МІНІСТРЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
ВСП «РІВНЕНСЬКИЙ ФАХОВИЙ КОЛЕДЖ НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ»

Відділення інформаційних технологій
Циклова комісія програмування та інформаційних дисциплін

ЗАТВЕРДЖУЮ
Завідувач навчально-виробничої практики
_____ Тарас САСОВСЬКИЙ
01 вересня 2025 р.

ПРОГРАМА ПРАКТИКИ

НАВЧАЛЬНА ПРАКТИКА
(вид практики)

ОРГАНІЗАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ
(назва практики)

галузь знань *12 Інформаційні технології*
(шифр і назва галузі знань)

спеціальність *125 Кібербезпека та захист інформації*
(шифр і назва спеціальності)

освітня програма *Кібербезпека та захист інформації*
(назва освітньої програми)

Рівне – 2025 рік

Програму практики розроблено на основі освітньо-професійної програми «Кібербезпека та захист інформації», затвердженої Вченою радою НУБіП України, протокол № 10 від 26 квітня 2023 року.

Розробник: *Новак Юрій Петрович, викладач програмування та інформаційних дисциплін, спеціаліст вищої категорії, викладач методист*
Павловський Тарас Мирославович, викладач програмування та інформаційних дисциплін, спеціаліст.
(вказати авторів, їхні посади, кваліфікаційні категорії)

Програму практики розглянуто та схвалено на засіданні циклової комісії *програмування та інформаційних дисциплін*

Протокол від *29 серпня* 2025 року № *1*
Голова циклової комісії *програмування та інформаційних дисциплін*

« 29 » серпня 2025 року _____ *Павло СТРИК*
(підпис) (ім'я та прізвище)

Погоджено методичною радою ВСП «РФК НУБіП України»
Протокол від *29 серпня* 2025 року № *1*

«29» *серпня* 2025 року Голова _____ Людмила БАЛДИЧ
(підпис) (ім'я та прізвище)

1. ОПИС НАВЧАЛЬНОЇ ПРАКТИКИ

Галузь знань, спеціальність, освітній ступінь	
Освітній ступінь	Фаховий молодший бакалавр
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека та захист інформації
Характеристика навчальної практики	
Вид	**Обов'язкова**
Загальна кількість годин	135
Кількість кредитів ECTS	4,5
Кількість змістових модулів	1
Мова викладання	Українська
Форма підсумкового контролю	Залік з практики
Показники навчальної практики для денної та заочної форм навчання	
Форма навчання	денна форма навчання
Рік підготовки	2025-2026
Семестр	6
Аудиторні години	54
Самостійна робота, год	81

2. МЕТА ТА ЗАВДАННЯ ПРАКТИКИ

Предметом вивчення навчальної практики з дисципліни «Організаційне забезпечення захисту інформації» є застосування методів впровадження та керування заходами з організації захисту інформації, розроблення політики безпеки, оцінка ризиків та забезпечення відповідності стандартам і вимогам інформаційної безпеки на підприємствах різних галузей, впровадження системи захисту, мінімізація інформаційних ризиків.

Міждисциплінарні зв'язки: «Ризики інформаційної безпеки», «Методи та засоби захисту інформації» та «Операційні системи».

Метою навчальної практики з дисципліни «Організаційне забезпечення захисту інформації» є формування у студентів знань, навичок та компетенцій, необхідних для організації та управління процесами захисту інформації на підприємствах і в установах.

Основними **завданнями** навчальної практики з дисципліни «Організаційне забезпечення захисту інформації» є виконання індивідуального завдання з впровадження методів захисту інформації на підприємстві, використовуючи отримані знання з навчального курсу. Виконується постановка та реалізація задач, які виконує база, формується електронний та паперовий звіт проходження навчальної практики.

Як результат вивчення навчальної дисципліни здобувач освіти повинен **уміти:**

- здійснювати аналіз і оцінку основних загроз інформаційної безпеки для заданого об'єкта;
- виконувати розрахунок потенційних збитків від протиправного розкриття інформації;
- розробляти структуру служби безпеки інформації;
- розробляти алгоритми підбору, розстановки та навчання кадрів;
- розробляти план організації режиму таємності;
- здійснювати оцінку існуючої системи пропускного та внутрішньо об'єктового режиму;
- здійснювати аналіз ризиків, пов'язаних із захистом інформації під час аварій та екстремальних ситуацій.

