

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ЕКОНОМІЧНИЙ ФАКУЛЬТЕТ
КАФЕДРА ЕКОНОМІЧНОЇ КІБЕРНЕТИКИ

ЗАТВЕРДЖУЮ

Декан економічного факультету

А.В. Череп

« 02 » 09 2021 р.

«Основи інформаційної безпеки»

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

підготовки бакалавра
очної (денної) форми здобуття освіти

вибіркова дисципліна для ВНЗ

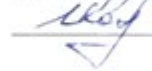
**Укладач Козін І.В., доктор фізико-математичних наук, професор,
професор кафедри економічної кібернетики**

Обговорено та ухвалено
на засіданні кафедри економічної кібернетики
Протокол №_1_ від «_27_»_серпня_2021 р.
Завідувач кафедри економічної кібернетики



Н.К. Максишко

Ухвалено науково-методичною радою
економічного факультету
Протокол №_1_ від «_30_» серпня 2021 р.
Голова науково-методичної ради
економічного факультету



І.І. Колобердянко

Погоджено
з навчально-методичним відділом



(підпис)

О.В. Шимчук

(ініціали, прізвище)

2021 рік

1. Опис навчальної дисципліни

1	2	3	
Галузь знань, спеціальність, освітня програма рівень вищої освіти	Нормативні показники для планування і розподілу дисципліни на змістові модулі	Характеристика навчальної дисципліни	
		очна (денна) форма здобуття освіти	заочна (дистанційна) форма здобуття освіти
Галузь знань	Кількість кредитів – 3	Вибіркова для ВНЗ	
		Цикл дисциплін	
Спеціальність	Загальна кількість годин – 90	Семестр:	
		4-й	
Освітньо-професійна програма	Змістових модулів – 4	Лекції	
		32 год.	
		Лабораторні	
		0 год.	
Рівень вищої освіти: бакалаврський	Кількість поточних контрольних заходів – 17	Самостійна робота	
		58 год.	
		Вид підсумкового семестрового контролю: залік	

2. Мета та завдання навчальної дисципліни

«*Основи інформаційних безпеки*» - викладення основ методів захисту інформаційних систем різного рівня від атак на інформацію, правилами організації систем захисту, сучасним законодавством в області захисту інформації.

Метою викладання навчальної дисципліни «*Основи інформаційних безпеки*» є ознайомлення з сучасними методами захисту інформації, засвоєння теоретичних знань і набуття практичних навичок з питань побудови ефективних інформаційних систем, моделей безпеки інформації, організації ефективного захисту інформації сучасними методами. Курс спрямований на формування знань та вмінь для реалізації аналітичної, проектної та організаційної функцій щодо захисту інформації в сучасних інформаційних системах різного рівня.

Об'єктом вивчення дисципліни є інформаційні системи, бази даних, інші сховища інформації, системи передачі інформації.

Предметом курсу є основні теоретичні результати і методи захисту інформації, їх застосування до побудови захищених інформаційних систем, та захисту інформації, що передається по каналам зв'язку.

Основними **завданнями** дисципліни «*Основи безпеки інформаційних систем*» є

- 1) ознайомити з основними системами і методами захисту інформації, з історією розвитку систем захисту інформації;
- 2) надати володіння методологією та методикою побудови ефективного захисту інформації;

- 3) розширити та поглибити теоретичні знання студентів з безпекових властивостей інформаційних систем;
- 4) вивчити типові моделі безпеки та отримати навички практичної роботи з даними, що використовуються в практиці;
- 5) навчити студентів використовувати методи захисту при створенні сучасних інформаційних систем.

У результаті вивчення навчальної дисципліни студент повинен набути таких результатів навчання (знання, уміння тощо) та компетентностей:

