усього за ЗМ 4 контр. заходів	**2**			**15**
Усього за змістові модулі контр. заходів	**8**			**60**

8. Підсумковий семестровий контроль

Форма	Види підсумкових контрольних заходів	Зміст підсумкового контрольного заходу	Критерії оцінювання	Усього балів
1	**2**	**3**	**4**	**5**
Підсумковий контроль	Залік	Питання для підготовки: Поняття кібервійни, кіберпростору та кібербезпеки. Класифікація кібервійн. Об'єкти кібервійн. Кібернетичні втручання і загрози, їх класифікація. Джерела інцидентів, об'єкти та результати їхнього впливу. Заходи при порушенні кібербезпеки. Поняття кіберзброя, кібератака. Кібернетичні потужності та кіберзброя. Кібератака та її операційні аспекти. Кіберармії світу. Фахівці кібервійни. Реалізація кібератак. Мета, об'єкт та суб'єкт кібератаки. Типи та властивості кібератаки. Механізми формування кібератаки. Типи кіберзброї, її засоби та застосування. Наступальна та оборонна кіберзброя. Характеристика кібератак та кібероперацій. Методи та моделі кібернападу та кіберзахисту. Розвідка ІТ-систем. Поняття кіберзахисту. Стратегія кібербезпеки України. Складові інформаційної безпеки. Проблеми та сутність кібербезпеки. Моніторинг кібервтручань і загроз. Безпека державних інформаційних ресурсів. Надійність інфраструктури.	Залік проводиться в усній формі при очній формі навчання. Підсумковий контроль містить два теоретичних питання. За відповіді на теоретичні питання підсумкового контролю студент може отримати до 10 балів за одне питання, всього за залік можна отримати до 20 балів. У разі дистанційної форми навчання залік проходить у тестовій формі через платформу Moodle. Підсумковий тест складається із 20 тестових питань. Правильна відповідь оцінюється у 1 бал або всього за підсумковий тест можна отримати до 20 балів.	20

		Партнерство у сфері кібербезпеки. Кібермир та миротворча діяльність. Військові стратегії в кіберпросторі. Інформаційна війна. Міжнародне співробітництво та взаємодопомога з кібербезпеки та кіберзахисту. Усна частина підсумкового контролю передбачає розгорнуту та обґрунтовану відповідь на два теоретичних питання (з письмовою фіксацією всіх відповідей) і розгорнуте розв'язання одного практичного завдання. У разі дистанційної форми навчання залік проходить у тестовій формі через платформу Moodle.		
	Практичне завдання: Індивідуальне дослідницьке завдання (ІДЗ)	Індивідуальне дослідницьке завдання (ІДЗ) складається з комплексного завдання. Звіт по виконаному ІДЗ оформлюється за вимогами, які висуваються до оформлення курсових і кваліфікаційних робіт для здобувачів ступеня вищої освіти бакалавра. ІДЗ здається до початку залікового тижня.	ІДЗ складається з 2 завдань, за кожне з яких студент може отримати до 10 балів, з урахуванням відповідей на запитання при захисті звіту.	20
Усього за підсумковий семестровий контроль	**2**			**40**

9. Рекомендована література

Основна:

1. Стратегія кібербезпеки України (2021 – 2025 роки). Режим доступу: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf
2. Концепція інформаційної безпеки України: Режим доступу: https://www.osce.org/files/f/documents/0/2/175056.pdf
3. Бурячок В.Л., Толубко В.Б., Хорошко В.О., Толюпа С.В. Інформаційна та кібербезпека: соціотехнічний аспект: підручник. - Київ : ДУТ, 2015. 288 с.
4. Курбан О.В. Сучасні інформаційні війни в мережевому он-лайн просторі : навчальний посібник. – Київ: ВІКНУ, 2016. 286 с.
5. Jajodia S., Shakarian P., Subrahmanian V.S., Swarup V. Cyber Warfare: Building the Scientific Foundation. London: Springer, 2015. 321 p.
6. Binary bullets: the ethics of cyberwarfare / edited by F.Allhoff, A.Henschke, B.J.Strawser. - New York: Oxford University Press, 2016. 296 p.

7. Greenberg A. Sandworm : a new era of cyberwar and the hunt for the Kremlin’s most dangerous hackers. - New York : Doubleday, 2019. 370 p.
8. Бараненко Р.В. Кібератаки як одна із форм кібертероризму // Вчені записки Таврійського національного університету ім. В.І. Вернадського, Серія: Технічні науки, Т.32(71), №1,Ч.1, 2021, С.45-50. DOI https://doi.org/10.32838/2663-5941/2021.1-1/07

Додаткова:

1. Дубов Д.В. Кіберпростір як новий вимір геополітичного суперництва : монографія. – Київ : НІСД, 2014. 328 с.
2. Tallinn manual on the international law applicable to cyber warfare : prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence / ed. M.N.Schmitt. - New York : Cambridge University Press, 2013. 282 p.
3. Tallinn manual 2.0 on the international law applicable to cyber operations : Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence / ed. M.N.Schmitt. - New York : Cambridge University Press, 2016. 598 p.
4. Cunningham Ch. Cyber Warfare – Truth, Tactics, and Strategies. BIRMINGHAM : Packt, 2020. 302 p.

Інформаційні ресурси

1. Наукова бібліотека Запорізького національного університету. URL: http://library.znu.edu.ua/
2. Кібервійна : Режим доступу: https://uk.wikipedia.org/wiki/Кібервійна