Кафедра телекомунікаційних та радіоелектронних систем

УЗГОДЖЕНО
Декан
_____ Сергій ЗАВГОРОДНІЙ
«24» 03 2023 р.

ЗАТВЕРДЖУЮ
Проректор з навчальної роботи
_____ Анатолій ПОЛУХІН
«31» 05 2023 р.

Система менеджменту якості

РОБОЧА ПРОГРАМА
навчальної дисципліни
«Безпека інформаційних мереж та систем»

Освітньо-професійна програма: «Телекомунікаційні системи та мережі»
Галузь знань: 17 «Електроніка та телекомунікації»
Спеціальність: 172 «Телекомунікації та радіотехніка»

Форма навчання	Сем.	Усього (год. / кредитів ECTS)	ЛК Ц	ПР .З	Л.З	СРС	ДЗ / РГР / К.р	КР / КП	Форма сем. контролю
Денна:	2	210 / 7,0	36	—	36	138		КР 2сем	Екз. 2 се
Заочна:	1,2	210 / 7,0	12	—	12	186	К.р. 2 сем	КР 2сем	Екз. 2 с

Індекс: НМ-2-172-1/21-2.1.6
Індекс: НМ-2-172-1з/21-2.1.6

СМЯ НАУ РП 22.06–01–2023

Робочу програму навчальної дисципліни «Безпека інформаційних мереж та систем» розроблено на основі освітньо-професійної програми «Телекомунікаційні системи та мережі», навчальних та робочих навчальних планів РМ-2-172-1/21 та РМ-2-172-1з/21 підготовки здобувачів вищої освіти освітнього ступеня «Магістр» за спеціальністю 172 «Телекомунікації та радіотехніка» та відповідних нормативних документів.

Робочу програму розробив
професор кафедри _____ Георгій КОНАХОВИЧ

Робочу програму обговорено та схвалено на засіданні випускової кафедри освітньо-професійної програми «Телекомунікаційні системи та мережі», спеціальності 172 «Телекомунікації та радіотехніка» – кафедри телекомунікаційних та радіоелектронних систем (випускова),
протокол №17 від « 03 » червня 2022 р.

Гарант освітньо-
професійної програми _____ Георгій КОНАХОВИЧ

Завідувач кафедри _____ Роман ОДАРЧЕНКО

Робочу програму обговорено та схвалено на засіданні науково-методично-редакційної ради факультету аеронавігації, електроніки та телекомунікацій, протокол №____ від «____» _____ 20__ р.

Голова НМРР _____ Олександр КРИВОНОСЕНКО

Рівень документа – 3б
Плановий термін між ревізіями – 1 рік
Врахований примірник

ЗМІСТ

ВСТУП

Робоча програма (РП) навчальної дисципліни «Безпека інформаційних мереж та систем» розроблена на основі «Методичних рекомендацій до розроблення і оформлення робочої програми навчальної дисципліни денної та заочної форм навчання», затверджених наказом ректора від 29.04.2021 № 249/од, та відповідних нормативних документів.

1. ПОЯСНЮВАЛЬНА ЗАПИСКА

1.1. Місце, мета, завдання навчальної дисципліни.

Дана навчальна дисципліна, будучи однією з базових дисциплін циклу професійної та практичної підготовки фахівців спеціальності 172 «Телекомунікації та радіотехніка», є теоретичною основою сукупності знань і вмінь, що формують професійний профіль фахівця в галузі забезпечення безпеки інформаційних мереж та систем (ІМС), з акцентом на принципи побудови і функціонування технологій інформаційної безпеки цих систем. Набуті при вивченні дисципліни знання та вміння дають необхідну базу для отримання освітнього ступеню (Магістр) з телекомунікацій та радіотехніки.

Метою навчальної дисципліни є розкриття методів побудови та принципів дії систем захисту телекомунікаційного та радіотехнічного обладнання безпровідного зв'язку.

Завданнями навчальної дисципліни є:

- оволодіння базовими знаннями з побудови корпоративних ІМС, як систем передавання захищеної інформації в різноманітних мережах;
- дослідження та аналіз загроз безпеці функціонування та захисту інформації в ІМС;
- дослідження методів і алгоритмів захисту периметру корпоративних мереж за допомогою між мережевих екранів ;
- дослідження технологій побудови віртуальних мереж (VPN);
- дослідження принципів захисту мереж на канальному, мережевому та прикладному рівнях, організації захищеного віддаленого доступу, побудови систем антивірусного захисту.