Заплановані робочою програмою результати навчання та компетентності	Методи і контрольні заходи
1	2
ЗК-01. Здатність до абстрактного мислення, аналізу та синтезу ЗК-03 Здатність до креативного та критичного мислення, до адаптації та дії в нових ситуаціях, до прийняття обґрунтованих рішень СК-04 Здатність застосовувати економіко-математичні методи та моделі для вирішення економічних задач та комп'ютерні технології обробки даних для вирішення економічних завдань, здійснення аналізу інформації та підготовки аналітичних звітів СК06. Навички використання сучасних джерел економічної, соціальної, управлінської, облікової інформації для складання службових документів та аналітичних звітів. СК-07 Здатність використовувати аналітичний та методичний інструментарій для обґрунтування економічних рішень. СК-10. Здатність до використання економіко-математичних методів для аналізу економічного об'єкта за допомогою надбаних знань та відповідних спеціальних методів.	Репродуктивні методи (лекція, пояснення, робота з методичними матеріалами). Наочні методи (схеми, моделі, алгоритми). Дискусійні методи.
РНЗн-02 Знання фундаментальних основ економіки та підприємництва в обсязі, що необхідний для володіння категоріальним апаратом професійної галузі знань, здатність використовувати методи досліджень в обраній професії. РНЗн-03 Знання основ застосування елементів теоретичного та експериментального дослідження в професійній діяльності, основ інформатики й сучасних інформаційних технологій, основ системного аналізу та управління підприємствами (установами), методів обробки економічної інформації в різних сферах економічної діяльності. РНЗЗ-02. Володіти навичками впровадження інформаційних систем і технологій; застосувати системний підхід та методи системного аналізу при створенні інформаційних систем, виявляти і враховувати тенденції глобального розвитку, середовищі фактори прямого і непрямого впливу на економічну діяльність господарюючих суб'єктів України. РНЗЗ-03. Використовувати сучасні інформаційні та комунікаційні технології, програмні пакети загального і спеціального призначення РНЗЗ-08. Використовувати програмні засоби і навички роботи в комп'ютерних мережах, уміння створювати бази даних і використовувати інтернет-ресурси.	Методи контролю і самоконтролю: усний, письмовий. – теоретичне тестування за кожним розділом; – залік.

Міждисциплінарні зв'язки. Викладанню курсу передують вивчення дисциплін «Вища математика», «Теорія ймовірностей і математична статистика», «Інформатика», «Елементи криптографії та захисту інформації».

Після вивчення курсу «Математичні основи економіки» студент повинен володіти системою знань про: основні поняття теорії чисел, методи лінійної алгебри, проблеми трудомісткості обчислень.

Після вивчення курсу «Теорія ймовірностей і математична статистика» студент повинен володіти такими поняттями як «дискретна випадкова величина», «частота випадкової величини». Студент повинен вміти генерувати випадкові та псевдовипадкові послідовності, виявляти закономірності окремого випадкового явища, прогнозування його характеристик, застосовувати для розв'язання криптографічних задач відповідні статистичні методи та проаналізувати результати їх застосування.

Після вивчення курсу «Інформатика» студент повинен володіти системою знань про організацію обчислювальних процесів на персональних комп'ютерах та їх алгоритмізацію, програмне забезпечення персональних комп'ютерів і комп'ютерних мереж, вміти працювати з основними видами функцій а також з масивами даних у програмному забезпеченні Microsoft Excel та спеціальному програмному забезпеченні.

Після вивчення курсу «Елементи криптографії та захисту інформації» студент повинен теоретичними основами сучасних криптографічних систем, знати основні стандарти і алгоритми шифрування, вміти використовувати електронний цифровий підпис.

Набуті студентами знання та навички з дисципліни «*Основи безпеки інформаційних систем*» будуть необхідні їм при виконанні аналітичних досліджень під час написання курсових робіт, кваліфікаційної роботи магістра, а також у подальшій професійній діяльності.

3. Програма навчальної дисципліни

Змістовий модуль 1. Основні поняття. Класифікація погроз ІС.

Предмет курсу «Основи безпеки інформаційних систем». Класифікація погроз інформації. Історія побудови платіжних систем. Історія створення системи електронних платежів НБУ Сучасні платіжні системи. Погрози інформації на локальному робочому місці

Змістовий модуль 2. Основні види атак на інформацію.

Віддалене проникнення(remote penetration). Локальне проникнення (local penetration) Відділена відмова в обслуговуванні (remote denial of service) Локальна відмова в обслуговуванні (local denial of service) Мережеві сканери (network scanners) Сканери вразливостей (vulnerability scanners). Зломики паролів (password crackers). Аналізатори протоколів (sniffers)

Змістовий модуль 3. Методи захисту інформації в ІС.

