ПРОЄКТ

(Ф 03.02 – 107)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний авіаційний університет

ОСВІТНЬО – ПРОФЕСІЙНА ПРОГРАМА

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

Другого (магістерського) рівня вищої освіти

за спеціальністю __125 Кібербезпека_
(шифр та найменування спеціальності)

галузі знань __12 Інформаційні технології__
(шифр та найменування галузі)

СМЯ НАУ ОПП 09.01.10 – 01 – 2020

Освітньо-професійна програма
Затверджена Вченою радою
протокол №____від_____20___р.

Вводиться в дію наказом ректора
Ректор
_____В.Ісаєнко
наказ №____від_____20__ р.

КИЇВ

ДІЄ ЯК ТИМЧАСОВА ДО ВВЕДЕННЯ СТАНДАРТУ ВИЩОЇ ОСВІТИ УКРАЇНИ

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми

ПОГОДЖЕНО

Радою з якості університету

протокол № _____

від "_____"_____20___ р.

Голова Ради з якості НАУ

__(Ісаєнко В.М.)

ПОГОДЖЕНО

Вченою радою Факультету кібербезпеки, комп'ютерної та програмної інженерії

протокол № _____

від "_____"_____20___ р.

Голова Вченої ради

Факультету кібербезпеки, комп'ютерної та програмної інженерії

_____(Азаренко О.В.)

ПОГОДЖЕНО

Кафедрою засобів захисту інформації

протокол засідання № _____

від "_____"_____20___ р.

Завідувач кафедри

_____(Лазаренко С.В.)

ПОГОДЖЕНО

Студентською радою Факультету кібербезпеки, комп'ютерної та програмної інженерії

протокол № _____

від "_____"_____20___ р.

Голова Студентської ради

Факультету кібербезпеки, комп'ютерної та програмної інженерії

_____(_____)

ПЕРЕДМОВА

РОЗРОБЛЕНО РОБОЧОЮ ГРУПОЮ (спеціальності 125 Кібербезпека) у складі:

Гарант освітньої програми:

ЛАЗАРЕНКО С.В. – (д.т.н., доцент, завідувач кафедри засобів захисту інформації Факультету кібербезпеки, комп'ютерної та програмної інженерії) _____

(підпис)

ЧЛЕНИ РОБОЧОЇ ГРУПИ:

ТЕМНІКОВ В.О. – (к.т.н., доцент, доцент кафедри засобів захисту інформації Факультету кібербезпеки, комп'ютерної та програмної інженерії) _____

(підпис)

ШВЕЦЬ В.А. – (к.т.н., доцент, доцент кафедри засобів захисту інформації Факультету кібербезпеки, комп'ютерної та програмної інженерії) _____

(підпис)

ВОЙТЕНКО С.Д. – (к.т.н., доцент, доцент кафедри засобів захисту інформації Факультету кібербезпеки, комп'ютерної та програмної інженерії) _____

(підпис)

МАРТИНЮК Г.В. – (к.т.н., доцент кафедри засобів захисту інформації Факультету кібербезпеки, комп'ютерної та програмної інженерії) _____

(підпис)

Зовнішній стейкхолдер Бондарчук С.В (Директор ТОВ "Світ інформаційно-телекомунікаційних рішень") _____

(підпис)

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, Факультет кібербезпеки, комп'ютерної та програмної інженерії, кафедра засобів захисту інформації
1.2.	Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Магістр; Магістр з кібербезпеки
1.3.	Офіційна назва освітньо-професійної програми та спеціалізації (за наявності)	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 4 місяці
1.5.	Наявність акредитації	Акредитаційна комісія, Міністерство освіти і науки України, сертифікат серія УД № 11005811 від 12.11.2018
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	До 01.07.2023 р.
1.10	Інтернет-адреса постійного розміщення опису освітньо-професійної програми	http://www.nau.edu.ua http://www.kzzi.nau.edu.ua
Розділ 2. Мета (ціль) освітньо-професійної програми		
2.1.	Мета освітньої програми полягає в оволодінні студентами знаннями, вміннями та навичками використовувати і впроваджувати системи та технології інформаційної та/або кібербезпеки	
Розділ 3. Характеристика освітньо-професійної програми		
3.1	Предметна область (Об'єкт діяльності, теоретичний зміст)	Об'єкт діяльності: системи та комплекси технічного захисту інформації на об'єктах інформаційної діяльності; системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків). Теоретичний зміст пердметної області: методи та технології створення, обробки, передачі, приймання, знищення, відображення, захисту (кіберзахисту) інформаційних ресурсів у кіберпросторі.
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 (за наявності)	Загальна вища освіта за спеціальністю Кібербезпека Ключові слова: технічний захист інформації, автоматизовані системи захисту інформації, обробка інформації з обмеженим доступом
3.4.	Особливості освітньо-професійної програми	Програма передбачає: – обов'язкове проходження переддипломної практики; – застосування практичних навичоку сфері технічного захисту інформації; – практичного використання методів та засобів технічного та криптографічного захисту інформації. На відміну від інших освітніх програм увага приділяється автоматизованих системам та комплексам технічного захисту інформації.
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 для отримання ступеня «Доктор філософії», отримання другої вищої освіти.
Розділ 5. Викладання та оцінювання		
5.1.	Викладання та навчання (методи, методики, технології, інструменти та обладнання)	Лекції, лабораторні роботи, семінари, практичні заняття, проєктна робота в командах, самостійна робота на основі підручників та конспектів, консультації з викладачами, переддипломна практика на підприємствах, підготовка кваліфікаційної магістерської роботи.
5.2.	Оцінювання	Усні та письмові екзамени, лабораторні звіти, курсові роботи, презентації, поточний контроль,

