(Ф 03.02 – 107)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний авіаційний університет

ОСВІТНЬО –ПРОФЕСІЙНА ПРОГРАМА

«Системи технічного захисту інформації, автоматизація її обробки»
(найменування ОПП)

Другого (магістерського) рівня вищої освіти

за спеціальністю 125 Кібербезпека
(шифр та найменування спеціальності)

галузі знань 12 Інформаційні технології
(шифр та найменування галузі)

кваліфікація: Професіонал з організації інформаційної безпеки;
Науковий співробітник (інформаційна безпека)
(найменування кваліфікації)

СМЯ НАУ ОПП 14.01.04 – 01 – 2018

Затверджено Вченою радою
Голова Вченої ради
_____ В. Ісаєнко
(протокол № 5 від 26.06. 2018р.)

Освітньо-професійна програма
вводиться в дію наказом ректора
Ректор
_____ В. Ісаєнко
(наказ №____від_____2018р.)

КИЇВ

ДІЄ ЯК ТИМЧАСОВА ДО ВВЕДЕННЯ СТАНДАРТУ ВИЩОЇ ОСВІТИ УКРАЇНИ

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми

ПОГОДЖЕНО

Науково-методичною радою університету

протокол № 5

від "07" 06 2018 р

Проректор НАУ з навчальної роботи
Голова НМР НАУ

_____ (Гудманян А.Г.)

ПОГОДЖЕНО

Вченою радою Навчально-наукового інституту інформаційно-діагностичних систем

протокол № 5

від "22" травня 2018 р

Голова Вченої ради Навчально-наукового інституту інформаційно-діагностичних систем

_____ (Гумен М.Б.)

ПОГОДЖЕНО

Кафедрою засобів захисту інформації

протокол засідання № 5

від "05" березня 2018 р

Завідувач кафедри

_____(Козловський В. В.)

ПОГОДЖЕНО

Науково-методично-редакційною радою

Навчально-наукового інституту інформаційно-діагностичних систем

протокол № 5

від "15" травня 2018 р

Голова НМР Навчально-наукового інституту інформаційно-діагностичних систем

_____(Павленко П.М.)

ПЕРЕДМОВА

РОЗРОБЛЕНО РОБОЧОЮ ГРУПОЮ (спеціальності 125 Кібербезпека) у складі:

КЕРІВНИК РОБОЧОЇ ГРУПИ:

ТЕМНІКОВ В.О., к.т.н., доцент, доцент кафедри засобів захисту інформації Навчально-наукового інституту інформаційно-діагностичних систем

(підпис)

ЧЛЕНИ РОБОЧОЇ ГРУПИ:

КОЗЛОВСЬКИЙ В.В., д.т.н., проф., завідувач кафедри засобів захисту інформації Навчально-наукового інституту інформаційно-діагностичних систем

(підпис)

ШВЕЦЬ В.А., к.т.н., доцент, доцент кафедри засобів захисту інформації Навчально-наукового інституту інформаційно-діагностичних систем

(підпис)

НІМЧЕНКО Т.В., к.т.н., доцент, доцент кафедри засобів захисту інформації Навчально-наукового інституту інформаційно-діагностичних систем

(підпис)

ЛАЗАРЕНКО С.В., к.т.н., доцент, доцент кафедри засобів захисту інформації Навчально-наукового інституту Інформаційно-діагностичних систем

(підпис)

Рецензент Оксіюк О.Г., завідувач кафедри кібербезпеки та захисту інформації Факультету інформаційних технологій Київського національного університету імені Тараса Шевченка, доктор технічних наук, професор.

Рецензії-відгуки зовнішніх стейкхолдерів (додаються).

