МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ

ЖИТОМИРСЬКИЙ ВІЙСЬКОВИЙ ІНСТИТУТ ІМЕНІ С. П. КОРОЛЬОВА

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

Кібербезпека

(назва)

Перший (бакалаврський) рівень
(рівень вищої освіти)

за спеціальністю 125 Кібербезпека та захист інформації

галузі знань 12 Інформаційні технології

кваліфікація Бакалавр з кібербезпеки

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ

Житомирського військового інституту імені С. П. Корольова
протокол № 15 від "31" 08 2023 р.

Освітньо-професійна програма вводиться в дію з "16" 09 2023 р.

Начальник Житомирського військового інституту імені С. П. Корольова
кандидат історичних наук
бригадний -генерал

Олексій ШЕВЧЕНКО

Наказ № 762 від "16" 09 2023 р.

Житомир 2023

ЛИСТ ПОГОДЖЕННЯ
ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

Кібербезпека
(назва)

Перший (бакалаврський) рівень
(рівень вищої освіти)

за спеціальністю 125 Кібербезпека та захист інформації

галузі знань 12 Інформаційні технології

кваліфікація Бакалавр з кібербезпеки

ПОГОДЖЕНО

Директор Департаменту військової освіти і науки Міністерства оборони України, доктор технічних наук, професор, Заслужений працівник освіти України
Володимир МІРНЕНКО

"____" _____ 2023 р.

ПЕРЕДМОВА

Освітня програма розроблена у відповідності до Закону України від 01.07.2015 № 1556-VII “Про вищу освіту” (із змінами), статуту Національного агентства із забезпечення якості вищої освіти, наказу Міністерства освіти і науки України від 11.07.2019 № 977 “Про затвердження Положення про акредитацію освітніх програм, за якими здійснюється підготовка здобувачів вищої освіти”, статуту Житомирського військового інституту імені С. П. Корольова, стандарту вищої освіти за спеціальністю 125 “Кібербезпека та захист інформації” для першого (бакалаврського) рівня вищої освіти, затвердженого наказом Міністерства освіти і науки України від 04.10.2018 № 1074 та інших актів законодавства.

Розроблено робочою групою у складі:

керівник робочої групи

ГРИЩУК Руслан Валентинович	заслужений діяч науки і техніки України, доктор технічних наук (зі спеціальності 21.05.01 – Інформаційна безпека держави), професор (зі спеціальності 125 – Кібербезпека), начальник кафедри захисту інформації та кібербезпеки факультету охорони державної таємниці та інформаційного протиборства Житомирського військового інституту імені С. П. Корольова

члени робочої групи

САМЧИШИН Олексій Володимирович	кандидат технічних наук, професор кафедри захисту інформації та кібербезпеки факультету охорони державної таємниці та інформаційного протиборства Житомирського військового інституту імені С. П. Корольова
ГУМЕНЮК Ігор Володимирович	кандидат технічних наук, старший викладач кафедри захисту інформації та кібербезпеки факультету охорони державної таємниці та інформаційного протиборства Житомирського військового інституту імені С. П. Корольова
ОХРІМЧУК Володимир Васильович	старший викладач кафедри захисту інформації та кібербезпеки факультету охорони державної таємниці та інформаційного протиборства Житомирського військового інституту імені С. П. Корольова.

І. ПРОФІЛЬ ОСВІТНЬОЇ ПРОГРАМИ

“Кібербезпека”

зі спеціальності 125 Кібербезпека та захист інформації

1 – Загальна інформація	
Повна назва закладу вищої освіти та базового структурного підрозділу	Житомирський військовий інститут імені С. П. Корольова (ЖВІ) Факультет охорони державної таємниці та інформаційного протиборства Кафедра захисту інформації та кібербезпеки.
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Бакалавр Бакалавр з кібербезпеки
Офіційна назва освітньої програми	Кібербезпека
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний, 240 кредитів ЄКТС, термін навчання 4 роки
Наявність акредитації	Акредитована Міністерством освіти і науки України Сертифікат акредитації спеціальності, від 09 вересня 2015 р. серія НД-ІІІ, № 0677443
Рівень з НРК	НРК України – 6 рівень
Передумови	Умови вступу визначаються «Правилами прийому до Житомирського військового інституту імені С. П. Корольова», затвердженими Вченою радою Наявність повної загальної середньої освіти/ ступеня «молодший бакалавр»
Мова викладання	Українська
Термін дії освітньої програми	Термін дії освітньої програми до 2025 р.
Інтернет-адреса постійного розміщення освітньої програми	https://kzmi.mil.gov.ua/uk/
2 – Мета освітньої програми	
Гарантоване забезпечення умов всебічного розвитку здобувачів вищої освіти, необхідних для здобуття ними вищої освіти за спеціальністю Кібербезпека та захист інформації з одночасним формуванням у них високих моральних і ділових якостей, патріотизму, суспільної свідомості, спрямованих на якісне засвоєння нових знань та набуття достатніх компетентностей у вигляді умінь і навичок для подальшого їх практичного застосування під час організації захисту інформації та кібернетичної безпеки	