Сформовані компетентності та очікувані результати навчання:

Після проходження практики «Придбання робітничої професії» у здобувачів освіти формуються такі **компетентності:**

Загальні (ЗК):

— Здатність застосовувати знання у практичних ситуаціях.

— Здатність здійснювати пошук, оброблення та аналіз інформації.

Фахові (ФК):

- Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.
- Здатність виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

Результати навчання (РН):

Після проходження практики «Придбання робітничої професії» здобувачі освіти повинні:

РН05. Вміти використовувати сучасні програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.

РН13. Вміти вирішувати задачі щодо управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).

РН20. Вміти вирішувати задачі аналізу програмного коду на наявність можливих загроз.

3. ЗМІСТ НАВЧАЛЬНОЇ ПРАКТИКИ

3.1. Організаційна частина. Мета та завдання навчальної практики

Вступ. Ознайомлення з робочою програмою практики. Інструктаж з техніки безпеки згідно з вимогами охорони праці. Підготовка робочого місця та обладнання. Вибір індивідуального завдання.

3.2. Поглиблене вивчення і здобуття компетенцій для організації та управління процесами захисту інформації

3.2.1. Дослідження особливостей підприємства за індивідуальним завданням

Аналіз і оцінка основних загроз інформаційної безпеки для заданого об'єкта. Розрахунок потенційних збитків від протиправного розкриття інформації. Оцінка існуючої системи пропускного та внутрішньо об'єктового режиму.

3.2.2. Розробка заходів з підвищення інформаційної безпеки на підприємстві

Розробка структури служби безпеки інформації. Розробка алгоритму підбору, розстановки та навчання робітничих кадрів. Розробка плану організації режиму таємності. Аналіз ризиків, пов'язаних із захистом інформації під час аварій та екстремальних ситуацій. Розробка механізму дій у екстремальних ситуаціях.

3.3. Захист звітів

Опис результатів виконаних робіт. Демонстрація плану організації захисту інформації на підприємстві та оформленого друкованого звіту згідно діючих інструкцій та вимог.

4. ТЕМАТИЧНИЙ ПЛАН

№	*Назви тем практики*	Кількість годин навчання					
		денна форма			заочна форма		
		всього	аудиторні	самостійне вивчення	всього	аудиторні	самостійне вивчення
Змістовий модуль 1. ОРГАНІЗАЦІЙНА ЧАСТИНА. МЕТА ТА ЗАВДАННЯ НАВЧАЛЬНОЇ ПРАКТИКИ							
Тема 1	Техніка безпеки. Мета та завдання навчальної практики.	5	2	3			
Разом за змістовим модулем 1		**5**	**2**	**3**			
Змістовий модуль 2. ПОГЛИБЛЕНЕ ВИВЧЕННЯ І ЗДОБУТТЯ КОМПЕТЕНЦІЙ ДЛЯ ОРГАНІЗАЦІЇ ТА УПРАВЛІННЯ ПРОЦЕСАМИ ЗАХИСТУ ІНФОРМАЦІЇ							
Тема 2	Дослідження особливостей підприємства за індивідуальним завданням.	52	22	30			
Тема 3	Розробка заходів з підвищення інформаційної безпеки на підприємстві	67	28	39			
Разом за змістовим модулем 2		**119**	**50**	**69**			
Змістовий модуль 3. ЗАХИСТ ЗВІТІВ							
Тема 4	Захист звітів.	11	2	9			
Разом за змістовим модулем 3		**11**	**2**	**9**			
Всього годин		**135**	**54**	**81**			

