МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Харківський національний університет радіоелектроніки

ОСВІТНЬО – ПРОФЕСІЙНА ПРОГРАМА

«Системи технічного захисту інформації, автоматизація її обробки»

другого рівня вищої освіти

за спеціальністю 125 Кібербезпека

галузі знань 12 Інформаційні технології

Кваліфікація: Магістр, Кібербезпека, Системи технічного захисту інформації, автоматизація її обробки

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ ХНУРЕ

Голова вченої ради

_____ / В.В. Семенець /

(протокол № __ від "___"_____ 2021 р.)

Освітня програма вводиться в дію з _____2021 р.

Ректор_____ / В.В. Семенець /

(наказ № __ від "___"_____ 2021р.)

Харків 2021 р.

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми
«Системи технічного захисту інформації, автоматизація її обробки»
другого рівня вищої освіти
за спеціальністю 125 «Кібербезпека»

УЗГОДЖЕНО
Перший проректор

_____ І.В. Рубан

«___» _____ 2020 р.

В.о. начальника відділу ЛА та ВСЗЯО
_____ С.Б. Макашев

«___» _____ 2020 р.

Начальник навчального відділу
_____ А.В. Міхнова

«___» _____ 20__ р.

Розглянуто на засіданні Вченої Ради
факультету ІРТЗІ
протокол № __ від ____.____.2021р.
декан факультету ІРТЗІ
_____ С.М. Сакало

Розглянутона засіданні кафедри КРіСТЗІ
протокол № __ від ____.____.2021р.
завідувач кафедри КРіСТЗІ
_____ І.Є. Антіпов

Представник роботодавця

Кравченко Володимир Дмитрович _____ _В.Д. Кравченко_
Виконавчий директор ПрАТ «ІІТ»

РОЗРОБЛЕНО

Проектна група:
Керівник проектної групи:
Руженцев Віктор Ігорович, д.т.н., доц.,
проф. кафедри БІТ, ХНУРЕ _____ __В.І. Руженцев_____

члени проектної групи:
Халімов Геннадій Зайдулович, д.т.н., проф.,
зав. каф. БІТ, ХНУРЕ _ _____ __Г.З. Халімов____

Олейніков Анатолій Миколайович, к.т.н., проф.,
професор каф. КРіСТЗІ, ХНУРЕ _____ __А.М. Олейніков___

Снігуров Аркадій Владіславович, к.т.н., доц.,
доц. каф. ІКІ декан факультету ІК, ХНУРЕ _____ _А.В. Снігуров_____

Заболотний Володимир Ілліч, к.т.н., доц.,
професор каф. БІТ, ХНУРЕ _____ __В.І. Заболотний_____

Представник студентського самоврядування

Голова студентського сенату факультету _____ _____

ПЕРЕДМОВА

Розроблено проектною групою у складі:

1. Руженцев Віктор Ігорович	– д-р техн. наук, доцент, професор кафедри Безпеки інформаційних технологій Харківського національного університету радіоелектроніки
2. Халімов Геннадій Зайдулович	– д-р техн. наук, професор, зав. кафедри Безпеки інформаційних технологій Харківського національного університету радіоелектроніки
2. Олейніков Анатолій Миколайович	– канд. техн. наук, професор, професор кафедри Комп'ютерної радіоінженерії та систем технічного захисту інформації Харківського національного університету радіоелектроніки
3. Снігуров Аркадій Владиславович	– канд. техн. наук, доцент, декан факультету Інфокомунікацій, доцент кафедри Інфокомунікаційної інженерії ім.В.В. Поповського Харківського національного університету радіоелектроніки
4. Заболотний Володимир Ілліч	– канд. техн. наук, доцент, професор кафедри Безпеки інформаційних технологій Харківського національного університету радіоелектроніки

1 Профіль освітньої програми «Системи технічного захисту інформації, автоматизація її обробки» за спеціальністю 125 Кібербезпека

