МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ
Кафедра комп'ютерної інженерії та інноваційних технологій

«ЗАТВЕРДЖУЮ»
Ректор Міжнародного гуманітарного університету д.ю.н., професор
_____ Костянтин ГРОМОВЕНКО
«29» серпня 2025 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Управління інформаційною та кібербезпекою

Галузь знань	12 «Інформаційні технології»
Спеціальність	125 «Кібербезпека та захист інформації»
Назва освітньої програми	Кібербезпека
Рівень вищої освіти	перший (бакалаврський) рівень

Одеса – 2025 рік

Робоча програма затверджена на засіданні кафедри комп'ютерної інженерії та інноваційних технологій протокол №1 від 28.08.2025 року.

Розробники і викладачі	**Контактний тел.**	**E-mail**
Професор кафедри комп'ютерної інженерії та інноваційних технологій **Радівілова Тамара Анатоліївна**	+380951609153	tamara.radivilova@gmail.com

Завідувач кафедри комп'ютерної інженерії
та інноваційних технологій
к.т.н., доцент _____ Лариса ЙОНА

Гарант освітньої програми
к.т.н., доцент _____ Лариса ЙОНА

Узгоджено
Начальник навчального відділу _____ Лілія САЄНКО

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

<table>
<tr><th rowspan="2">Найменування показників</th><th rowspan="2">Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень</th><th colspan="2">Характеристика навчальної дисципліни</th></tr>
<tr><th>денна форма навчання</th><th>заочна форма навчання</th></tr>
<tr><td rowspan="10">Кількість кредитів – 4
Загальна кількість годин – 120</td><td>Галузь – 12 Інформаційні технології</td><td colspan="2">обов’язкова</td></tr>
<tr><td rowspan="9">Спеціальність – 125 Кібербезпека та захист інформації</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td colspan="2">2-й</td></tr>
<tr><td colspan="2">Семестр</td></tr>
<tr><td>7-й</td><td>7-й</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td rowspan="8">Мова навчання – українська</td><td rowspan="8">Рівень вищої освіти – перший (бакалаврський) рівень</td><td>26 год.</td><td>6 год.</td></tr>
<tr><td colspan="2">Практичні, семінарські</td></tr>
<tr><td>20 год.</td><td>2 год.</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>6 год.</td><td>2 год.</td></tr>
<tr><td colspan="2">Самостійна робота та індивідуальні завдання</td></tr>
<tr><td>68 год.</td><td>110 год.</td></tr>
<tr><td colspan="2">Вид контролю:</td></tr>
<tr><td>Залік</td><td>Залік</td></tr>
</table>

Дисципліна «Управління інформаційною та кібербезпекою» є обов'язковим компонентом освітньо-професійної програми підготовки бакалаврів зі спеціальності 125 «Кібербезпека та захист інформації» та спрямована на формування у здобувачів компетентностей у сфері організації, планування та контролю заходів із забезпечення інформаційної безпеки на рівні підприємства чи установи. Дисципліна охоплює нормативно-правове регулювання, розробку політик безпеки, методології оцінки ризиків, управління інцидентами, аудит систем захисту та забезпечення безперервності бізнес-процесів у контексті сучасних викликів кібербезпеки.

Метою дисципліни є забезпечення здобувачів знаннями з принципів побудови системи управління інформаційною безпекою (СУІБ), методик кількісної та якісної оцінки ризиків, вимог міжнародних стандартів (ISO/IEC 27000-series), а також набуття практичних навичок розробки політик безпеки, планування реагування на інциденти, проведення аудиту захищеності та інтеграції заходів кібербезпеки в організаційну структуру та бізнес-процеси відповідно до чинного законодавства та найкращих світових практик.

ПРЕРЕКВІЗИТИ. Передумовами для вивчення дисципліни є знання, уміння та навички, отримані при вивченні «Комплексних систем захисту інформації» (ОК 24), «Безпеки програм та даних» (ОК 16), «Криптографії та криптоаналізу» (ОК 23), «Операційних систем» (ОК 20), а також «Комп'ютерних мереж» (ОК 13). Додатково спирається на навички критичного мислення та аналізу («Філософія», ОК 4).