		кваліфікаційний екзамен та захист кваліфікаційної магістерської роботи.
Розділ 6. Програмні компетентності		
6.1.	Інтегральна Компетентність (ІК)	ІК. 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 проєктування складних комплексів засобів захисту та охорони об'єктів інформаційної

		діяльності відповідно до сфери їх застосування. ФК5. Здатність до керівництва проєктами 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 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 проєктну 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 проєкти методичних і нормативних документів, технічної документації, а також пропозиції та заходи з реалізації розроблених проєктів.
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 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 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. З метою якісної підготовки студентів використовуються охоронні системи відеоспостереження, засоби та комплекси виявлення закладних пристроїв, засоби просторового та мережевого захисту інформації.
8.3	Інформаційне та навчально-методичне забезпечення	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 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 Національним технічним університетом України «Київським політехнічним інститутом імені Ігоря Сікорського» 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

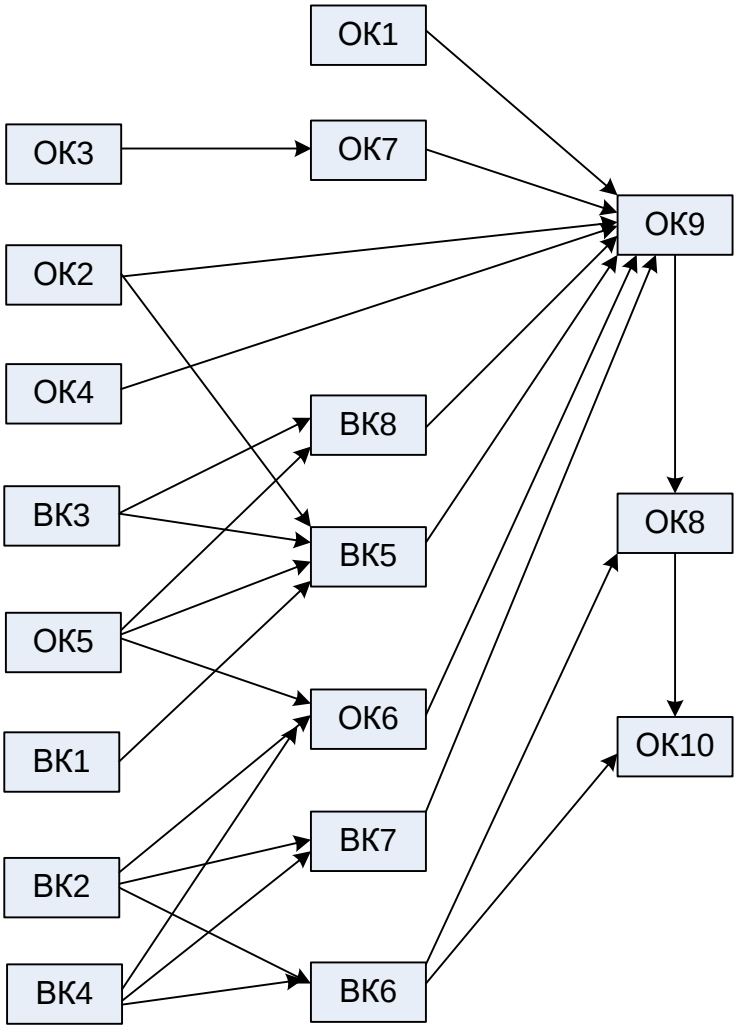
2.1. Перелік компонент

Код н/д	Компоненти освітньо-професійної програми (навчальні дисципліни, курсові проєкти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю	Семестр
1	2	3	4	5
Обов'язкові компоненти				
ОК1.	Ділова іноземна мова	7,0	Екзамен	Другий
ОК2.	Методологія наукових досліджень в сфері кібербезпеки	4,5	Екзамен	Перший
ОК3.	Методи побудови та аналізу криптосистем	4,5	Екзамен	Перший
ОК4.	Методи моделювання та оптимізація процесів в сфері захисту інформації	4,5	Екзамен	Перший
ОК5.	Безпека в кібернетичному просторі	4,5	Екзамен + курсовий проєкт	Перший
ОК6.	Спеціальні вимірювання	7,0	Екзамен	Другий
ОК7.	Автоматизація обробки інформації з обмеженим доступом	7,0	Екзамен + курсова робота	Другий
ОК8.	Переддипломна практика	12,0	Диферен-ційований залік	Третій
ОК9.	Кваліфікаційний екзамен	1,5	Екзамен	Третій
ОК10.	Кваліфікаційна магістерська робота	13,5		Третій
Загальний обсяг обов'язкових компонент:		66 кредитів		
Вибіркові компоненти				
Дисципліни вільного вибору студента за фахом				
ВК 1.	Випробування та атестація систем технічного захисту інформації	4,0	Диферен-ційований залік	Перший
ВК 2.	Автоматизовані комплекси захисту і охорони об'єктів інформаційної діяльності	4,0	Диферен-ційований залік	Перший