1 – Загальна інформація	
Повна назва ви-щого навчального закладу та струк-турного підрозділу	Харківський національний університет радіоелектроніки Факультет Інформаційних радіотехнологій та технічного захисту інформації Кафедра комп'ютерної радіоінженерії та систем технічного захисту інформації
Ступінь вищої освіти та назва кваліфікації мо- вою оригіналу	Магістр Магістр, Кібербезпека, Системи технічного захисту інформації, автоматизація її обробки
Офіційна назва освітньої програми	Системи технічного захисту інформації, автоматизація її обробки
Тип диплому та обсяг освітньої програми	Диплом магістра, одиничний, 90 кредитів ЄКТС, термін навчання, 1 рік 4 місяці
Наявність акредитації	
Цикл/рівень	НРК України – 8 рівень, FQ-EHEA – другий цикл, EQF-LLL – 7 рівень
Передумови	Наявність ступеня бакалавра (або освітньо-кваліфікаційний рівень спеціаліста)
Мова(и) викладання	Українська мова
Термін дії освітньої програми	До повного завершення періоду навчання або наступного оновлення програми
Інтернет-адреса постійного розмі-щення опису осві-тньої програми	http://nure.ua/abituriyentam/spetsialnosti-ta-spetsializatsiyi/spetsialnist-125-kiberbezpeka/osvitnja-programa-sistemi-tehnichnogo-zahistu-informacii
2 – Мета освітньої програми	
Мета освітньої програми полягає в оволодінні студентами знаннями, вміннями та навичками використовувати і впроваджувати технології інформаційної та/або кібербезпеки; набуття компетентностей у використанні методів дослідження і проектування систем та комплексів забезпечення інформаційної та кібербезпеки.	
3 – Характеристика освітньої програми	
Предметна область (галузь знань, спе-ціальність,)	12 Інформаційні технології, 125 Кібербезпека
Орієнтація освіт-ньої програми	Освітньо-професійна програма Акцентована на розвиток здатності розв'язувати складні задачі і проблеми у галузі професійної діяльності, що передбачає проведення досліджень та/або здійснення інновацій та характеризується невизначеністю умов і вимог
Основний фокус освітньої програми та спеціалізації	Загальна вища освіта другого (магістерського) рівня в галузі інформаційної та кібербезпеки за спеціальністю Кібербезпека Ключові слова: кібербезпека, технічний захист інформації, захист від несанкціонованого доступу
Особливості про-грами	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; – методів та засобів оцінювання захищеності інформації; – методів та засобів технічного захисту інформації; – сучасних інформаційно-комунікаційних технологій; автоматизованих систем проектування. Підготовка висококваліфікованих фахівців на високому методичному та професійному рівні.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Назви професій згідно Національного класифікатора України: Класифікатор професій (ДК 003:2010) 2149.2 Професіонал із організації захисту інформації з обмеженим доступом 2149.2 Професіонал із організації інформаційної безпеки
Подальше навчання	Можливість навчання за програмою третього (освітньо-наукового) рівня вищої освіти. . Набуття додаткових кваліфікацій в системі післядипломної освіти.
5 – Викладання та оцінювання	
Викладання та навчання	Лекції, практичні заняття, виконання курсової роботи, лабораторні роботи, самостійна робота на основі підручників, навчальних посібників та конспектів лекцій, консультації з викладачами, науково-дослідна практика, підготовка атестаційної роботи.
Оцінювання	Оцінювання навчальних досягнень студентів здійснюється за національною шкалою (відмінно, добре, задовільно, незадовільно; зараховано, незараховано); 100-бальною шкалою та шкалою ECTS (A, B, C, D, E, FX, F)
6 – Програмні компетентності	
Інтегральна компетентність	Здатність особи розв’язувати складні задачі і проблеми у галузі інформаційної безпеки та/або кібербезпеки,а також у процесі навчання, що передбачає проведення досліджень та/або здійснення інновацій та характеризується невизначеністю умов і вимог
Загальні компетентності (ЗК)	КЗ 1. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. КЗ 2. Здатність проведення досліджень на відповідному рівні. КЗ 3. Здатність професійно спілкуватися державною мовою як усно, так і письмово. КЗ 4. Здатність професійно спілкуватися іноземною мовою як усно, так і письмово. КЗ 5. Здатність до пошуку, оброблення та аналізу інформації з різних джерел. КЗ 6. Здатність до абстрактного мислення, аналізу та синтезу. КЗ 7. Здатність оцінювати та забезпечувати якість виконуваних робіт. КЗ 8. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).

Фахові компетентності спеціальності (ФК)	КФ1.Здатність обґрунтовано застосовувати,інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, науково-технічні розробки, фізичні та математичні фундаментальні знання і моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у галузі інформаційної безпеки та/або кібербезпеки. КФ2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти з метою здійснення професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. КФ4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог. КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення уразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання,згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ 9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому. КФ10. Здатність проводити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також здійснювати наукові дослідження в сфері безпеки інформаційних систем і технологій,відповідно вітчизняним та світовим стандартам і вимогам.