ПОСТРЕКВІЗИТИ. Знання стандартів, нормативної бази та управлінських аспектів інформаційної безпеки є безпосередньою базою для вивчення «Основ цифрової криміналістики» (ОК 26), паралельного вивчення «Безпеки бездротових мереж Інтернету речей (IoT)» (ОК 27) та

«Етичного хакінгу та тестування на проникнення» (ОК 18), а також для проходження переддипломної практики (ОК 35) і підготовки та захисту кваліфікаційної роботи (ОК 36).

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

У процесі реалізації програми дисципліни «Криптографія та криптоаналіз» формуються наступні компетентності із передбачених освітньою програмою:

Інтегральна компетентність

ІК. Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі кібербезпеки та захисту інформації.

Загальні компетентності (ЗК)

ЗК1. Здатність застосовувати знання у практичних ситуаціях.

ЗК 2. Знання та розуміння предметної області та розуміння професійної діяльності

Спеціальні (фахові, предметні) компетентності

СК 1. Здатність застосовувати законодавчу та нормативно правову базу, а також державні та міжнародні вимоги, практики і стандарти у професійній діяльності

СК 6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо).

СК 7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.

СК 11. Здатність здійснювати проєктування, адміністрування та керування інформаційно-комунікаційними системами, забезпечуючи їхню надійність, безпеку та ефективність функціонування.

Навчальна дисципліна «Управління інформаційною та кібербезпекою» забезпечує досягнення програмних результатів навчання (РН), передбачених освітньою програмою:

РН 9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації

РН 17. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.

РН 22. Вміти застосовувати методи та інструменти проєктування й адміністрування мереж і систем, виконувати налаштування, моніторинг та підтримку їхньої працездатності з урахуванням вимог інформаційної безпеки.

3. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Тема 1. Нормативно-правове забезпечення інформаційної безпеки. Основні закони України та міжнародні стандарти (ISO/IEC 27001, GDPR, NIST). Роль державних органів у сфері кібербезпеки. Етичні та правові аспекти захисту інформації.

Тема 2. Політики безпеки та управління кібербезпекою в організації. Структура політики інформаційної безпеки. Принципи управління доступом та ролями. Організаційні моделі управління кібербезпекою.

Тема 3. Управління ризиками інформаційної безпеки. Поняття ризику та методи його оцінки. Кількісні та якісні моделі (факторний аналіз, байєсівські мережі). Інструменти управління ризиками (ISO 31000, OCTAVE).

Тема 4. Моніторинг, виявлення та реагування на інциденти. Системи SIEM та SOC. Методи виявлення атак (ентропійний аналіз, сигнатурний та поведінковий підходи). План реагування на інциденти.

Тема 5. Аудит та тестування безпеки інформаційних систем. Види аудиту (внутрішній, зовнішній, комплаєнс). Методи тестування: penetration testing, vulnerability scanning.

Тема 6. Комплексні системи захисту інформації та безперервність бізнесу. Архітектура комплексних систем захисту (мережеві екрани, IDS/IPS, криптографія). Планування безперервності бізнесу та disaster recovery.

Тема 7. Перспективи та стратегічні тенденції управління кібербезпекою. Використання штучного інтелекту та машинного навчання у кіберзахисті. Кіберзагрози для критичної інфраструктури, IoT, квантові обчислення. Стратегії розвитку кібербезпеки на рівні держави та бізнесу.

4. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви змістових модулів і тем	Кількість годин									
	денна форма					Заочна форма				
	усього	у тому числі				усього	у тому числі			
		лекц.	лабор	практ	сам. роб.		лекц.	лабор	практ	сам. роб.
Тема 1. Нормативно-правове забезпечення інформаційної безпеки.	12	2		2	8	16	2			14
Тема 2. Політики безпеки та управління кібербезпекою в організації.	16	4		2	10	16				16
Тема 3. Управління ризиками інформаційної безпеки.	18	4		4	10	18	2			16
Тема 4. Моніторинг, виявлення та реагування на інциденти.	18	4	2	2	10	18		2		16
Тема 5. Аудит та тестування безпеки інформаційних систем.	20	4	2	4	10	16				16
Тема 6. Комплексні системи захисту інформації та безперервність бізнесу.	20	4	2	4	10	18			2	16
Тема 7. Перспективи та стратегічні тенденції управління кібербезпекою.	16	4		2	10	18	2			16
Усього годин	**120**	**26**	**6**	**20**	**68**	**120**	**6**	**2**	**2**	**110**
ПІДСУМКОВИЙ КОНТРОЛЬ – **Залік**										