1.2. Результати навчання, які дає можливість досягти навчальна дисципліна.

У результаті вивчення даної навчальної дисципліни студент повинен набути таких результатів навчання (у комплексі з іншими освітніми компонентами):

-здатність застосовувати сучасні технічні та програмні методи забезпечення інформаційної безпеки телекомунікаційних та радіотехнічних систем та мереж (ПРН12);

-здатність використовувати основні терміни та критерії інформаційної безпеки, попереджати ризики та аналізувати їх вплив на соціальну та екологічну безпеку, використовувати зарубіжний досвід та основні тенденції забезпечення інформаційної безпеки інноваційної діяльності. (ПРН16);

1.3. Компетентності, які дає можливість здобути навчальна дисципліна.

У результаті вивчення даної навчальної дисципліни студент повинен набути таких компетентностей (у комплексі з іншими освітніми компонентами):

– Здатність вчитися і бути сучасно освіченим, усвідомлювати можливість навчання упродовж життя. (ЗК5);

– Здатність до пошуку, оброблення та аналізу інформації з різних джерел.(ЗК6)

– володіти сучасними комплексними методами забезпечення інформаційної безпеки телекомунікаційних та радіотехнічних систем. (ФК13);

– володіти організаційними та технічними основами інформаційної безпеки інноваційної діяльності а також інформаційною безпекою проектів і програм (ФК17);

1.4. Міждисциплінарні зв'язки.

Навчальна дисципліна "Безпека інформаційних мереж та систем" базується на знаннях дисциплін: "Захист безпровідних телекомунікаційних та радіотехнічних систем", "Стратегії обслуговування та ремонту авіаційних телекомунікаційних систем " .

Навчальна дисципліна "Безпека інформаційних мереж та систем" є базою для вивчення дисциплін (у комплексі з іншими освітніми компонентами) а також для написання у подальшому кваліфікаційної магістерської роботи.

2. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

2.1. Зміст навчальної дисципліни

Навчальний матеріал дисципліни структурований за модульним принципом і складається з двох навчального модулів, а саме: навчального **модуля № 1 «Дослідження особливостей побудови та загроз безпеки ІМС» модуля №2 Аналіз методів організації захисту інформації в ІМС** , , засвоєння яких передбачає проведення модульної контрольних робіт та аналіз результатів її виконання. Окремим (третім) модулем є курсова робота (КР), яка виконується у семестрі № 2, що є важливою складовою закріплення та поглиблення теоретичних і практичних знань та вмінь, набутих студентом у процесі засвоєння навчального матеріалу дисципліни.

2.2. Модульне структурування та інтегровані вимоги до кожного модуля

Модуль № 1 «Дослідження особливостей побудови та загроз безпеки ІМС»

Інтегровані вимоги модуля №1:

Студент повинен знати: принципи побудови та тенденції розвитку технологій побудови корпоративних систем та мереж , методи аналізу загроз та уразливостей систем та мереж, вплив зовнішніх факторів на роботу мережі, проблеми сучасних політик безпек, вплив шкідливих програм, комп'ютерних вірусів, шпигунських та троянських програм на роботу ІМС.

Студент повинен вміти: проводити аналіз тенденцій удосконалення способів та методів розвитку загроз інформаційній безпеці ІМС за допомогою різноманітних шпигунських програм, комп'ютерних вірусів, троянських закладок та таке інше.

Тема 1. Структура корпоративної мережі та загрози інформаційній безпеці. Аналіз загроз інформаційній безпеці, тенденції розвитку, класифікація загроз.

Тема 2. Принципи функціонування шкідливих програм. Комп'ютерні віруси, програмні закладки, шпигунські програми.

Тема 3. Комп'ютерні віруси та троянські програми. Терміни та визначення. Класифікація комп'ютерних вірусів. Особливості застосування вірусів як різновиду кіберзброї.

Тема 4. Програмні закладки їх сутність та принципи реалізації. Загрози програмних закладок та їх класифікація. Різновиди програмних закладок. Основні принципи реалізації програмних закладок. Програмні бекдори в комп'ютерних системах. Моделі дії програмних закладок на комп'ютери. Засоби впровадження програмних закладок. Способи взаємодії програмної закладки та порушника.