7 – Програмні результати навчання	
ПРН - 1	Розв’язувати складні науково-технічні та прикладні завдання та проблеми з інформаційної безпеки та/або кібербезпеки, що потребують оновлення та інтеграції фундаментальних знань, у тому числі в умовах неповної інформації та суперечливих вимог.
ПРН - 2	Проводити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також здійснювати наукові дослідження в сфері технічного та криптографічного захисту інформації у кіберпросторі.
ПРН - 3	Вільно користуватися державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки
ПРН - 4	Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, науково-технічні методи і моделі, фізичні та математичні фундаментальні знання в галузі інформаційної безпеки та/або кібербезпеки.
ПРН - 5	Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міжпредметному рівні, зокрема з використанням інженерно-технічнихі математичних наук, а також напрямів технологій створення та використання спеціалізованого програмного забезпечення.
ПРН - 6	Критично оцінювати захищеність систем, комплексів та засобів кіберзахисту, технологій створення та використання спеціалізованого програмного забезпечення, зокрема з використанням сучасних програмних та програмно-апаратних рішень та сучасних підходів.
ПРН - 7	Обґрунтовувати використання,впроваджувати та аналізувати кращі світові стандарти, практики з метою здійснення професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
ПРН - 8	Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.
ПРН - 9	Проводити аналіз, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі концептуальних питань стратегії і політики інформаційної безпеки
ПРН - 10	Досліджувати та проводити системний аналіз забезпечення безперервності бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, проводити аналіз ризиків та визначати оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації
ПРН - 11	Аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
ПРН - 12	Проводити дослідження, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.
ПРН - 13	Проводити дослідження, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також проводити аналіз і надавати оцінку ефективності їх використання в інформаційних системах,на об’єктах

	інформаційної діяльності та критичної
ПРН - 14	Здійснювати аналіз, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів в галузі інформаційної та\або кібербезпеки в цілому.
ПРН - 15	Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують.
ПРН - 16	Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.
ПРН - 17	Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпекиі дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання
ПРН - 18	Проводити науково-педагогічну діяльність, планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.
ПРН - 19	Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розуміти основні аспекти впровадження та супроводження проектів з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.
ПРН - 20	Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.
ПРН - 21	Використовувати методи натурного, фізичного і комп'ютерного моделювання з метою детального вивчення і дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.
ПРН - 22	Планувати та виконувати експериментальні і теоретичні дослідження, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати адекватність результатів досліджень, аргументувати висновки.
ПРН - 23	Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.
ПРН - 24	Мати навички керування, розроблення, впровадження та супроводження проектів з забезпечення інформаційної безпеки та/або кібербезпеки
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Реалізація програми забезпечується кадрами високої кваліфікації з науковими ступенями та вченими званнями, які мають великий досвід навчально-методичної, науково-дослідної роботи та відповідають кваліфікації відповідно до спеціальності згідно ліцензійних умов.
Матеріально-технічне забезпечення	1.Забезпеченість приміщеннями для проведення навчальних занять та контрольних заходів. 2. Забезпеченість мультимедійним обладнанням для одночасного використання в навчальних аудиторіях. 3. Наявність соціально-побутової інфраструктури. 4. Забезпеченість здобувачів вищої освіти гуртожитком. 5. Забезпеченість комп'ютерними робочими місцями, лабораторіями, полігонами, обладнанням, устаткуванням, необхідними для виконання

	навчальних планів.
Інформаційне та навчально-методичне забезпечення	1. Забезпеченість бібліотеки вітчизняними та закордонними фаховими періодичними виданнями відповідного або спорідненого профілю, в тому числі в електронному вигляді. 2. Наявність доступу до баз даних періодичних наукових видань англійською мовою відповідного або спорідненого профілю. 3. Наявність офіційного веб-сайту закладу освіти, на якому розміщена основна інформація про його діяльність (структура, ліцензії та сертифікати про акредитацію, освітня/освітньо-наукова/ видавнича/ атестаційна (наукових кадрів) діяльність, навчальні та наукові структурні підрозділи та їх склад, перелік навчальних дисциплін, правила прийому, контактна інформація). 4. Наявність електронного ресурсу закладу освіти, який містить навчально-методичні матеріали з дисциплін навчального плану, в тому числі в системі дистанційного навчання.
9 – Академічна мобільність	
Національна кредитна мобільність	На основі двосторонніх договорів між Харківським національним університетом радіоелектроніки та закладами вищої освіти України.
Міжнародна кредитна мобільність	На основі двосторонніх договорів між Харківським національним університетом радіоелектроніки та закладами вищої освіти зарубіжних країн-партнерів.
Навчання іноземних здобувачів вищої освіти	На основі договорів (угод) між Харківським національним університетом радіоелектроніки та закладами вищої освіти іноземних країн.