Ідентифікація та аудентифікація користувачів. Ведення протоколів роботи ІС. Розподіл повноважень. Контроль цілісності. Шифрування інформації. Резервне копіювання. Політика безпеки. Моделі політики безпеки. Модель Бела-Лападулла.

Змістовий модуль 4. Криптографічний захист інформації

Кодування інформації в ІС. Коди, що захищають від помилок. Шифрування бінарних даних. Сучасні алгоритми шифрування. Проблеми, пов'язані з шифруванням інформації.

4. Структура навчальної дисципліни

Змістовий модуль	Усього годин	Аудиторні (контактні) години					Самостійна робота, год		Система накопичення балів		
		Усього годин	Лекційні заняття, год		Семінарські/ Практичні /Лабораторні 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.	о/д ф.	з/дист ф.			
1	2	3	4	5	6	7	8	9	10	11	12
1	15	6	8	-	2	-	5	-	4	6	10
2	15	5	8	-	2	-	5	-	14	6	20
3	15	6	8	-	2	-	5	-	4	6	10
4	15	10	8	-	2	-	5	-	10	10	20
Усього за змістові модулі	60										60
Підсумковий семестровий контроль екзамен	30						30	30			40
Загалом	90								100		

5. Темі лекційних занять

№ змістового модуля	Назва теми	Кількість годин	
		о/д ф.	з/дист ф.
1	2	3	4
1	Предмет курсу «Основи безпеки інформаційних систем». Класифікація погроз інформації. Історія побудови платіжних систем.	4	
1	Історія створення системи електронних платежів НБУ Сучасні платіжні системи. Погрози інформації на локальному робочому місці	4	
2	Віддалене проникнення(remote penetration). Локальне проникнення (local penetration) Відділена відмова в обслуговуванні (remote denial of service) Локальна відмова в обслуговуванні (local denial of service)	4	
2	Мережеві сканери (network scanners) Сканери вразливостей (vulnerability scanners). Зломщики паролів (password crackers). Аналізатори протоколів (sniffers)	4	
3	Ідентифікація та аутентифікація користувачів. Ведення протоколів роботи ІС. Розподіл повноважень. Контроль цілісності. Шифрування інформації. Резервне копіювання.	4	
3	Політика безпеки. Моделі політики безпеки. Модель Бела-Лападулла.	4	
4	Кодування інформації в ІС. Коди, що захищають від помилок. Шифрування бінарних даних.	4	
4	Сучасні алгоритми шифрування. Проблеми, пов'язані з шифруванням інформації.	4	
Разом		32	...

6. Теми лабораторних занять

№ змістового модуля	Назва теми	Кількість годин	
		о/д ф.	з/дист ф.
1	2	3	4
1	Класифікація погроз інформації. Погрози інформації на локальному робочому місці	4	...
2	Захист інформації в офісних системах. Політики безпеки в ОС Windows.	4	
3	Розробка модуля входу в системі MS ACCESS.	4	
4	Кодування інформації. Криптографічний захист інформації.	4	
Разом		16	...

7. Види і зміст поточних контрольних заходів

№ змістового модуля	Вид поточного контрольного заходу	Зміст поточного контрольного заходу	Критерії оцінювання*	Усього балів
1	2	3	4	
1	Усне опитування	Теоретичні питання з навчального матеріалу за ЗМ 1 (розділ 3 Робочої програми)	Теоретичні знання студента оцінюються в 2 бали, викладач задає два теоретичних питання (правильна відповідь на одне питання- 1 бал)	4
	Практичне завдання	Лабораторна робота 1	Практичне навички студента оцінюються так: 0 балів -завдання не виконано; 1 бал - практичне завдання виконано частково з помилками; 2-3 бали - практичне завдання виконано з помилками; 4-5 балів - практичне завдання виконано з незначними помилками, немає звіту; 6 балів - практичне завдання виконано без помилок представлено звіт	6
Усього за ЗМ 1 контр. заходів	2			10
2	Усне опитування	Теоретичні питання з навчального матеріалу за ЗМ 2 (розділ 3 Робочої програми)	Теоретичні знання студента оцінюються в 2 бали, викладач задає два теоретичних питання (правильна відповідь на одне питання- 1 бал)	4
	Практичне завдання	Лабораторна робота 2	Практичне навички студента оцінюються так: 0 балів -завдання не виконано; 1 бал - практичне завдання виконано частково з помилками; 2-3 бали - практичне завдання виконано з помилками; 4-5 балів - практичне завдання виконано з незначними помилками, немає звіту; 6 балів - практичне завдання виконано без помилок представлено звіт	6
	Тестування Атестація 1	Тестування за ЗМ 1-2 (розділ 3 Робочої програми) дозволяє перевірити теоретичні знання	Тестове завдання складається з 10 тестових питань. За правильну відповідь на одне питання студент отримує 1 бал.	10