5. ПРАКТИЧНІ РОБОТИ

Назва теми	Кількість годин	
	Денна форма	Заочна форма
1. Аналіз нормативних документів для конкретної організації.	2	
2. Розробка фрагмента політики безпеки для університетської мережі.	2	
3. Складання матриці ризиків для IT-системи.	4	
4. Моделювання сценарію реагування на DDoS-атаку.	2	
5. Складання чек-листа аудиту для веб-додатку.	4	
6. Розробка плану резервного копіювання та відновлення.	4	2
7 Підготовка аналітичного огляду сучасних тенденцій.	2	
Всього	**20**	**2**

6. ЛАБОРАТОРНІ РОБОТИ

Назва теми	Кількість годин	
	Денна форма	Заочна форма
1. Виявлення ознак DDoS-атаки чи несанкціонованого доступу.	2	
2. Аудит інформаційних систем та виявлення вразливостей.	2	
3. Проєктування комплексної системи захисту та плану безперервності бізнесу.	2	
Всього	**6**	**2**

7. САМОСТІЙНА РОБОТА

До самостійної роботи студентів щодо вивчення дисципліни 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 контрольних робіт.
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. Нормативно-правове забезпечення інформаційної безпеки.** Законодавча база України у сфері інформаційної безпеки та захисту інформації. Міжнародні нормативні документи та стандарти (ISO/IEC 27000-series, рекомендації ITU, директиви ЄС).	8	14
2	**Тема 2. Політики безпеки та управління кібербезпекою в організації.** Поняття, структура, типи політик. Політики Zero Trust, адаптивні політики безпеки, інтеграція з хмарними сервісами. Організаційна структура служби безпеки.	10	16
3	**Тема 3. Управління ризиками інформаційної безпеки.** Методологія управління ризиками (ISO/IEC 27005, NIST Risk Management Framework). Процедури кількісної та якісної оцінки ризиків. Методики OCTAVE, FAIR.	10	16
4	**Тема 4. Моніторинг, виявлення та реагування на інциденти.** Принципи безперервного моніторингу. Використання SIEM-систем. План реагування на інциденти (Incident Response Plan). Взаємодія з CERT та кіберполіцією.	10	16
5	**Тема 5. Аудит та тестування безпеки інформаційних систем.** Методології аудиту (ISO/IEC 27001, COBIT, NIST). Рекомендації з безпеки (ISO/IEC 27002). OWASP Testing Guide для веб-додатків. Рекомендації CERT щодо тестування та аудиту.	10	16
6	**Тема 6. Комплексні системи захисту інформації та безперервність бізнесу.**	10	16

	Принципи побудови системи «захист у глибину» (defense in depth). Забезпечення неперервності бізнес-процесів згідно встановленої політики кібербезпеки. Узгодження організаційних і технічних заходів.		
7	**Тема 7. Перспективи та стратегічні тенденції управління кібербезпекою.** Значення інформаційної безпеки в умовах цифрової трансформації. Використання штучного інтелекту та машинного навчання для управління безпекою. Інтеграція кібербезпеки у всі бізнес-процеси.	10	16
	Всього	**68**	**110**

7. ВИДИ ТА МЕТОДИ КОНТРОЛЮ

Види контролю	**Складові оцінювання**	
	Для екзамену	**Для заліку**
поточний контроль, який здійснюється у ході: проведення практичних (лабораторних) занять, виконання самостійної роботи, індивідуальних завдань, дослідна робота здобувача тощо.	**50%**	**100%**
підсумковий контроль	**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, екзамен

8. ОЦІНЮВАННЯ ЗДОБУВАЧІВ ВИЩОЇ ТА ФАХОВОЇ ПЕРДВИЩОЇ ОСВІТИ ЗА НАВЧАЛЬНУ ДИСЦИПЛІНУ У МІЖНАРОДНОМУ ГУМАНІТАРНОМУ УНІВЕРСИТЕТІ