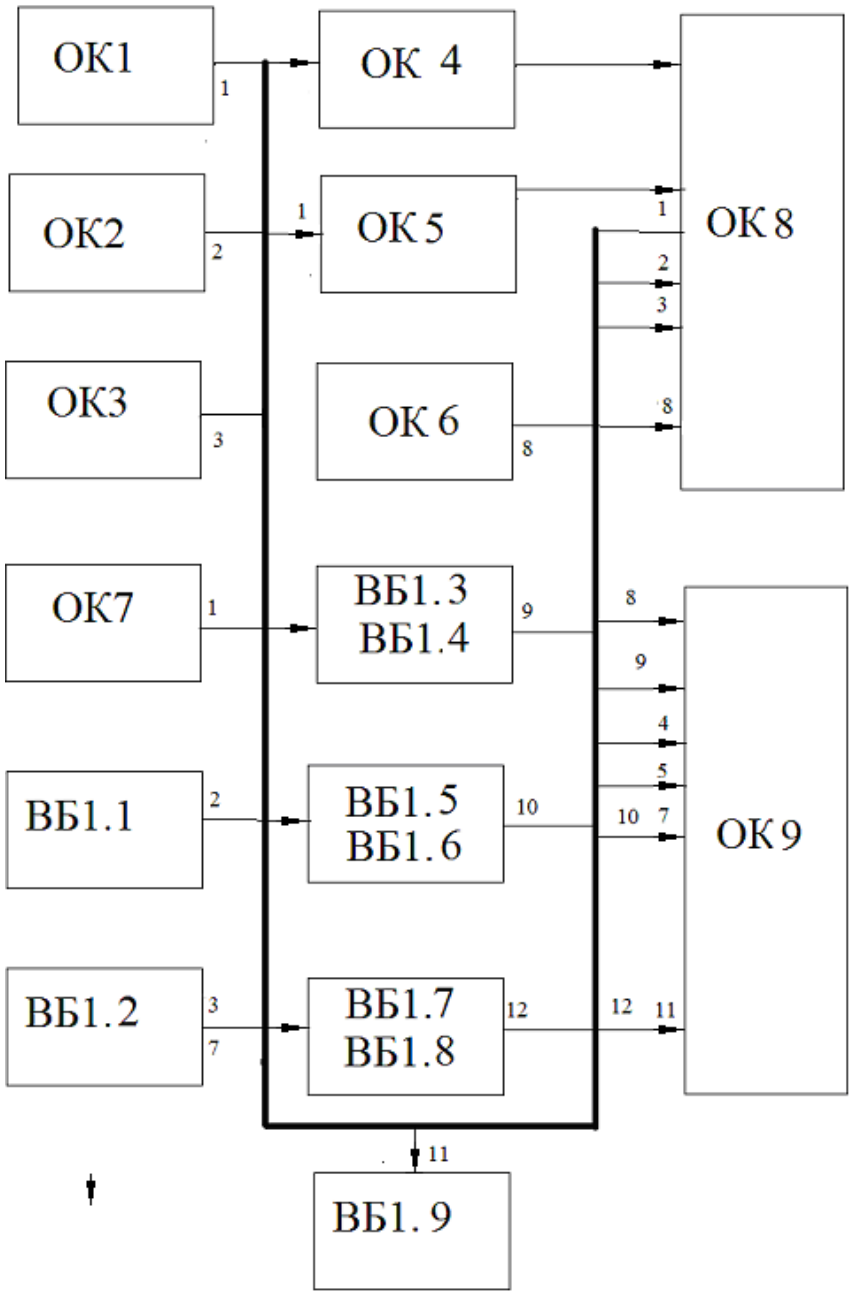
2 Перелік компонент освітньо-професійної програми та їх логічна послідовність