5. КАЛЕНДАРНО-ТЕМАТИЧНИЙ ПЛАН НАВЧАЛЬНОЇ ПРАКТИКИ

№ заняття	Тижні		Назва розділу, теми і зміст практики	К-сть год.		Місце та об'єкт проведення	Інструменти, матеріали, та обладнання	Організація форми робіт	Завдання на самостійне опрацювання	Примітка
	№	Дата		всього	аудиторних					
1.	1		**Організаційна частина. Вступ.** Ознайомлення з робочою програмою практики. Інструктаж з техніки безпеки. Підготовка робочого місця. Вибір індивідуального завдання.	5	2	ТзОВ «МВКОМ»	мультимедійний проектор, комп'ютери та програмне забезпечення	індивідуальна	оформити звіт-щоденник практики	
2	1		**Дослідження особливостей підприємства.** Аналіз і оцінка основних загроз інформаційної безпеки для заданого об'єкта. Розрахунок потенційних збитків від розкриття інформації.	10	4	ТзОВ «МВКОМ»	мультимедійний проектор, комп'ютери та програмне забезпечення	індивідуальна	оформити звіт-щоденник практики	
3	1		**Аналіз існуючої системи захисту.** Оцінка пропускного та внутрішньооб'єктового режиму. Виявлення недоліків у поточній системі безпеки.	10	4	ТзОВ «МВКОМ»	мультимедійний проектор, комп'ютери та програмне забезпечення	індивідуальна	оформити звіт-щоденник практики	
4	1		**Розробка заходів з підвищення інформаційної безпеки.** Створення структури служби безпеки інформації.	10	4	ТзОВ «МВКОМ»	мультимедійний проектор, комп'ютери та програмне забезпечення	індивідуальна	оформити звіт-щоденник практики	
5	2		**Алгоритм підбору кадрів.** Розробка механізмів навчання персоналу та оцінки рівня їхньої підготовки у сфері безпеки.	10	4	ТзОВ «МВКОМ»	мультимедійний проектор, комп'ютери та програмне забезпечення	індивідуальна	оформити звіт-щоденник практики	
6	2		**Організація режиму таємності.** Розробка плану обмеження доступу до інформації. Створення політики класифікації даних.	10	4	ТзОВ «МВКОМ»	мультимедійний проектор, комп'ютери та програмне забезпечення	індивідуальна	оформити звіт-щоденник практики	
7	2		**Оцінка ризиків при аваріях та надзвичайних ситуаціях.** Аналіз можливих загроз під час форс-мажорних ситуацій.	9	4	ТзОВ «МВКОМ»	мультимедійний проектор, комп'ютери та програмне забезпечення	індивідуальна	оформити звіт-щоденник практики	
8	2		**Розробка механізмів реагування на інциденти.** Планування заходів у разі загроз безпеці інформації.	9	4	ТзОВ «МВКОМ»	мультимедійний проектор, комп'ютери та програмне забезпечення	індивідуальна	оформити звіт-щоденник практики	

9	3		**Розробка плану заходів для забезпечення безпеки комунікаційних каналів**. Дослідження структури локальної мережі, визначення наявності слабких ділянок.	9	4	ТзОВ «МВКОМ»	мультимедійний проектор, комп'ютери та програмне забезпечення	індивідуальна	оформити звіт-щоденник практики	
10	3		**Захист передавання даних між підрозділами.** Оцінка стану криптографічного захисту інформації.	9	2	ТзОВ «МВКОМ»	мультимедійний проектор, комп'ютери та програмне забезпечення	індивідуальна	оформити звіт-щоденник практики	
11	3		**Створення та впровадження політик безпеки для користувачів.** Розробка стандартів доступу та обмежень. Ідентифікація та аутентифікація користувачів.	9	4	ТзОВ «МВКОМ»	мультимедійний проектор, комп'ютери та програмне забезпечення	індивідуальна	оформити звіт-щоденник практики	
12	3		**Тестування безпеки системи.** Перевірка ефективності впроваджених заходів захисту інформації.	9	4	ТзОВ «МВКОМ»	мультимедійний проектор, комп'ютери та програмне забезпечення	індивідуальна	оформити звіт-щоденник практики	
13	3		**Розробка звіту щодо впроваджених заходів.** Опис запропонованих рішень для покращення інформаційної безпеки.	9	2	ТзОВ «МВКОМ»	мультимедійний проектор, комп'ютери та програмне забезпечення	індивідуальна	оформити звіт-щоденник практики	
14	3		**Створення базових правил для користувачів щодо безпечної роботи з інформацією.** Розробка інструкції для служби безпеки інформації.	9	4	ТзОВ «МВКОМ»	мультимедійний проектор, комп'ютери та програмне забезпечення	індивідуальна	оформити звіт-щоденник практики	
15	3		**Захист звітів.** Презентація результатів практики. Оцінка роботи студентів.	11	2	ТзОВ «МВКОМ»	мультимедійний проектор, комп'ютери та програмне забезпечення	індивідуальна	оформити звіт-щоденник практики	
Всього				**135**	**54**					