ВК 3.	Нейронні мережі	4,0	Диферен-ційований залік	Перший

1	2	3	4	5
ВК 4.	Аудит кібербезпеки та оцінка стану захищеності інформації	4,0	Диферен-ційований залік	Перший
ВК 5.	Дослідження кіберпростору і запобігання кіберзагроз	4,0	Диферен-ційований залік	Другий
ВК 6.	Організація управління персоналом	4,0	Диферен-ційований залік	Другий
ВК 7.	Захищеність кіберпростору	4,0	Диферен-ційований залік	Другий
ВК 8.	Програмне забезпечення моделювання та оптимізації процесів	4,0	Диферен-ційований залік	Другий
Загальноуніверситетські дисципліни				
ВЗ1	Дисципліна 1	4,0		
ВЗ2	Дисципліна 2	4,0		
Загальний обсяг вибіркових компонент		24 кредити		
Загальний обсяг освітньо-професійної програми		90 кредитів		

2.2. Структурно-логічна схема освітньо-професійної програми

1 семестр **2 семестр** **3 семестр**



3. Форма атестації здобувачів вищої освіти

Атестація випускників освітньо-професійної програми проводиться у формі кваліфікаційного екзамену та захисту кваліфікаційної магістерської роботи і завершується видачею документу встановленого зразку про присудження йому освітнього ступеня магістра із присвоєнням освітньої кваліфікації: Магістр з кібербезпеки, за спеціальністю 125 «Кібербезпека»

4. Матриця відповідності програмних компетентностей компонентам освітньо-професійної програми

Компоненти / Компетентності	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ВК 1	ВК 2	ВК 3	ВК 4	ВК 5	ВК 6	ВК 7	ВК 8
ІК1			+	+	+	+	+	+	+		+	+	+	+	+	+	+	+
ЗК1	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ЗК2	+	+		+	+			+	+		+	+		+	+		+	+
ЗК3	+			+	+			+	+		+	+		+	+	+	+	
ЗК4	+	+					+	+	+									+
ЗК5		+		+				+	+	+						+		
ФК1	+			+	+			+	+		+				+	+	+	
ФК2				+	+		+	+	+				+		+		+	+
ФК3			+	+	+			+	+			+		+				+
ФК4				+	+			+	+			+	+	+	+		+	+
ФК5		+		+	+			+	+			+		+	+	+	+	
ФК6				+	+		+	+	+				+					+
ФК7				+	+			+	+			+		+	+	+	+	
ФК8				+	+			+	+		+	+		+	+		+	
ФК9				+	+	+		+	+			+	+	+	+		+	+
ФК10		+		+		+		+	+			+		+	+		+	+
ФК11		+		+	+			+	+						+		+	+
ФК12		+		+				+	+						+		+	+

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

Компоненти / Програмні результати навчання	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ОК10	ВК 1	ВК 2	ВК 3	ВК 4	ВК 5	ВК 6	ВК 7	ВК 8
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

(Ф 03.02 - 02)

АРКУШ ОЗНАЙОМЛЕННЯ З ДОКУМЕНТОМ

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

(Ф 03.02 - 03)

АРКУШ ОБЛІКУ ЗМІН

№ зміни	№ листа (сторінки)				Підпис особи, яка внесла зміну	Дата внесення зміни	Дата введення зміни
	зміненого	заміненого	нового	анульованого			

(Ф 03.02 - 04)

АРКУШ РЕЄСТРАЦІЇ РЕВІЗІЙ

№ пор.	Прізвище ім'я по-батькові	Дата ревізії	Підпис	Висновок щодо адекватності