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

1. Профіль освітньо-професійної програми

Розділ 1. Загальна інформація		
1.1.	Повна назва закладу вищої освіти та структурного підрозділу	Національний авіаційний університет, Навчально-науковий інститут інформаційно-діагностичних систем Кафедра засобів захисту інформації
1.2.	Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Магістр; Професіонал з організації інформаційної безпеки; Науковий співробітник (інформаційна безпека)
1.3.	Офіційна назва освітньо-професійної програми	Освітньо-професійна програма Системи технічного захисту інформації, автоматизація її обробки
1.4.	Тип диплому та обсяг освітньо-професійної програми	Диплом магістра, одиничний, 90 кредитів ЄКТС, термін навчання 1 рік 6 місяців
1.5.	Наявність акредитації	Акредитаційна комісія, Міністерство освіти і науки України, сертифікат серія НД-ІІ № 1181256 від 18.01.2017
1.6.	Цикл/рівень	FQ-EHEA – другий цикл, НРК – 8 рівень
1.7.	Передумови	На базі освітнього ступеня - бакалавр
1.8.	Мова(и) викладання	Українська
1.9.	Термін дії освітньо-професійної програми	-
1.10	Інтернет-адреса постійного розміщення опису освітньо-професійної програми	http://www.nau.edu.ua http://www.iids.nau.edu.ua
Розділ 2. Мета освітньо-професійної програми		
2.1.	Мета освітньої програми полягає в оволодінні студентами знаннями, вміннями та навичками використовувати і впроваджувати технології інформаційної та/або кібербезпеки	
Розділ 3. Характеристика освітньо-професійної програми		
3.1	Предметна область (галузь знань, спеціальність, спеціалізація (за наявності))	Галузь знань: 12 Інформаційні технології Спеціальність: 125 Кібербезпека
3.2.	Орієнтація освітньо-професійної програми	Освітньо-професійна, базується на загальновідомих наукових результатах в галузі інформаційних технології у рамках яких можлива подальша професійна кар'єра і подальше навчання.
3.3.	Основний фокус освітньо-професійної програми та спеціалізації	Загальна вища освіта
3.4.	Особливості освітньо-професійної програми	Програма передбачає вивчення: – законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності;

		– принципів супроводу систем та комплексів інформаційної та/або кібербезпеки; – теорії, моделей та принципів управління доступом до інформаційних ресурсів; – теорії систем управління інформаційною та/або кібербезпекою; – методів та засобів оцінювання захищеності інформації; – методів та засобів технічного та криптографічного захисту інформації; – сучасних інформаційно-комунікаційних технологій; – автоматизованих систем проектування.
Розділ 4. Придатність випускників до працевлаштування та подальшого навчання		
4.1.	Придатність до працевлаштування	Випускники підготовлені до роботи за національним класифікатором України : - професіонал з організації інформаційної безпеки; - професіонал із організації захисту інформації з обмеженим доступом; - науковий співробітник (інформаційна безпека); - фахівець з режиму секретності; - фахівець з досліджень та розробок; - інспектор з організації захисту секретної інформації.
4.2.	Подальше навчання	Продовження навчання за програмою другого рівня вищої освіти (магістр), отримання другої вищої освіти.
Розділ 5. Викладання та оцінювання		
5.1.	Викладання та навчання	Лекції, лабораторні роботи, семінари, практичні заняття, проектна робота в командах, самостійна робота на основі підручників та конспектів, консультації з викладачами, виробнича та переддипломна практика на підприємствах, підготовка дипломній роботи.
5.2.	Оцінювання	Усні та письмові екзамени, лабораторні звіти, курсові роботи, презентації, поточний контроль, захист дипломного проекту.
Розділ 6. Програмні компетентності		
6.1.	Інтегральні Компетентності (ІК)	ІК1. Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки та/або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.