в інформаційно-телекомунікаційних системах військового та/або подвійного призначення в інтересах забезпечення кібероборони держави.	
3 – Характеристика освітньої програми	
Предметна область **Галузь знань** **Спеціальність**	12 Інформаційні технології. 125 Кібербезпека та захист інформації.
Орієнтація освітньої програми	Освітньо-професійна.
Основний фокус освітньої програми та спеціалізації	Спеціальна освіта в галузі кібербезпеки та захисту інформації в інформаційно-комунікаційних системах військового та/або подвійного призначення.
Особливості програми	**а) по-перше, <u>міжнародний вектор спрямованості освітньої програми гарантує:</u>** – узгодженість даної освітньої програми із програмами держав-членів НАТО, що досягнуто за рахунок впровадження передового світового досвіду в галузі кібербезпеки, набутого в ході міжнародного співробітництва між ЖВІ та представниками Консорціуму оборонних академій та дослідницьких інституцій програми НАТО "Партнерство заради миру", зокрема з вченими і дослідниками із Республіки Ірландія (професор Дінос Керіган-Кайру), Республіки Болгарія (професор Тодор Тагарев, доктор Ніколай Стоянов), Чеської Республіки (магістр Даніель Педер Багге), Республіки Польща (професор Богуслав Пацек), Канади (професор Скотт Найт). При розробленні освітньої програми враховано Типовий навчальний план НАТО з кібербезпеки (*https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_10/20171004_1610-cybersecurity-curriculum-r.pdf*); – взаємопов'язаність освітніх компонентів, що досягнуто унаслідок урахування досвіду провідних академічних інституцій Європейського Союзу таких, як Інституту інформаційних систем Військового технологічного університету імені Ярослава Домбровського (Республіка Польща), Інституту оборони імені Цветана Лазарева Міністерства оборони Республіка Болгарія та держави-члена НАТО, зокрема Королівського військового коледжу Канади; **б) по-друге <u>освітня програма ґрунтується на національних рамках з кібербезпеки</u>**, що гарантує

	якомога швидку адаптацію випускника до вирішення практичних завдань з організації захисту інформації та кібербезпеки в інформаційно-телекомунікаційних системах на первинних офіцерських посадах в Міністерстві оборони України, Збройних Силах України та інших міністерствах і відомствах сектору безпеки та оборони держави; **в) по-третє, <u>збалансованість</u>** співвідношення між забезпеченням загальних та спеціальних (фахових) компетентностей за спеціальністю та вибірковою частиною програми, що **<u>робить програму більш гнучкою до задоволення освітніх потреб стейкхолдерів</u>** з числа здобувачів вищої освіти та практичних завдань стейкхолдерів з числа потенційних роботодавців (*Міністерства оборони України, Збройних Сил України та інших міністерств і відомств сектору безпеки та оборони держави*) та відповідної професійної спільноти (*навчально-виробничого центру "Інфозахист", мережної академії Cisco*); **г) по-четверте, <u>освітня програма передбачає дуальний характер</u>,** що дозволяє здобувачам вищої освіти з числа військовослужбовців військової служби за контрактом після вивчення теорії та набуття первинних практичних навичок в спеціалізованих лабораторіях закріплювати набуті ними уміння безпосередньо на практиці – в пунктах постійної дислокації військових частин та в зоні проведення операції Об'єднаних сил, перебуваючи на відповідних штатних посадах; **д) по-п'яте, <u>освітня програма розрахована та адаптована на здобувачів вищої освіти, які є військовослужбовцями військової служби за контрактом</u>** Збройних Сил України та інших військових формувань, утворених відповідно до чинного законодавства; **е) по-шосте, <u>програма передбачає залучення</u>** (за згодою) **до освітнього процесу <u>стейкхолдерів</u> з числа потенційних роботодавців,** що зводить до мінімуму розрив між теорією та практикою організації захисту інформації та кібербезпеки в інформаційно-телекомунікаційних системах; **к) по-сьоме, <u>100% працевлаштування випускників;</u>**

	л) по-восьме, <u>ключовим принципом</u> програми є **<u>ґендерна рівність</u>** у правах та можливостях жінок і чоловіків з числа здобувачів вищої освіти **<u>у здобутті освіти;</u>** **м)** по-дев'яте, **потужна та сучасна матеріально-технічна база за місцем постійної дислокації;** **н) по-десяте, спадковість програми**, адже підготовка здобувачів вищої освіти за очною формою навчання у галузі знань 1701"Інформаційн безпека" за напрямком підготовки 6.17.0101 "Безпека інформаційних та комунікаційних систем" за кваліфікацією 3439 "Фахівець із захисту інформації в інформаційно-комунікаційних системах", що була схвалена та введена в дію Вченою радою Державного університету телекомунікації від 26.11.2014, протокол №14, здійснювалася на кафедрі безпеки інформаційних та комунікаційних систем Житомирського військового інституту починаючи з 2007 року. Кафедра захисту інформації та кібербезпеки, що утворена внаслідок організаційно-штатних змін у 2017 р. стала правонаступницею кафедри безпеки інформаційних та комунікаційних систем.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	**Виходячи з особливостей контингенту здобувачів вищої освіти**, які є військовослужбовцями військової служби за контрактом Збройних Сил України та інших військових формувань, утворених відповідно до чинного законодавства, **<u>всі випускники 100% придатні до працевлаштування за військово обліковою спеціальністю (ВОС) 121501</u>** *Організація захисту інформації та кібернетичної безпеки в інформаційно-телекомунікаційних системах та проходять військову службу*, **затверджену наказом Міністерства оборони України від 05.02.2020 № 26** *"Про затвердження змін до Переліку військово-облікових спеціальностей осіб офіцерського складу, Переліку військових посад осіб офіцерського складу, які можуть бути заміщені військовослужбовцями-жінками, Переліку військово-облікових спеціальностей, за якими може бути присвоєно первинне військове звання молодшого лейтенанта запасу*" та **<u>можуть проходити військову службу за здобутою спеціалізацією на посадах молодшого</u>**