Тема 5. Програмні клавіатурні шпигуни. Методи спостереження за клавіатурним вводом. Програмні засоби для враження комп'ютерів . Принципи роботи клавіатурних шпигунів. Шпигунські засоби для контролю обладнання в приміщеннях типових офісів.

Тема 6. Трояни в електронній апаратурі . Програмно-апаратні трояни в телекомунікаційних системах. Трояни в мережевому обладнанні. Трояни в маршрутизаторах та в безпровідних мережах. Трояни в робочих серверах. Трояни в обладнанні операторів телекомунікаційних систем.

Тема 7. Апаратні трояни в комп'ютерах. Апаратні трояни в системному блоці. Апаратні трояни для підключення до USB. Трояни для перехоплення інформації, яка вводиться через клавіатуру комп'ютера. Троянські програми на жорстких дисках.

Тема 8. Трояни у мобільних телефонах. Впровадження закладки у запчастини смартфона. Мінішпигуни у мобільному телефоні. Шляхи впровадження трояна у мобільний телефон.

Модуль №2 Аналіз методів організації захисту інформації в ІМС.

Інтегровані вимоги до модуля №2

Студент повинен знати: принципи організації захисту корпоративних мереж, технології використання мережевих екранів для захисту корпоративних мереж, основні технології забезпечення захисту віртуальних мереж, протоколи захисту на канальному, мережевому, сеансовому рівнях, організацію захищеного віддаленого доступу, технології виявлення атак.

Студент повинен вміти: будувати та обгрунтовувати структуру побудови захищених віртуальних мереж.

Тема 9. Технології міжмережевих екранів. Функції міжмережевих екранів (МЕ). Особливості функціонування МЕ на різних рівнях моделі OSI. Схеми мережевого захисту на базі МЕ.

Тема 10. Основи технології віртуальних захищених мереж VPN. Концепція побудови віртуальних захищених мереж. Варіанти побудови віртуальних захищених каналів. Засоби

забезпечення безпеки VPN. VPN рішення для побудови захищених мереж. Переваги застосування технологій VPN.

Тема 11. Захист на канальному і сеансовому рівнях. Протоколи формування захищених каналів на канальному рівні. Протоколи формування захищених каналів на сеансовому рівні.

Тема 12. Захист на мережевому рівні. Архітектура засобів безпеки IPSec. Захист передавання даних за допомогою протоколів AH та ESP. Алгоритми аутентифікації і шифрування в IPSec. Протокол управління криптоключами IKE. Встановлення безпечної асоціації SA. Основні схеми застосування IPSec. Переваги засобів безпеки IPSec.

Тема 13. Інфраструктура захисту на прикладному рівні. Управління ідентифікацією і доступом. Функціонування системи управління доступом.

Тема 14. Організація захищеного віддаленого доступу. Протоколи аутентифікації віддалених користувачів. Централізований контроль віддаленого доступу. Управління доступом за схемою одноразового входу з авторизацією. Проста схема одноразового входу. Протокол Kerberos. Інфраструктура управління відкритими ключами PKI. Принципи функціонування PKI. Логічна структура і компоненти PKI.

Тема 15. Аналіз захищеності та виявлення атак. Концепція адаптивного управління безпекою. Технології аналізу захищеності. Засоби аналізу захищеності мережевих протоколів і сервісів. Засоби аналізу захищеності ОС.

Тема 16. Технології виявлення атак. Методи аналізу мережевої інформації. Класифікація систем виявлення атак IDS. Компоненти і архітектура IDS. Методи реагування.

Модуль №3. «Курсова робота»

КР виконується у 2-му семестрі, відповідно до затверджених у встановленому порядку методичних рекомендацій, з метою закріплення та поглиблення теоретичних знань та вмінь студента з методів генерування стійких паролів доступу до захищеної мережі зв'язку. Мета КР: закріплення і практичне поглиблення знань загальних принципів забезпечення безпеки інформаційних мереж та систем.

Для успішного виконання КР студент має знати призначення та принципи побудови ІМС, вміти аналізувати загрози інформації, яка функціонує в цих системах; знати принципи впровадження та загрози безпеці різноманітних вірусів, троянських та шпигунських програм в комп'ютерне та телекомунікаційне обладнання ІМС; методи й алгоритми організації захисту мереж та систем на канальному, мережевому, прикладному рівня; принципи застосування віртуальних захищених мереж для вирішення поставленої задачі; Результатом виконання роботи є обґрунтування структури захищеної корпоративної мереж за відповідним завданням.