6.2.	Загальні компетентності (ЗК)	ЗК1. Здатність застосовувати знання у практичних ситуаціях, професійно спілкуватися державною та іноземною мовами як усно, так і письмово. ЗК2. Знання та розуміння предметної області та розуміння професії, методологічні знання і дослідницькі уміння, що забезпечують виконання завдань науково-дослідної, науково-педагогічної, управлінської і інноваційної діяльності. ЗК3. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням, бути здатним до роботи в команді. ЗК4. Здатність до самостійної науково-дослідної діяльності, пошуку, оброблення та аналізу інформації. ЗК5. Здатність до критики й самокритики, креативність, адаптивність і комунікабельність, наполегливість у досягненні мети, толерантність.
6.3.	Фахові компетентності (ФК)	ФК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки. ФК2. Здатність до використання сучасних інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної та/або кібербезпеки. ФК3. Здатність до використання програмних, апаратних та програмно-апаратних комплексів засобів захисту інформації на об'єктах інформаційної діяльності. ФК4. Здатність виконувати роботи з проектування складних комплексів засобів захисту та охорони об'єктів інформаційної діяльності відповідно до сфери їх застосування. ФК5. Здатність до керівництва проектами зі створення інформаційних ресурсів обмеженого доступу. ФК6. Здатність до організації розроблення, впровадження та експлуатації систем автоматизованого оброблення інформації з обмеженим доступом. ФК7. Здатність здійснювати процедури управління інцидентами, проводити

6.3.	Фахові компетентності (ФК)	розслідування, надавати їм оцінку. ФК8. Здатність проводити ліцензування, атестацію та сертифікацію об'єктів інформаційної діяльності. ФК9. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному/кібернетичному простору та інформаційним ресурсам. ФК10. Здатність розробляти проектну документацію, програми та методики випробувань та організовувати тестування і налагодження комплексів засобів захисту і охорони об'єктів інформаційної діяльності. ФК11. Здатність представляти результати досліджень у вигляді звітів, публікацій. ФК12. Здатність розробляти проекти методичних і нормативних документів, технічної документації, а також пропозиції та заходи з реалізації розроблених проектів.
Розділ 7. Програмні результати навчання		
7.1.	Програмні результати навчання (ПРН)	ПРН1. Здійснювати професійну діяльність на основі законодавчої та нормативно-правової бази держави, а також у відповідності до вітчизняних і міжнародних вимог і стандартів в галузі інформаційної безпеки і \або кібербезпеки; приймати участь у розробці нормативних документів, концепцій, політик, внутрішніх стандартів, положень, інструкцій, рекомендацій, готувати пропозиції до нормативних актів і документів з метою забезпечення встановленої політики інформаційної безпеки і \або кібербезпеки. ПРН2. Здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних та наукоємних технологій та методів; забезпечувати професійну діяльність на основі знань і навичок про архітектуру інформаційної системи на основі визначення інформаційних суб'єктів та об'єктів інформаційної діяльності, корпоративної архітектури, периметру безпеки (контрольованої зони), політики безпеки, привілеїв. ПРН3. Використовувати методи аналізу й діагностики стану програмних, апаратних та програмно-апаратних засобів і систем захисту інформації; забезпечувати функціонування спеціального програмного забезпечення, щодо

7.1.	Програмні результати навчання (ПРН)	захисту даних від руйнуючих програмних впливів, руйнуючих кодів в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах. ПРН4. Визначати відомості, які відносяться до інформації з обмеженим доступом, організовувати допуск та доступ персоналу до інформації з обмеженим доступом згідно чинного законодавства та встановленої політики інформаційної та/або кібербезпеки. ПРН5. Організовувати внутрішньо-об'єктовий та пропускний режими на підприємстві. ПРН6. Організовувати контроль за станом захисту інформації з обмеженим доступом на об'єктах інформаційної діяльності. ПРН7. Забезпечувати систему безперервності бізнес процесів та відновлення штатного функціонування комплексів засобів захисту інформації на основі встановленої процедури планування, вимог, правил безпеки з урахуванням аналізу небезпечних впливів, превентивних мір, стратегій відновлення інфраструктури, резервування різних типів; здійснювати задачі корекції та тестування, перегляду цілей, стратегій, планів після реалізації загроз порушником, здійснення кібератак, збоїв та відмов різних класів, що привело до порушень штатного функціонування комплексів засобів захисту інформації. ПРН8. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованим вторгненням до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки. ПРН9. Здатність продемонструвати знання та вміння забезпечувати систему виявлення, ідентифікації, аналізу та реагування на інциденти з метою забезпечення захисту інформації від різного класу загроз та кібератак; застосовувати національні та міжнародні регулюючі акти, процедури та положення в сфері інформаційної безпеки та/або кібербезпеки для збору доказів і проведення розслідування інцидентів порушення безпеки інформації. ПРН10. Вирішувати задачі захисту інформації, що обробляється в АС (ІТС) з використанням