	офіцерського складу Міністерства оборони України та Збройних Сил України, інших міністерств і відомств сектору безпеки та оборони держави. **До первинних посад,** що обійматимуться випускниками віднесено такі основні посади: - первинні офіцерські посади в підрозділах кібербезпеки *Командування Військ зв'язку та кібернетичної безпеки Збройних Сил України*; - первинні офіцерські посади (начальник групи/відділення захисту інформації та кібернетичної безпеки в ІТС, інженер групи/відділення захисту інформації та кібернетичної безпеки в ІТС тощо) у військових частинах *Сухопутних військ* Збройних Сил України, *Військово-морських сил* Збройних Сил України, *Повітряних сил* Збройних Сил України, Сил спеціальних операцій Збройних Сил України, *Десантно-штурмових військ* Збройних Сил України; - первинні офіцерські посади інших міністерств і відомств сектору безпеки та оборони держави за напрямком організації захисту інформації та кібернетичної безпеки в інформаційно-телекомунікаційних системах. **Додаткова професійна сертифікація Cisco –** *CCNA Routing & Switching, CCNA CyberOps, Cybersecurity Essentials* (***підготовка до сертифікації проводиться в рамках освітньої програми***), ЖВІ – **10 кроків кібербезпеки** (***розробка ЖВІ у взаємодії з експертами за програмою DEEP NATO***) та іншими провідними вендорами, такими як ***CISSP, CISM, CEH. CHFI, ECSA, ECIH, CND*** тощо відкриває перед випускниками можливості з влаштування й за цивільними посадами, зокрема: - спеціаліста/інспектора з технічного захисту інформації та кібербезпеки; - спеціаліст відділу інформаційно-комп'ютерного забезпечення та захисту інформації тощо.
Подальше навчання	Здобуття освіти на **другому (магістерському) рівні** вищої освіти в системі вищої освіти України, а також навчання на курсах **професійної військової освіти** відповідних рівнів військової освіти офіцерського складу в системі військової освіти і підготовки офіцерського складу ЗС України.
	5 – Викладання та оцінювання
Викладання та навчання	В основу викладання покладено **особистісно-орієнтований підхід** до навчання для забезпечення

	всебічного розвитку особистості здобувача вищої освіти, врахування його індивідуальних особливостей, здібностей, інтересів, потреб, можливостей, індивідуального профілю компетенцій. При цьому навчальний матеріал викладається в межах можливостей засвоєння здобувачами, адекватно поєднуючи в собі прикладну спрямованість та вимоги стандарту вищої освіти за спеціальністю. **<u>В основу навчання покладено сучасні дидактичні принципи,</u>** такі як гуманізація та демократизація навчання, принцип нерозривності навчання та національно-патріотичного виховання й всебічного гармонійного розвитку тих, хто навчається, принцип проблемності та нерозривності теорії з практикою. Освітній процес здійснюється в таких формах: навчальні заняття (*у тому числі з використанням елементів дистанційної форми*), самостійна робота здобувачів вищої освіти, практична підготовка, контрольні заходи. Викладання проводиться за такими видами навчальних занять є: лекція, семінарське заняття, групове заняття, практичне заняття, лабораторне заняття, індивідуальне завдання з освітнього компонента, консультація.
Оцінювання	Оцінювання результатів навчання здобувачів освіти здійснюється у відповідності до "Положення про поточний та семестровий контроль навчальної діяльності здобувачів вищої освіти у ЖВІ" та включає весь спектр контрольних заходів, передбачених робочою програмою навчальної дисципліни та здійснюється за 100-бальною шкалою, шкалою ЄКТС та національною шкалою і становить: 90 - 100 балів, за національною шкалою – “відмінно”; 80 - 89 балів – “дуже добре”; 65 - 79 балів – “добре”; 55 - 64 балів – “задовільно”; 50 - 54 балів – “достатньо”; 1 - 49 балів – “незадовільно” з можливістю повторного складання. **Види контролю:** вхідний, поточний, самоконтроль, семестровий, підсумковий. **Форми контролю:** <u>екзамен, залік</u>, усне та письмове опитування, тестові завдання, лабораторні звіти, презентації, захист курсових робіт та проєктів, звітів з практик.