Виконання, оформлення та захист КР здійснюється студентом в індивідуальному порядку відповідно до методичних рекомендацій. Час, потрібний для виконання КР, — до30 годин СРС.

2.3. Тематичний план.

№ пор.	Назва теми	Обсяг навчальних занять (*год.*)							
		Денна форма навчання (ДФН)				Заочна форма навчання (ЗФН)			
		Усього	Лекції	Лабораторні заняття	СРС	Усього	Лекції	Лабораторні заняття	СРС
Модуль №1 «Дослідження особливостей побудови та загроз безпеки ІМС»									
		Семестр 1				Семестр 1			
1.1	Структура корпоративної мережі та загрози її інформаційній безпеці.	7	2	2	3	6	2		4
1.2	Принципи функціонування шкідливих програм.	11	2	2	7	6	2		4
1.3	Комп'ютерні віруси та троянські програми.	11	2	2	7	6	2	—	4
1.4	Програмні закладки, їх сутність та принципи реалізації.	11	2	2	7	4			4
1.5	Програмні клавіатурні шпигуни.	11	2	2	7	4			4
1.6	Трояни в електронній апаратурі.	11	2	2	7	4			4
1.7	Апаратні трояни в комп'ютерах.	11	2	2	7	4			4
1.8	Трояни в мобільних телефонах.	13	2	2 2	7	6	2	—	4
1.9	Контрольна (домашня) робота №1	—	—	—	—		—	—	
1.10	Модульна к.р. №1	4	2	—	2	—	—	—	—
Усього за модулем № 1		***90***	***18***	***18***	***54***	***40***	***8***		***32***
Модуль №2 «Аналіз методів організації захисту інформації в ІМС»									
2.1	Технології міжмережевих екранів.	7	2	2	3	20		2	18
2.2	Основи технології віртуальних захищених мереж VPN.	11	2	2	7	18	2	2	14
2.3	Захист на канальному та сеансовому рівнях.	11	2	2	7	16		2	14
2.4	Захист на мережевому рівні.	11	2	2	7	18	2	2	14
2.5	Методи захисту на прикладному рівні.	11	2	2	7	16		2	14
2.6	Організація захищеного віддаленого доступу.	11	2	2	7	16		2	14
2.7	Аналіз захищеності та виявлення атак.	11	2	2	7	14			14
2.8	Технології виявлення атак. Методи реагування.	13	2	2 2	7	14		—	14
2.9	Контрольна (домашня) робота №1	—	—	—	—	8	—	—	8
2.10	Модульна к.р. №2	4	2	—	2	—	—	—	—
Усього за модулем № 2		***90***	***18***	***18***	***54***	***140***	***4***	***12***	***124***
Модуль №3 «Курсова робота»									
2.1	Програмна модель……	30	—	—	30	30	—	—	30
Усього за модулем № 3		***30***	—	—	***30***	***30***	—	—	***30***
Усього за навчальною дисципліною		**210**	**36**	**36**	**138**	**210**	**12**	**12**	**186**

2.4. Завдання на контрольну (домашню) роботу (ЗФН).

Контрольна (домашня) робота (ЗФН) виконується в 2-му семестрі, відповідно до затверджених у встановленому порядку методичних рекомендацій, з метою закріплення та поглиблення теоретичних знань та вмінь студента з методів обґрунтування вибору структури побудови захищених ІМС за допомогою міжмережевих екранів. Виконання, оформлення та захист контрольної (домашньої) роботи здійснюється студентом в індивідуальному порядку відповідно до методичних рекомендацій. Час, потрібний для виконання роботи — до 8 годин СРС.

2.5. Перелік питань для підготовки до екзамену

Перелік питань та зміст завдань для підготовки до екзамену розробляються провідним викладачем кафедри відповідно до робочої програми, затверджується на засіданні кафедри та доноситься до відома студентів.

3. НАВЧАЛЬНО-МЕТОДИЧНІ МАТЕРІАЛИ З ДИСЦИПЛІНИ

3.1. Методи навчання

При вивченні навчальної дисципліни використовуються наступні методи навчання.