7.1.	Програмні результати навчання (ПРН)	сучасних методів та засобів криптографічного та стеганографічного захисту інформації. ПРН11. Здатність здійснювати оцінювання захищеності інформації усіх видів, що циркулює на об'єкті інформаційної діяльності. ПРН12. Здатність забезпечення функціонування системи моніторингу управління доступом до інформації на об'єктах інформаційної діяльності і процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем в умовах реалізації загроз різних класів та протидії порушникам. ПРН13. Здатність застосування систем виявлення та протидії несанкціонованим вторгненням на об'єкти інформаційної діяльності. ПРН14. Здатність продемонструвати знання та розуміння сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. ПРН15. Здатність продемонструвати знання та навички складання звітів, публікацій, розроблення технічної документації. ПРН16. Здатність володіння англійською мовою, використовувати спеціальну термінологію для проведення літературного пошуку.
Розділ 8. Ресурсне забезпечення реалізації програми		
8.1.	Кадрове забезпечення	Всі науково-педагогічні працівники, що забезпечують освітньо- професійну програму за кваліфікацією відповідають профілю і напряму дисциплін, що викладаються, мають необхідний стаж педагогічної роботи та досвід практичної роботи. В процесі організації навчального процесу залучаються професіонали з досвідом дослідницької, управлінської, інноваційної, творчої та фахової роботи, іноземні лектори.
8.2.	Матеріально-технічне забезпечення	Навчальні приміщення, комп'ютерні робочі місця, мультимедійні класи дозволяють повністю забезпечити освітній процес протягом усього циклу підготовки за освітньою програмою.
		Офіційний веб-сайт www.nau.edu.ua містить інформацію про освітні програми, навчальну, наукову і виховну діяльність, структурні підрозділи, правила прийому, контакти. Матеріали навчально-методичного забезпечення

8.3	Інформаційне та навчально-методичне забезпечення	освітньої програми викладені в репозитарії НАУ за посиланням: http://er.nau.edu.ua/handle/NAU/9190 Всі ресурси науково-технічної бібліотеки доступні через сайт університету: http://www.lib.nau.edu.ua Читальний зал забезпечений бездротовим доступом до мережі Інтернет. Електронний репозитарій наукової бібліотеки НАУ: http://er.nau.edu.ua
Розділ 9. Академічна мобільність		
9.1.	Національна кредитна мобільність	Двосторонні договори між Національним авіаційним університетом та Технічним університетом України (КПІ) та Харківським національним університетом радіоелектроніки.
9.2.	Міжнародна кредитна мобільність	У рамках Еразмус+К1 договір про співробітництво між Національним авіаційним університетом та навчальними закладами ЕС.
9.3.	Навчання іноземних здобувачів вищої освіти	Створено умови для навчання іноземних здобувачів вищої освіти.