6. ІНДИВІДУАЛЬНІ ЗАВДАННЯ СТУДЕНТАМ

№ п/п	Вид завдання: виготовлення таблиць, плакатів, схем, рефератів; звіти про практику тощо.	Виконання завдання		Видача завдання	
		№ тижня	дата	№ тижня	дата
1	Розробка плану організації захисту інформації на автостанції	3		1	
2	Розробка плану організації захисту інформації в Управлінні праці та соціального захисту населення.	3		1	
3	Розробка плану організації захисту інформації на підприємстві у Міській раді	3		1	
4	Розробка плану організації захисту інформації у відділі поліції	3		1	
5	Розробка плану організації захисту інформації у банку	3		1	
6	Розробка плану організації захисту інформації у страховій компанії	3		1	
7	Розробка плану організації захисту інформації для державного архіву	3		1	
8	Розробка плану організації захисту інформації у нотаріальній конторі	3		1	
9	Розробка плану організації захисту інформації у суді	3		1	
10	Розробка плану організації захисту інформації в коледжі	3		1	
11	Розробка плану організації захисту інформації у школі	3		1	
12	Розробка плану організації захисту інформації у військовій частині	3		1	
13	Розробка плану організації захисту інформації у телекомунікаційній компанії	3		1	
14	Розробка плану організації захисту інформації у центрі зайнятості	3		1	
15	Розробка плану організації захисту інформації на підприємстві «Обленерго»	3		1	
16	Розробка плану організації захисту інформації у лабораторії медичних досліджень	3		1	
17	Розробка плану організації захисту інформації у центрі екстреної медичної допомоги	3		1	
18	Розробка плану організації захисту інформації у транспортній компанії	3		1	
19	Розробка плану організації захисту інформації у готелі	3		1	
20	Розробка плану організації захисту інформації у видавництві	3		1	
21	Розробка плану організації захисту інформації у рекламному агентстві	3		1	
22	Розробка плану організації захисту інформації у фармацевтичній компанії	3		1	
23	Розробка плану організації захисту інформації у будівельній компанії	3		1	
24	Розробка плану організації захисту інформації у логістичній компанії	3		1	
25	Розробка плану організації захисту інформації у волонтерській організації	3		1	

26	Розробка плану організації захисту інформації у страховій агенції	3		1	
27	Розробка плану організації захисту інформації у сервісному центрі МВС	3		1	
28	Розробка плану організації захисту інформації у спортивному комплексі	3		1	
29	Розробка плану організації захисту інформації у фермерському господарстві	3		1	
30	Розробка плану організації захисту інформації у сервісному центрі МВС	3		1	

7. ВИМОГИ ДО ЗВІТНОЇ ДОКУМЕНТАЦІЇ

1. Звіт-щоденник з навчальної практики виконується самостійно кожним студентом у відповідності з графіком, який встановлюється викладачем. **Дата написання звіту** ставиться у лівому верхньому кутку над кожною новою темою.
2. Звіт має виконуватися державною (українською) мовою. Викладення повинно бути чітким, без орфографічних і синтаксичних помилок, логічно послідовним.
3. **Робота має бути** надрукована на принтері через ПК з одного боку через 1,5 міжрядкового інтервалу з вирівнювання заголовків по центру, основного тексту – по ширині. Сторінки повинні мати поля: ліве – 20 мм, праве – 10 мм, верхнє – 20 мм, нижнє – 20 мм. Надрукований текст повинен бути чітким, чорного кольору. Щільність тексту – однакова по всій роботі.
4. Першою сторінкою роботи є **титульна сторінка**, яка оформлюється за зразком з додатку А.
5. Далі подається **зміст практики** із зазначенням сторінок. Зміст містить усі заголовки інструкційних карток, які є у роботі, починаючи з першої і закінчуючи висновками. Приблизний зміст наведений у додатку Б.
6. При необхідності у звіті вказується перелік скорочень та умовних позначень.
7. **Заголовки структурних частин звіту** (теми інструкційних карток) друкуються великими літерами. Крапка у кінці заголовка не ставиться. Якщо заголовок складається з двох або більше речень, їх розділяють крапкою. Відстань між заголовком та текстом має дорівнювати 2 інтервалам основного тексту.
8. **Сторінки звіту мають бути пронумеровані** арабськими цифрами (у правому верхньому куті без тире, крапки та знака №). Нумерація має бути наскрізною від титульної до останньої сторінки, включаючи всі ілюстрації та додатки. На титульній сторінці номер не ставиться.
9. Усі **таблиці** з кожної теми, які подаються у звіті, повинні мати номер (наприклад, «Таблиця 1.2» – таблиця з першого розділу другої інструкційної картки) та назву з нового рядка.
10. **Графічні зображення** вставляються у текст звіту та нумеруються з назвою (наприклад, «Рисунок 1.3. Модель «сутність-зв’язок» бази даних «Інвентар» – зображення з першого розділу третьої інструкційної картки).
11. **Висновки** про проходження навчальної практики друкуються у кінці звіту-щоденника.
12. За висновками вказати перелік використаних **літературних джерел**.
13. Якщо є **додатки** до звіту-щоденника, то їх необхідно вставити у кінці. Додатки оформлюються як продовження звіту. Додаток повинен мати заголовок, написаний або надрукований малими літерами з першої великої літери посередині рядка. Справа рядка над заголовком малими літерами з першої великої друкується слово «Додаток» і поряд – велика літера, що позначає його. Додатки слід позначати послідовно великими літерами української абетки, за винятком літер Ґ, Є, І, Ї, Й, О, Ч, Ь, наприклад: Додаток А, Додаток Б і т. д.