Лекційна робота, рівень якої головним чином визначає якість вивчення і розуміння предмету, ефективність проведення інших форм навчальної роботи. Читання лекцій з навчальної дисципліни відбувається у традиційній формі — у вигляді усного обговорення винесеної на заняття теми для всього потоку слухачів, супроводжуючись задиктовуванням ключових для розуміння теми тезисів, наведенням формул, таблиць і графіків на дошці.

Робота на лабораторних заняттях проводиться у групах (підгрупах) і передбачає розв'язання ситуаційних завдань з використанням прикладного програмного забезпечення для імітаційного математичного моделювання процесів, винесених в якості предмету дослідження.

Навчально-методичний комплекс з дисципліни розміщується у відповідному класі на базі веб-сервісу Google Classroom (https://classroom.google.com). Приватний ключ доступу до класу видається викладачем на першому занятті з дисципліни. Через Ґуґл-клас видаються вихідні дані до передбачених програмою навчальних робіт, проводяться додаткові консультації, відстежується прогрес кожного студента у засвоєнні матеріалів.

3.2. Рекомендована література

Базова література

3.2.1. Конахович Г.Ф. та інш. Захист інформації в телекомунікаційних системах. — К.: «МК-Прес», 2005. — 279 с.
3.2.2. Жилін А.В., Шаповал О. М., Успенський О.А. Технології захисту інформації в інформаційно-комунікаційних системах. Навчальний посібник, ІСЗЗІ КПІ ім. Ігоря Сікорського. – Київ. Вид. "Політехніка , 2021.-213 с.
3.2.3. Жаровський Р.О. Захист інформації в компютерних системах. Навчальний посібник. Тернопіль. ТНТУ ім. Івана Пулюя, 2019.-268с.
3.2.4. Слобожанюк Р.І. Інформаційна безпека. Конспект лекцій. Харків.-ХДПК, 2019. -137с.
3.2.5. Королькова Т.І. Технології захисту локальних мереж на основі обладнання CISCO . Навчальний посібник. .-Львів: Вид. Львівська політехніка, 2021-232с.
3.2.6. Смірнов О.А. та інш. Інформаційна безпека в комп ютерних мережах. Навчальний посібник.— Кропивницький Вид. Л.В.Ф., 2020.—295с.

Допоміжна література

3.2.7. Y.Akaiwa. Introduction to Digital Mobile Communication. Wiley, 2015, pp.643.
3.2.8. Соколов В.Ю. Безпека безпроводових і мобільних мереж. Навчальний посібник. –К. КУБГ, 2019.-130с.
3.2.9. Технічна документація виробників телекомунікаційного обладнання.

3.3. Інформаційні ресурси в Інтернет

3.3.1. https://www.3gpp.org/
3.3.2. http://www.3gpp2.org/
3.3.3. https://www.etsi.org/
3.3.4. http://www.broadband.org.ua/
3.3.5. http://celnet.ru/sitemap.html
3.3.6. http://tks.nau.edu.ua/

4. РЕЙТИНГОВА СИСТЕМА ОЦІНЮВАННЯ НАБУТИХ СТУДЕНТОМ ЗНАНЬ ТА ВМІНЬ

4.1. Оцінювання окремих видів виконаної студентом навчальної роботи здійснюється в балах відповідно до табл.4.1.

Таблиця 4.1.