	Атестація: Атестація випускників може проводиться у формі єдиного державного кваліфікаційного іспиту (атестаційного екзамену) або захисту кваліфікаційної роботи. Атестація здійснюється відкрито та публічно з дотриманням вимог законодавства України у сфері охорони державної таємниці та міжнародних принципів академічної доброчесності. Кваліфікаційні роботи (проєкти) оприлюднюються на офіційному сайті військового інституту. Рішення щодо оприлюднення таких робіт приймається екзаменаційною комісією військового інституту із залученням представників режимно-секретного органу з дотриманням вимог законодавства України у сфері охорони державної таємниці.
6 – Програмні компетентності	
Інтегральна компетентність	КЗ 0 Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і\або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.
Загальні компетентності (КЗ)	КЗ 1. Здатність застосовувати знання у практичних ситуаціях
	КЗ 2. Знання та розуміння предметної області та розуміння професії
	КЗ 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово
	КЗ 4 Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням
	КЗ 5. Здатність до пошуку, оброблення та аналізу інформації
	КЗ 6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні
	КЗ 7. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати

	різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя
Фахові компетентності за спеціальністю (визначені стандартом вищої освіти)	КФ 1. 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.
	КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів та моделей інформаційної та/або кібербезпеки.
	КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.
	КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.
	КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.
	КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класів та походження.
	КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).
	КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.
	КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.
	КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.
	КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно

	встановленої політики інформаційної та/або кібербезпеки.
	КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки
Фахові компетентності за спеціалізацією (визначені вищим військовим навчальним закладом)	КФ 13. Здатність до створення моделей кібербезпеки та проектування на їх основі систем кіберзахисту інформаційно-телекомунікаційних систем.
	КФ 14. Здатність розробляти та впроваджувати заходи із захисту інформації та/або кібербезпеки на об’єктах інформаційної діяльності.
	КФ 15. Здатність застосовувати знання особливостей алгоритмізації, основ сучасних мов програмування для автоматизації процесів захисту інформації в кіберпросторі.
	КФ 16. Здатність застосовувати знання основ технологій програмування, володіння методами та засобами розроблення програмних додатків систем забезпечення кібербезпеки
	КФ 17. Здатність до безпечної експлуатації систем передачі інформації в інформаційно-телекомунікаційних системах
	КФ 18. Здатність до організації контролю за дотриманням правил захисту інформації та кібербезпеки з боку штатних або позаштатних служб захисту інформації та кібернетичної безпеки й інженерно-технічних підрозділів, які неналежним чином стежать за справністю інформаційно-телекомунікаційних систем та їх складових
7 – Програмні результати навчання	
Програмні результати навчання, визначені стандартом вищої освіти	
РН 1: застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації	
РН 2: організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність	
РН 3: використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності	
РН 4: аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач та практичних проблем у професійній	

діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення
РН 5: адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат
РН 6: критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності
РН 7: діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки
РН 8: готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки
РН 9: впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки
РН 10: виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем
РН 11: виконувати аналіз зв’язків між інформаційними процесами на віддалених обчислювальних системах
РН 12: розробляти моделі загроз та порушника
РН 13: аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних
РН 14: вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень
РН 15: використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій
РН 16: реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів
РН 17: забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв’язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент
РН 18: використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів
РН 19: застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах
РН 20: забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах
РН 21: вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої

політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах
РН 22: вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки
РН 23: реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах
РН 24: вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових)
РН 25: забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту
РН 26: впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем
РН 27: вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах
РН 28: аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки
РН 29: здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів
РН 30: здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем
РН 31: застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем
РН 32: вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки
РН 34: приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації
РН 35: вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-

телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки
РН 36: виявляти небезпечні сигнали технічних засобів
РН 37: вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації
РН 38: інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації
РН 39: проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах
РН 40: інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації
РН 41: забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур
РН 42: впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки
РН 43: застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів
РН 44: вирішувати задачі безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами
РН 45: застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів
РН 46: здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах
РН 47: вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації
РН 48: виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах
РН 49: забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах
РН 50: забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних)

РН 51: підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах
РН 52: використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах
РН 53: вирішувати задачі аналізу програмного коду на наявність можливих загроз
РН 54: усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні
Програмні результати навчання, визначені вищим військовим навчальним закладом
РН 55: здійснювати оцінку рівня захищеності інформації, що обробляється в інформаційно-телекомунікаційних системах використовувати інструментальні засоби оцінювання наявності потенційних вразливостей
РН 56: вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації, користувачів і процесів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних (автоматизованих) системах
РН 57: вирішувати задачі супроводу та впровадження комплексних систем захисту інформації, а також протидії несанкціонованому доступу до ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах
РН 58: вирішувати задачі управління комплексною системою захисту інформації в інформаційних та інформаційно-телекомунікаційних (автоматизованих)
РН 59: здійснювати експертизу, випробування комплексних систем захисту інформації
РН 60: розробляти алгоритми розв’язку типових прикладних задач забезпечення інформаційної та кібернетичної безпеки
РН 61: використовувати мову високого рівня вирішення прикладних задач забезпечення інформаційної та кібернетичної безпеки
РН 62: використовувати сучасні інтегровані середовища розробки програмного забезпечення в інтересах забезпечення захисту інформації та кібербезпеки
РН 63: застосовувати технології та методології використання засобів обчислювальної техніки з метою створення програмних додатків систем забезпечення кібербезпеки
РН 64: виконувати функціональну композицію програмних систем захисту інформації та проводити її об’єктно-орієнтований аналіз та візуальне проектування
РН 65: проектувати бази даних систем захисту інформації та кібернетичної безпеки з використанням ER-моделі