8. ФОРМА ПІДСУМКОВОГО КОНТРОЛЮ З ПРАКТИКИ

Контроль знань студентів здійснюється за модульно-рейтинговою системою.

Засобами діагностики та методами демонстрування результатів навчання здобувачів освіти з навчальної практики є:

- індивідуальне опитування;
- презентація змісту практики;
- захист звіту практики;
- залік з практики.

9. КРИТЕРІЇ ОЦІНЮВАННЯ НАВЧАЛЬНОЇ ПРАКТИКИ:

Оцінка «відмінно» виставляється студенту, який своєчасно пройшов усі етапи навчальної практики, під час виконання завдань проявив стійкі системні, глибокі і різнобічні знання, відмінно володіє матеріалом, знає нормативну і законодавчу базу та її застосування за певних умов, дає обґрунтовані, правильні відповіді на питання, доцільно використовує термінологію, усвідомлює взаємозв'язок окремих розділів практики, їхнє значення для майбутньої професії, виявляє творчі здібності у розумінні та використанні навчально-програмного матеріалу, проявляє здатність до самостійного оновлення і поповнення знань. Практичні завдання і задачі вирішує правильно, розрахунки проводить без помилок, отримує достовірні результати, правильно заповнює і складає документи, робить відповідні узагальнення і висновки та охайно оформляє виконані завдання та звіти.

- глибоке, теоретично обґрунтоване розкриття питання; розрахунки, зроблені без помилок, проведено повний аналіз, відображена власна позиція – оцінюються в **48-50 балів**;
- обґрунтоване розкриття питання чи/та розрахунки, зроблені з незначними неточностями, які істотно не впливають на правильність відповіді – **45-47 балів**;

Оцінка «добре» виставляється студенту, який знає вивчений матеріал і добре ним володіє але допускає незначні помилки у формулюванні термінів, категорій, понять, використанні нормативно-правової бази, показує стійкий рівень знань з дисципліни і та професійної діяльності. Під час виконання практичних завдань, вирішення задач, проведення розрахунків допускає незначні помилки, але за допомогою викладача швидко орієнтується і знаходить правильні відповіді, правильно або з незначними помилками заповнює і складає документи, робить відповідні узагальнення і висновки та охайно оформляє виконані завдання та звіти.

- відповідь не дає повного розкриття питання, не проведено повний аналіз результатів розрахунків, немає власної позиції – **42-44 балів**;
- неповне розкриття питання, доведені до завершення розрахунки але не зроблено їх аналіз; загалом наявні достатні знання – **38-41 балів**;

Оцінка «задовільно» виставляється студенту, який посередньо володіє матеріалом, допускав порушення в графіку виконання практики, проте виявив знання основного навчально-програмного матеріалу в обсязі, необхідному для подальшого навчання та наступної роботи за професією, справляється з виконанням завдань, передбачених програмою, дає неправильну відповідь на

окремі питання або на всі питання дає малообґрунтовані, невичерпні відповіді, знання має обмежені, несистемні, слабо орієнтується у нормативно-правових документах. Під час виконання практичних завдань, вирішення задач, проведення розрахунків припускається грубих помилок і тільки за допомогою викладача може виправити допущені помилки, із значними помилками заповнює і складає документи, поверхово робить узагальнення і висновки та не зовсім охайно оформляє виконані завдання та звіти.