2.1. Перелік компонент ОП

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумк. контролю
1	2	3	4
Обов'язкові компоненти ОП			
ЦИКЛ ЗАГАЛЬНОЇ ТА СПЕЦІАЛЬНОЇ (ФАХОВОЇ) ПІДГОТОВКИ			
Дисципліни базової (професійної) підготовки за спеціальністю			
ОК 1.1	Основи наукових досліджень в сферах кібернетичного і технічного захисту інформації	5	Зл
ОК* 1.1	Моделювання та оцінка ефективності засобів технічного захисту інформації	4	Зл
ОК 1.2	Моделювання та оцінка ефективності засобів криптографічного захисту інформації	5	Ек
ОК 1.3	Моніторинг та аудит інформаційно-комунікаційних систем	5	Зл
ОК 1.4	Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем	5	Ек
ОК 1.5	Методи та заходи протидії кіберінцидентам	5	Ек
		5	Зл
Всього:		**32**	
ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ			
Дисципліни професійної та практичної підготовки за освітньою програмою Системи технічного захисту інформації, автоматизація її обробки за профілем випускової кафедри комп'ютерної радіоінженерії та систем технічного захисту інформації			
ОК 2.1	Комплекси захисту і охорони об'єктів інформаційної діяльності	4	Ек
ОК 2.2	Автоматизація обробки інформації з обмеженим доступом	4	Ек
ОК 2.3	Практична підготовка	15	Зл
ОК 2.4	Кваліфікаційна робота	15	Зл
Всього:		**38**	
Загальний обсяг обов'язкових компонент:		**67**	
Вибіркові компоненти ОП			
ЦИКЛ ЗАГАЛЬНОЇ ТА СПЕЦІАЛЬНОЇ (ФАХОВОЇ) ПІДГОТОВКИ			
Гуманітарні та соціально-економічні дисципліни			
ВБ 1.1	Інтелектуальна власність	3	Зл
ВБ 1.2	Ділова іноземна мова	3	Зл
ВБ 1.3	Філософські проблеми наукового пізнання	3	Зл
ВБ 1.4	Педагогіка вищої школи	3	Зл
ВБ 1.5	Економічне обґрунтування проектів	3	Зл
Всього		**3**	
Дисципліни професійної та практичної підготовки за освітньою програмою Системи технічного захисту інформації, автоматизація її обробки			
ВБ 2.1	Захист від технічних розвідок	5	Зл

ВБ 2.2	Протидія засобам технічної розвідки	5	Зл
ВБ 2.3	Обробка сигналів у системах ТЗІ	5	Зл
ВБ 2.4	Проектування цифрових систем ТЗІ	5	Зл
ВБ 2.5	Спеціальні дослідження в галузі ТЗІ	5	Зл
ВБ 2.6	Електродинаміка в СТЗІ	5	Зл
ВБ 2.7	Радіомоніторінг	5	Зл
ВБ 2.8	Виявлення радіосигналів	5	Зл
Всього		**20**	
Загальний обсяг вибіркових компонент:		**23**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**90**	

2.2 Структурно-логічна схема ОПП



3 Форма атестації здобувачів вищої освіти

Атестація випускників освітньої програми «Системи технічного захисту інформації, автоматизація її обробки» спеціальності 125 Кібербезпека проводиться у формі захисту атестаційної роботи та завершується видачею документу встановленого зразка про присудження йому ступеня магістра із присвоєнням кваліфікації: Магістр, Кібербезпека, Системи технічного захисту інформації, автоматизація її обробки.

Атестація здійснюється відкрито і публічно.

4 Матриця відповідності програмних компетентностей компонентам освітньої програми

	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ВБ 1	ВБ 2	ВБ 3	ВБ 4	ВБ 5	ВБ 6	ВБ 7	ВБ 8	ВБ 9
ЗК-1		*	*	*				*	*	*	*			*	*	*	*	
ЗК-2					*				*									
ЗК-3			*	*					*									
ЗК-4		*		*					*					*				
ЗК-5	*							*	*	*								
ЗК-6	*		*			*			*		*			*				
ЗК-7	*	*		*		*	*		*			*	*		*			
ФК-1	*	*					*		*									
ФК-2		*	*	*	*	*		*	*		*					*	*	
ФК-3	*			*					*	*			*				*	
ФК-4		*	*	*					*		*					*	*	
ФК-5		*	*	*					*		*							
ФК-6		*		*					*	*				*	*			
ФК-7	*	*	*	*					*									
ФК-8	*								*					*	*			
ФК-9			*				*		*									
ФК-10		*	*			*			*		*							
ФК-11		*				*			*									

5 Матриця забезпечення програмних результатів навчання (ПРН) відповідними компонентами освітньої програми

	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ВБ 1	ВБ 2	ВБ 3	ВБ 4	ВБ 5	ВБ 6	ВБ 7	ВБ 8	ВБ 9
ПРН - 1	*			*			*							*	*			
ПРН - 2		*	*	*	*				*	*	*							
ПРН - 3		*		*	*		*	*	*									
ПРН - 4		*	*			*								*	*			
ПРН - 5	*	*	*	*					*			*	*					
ПРН - 6	*	*			*				*			*	*			*	*	
ПРН - 7			*	*			*		*									
ПРН - 8		*	*	*			*	*	*									
ПРН - 9		*	*	*		*			*	*	*			*	*			
ПРН-10		*			*		*		*					*	*	*	*	*
ПРН-11		*	*	*		*											*	
ПРН-12								*	*									