Модуль № 1 «Дослідження особливостей побудови та загроз безпеки ІМС»					
Вид навчальної роботи	Макс. кількість балів		Вид навчальної роботи	Макс. кількість балів	
	ДФН	ЗФН		ДФН	ЗФН
Виконання і захист ЛР № 1.1	3	3	Виконання і захист ЛР № 1.5	3	3
Виконання і захист ЛР № 1.2	3	3	Виконання і захист ЛР № 1.6	3	3
Виконання і захист ЛР № 1.3	3	3	Виконання і захист ЛР № 1.7	3	2
Виконання і захист ЛР № 1.4	3	3	Виконання і захист ЛР № 1.8	3	2
Усього за модулем№1				24	
Виконання і захист КДР №1				—	8
Для допуску до виконання МКР №1 студент ДФН має набрати не менше 14 балів.					
Виконання МКР №1				16	—
Усього за модулем № 1				**40**	**30**
Модуль № 2 «Аналіз методів організації захисту інформації в ІМС»					
Вид навчальної роботи	Макс. кількість балів		Вид навчальної роботи	Макс. кількість балів	
	ДФН	ЗФН		ДФН	ЗФН
Виконання і захист ЛР № 1.1	3	4	Виконання і захист ЛР № 1.5	3	4
Виконання і захист ЛР № 1.2	3	4	Виконання і захист ЛР № 1.6	3	4
Виконання і захист ЛР № 1.3	3	4	Виконання і захист ЛР № 1.7	3	3
Виконання і захист ЛР № 1.4	3	4	Виконання і захист ЛР № 1.8	3	3
Усього за модулем№2				24	
Для допуску до виконання МКР №2 студент ДФН має набрати не менше 14 балів.					
Виконання МКР №2				16	—
Усього за модулем № 2				**40**	**30**
Семестровий екзамен				**20**	**40**
Усього за семестр (за дисципліною)				**100**	
Модуль №3 «Курсова робота»				Макс. кількість балів	
Виконання курсової роботи				**60**	
Захист курсової роботи				**40**	
Виконання та захист курсової роботи				**100**	

[1] Тут і надалі прийнято наступні абревіатури: ДФН – денна форма навчання, ЗФН – заочна форма навчання, ЛР — лабораторна робота, КДР — контрольна (домашня) робота, МКР — модульна контрольна робота.

4.2. Виконані види навчальної роботи зараховуються студенту, якщо він отримав за них позитивну рейтингову оцінку (Додаток 3).

4.3. Сума рейтингових оцінок, отриманих студентом за окремі види виконаної навчальної роботи, становить поточну модульну рейтингову оцінку, яка заноситься до відомості модульного контролю.

4.4. Сума поточної та контрольної модульних рейтингових оцінок становить підсумкову модульну рейтингову оцінку, якій відповідає певний рівень оцінки за національною шкалою (Додаток 3).

4.5. Підсумкова модульна рейтингова оцінка, отримана студентом за результатами виконання та захисту КР у балах, за національною шкалою та шкалою ECTS заноситься до відомості модульного контролю, а також до навчальної картки, залікової книжки та Додатку до диплома, наприклад, так: *99/відм./A, 88/добре/B, 77/добре/C, 69/задов./D, 66/задов./E* тощо.

4.6. Сума підсумкової семестрової модульної та екзаменаційної рейтингових оцінок, у балах становить підсумкову семестрову рейтингову оцінку, яка перераховується в оцінки за національною шкалою та шкалою ECTS (Додаток 4).

4.7. Підсумкова семестрова рейтингова оцінка в балах, за національною шкалою та шкалою ECTS заноситься до заліково-екзаменаційної відомості, навчальної картки та залікової книжки студента, наприклад, так: *99/відм./A, 88/добре/B, 77/добре/C, 69/задов./D, 66/задов./E* тощо.

4.8. Підсумкова рейтингова оцінка з дисципліни дорівнює підсумковій семестровій рейтинговій оцінці. Зазначена підсумкова рейтингова оцінка з дисципліни заноситься до Додатку до диплома.

(Ф 03.02 – 01)

АРКУШ ПОШИРЕННЯ ДОКУМЕНТА

№ прим.	Куди передано (підрозділ)	Дата видачі	П.І.Б. отримувача	Підпис отримувача	Примітки

(Ф 03.02 – 02)

АРКУШ ОЗНАЙОМЛЕННЯ З ДОКУМЕНТОМ

№ пор.	Прізвище, ім’я, по батькові	Підпис ознайомленої особи	Дата ознайом-лення	Примітки

(Ф 03.02 – 04)

АРКУШ РЕЄСТРАЦІЇ РЕВІЗІЇ

№ пор.	Прізвище, ім’я, по батькові	Дата ревізії	Підпис	Висновок щодо адекватності

(Ф 03.02 – 03)

АРКУШ ОБЛІКУ ЗМІН

№ зміни	№ листа (сторінки)				Підпис особи, яка внесла зміну	Дата внесення зміни	Дата введен-ня зміни
	Зміненого	Заміненого	Нового	Анульо-ваного			

(Ф 03.02 – 32)

УЗГОДЖЕННЯ ЗМІН

	Підпис	Ініціали, прізвище	Посада	Дата
Розробник				
Узгоджено				
Узгоджено				
Узгоджено				