(*поточний контроль, підсумковий контроль, загальний результат оцінювання)*

ЗАЛІК

Поточний контроль			
Види роботи	**Планові терміни виконання**	**Форми контролю та звітності**	**Максимальний відсоток оцінювання**
Систематичність і активність роботи на практичних (лабораторних) заняттях			
1.1. Підготовка до практичних (лабораторних) занять	Відповідно до робочої програми та розкладу занять	Перевірка обсягу та якості засвоєного матеріалу під час практичних (лабораторних) занять	**60**
Виконання завдань для самостійного опрацювання			
1.2. Індивідуальне тестування, завдання, підготовка реферату (есе) за заданою тематикою	Відповідно до робочої програми та розкладу занять	Розгляд відповідного матеріалу під час аудиторних занять або ІКР[1], перевірка конспектів навчальних текстів тощо	**20**
Виконання індивідуальних завдань, дослідна робота здобувача			
1.3. Інші види індивідуальних завдань, в т.ч.підготовка наукових публікацій, участь у роботі круглих столів, конференцій тощо.	Відповідно до робочої програми та розкладу занять	Обговорення результатів проведеної роботи під час аудиторних занять, наукових конференцій та круглих столів.	**20**
Разом балів за поточний контроль			**100**
Загальний результат оцінювання			**100**

Поточний контроль знань здобувачів освіти при формі контролю **залік** (максимум 100 балів) оцінюється за шкалою *(«2», «3», «4», «5»)*, з обов'язковим переведенням балів за кожний вид роботи таким чином:

- за підготовку до аудиторних занять (максимум 60 балів) здобувачу освіти необхідно мати не менше 1/2 оцінок від загальної кількості практичних (лабораторних) занять, для переводу балів за підготовку до аудиторних занять середньоарифметична оцінка множиться на коефіцієнт 12;
- за виконання завдань для самостійного опрацювання (тестування, завдання, підготовка реферату (есе) за заданою тематикою) (максимум 20 балів) здобувачу освіти необхідно мати не менше 1/2 оцінок від загальної кількості програмного матеріалу, що виноситься на самостійне вивчення, для переводу зазначених балів середньоарифметична оцінка множиться на коефіцієнт 4;
- за інші види індивідуальних завдань, в т.ч. підготовку наукових публікацій, участь у роботі круглих столів, конференцій тощо (максимум 20- балів) здобувачу освіти необхідно мати не менше 1/2 оцінок від загальної кількості інших видів індивідуальних завдань, для переводу балів за підготовку до аудиторних занять середньоарифметична оцінка множиться на коефіцієнт 4.

КРИТЕРІЇ ОЦІНЮВАННЯ ЗА ПОТОЧНИЙ КОНТРОЛЬ

- «2»- виставляється за неправильну відповідь (письмову роботу), яка не відповідає змісту теми та свідчить про нерозуміння її основних положень;
- «3» -виставляється за відповідь (письмову роботу), яка відповідає змісту теми, але є неповною і неточною у визначенні понять, свідчить про неповне розуміння основних положень навчального матеріалу, свідчить про те, що знання студента мають фрагментарний, поверховий характер;
- «4» - оцінюється правильна і обґрунтована відповідь (письмова робота), з якої видно, що студент знає й розуміє теоретичний матеріал в обсязі навчальної теми, володіє необхідними навичками, не допускає суттєвих помилок.

«5» - оцінюється повна, правильна, ґрунтовна відповідь (письмова робота) на запитання теми, що передбачає логічність і послідовність викладу матеріалу, володіння термінологією, показує вміння повно й глибоко використовувати

9. КРИТЕРІЇ ЗАГАЛЬНИХ РЕЗУЛЬТАТІВ ОЦІНЮВАННЯ ЗНАНЬ ЗДОБУВАЧІВ (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,

[1] Індивідуально-консультативна робота викладача зі здобувачами

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.