		студента та проводиться в СЕЗН MOODLE.		
Усього за ЗМ 2 контр. заходів	3			20
3	Усне опитування	Теоретичні питання з навчального матеріалу за ЗМ 3 (розділ 3 Робочої програми)	Теоретичні знання студента оцінюються в 2 бали, викладач задає два теоретичних питання (правильна відповідь на одне питання- 1 бал)	4
	Практичне завдання	Лабораторна робота 3	Практичне навички студента оцінюються так: 0 балів -завдання не виконано; 1 бал - практичне завдання виконано частково з помилками; 2-3 бали - практичне завдання виконано з помилками; 4-5 балів - практичне завдання виконано з незначними помилками, немає звіту; 6 балів - практичне завдання виконано без помилок представлено звіт	6
Усього за ЗМ 3 контр. заходів	2			10
4	Практичне завдання	Лабораторна робота 4	Практичне навички студента оцінюються так: 0 балів -завдання не виконано; 1 2 бали - практичне завдання виконано частково з помилками; 3-4 бали - практичне завдання виконано з помилками; 5-6 бали - практичне завдання виконано з незначними помилками, немає звіту; 7-9 бали - практичне завдання виконано з незначними помилками, представлено звіт; 10 бали - практичне завдання виконано без помилок представлено звіт.	10
	Тестування Атестація 2	Тестування за ЗМ 3-4 (розділ 3 Робочої програми) дозволяє перевірити теоретичні знання студента та проводиться в СЕЗН MOODLE.	Тестове завдання складається з 10 тестових питань. За правильну відповідь на одне питання студент отримує 1 бал.	10
Усього за ЗМ 4 контр. заходів	2			30

Усього за змістові модулі контр. заходів	9			60
---	---	--	--	----

* Критерії оцінювання, система накопичення балів <https://moodle.znu.edu.ua/course/view.php?id=3632>

8. Підсумковий семестровий контроль

Форма	Види підсумкових контрольних заходів	Зміст підсумкового контрольного заходу	Критерії оцінювання	Усього балів
1	2	3	4	5
Залік				
	Тестування	Тестування за темами курсу (розділ 3 Робочої програми) дозволяє перевірити теоретичні знання студента та проводиться в CE3H MOODLE.	Тестове завдання складається з 10 тестових питань. Тестове питання містить 4 відповіді, одна з яких є правильною. За правильну відповідь на одне питання студент отримує 2 бали.	20
	Практичне завдання	Розв'язок типової задачі, які було розглянуто на лабораторних заняттях	Результат розв'язку студентом задачі оцінюється за такою шкалою: <u>10 балів</u> : студент правильно розв'язав задачу; - <u>9-8 балів</u> : студент розв'язав задачу з помилками, але зрозуміло, що він знає алгоритм розв'язку задачі; - <u>7-6 балів</u> : студент розв'язав задачу з помилками, з яких зрозуміло, що він частково знає алгоритм розв'язку задачі; - <u>5-4 бали</u> : студент правильно вписав формулу, за якою можна розв'язати задачу та зробив спробу її розв'язання, наприклад виконав значні допоміжні розрахунки; - <u>3-2 бали</u> : студент правильно вписав формулу, за якою можна розв'язати задачу та намагався зробити допоміжні розрахунки; - <u>1 бал</u> : студент правильно вписав формулу, за якою можна розв'язати задачу; - <u>0 балів</u> : студент не розв'язав задачу.	20
Усього за підсумковий семестровий контроль				40

9. Рекомендована література

Основна:

1. Гришук Р.В. Основи кібернетичної безпеки: Монографія / Р.В. Гришук, Ю.Г. Даник; за заг. ред. Ю.Г. Данника. – Житомир: ЖНАЕУ, 2016. – 636 с. Допоміжна література
2. Остапов С. Е. Технології захисту інформації / С. Е. Остапов, С. П. Євсєєв, О. Г. Король. – Чернівці : Видавничий дім "РОДОВІД", 2014. – 428 с.
3. Корченко А. О. Банківська безпека. / А. О. Корченко, Л. М. Скачек, В. О. Хорошко. – К. : ПВП «Задруга». – 2014. – 185 с.