- питання розкиває фрагментарно, наявні фактологічні помилки під час викладу чи/та помилки під час проведення розрахунків – **34-37 балів**;
- відповіді неповні, наявні суттєві помилки при викладі та проведенні розрахунків – **30-33 балів**;

Оцінка «незадовільно» виставляється студенту, який не виконав завдання практики у визначений термін, із значними помилками заповнив і склав документи, не зробив узагальнення і висновки та не охайно оформив виконані завдання та звіти, а також не виявив достатніх знань основного навчально-програмного матеріалу, дає відповіді лише на деякі питання або дає неправильні відповіді на питання, може відтворити кілька термінів, не знає термінології дисципліни і основних нормативно-правових документів, не може без допомоги викладача використати знання у подальшому навчанні, не спромігся оволодіти навичками самостійної роботи. Допускає принципові помилки у виконанні передбачених програмою практики завдань, вирішенні задач, проведенні розрахунків припускається грубих помилок і не може їх виправити,

- відповідь має значні помилки елементарного рівня – **1-30 бали**;
- відсутність відповіді на питання – **0 балів**.

Шкала відповідності балів рейтингу заліковим оцінкам відповідно до модульно-рейтингової системи навчання:

45-50 балів – «**відмінно**»;
38-44 балів – «**добре**»;
30-37 балів – «**задовільно**»;
менше 30 балів – «**незадовільно**».

10. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Дубровський, В. М. Захист інформації: організаційні, правові та технічні аспекти. — Київ: Видавництво НТУУ «КПІ», 2020.
2. Наконечний, В. М. Організаційне забезпечення захисту інформації в інформаційних системах. — Львів: Вид-во ЛНУ, 2019.
3. Селезньов, О. В. Основи інформаційної безпеки. — Харків: ХНУРЕ, 2021.
4. Закон України «Про захист інформації в інформаційних системах»
5. Бабенко, О. О. Кризове управління в сфері інформаційної безпеки. — Київ: НТУ «ДП»., 2022.
6. Захист інформації в автоматизованих системах управління : навчальний посібник /Уклад. І. А. Пількевич, Н. М. Лобанчикова, К. В. Молодецька. – Житомир : Вид-во ЖДУ ім. І. Франка, 2015. – 226 с.
7. Комплексні системи захисту інформації : навчальний посібник / [Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В.] – Вінниця : ВНТУ, 2017. – 120 с.
8. Логінова Н. І. Правовий захист інформації : навчальний посібник / Н. І. Логінова, Р. Р. Дробожур. – Одеса : Фенікс, 2015. – 264 с.
9. Остапов С. Е. Технологія захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.
10. Національний центр кібербезпеки України: ncss.gov.ua — інформація про національні стратегії безпеки, звіти та ресурси з кіберзахисту.
11. ISACA: isaca.org — міжнародна організація, що пропонує ресурси, курси та сертифікації в галузі управління ризиками та інформаційної безпеки.
12. Cybersecurity & Infrastructure Security Agency (CISA): cisa.gov — матеріали про кіберзахист, стандарти та рекомендації для організацій.
13. SANS Institute: sans.org — навчальні курси, ресурси та дослідження у сфері інформаційної безпеки.
14. European Union Agency for Cybersecurity (ENISA): enisa.europa.eu — звіти, дослідження та ресурси про безпеку інформаційних систем в Європі.

Додаток А

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ ТА ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
ВІДОКРЕМЛЕНИЙ СТРУКТУРНИЙ ПІДРОЗДІЛ
«РІВНЕНСЬКИЙ ФАХОВИЙ КОЛЕДЖ НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ БІОРЕСУРСІВ ТА ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ»

Відділення інформаційних технологій
Циклова комісія програмування та інформаційних дисциплін

ЗВІТ
з навчальної практики
з дисципліни «Організаційне забезпечення захисту інформації»

Виконав:
студент ІІІ курсу
31-К групи Іваненко І.І

Перевірив:
викладач Іваненко І.І.

Оцінка_____ _____
(підпис викладача)

Рівне – 2025

Додаток Б

ЗМІСТ