ТАБЛИЦЯ ВІДПОВІДНОСТІ ЗАГАЛЬНИХ РЕЗУЛЬТАТІВ ОЦІНЮВАННЯ ЗНАНЬ ЗА РІЗНИМИ ШКАЛАМИ

100-бальною шкалою	Шкала за ECTS	За національною шкалою	
		екзамен	залік
90-100	A	Відмінно	Зараховано
82-89	B	Добре	
74-81	C		
64-73	D	Задовільно	
60-63	E		
35-59	FX	Незадовільно	Не зараховано
1-34	F		

10. ДОТРИМАННЯ ВИМОГ АКАДЕМІЧНОЇ ДОБРОЧЕСНОСТІ

Викладання та засвоєння навчальної дисципліни передбачає неухильне дотримання вимог академічної доброчесності, яка регулюється Законом України "Про освіту" (Відомості Верховної Ради (ВВР), 2014, № 37-38, ст.2004), «Методичними рекомендаціями для закладів вищої освіти з підтримки принципів академічної доброчесності» (Лист МОН № 1/9-650 від 23.10.18 року), іншими нормативними документами. Зокрема, основні засади дотримання академічної доброчесності визначено у «Положенні про академічну доброчесність у Міжнародному гуманітарному університеті», «Кодексі академічної доброчесності Міжнародного гуманітарного університету» та «Інструкції щодо процедури технічної перевірки на наявність текстових запозичень (академічного плагіату)», затвердженої наказом МГУ від 03.05.2024 р., № 708а.

Відповідно до ст.42 Закону України "Про освіту" академічна доброчесність - це сукупність етичних принципів та визначених законом правил, якими мають керуватися учасники освітнього процесу під час навчання, викладання та провадження наукової (творчої) діяльності з метою забезпечення довіри до результатів навчання та/або наукових (творчих) досягнень.

Дотримання академічної доброчесності передбачає:

- самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю результатів навчання (для осіб з особливими освітніми потребами ця вимога застосовується з

урахуванням їхніх індивідуальних потреб і можливостей);

- посилання на джерела інформації у разі використання ідей, розробок, тверджень, відомостей;
- дотримання норм законодавства про авторське право і суміжні права;
- надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності, використані методики досліджень і джерела інформації.

11. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Жилін А. В., Шаповал О. М., Успенський О. А. Технології захисту інформації в інформаційно-телекомунікаційних системах: навчальний посібник. Київ: КПІ ім. Ігоря Сікорського, 2020.
2. Остапов С. Е., Євсеєв С. П., Король О. Г. Кібербезпека: сучасні технології захисту: навчальний посібник. Львів: Новий Світ-2000, 2020.
3. Носок С. О., Фаль О. М., Ткач В. М. Управління інформаційною безпекою : конспект лекцій. Київ : КПІ ім. Ігоря Сікорського, 2021. 258 с.
4. Управління інформаційною безпекою : навч. посіб. / за ред. О. В. Баранова. Дніпро : ДДУВС, 2020. 312 с. ISBN 978-617-627-148-2.
5. Онацький О.В., Йона Л.Г., Бєлова Ю.В. Криптографічний захист інформації: Навч.посібник. - Одеса: Одеса : «Астропринт» 2023. 252с.

Допоміжна

1. Андерсон Р. Дж. Інженерія безпеки: посібник для створення захищених систем. Пер. з англ. Київ: Логос, 2010.
2. Radivilova, T., Kirichenko, L., Tawalbeh, M., & Ilkov, A. (2021). Виявлення аномалій в телекомунікаційному трафіку статистичними методами. Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка, 3(11), 2021, 183-194.
3. Dobrynin, I., Radivilova, T., Maltseva, N., & Ageyev, D. (2022). Use of approaches to the methodology of factor analysis of information risks for the quantitative assessment of information risks based on the formation of cause-and-effect links. *Kharkiv National University of Radio Electronics*.
4. ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки.

Інформаційні ресурси

1 Національна бібліотека України ім. В.І. Вернадського. URL: http://www.nbuv.gov.ua.
2 Портал кіберполіції України. URL: https://cyberpolice.gov.ua/
3 ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Женева: International Organization for Standardization, 2022. Режим доступу: https://www.iso.org/standard/27001