Додаткова:

1. Комп'ютерна злочинність і інформаційна безпека / А. П. Леонов ; за заг. ред. А. П. Леонова. - Мінськ : АРІЛ, 2000. - 552 с.
2. Системы поддержки принятия решений: учебное пособие / Уринцов А. И, Дик В. В - М. : МЭСИ, 2008. – 230 с.
3. Галатенко В.А. Основы информационной безопасности. М.: Изд-во ИНТУИТ.ру, 2005. - 208 с
4. Задірака В. К., Олексюк О. С. Методи захисту фінансової інформації. Київ: Вища школа, 2009. 460 с.
5. Закон України «Про державну таємницю». URL: <https://zakon.rada.gov.ua/laws/show/3855-12>.
6. Закон України «Про захист інформації в автоматизованих системах». URL: <https://zakon.rada.gov.ua/laws/show/2594-15>.
7. Закон України «Про інформацію». URL: <https://zakon.rada.gov.ua/laws/show/2657-12>.
8. Закон України «Про науково-технічну інформацію». URL: <https://zakon.rada.gov.ua/laws/show/848-19>.
9. ДСТУ 3396.2–97. Захист інформації. Технічний захист інформації. Терміни і визначення. Київ: Держстандарт України, 1998.
10. Andress, J. The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. — Syngress, 2014. — 240 p. — ISBN 9780128008126.
11. Stewart, James Michael. CISSP® : Certified Information Systems Security Professional Study Guide : [англ.] / James Michael Stewart, Mike Chapple, Darril Gibson. — Seventh Edition. — Canada : John Wiley & Sons, Inc., 2015. — 1023 p. — ISBN 978-1-119-04271-6.
12. Moore, Robert. Cybercrime : Investigating High Technology Computer Crime : [англ.]. — 2nd ed. — Boston : Anderson Publ., 2011. — 318 p. — ISBN 9781437755824.
13. Phishing attacks and countermeasures / Ramzan, Zulfikar // Handbook of Information and Communication Security : [англ.] / Peter Stavroulakis, Mark Stamp. — L. : Springer Science & Business Media, 2010. — 867 p. — ISBN 978-3-642-04117-4.
14. Johnson, John. The Evolution of British Sigint : 1653–1939 : [англ.]. — Her Majesty's Stationary Office, 1998. — 58 p.
15. Щербаков А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. Москва: Книжный мир, 2009. 352 с.
16. Кузнецов О. О., Євсєєв С. П., Король О. Г. Захист інформації в інформаційних системах. Методи традиційної криптографії. Харків : Вид. ХНЕУ, 2010. 316 с.
17. Остапов С. Е., Євсєєв С. П., Король О. Г. Технології захисту інформації. Чернівці: Видавничий дом «Родовід», 2014. 428 с.
18. Столлингс Вильям. Криптография и защита сетей: принципы и практика. 2-е изд. Москва: Издательский дом «Вильямс», 2008. 672 с.

19. Поповский В. В., Персиков А. В. Защита информации в телекоммуникационных системах: учебн.: в 2 т. Харьков: ООО «Компания СМІТ», 2006. Т. 1. 292 с.
20. Вербицький О. В. Вступ до криптології. Львів: Наук.-техн. літ., 1998. 248 с.
21. Родичев Ю. Информационная безопасность: Нормативно-правовые аспекты. Санкт-Петербург: Питер, 2008. 272 с.
22. Бабаш А. В., Шанкин Г. П. История криптографии. Часть I. Москва: Гелиос АРВ, 2002.
23. Петров А. А. Компьютерная безопасность. Криптографические методы защиты. Москва: ДМК, 2000. 448 с.
24. Гайкович В., Першин А. Безопасность электронных банковских систем. Москва: Единая Европа, 1994.