РН 66: використовувати мову SQL для визначення даних та їх маніпулювання в сучасних СУБД	
РН 67: аналізувати дані засобами сучасних СУБД	
РН 68: забезпечувати авторизацію доступу до даних та їх захист від несанкціонованого втручання	
РН 69: вирішувати задачі забезпечення безперервності функціонування інформаційно-телекомунікаційних систем у військовій частині (органі військового управління) на основі теорії ризиків та встановленої системи управління інформаційною безпекою з підтвердженою відповідністю згідно з вітчизняними та міжнародними (у разі потреби участі у міжнародних спільних військових навчаннях із залученням інформаційно-телекомунікаційних систем або їх складових) вимогами та стандартами	
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	До реалізації програми залучаються науково-педагогічні працівники з науковими ступенями та/або вченими званнями, які мають досвід навчальної, методичної, наукової роботи, службової діяльності та відповідають кадровим вимогам щодо забезпечення провадження освітньої діяльності у сфері вищої освіти згідно з діючими ліцензійними вимогами Міністерства освіти і науки України.
Матеріально-технічне забезпечення	**Матеріально-технічна база за місцем постійної дислокації:** – *навчальні приміщення:* лекційні аудиторії, лінгафонна аудиторія, навчально-методичний кабінет, аудиторії для курсового та дипломного проєктування; – *навчально-лабораторна база* (лабораторне обладнання, вимірювальна та електронно-обчислювальна техніка, технічні засоби навчання, наочне приладдя); – *навчально-допоміжні приміщення* для науково-педагогічних працівників, службові приміщення для інженерно-технічного складу; – *підсобні приміщення:* коридори оснащені стендами, гардеробна; – *клінічна база* (поліклініка військового інституту); – *поліграфічна база* (друкарня військового інституту); – *база для виконання наукових досліджень* (науково-дослідний відділ інформаційної та кібернетичної безпеки наукового центру ЖВІ, інформаційно-обчислювальний центр); – спортивні комплекси і споруди (*спортивний комплекс зі стадіоном та басейном, ігровими*

	майданчиками та декількома тренажерними залами); *– гуртожиток*. **Унікальне матеріально-технічного забезпечення за спеціалізацією, яке сприяє розвитку визначених компетенцій та досягненню програмних результатів навчання:** *– Навчальний кіберполігон* (устаткування на спонсорській основі надано стейкхолдером ТОВ "НВЦ" "ІНФОЗАХИСТ" *https://infozahyst.com*); *– Локальна мережна академія CISCO* (*Korolyov Zhytomyr Military Institute Cisco Academy), https://www.netacad.com/ru/node/26353, ID 20049039);* *– навчальна лабораторія технічного захисту інформації та спецдосліджень*; *– науково-дослідний відділ інформаційної та кібернетичної безпеки наукового центру*; *– програмне забезпечення вільного поширення* Фонду вільного програмного забезпечення (*https://directory.fsf.org/wiki/Main_Page*); – лабораторія радіотехнічних пристроїв спеціального призначення.
Інформаційне та навчально-методичне забезпечення	**Інформаційне забезпечення освітньої діяльності** здійснює як *"класична" бібліотека* з друкованими виданнями, так і *електронна бібліотека* з доступом до електронних баз даних у локальній комп'ютерній мережі в усіх навчальних корпусах військового інституту а також розміщення на платформах дистанційного навчання Moodle, Elearn та інші. Здобувачі вищої освіти мають доступ до української науково-освітньої телекомунікаційної мережі УРАН (*http://www.uran.net.ua/~ukr/uran-members.htm*), а також доступ до мережі Інтернет. Наявний офіційний веб-сайт військового інституту: https://kzmi.mil.gov.ua/uk/, на якому розміщена основна інформація про освітню, наукову, науково-технічну діяльність військового інституту, структуру, ліцензії та сертифікати про акредитацію, навчальні та наукові структурні підрозділи та їх склад, правила прийому, контактна інформація тощо. **Навчально-методичне забезпечення освітньої діяльності** включає: навчальні плани; графіки - календарі освітнього процесу; робочі програми

	навчальних дисциплін; належне навчально-методичне забезпечення з кожного освітнього компоненту; дидактичні матеріали для самостійної та індивідуальної роботи здобувачів із навчальних дисциплін; методичні вказівки для самостійної роботи, виконання курсових та кваліфікаційних робіт; критерії оцінювання рівня підготовки; підручники, навчальні посібники, конспекти лекцій тощо згідно з переліком рекомендованої літератури з кожної навчальної дисципліни, кількість яких відповідає встановленим вимогам; методичні матеріали для проведення атестації здобувачів.
9 – Академічна мобільність	
Національна кредитна мобільність	Національна кредитна мобільність забезпечується на підставі вимог законодавства в сфері вищої освіти України.
Міжнародна кредитна мобільність	Міжнародна кредитна мобільність та міжнародне освітнє і науково-технічне співробітництво навчальних закладів забезпечується відповідно до підписаних міжнародних документів, зокрема меморандуму від 02.10.2015 р. про співробітництво ЖВІ з Військово-технологічною академією імені Ярослава Домбровського (Республіка Польща).
Навчання іноземних здобувачів вищої освіти	На підставі вимог законодавства в сфері вищої освіти України та у разі укладання міжнародних договорів (угод) із дотриманням режиму секретності.