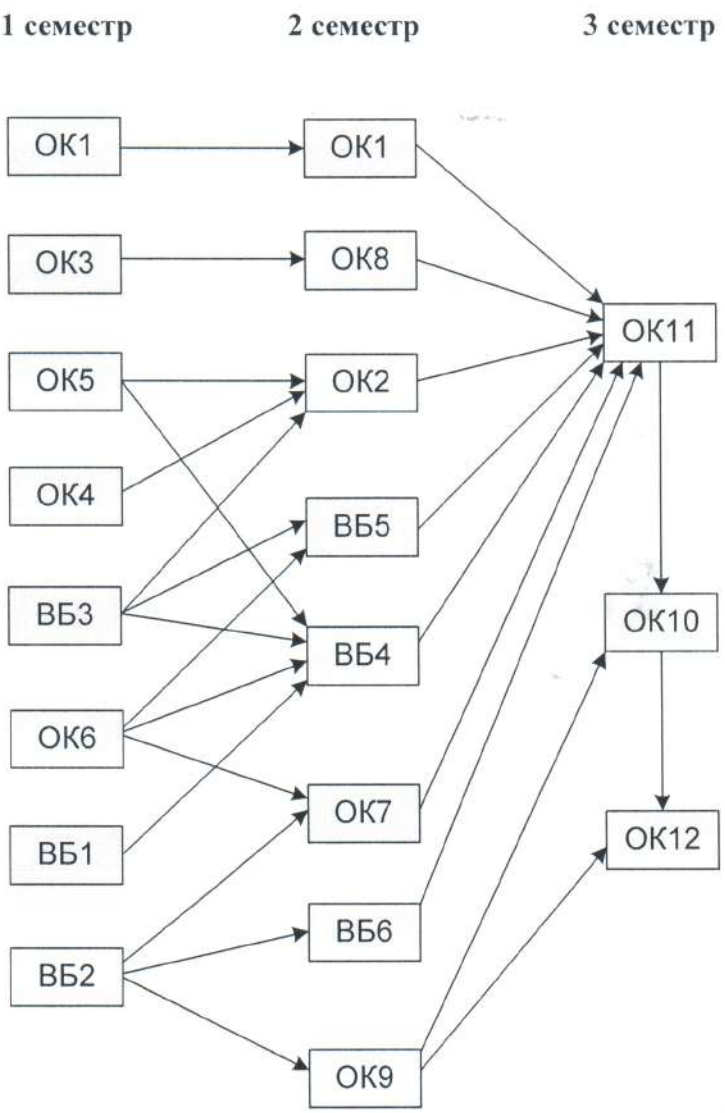
2. Перелік компонент освітньо-професійної програми та їх логічна послідовність

2.1. Перелік компонент ОПП

Код н/д	Компоненти освітньо-професійної програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
Обов'язкові компоненти ОПП			
ОК1.	Ділова іноземна мова	4.0	Екзамен, Диференційований залік
ОК2.	Наукові комунікації у фаховій діяльності	4.0	Екзамен
ОК3.	Методи побудови та аналізу криптосистем	4.0	Екзамен
ОК4.	Методи моделювання та оптимізація процесів в сфері захисту інформації	4.0	Екзамен
ОК5.	Методологія та організація наукових досліджень	4.0	Екзамен
ОК6.	Безпека в кібернетичному просторі	5.0	Екзамен
ОК7.	Спеціальні вимірювання	4.5	Екзамен

ОК8.	Автоматизація обробки інформації з обмеженим доступом	4.5	Екзамен
ОК9.	Науково-дослідна практика	3.0	Диференційований залік
ОК10.	Переддипломна практика	7.5	Диференційований залік
ОК11.	Кваліфікаційний екзамен	1.5	Диференційований залік
ОК12.	Дипломна робота	21.0	Захист
Загальний обсяг обов'язкових компонент:		67 кредитів	
1	2	3	4
Вибіркові компоненти ОПП			
ВБ1.	Ліцензування систем технічного захисту інформації	3.0	Диференційований залік
ВБ2.	Автоматизовані комплекси захисту і охорони об'єктів інформаційної діяльності	3.5	Диференційований залік
ВБ3.	Нейронні мережі	4.5	Диференційований залік
ВБ4.	Дослідження кіберпростору і запобігання кіберзагроз	4.0	Екзамен
ВБ5.	Програмне забезпечення моделювання та оптимізації процесів	4.0	Диференційований залік
ВБ6.	Організація управління персоналом	4.0	Диференційований залік
Загальний обсяг вибіркових компонент		23 кредита	
Загальний обсяг освітньо-професійної програми		90 кредитів	