Інформаційні джерела:

1. Виды и классификация атак на информационные системы <https://igorosa.com/vidy-i-klassifikaciya-atak-na-informacionnye-sistemy/>
2. ISO/IEC 15408-1:2009 – Information technology – Security techniques – Evaluation criteria for IT security – Part1: Introduction and general model. management [Електронний ресурс]. – Режим доступа к ресурсу: http://www.iso.org/iso/catalogue_detail.htm?csnumber=50341 1 6
3. ISO/IEC 15408-2:2008 – Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements. [Електронний ресурс]. – Режим доступа к ресурсу: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=46414
4. ISO/IEC 15408-3:2008 – Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements. [Електронний ресурс]. – Режим доступа к ресурсу: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=46413
5. ДСТУ ISO/IEC TR 13335-1:2003 Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 1. Концепції та моделі безпеки інформаційних технологій. [Електронний ресурс]. – Режим доступа к ресурсу: <http://lindex.net.ua/ua/shop/bibl/500/doc/11423>
6. ДСТУ ISO/IEC TR 13335-2:2003 Інформаційні технології. Частина 2. Настанови з керування безпекою інформаційних технологій. [Електронний ресурс]. – Режим доступа к ресурсу: <http://www.premier-hs.com.ua/ru/content/dstu-isoiec-tr-13335-22003-nastanoviz-kieruvannia-biezpiekoiu-informatsiinih-tiekhnologii>
7. ДСТУ ISO/IEC TR 13335-3:2003 Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 3. Методи керування захистом інформаційних технологій. [Електронний ресурс]. – Режим доступа к ресурсу: <http://lindex.net.ua/ua/shop/bibl/500/doc/11425>
8. ДСТУ ISO/IEC TR 13335-4:2005 Інформаційні технології. Настанови з управління безпекою інформаційних технологій. Частина 4. Вибір засобів захисту. [Електронний ресурс]. – Режим доступа к ресурсу: <http://metrology.com.ua/download/iso-iec-ohsas-i-dr/61-iso/290-dstu-iso-iec-tr13335-4-2005>.
9. ДСТУ ISO/IEC TR 13335-5:2005 Інформаційні технології. Настанови з управління безпекою інформаційних технологій. Частина 5. Настанова з управління мережною безпекою. [Електронний ресурс]. – Режим доступа к ресурсу: <http://lindex.net.ua/ua/shop/bibl/500/doc/11427>. 16. ISO/IEC 27001:2013
10. Information technology – Security techniques – Information security management systems – Requirements. [Електронний ресурс]. – Режим доступа к ресурсу: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534.

11. ISO/IEC 27002:2013 – Information technology -- Security techniques – Code of practice for information security controls. [Електронний ресурс]. – Режим доступа к ресурсу: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54533
12. ISO/IEC 27006:2015 – Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems [Електронний ресурс]. – Режим доступа к ресурсу: <http://www.iso.org/iso/home/search.htm?qt=ISO%2FIEC+27006%3A2015+&sort=rel&type=simple&published=on>.
13. Стандарт України СОУ Н НБУ 65.1 СУІБ 1.0:2010. Методи захисту в банківській діяльності. Система управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2005, MOD). [Електронний ресурс]. – Режим доступа к ресурсу: <https://kyianyn.files.wordpress.com/2010/12/nbu-27001.pdf>
14. Стандарт України СОУ Н НБУ 65.1 СУІБ 1.0:2010. Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою (ISO/IEC 27002:2005, MOD) [Електронний ресурс]. – Режим доступа к ресурсу: <http://s-byte.com/useful/27002.pdf>
15. Безпека інформаційних систем [Електронний ресурс]. – Режим доступа к ресурсу: <https://naurok.com.ua/test/bezpeka-informaciynih-sistem-219481.html>
16. Методи захисту інформації: види загроз і засоби захисту, класи безпеки [Електронний ресурс]. – Режим доступа к ресурсу: <http://guverina.org.ua/news/uk/bezopasnost-metodi-zahistu-informacii-vidi-zagrozi-zasobi-zahistu-klasi-bezpeki/>
17. Європейські стандарти захисту інформації в Україні [Електронний ресурс]. – Режим доступа к ресурсу: <https://nt.ua/blog/isms>
18. Про засади інформаційної безпеки України: проект Закону № 4949 від 28.05.2014 р. [Електронний ресурс]. – Режим доступа к ресурсу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=51123.