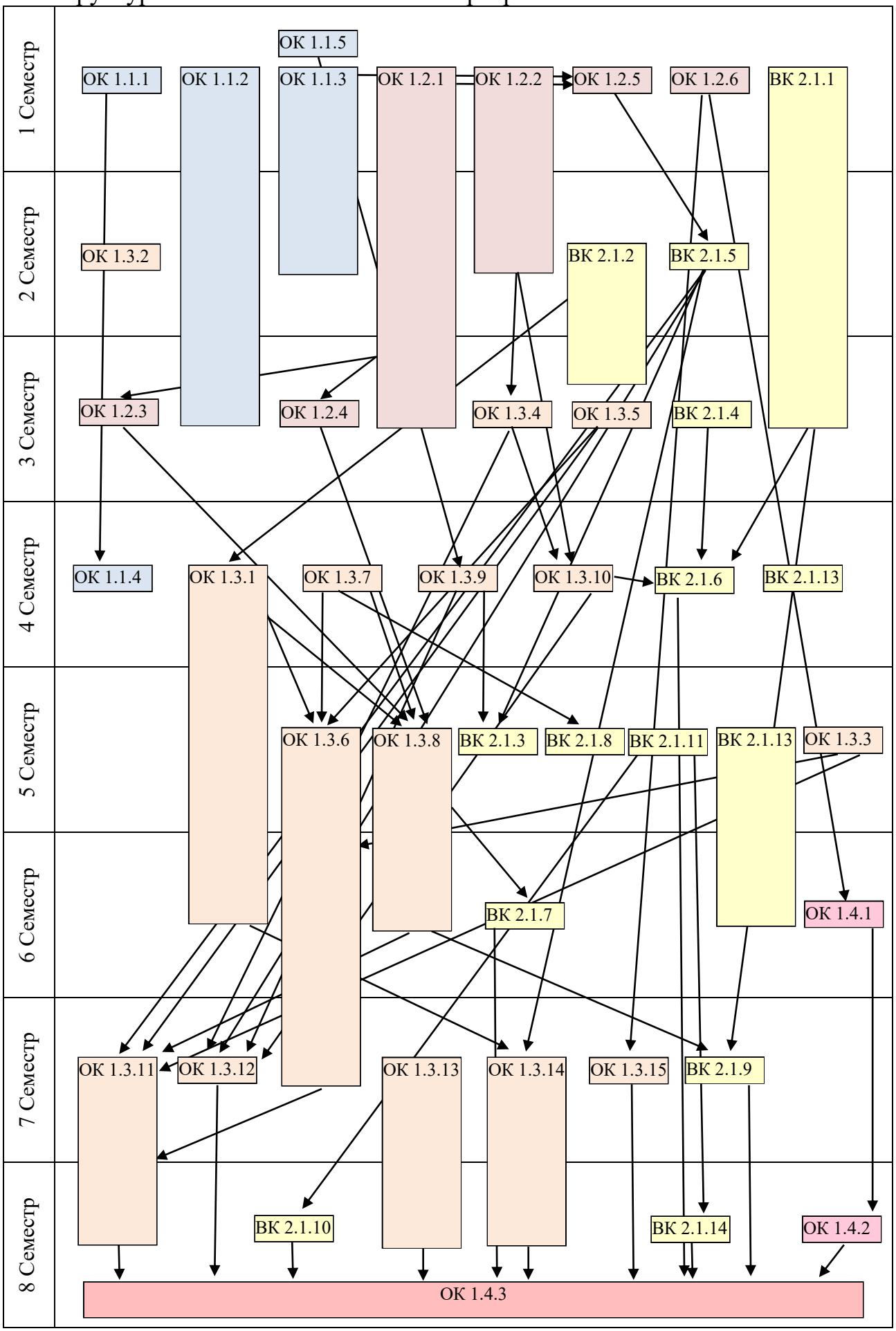
ІІ. ПЕРЕЛІК КОМПОНЕНТ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ ТА ЇХ ЛОГІЧНА ПОСЛІДОВНІСТЬ