2.2. Структурно-логічна схема ОПП



3. Форма атестації здобувачів вищої освіти

Атестація випускників освітньо-професійної програми проводиться у формі захисту дипломної роботи та завершується видачею документу встановленого зразка про присудження йому освітнього ступеня магістра із присвоєнням кваліфікації: Професіонал з організації інформаційної безпеки; Науковий співробітник (інформаційна безпека); за спеціальністю 125 Кібербезпека.

4. Матриця відповідності програмних компетентностей компонентам освітньо-професійної програми

	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ВБ 1	ВБ 2	ВБ 3	ВБ 4	ВБ 5	ВБ 6
ІК1			+	+		+	+	+	+	+		+	+	+	+	+	+	+
ЗК1	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ЗК2	+	+		+	+	+			+	+			+	+		+	+	
ЗК3	+	+		+		+			+	+			+	+		+		+
ЗК4	+	+			+			+	+	+		+					+	
ЗК5		+		+	+				+	+	+	+						+
ФК1	+			+		+			+	+		+	+			+		+
ФК2		+		+		+		+	+	+		+			+	+	+	
ФК3			+	+		+			+	+		+		+			+	
ФК4				+		+			+	+		+		+	+	+	+	
ФК5		+		+	+	+			+	+				+		+		+
ФК6				+		+		+	+	+		+			+		+	
ФК7		+		+		+			+	+				+		+		+
ФК8		+		+		+			+	+			+	+		+		
ФК9		+		+		+	+		+	+		+		+	+	+	+	
ФК10		+		+	+		+		+	+		+		+		+	+	
ФК11		+		+	+	+			+	+		+				+	+	
ФК12		+		+	+				+	+		+				+	+	

Матриця забезпечення програмних результатів навчання (ПРН) відповідними компонентами освітньо-професійної програми

	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ВБ 1	ВБ 2	ВБ 3	ВБ 4	ВБ 5	ВБ 6
ПРН1	+	+		+	+	+			+	+	+	+	+			+	+	
ПРН2	+	+		+	+	+		+	+	+		+			+	+	+	
ПРН3		+	+	+		+	+	+	+	+		+				+	+	
ПРН4				+		+		+	+	+	+	+	+	+		+		+
ПРН5				+		+			+	+		+		+		+		+
ПРН6			+			+		+	+	+		+		+		+		+
ПРН7		+		+		+	+		+	+		+		+	+	+	+	
ПРН8		+	+	+		+			+	+		+		+		+	+	
ПРН9	+			+		+			+	+		+		+	+	+	+	
ПРН10			+			+		+	+	+		+				+	+	
ПРН11			+	+		+	+		+	+		+	+	+	+	+	+	
ПРН12				+		+			+	+		+		+		+	+	+
ПРН13				+		+			+	+		+		+		+	+	
ПРН14		+	+	+		+			+	+		+		+	+	+	+	
ПРН15	+	+		+	+	+	+		+	+		+	+			+	+	
ПРН16	+	+		+	+	+		+	+	+	+	+			+	+	+	

(Ф 03.02 – 01)

АРКУШ ПОШИРЕННЯ ДОКУМЕНТА

№ прим.	Куди передано (підрозділ)	Дата видачі	П.І.Б. отримувача	Підпис отримувача	Примітки
1		09.07.18	Мельниківська В.А.		

(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 введення зміни
	Зміненого	Заміненого	Нового	Анульо-ваного			

(Ф 03.02 – 32)

УЗГОДЖЕННЯ ЗМІН

	Підпис	Ініціали, прізвище	Посада	Дата
Розробник				
Узгоджено				
Узгоджено				
Узгоджено				
Узгоджено				