2.1 Перелік компонент ОПП

Код н/дисц.	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
ОБОВ`ЯЗКОВІ КОМПОНЕНТИ ОП			
1. ЦИКЛ ЗАГАЛЬНОЇ ПІДГОТОВКИ			
ОК 1.1.1.	Історія України та українського війська	3,0	екзамен
ОК 1.1.2.	Іноземна мова	6,0	залік, екзамен
ОК 1.1.3.	Українська мова (за професійним спрямуванням)	3,0	залік, екзамен
ОК 1.1.4.	Філософія	3,0	екзамен
ОК 1.1.5.	Право та інтелектуальна власність	2,0	залік
ОК 1.2.1.	Вища математика	19,0	екзамен
ОК 1.2.2.	Фізика	11,0	екзамен
ОК 1.2.3.	Теорія ймовірності і математична статистика	4,0	екзамен
ОК 1.2.4.	Дискретна математика	3,5	залік
ОК 1.2.5.	Інформаційні технології	4,5	екзамен
ОК 1.2.6.	Екологія та безпека життєдіяльності	2,0	залік
2. ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ			
ОК 1.3.1.	Основи алгоритмізації та програмування в кібербезпеці	15	екзамен, залік, КР
ОК 1.3.2.	Основи теорії кіл, сигнали та процеси в кіберпросторі	4,0	залік
ОК 1.3.3.	Операційні системи	6,0	екзамен
ОК 1.3.4.	Електроніка і мікросхемотехніка засобів технічного захисту інформації	3,0	залік
ОК 1.3.5.	Архітектура комп`ютерних систем	3,0	екзамен
ОК 1.3.6.	Комп'ютерні мережі	13,0	екзамен, залік
ОК 1.3.7.	Теорія інформації та кодування	5,0	екзамен
ОК 1.3.8.	Прикладна криптологія	10,0	екзамен
ОК 1.3.9.	Нормативно-правове забезпечення технічного захисту інформації	3,0	залік
ОК 1.3.10	Системи технічного захисту інформації	9,0	екзамен, КР
ОК 1.3.11	Основи пентестінгу	8,0	екзамен, залік, КР
ОК 1.3.12	Комплексні системи захисту інформації: проектування, впровадження, супровід	4,0	екзамен
ОК 1.3.13	Управління кібербезпекою	7,0	екзамен, залік
ОК 1.3.14	Прикладні системи оцінювання ризиків в кібербезпеці	8,0	екзамен, залік, КР
ОК 1.3.15	Основи охорони праці	3,0	екзамен
ОК 1.4.1.	Виробнича практика	4,5	залік

ОК 1.4.2.	Переддипломна практика	4,5	залік
ОК 1.4.3.	Атестація	9,0	захист кваліфікаційної роботи
Загальний обсяг обов'язкових компонент:		**180**	
ВИБІРКОВІ КОМПОНЕНТИ ОПП			
ВК 2.1.1.	Вибіркова дисципліна 1	7,0	залік
ВК 2.1.2.	Вибіркова дисципліна 2	9,0	залік, екзамен, КР
ВК 2.1.3.	Вибіркова дисципліна 3	3,0	залік
ВК 2.1.4.	Вибіркова дисципліна 4	3,0	залік
ВК 2.1.5.	Вибіркова дисципліна 5	3,0	залік
ВК 2.1.6.	Вибіркова дисципліна 6	3,5	залік
ВК 2.1.7.	Вибіркова дисципліна 7	7,0	екзамен, КР
ВК 2.1.8.	Вибіркова дисципліна 8	4,0	екзамен
ВК 2.1.9.	Вибіркова дисципліна 9	7,5	екзамен
ВК 2.1.10	Вибіркова дисципліна 10	2,0	залік
ВК 2.1.11	Вибіркова дисципліна 11	2,0	залік
ВК 2.1.12	Вибіркова дисципліна 12	3,0	залік
ВК 2.1.13	Вибіркова дисципліна 13	3,0	залік
ВК 2.1.14	Вибіркова дисципліна 14	3,0	залік
ВК 2.2.1.	Вибіркова дисципліна 15	7,0	залік
ВК 2.2.2.	Вибіркова дисципліна 16	9,0	екзамен, залік, КР
ВК 2.2.3.	Вибіркова дисципліна 17	3,0	залік
ВК 2.2.4.	Вибіркова дисципліна 18	3,0	залік
ВК 2.2.5.	Вибіркова дисципліна 19	3,0	залік
ВК 2.2.6.	Вибіркова дисципліна 20	3,5	залік
ВК 2.2.7.	Вибіркова дисципліна 21	7,0	екзамен, КР
ВК 2.2.8.	Вибіркова дисципліна 22	4,0	екзамен
ВК 2.2.9.	Вибіркова дисципліна 23	7,5	екзамен
ВК 2.2.10.	Вибіркова дисципліна 24	2,0	залік
ВК 2.2.11.	Вибіркова дисципліна 25	2,0	залік
ВК 2.2.12.	Вибіркова дисципліна 26	3,0	залік
ВК 2.2.13.	Вибіркова дисципліна 27	3,0	залік
ВК 2.2.14.	Вибіркова дисципліна 28	3,0	залік
Загальний обсяг вибіркових компонент блоку 2		**60,0**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**240**	

2.2. Структурно-логічна схема освітньої програми



ІІІ. ФОРМА ВИПУСКНОЇ АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Атестація випускників за освітньою програмою “КІБЕРБЕЗПЕКА” спеціальності № 125 – Кібербезпека та захист інформації проводиться у формі єдиного державного кваліфікаційного іспиту. Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених стандартом вищої освіти України: перший (бакалаврський) рівень, галузь знань 12 – Інформаційні технології, спеціальність 125 – Кібербезпека та захист інформації та цією освітньою програмою.

У разі неуспішного складання кваліфікаційного іспиту особа вважається такою, що не виконала індивідуальний навчальний план та відраховується з Житомирського військового інституту імені С. П. Корольова відповідно до пункту 4 частини першої статті 46 Закону України “Про вищу освіту”. Таку особу може бути поновлено на навчання для однократного повторного складання кваліфікаційного іспиту.

Відповідно до постанови Кабінету міністрів України від 19 травня 2021 р. № 497 зі змінами у період воєнного стану та протягом одного року після його припинення або скасування атестація випускників за освітньою програмою “КІБЕРБЕЗПЕКА” спеціальності № 125 – Кібербезпека та захист інформації здійснюється без проведення єдиного державного кваліфікаційного іспиту у формі захисту кваліфікаційної роботи, яка має передбачати розв’язання спеціалізованої задачі в галузі кібербезпеки. Кваліфікаційна робота не повинна містити плагіату, фальсифікації та фабрикацій.

Роботи оприлюднюються на офіційному сайті військового інституту. Рішення щодо оприлюднення таких робіт приймається екзаменаційною комісією військового інституту із залученням представників режимно-секретного органу з дотриманням вимог законодавства України у сфері охорони державної таємниці.

Рішенням екзаменаційної комісії особі, яка успішно виконала освітню програму, присуджується ступінь вищої освіти *бакалавра*, присвоюється кваліфікація *“Бакалавр з кібербезпеки”* за спеціальністю *125 Кібербезпека та захист інформації* й спеціалізацією *121501 Організація захисту інформації та кібернетичної безпеки в інформаційно-телекомунікаційних системах*, а також видаються документи про вищу освіту державного зразка.

Рішення про присудження ступеня вищої освіти та присвоєння відповідної кваліфікації скасовується Житомирським військовим інститутом імені С. П. Корольова у разі виявлення фактів порушення здобувачем вищої освіти академічної доброчесності, зокрема наявності у бакалаврській роботі академічного плагіату, фабрикації, фальсифікації, у порядку, встановленому Кабінетом Міністрів України.

Атестація здійснюється відкрито та публічно з дотриманням вимог законодавства України у сфері охорони державної таємниці.

IV. МАТРИЦЯ ВІДПОВІДНОСТІ ПРОГРАМНИХ КОМПЕТЕНТНОСТЕЙ КОМПОНЕНТАМ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

	1. ОБОВ`ЯЗКОВІ НАВЧАЛЬНІ ДИСЦИПЛІНИ																													2. ВИБІРКОВІ НАВЧАЛЬНІ ДИСЦИПЛІНИ													
	ОК 1.1.1.	**ОК 1.1.2**	**ОК 1.1.3.**	**ОК 1.1.4.**	**ОК 1.1.5**	**ОК 1.2.1.**	**ОК 1.2.2.**	**ОК 1.2.3.**	**ОК 1.2.4**	**ОК 1.2.5.**	**ОК 1.2.6.**	**ОК 1.3.1.**	**ОК 1.3.2.**	**ОК 1.3.3.**	**ОК 1.3.4.**	**ОК 1.3.5.**	**ОК 1.3.6.**	**ОК 1.3.7.**	**ОК 1.3.8.**	**ОК 1.3.9.**	**ОК 1.3.10.**	**ОК 1.3.11.**	**ОК 1.3.12.**	**ОК 1.3.13.**	**ОК 1.3.14.**	**ОК 1.3.15.**	**ОК 1.4.1.**	**ОК 1.4.2.**	**ОК 1.4.3.**	**ВК 2.1.1.**	**ВК 2.1.2.**	**ВК 2.1.3.**	**ВК 2.1.4.**	**ВК 2.1.5.**	**ВК 2.1.6.**	**ВК 2.1.7.**	**ВК 2.1.8.**	**ВК 2.1.9.**	**ВК 2.1.10.**	**ВК 2.1.11**	**ВК 2.1.12.**	**ВК 2.1.13.**	**ВК 2.1.14**
КЗ 0	х	х	х	х	х	х	х	х	х	х	х	х	х	х	х	х	х	х	х	х	х	х	х	х	х	х	х	х			х		х									
КЗ 1										х	х	х		х							х	х				х																
КЗ 2											х								х		х	х											х									
КЗ 3		х	х																																				х		
КЗ 4					х							х	х	х	х	х	х	х	х	х	х	х											х					х				
КЗ 5								х	х	х		х		х								х																				
КЗ 6	х		х	х																х						х							х					х				
КЗ 7	х		х	х																																			х			
КФ 1																				х	х		х	х			х	х		х		х								х			
КФ 2																	х			х				х			х	х			х		х										
КФ 3																								х				х					х									
КФ 4																															х											
КФ 5																												х														

	1. ОБОВ`ЯЗКОВІ НАВЧАЛЬНІ ДИСЦИПЛІНИ																															2. ВИБІРКОВІ НАВЧАЛЬНІ ДИСЦИПЛІНИ													
	ОК 1.1.1.	**ОК 1.1.2**	**ОК 1.1.3.**	**ОК 1.1.4.**	**ОК 1.1.5**	**ОК 1.2.1.**	**ОК 1.2.2.**	**ОК 1.2.3.**	**ОК 1.2.4**	**ОК 1.2.5.**	**ОК 1.2.6.**	**ОК 1.3.1.**	**ОК 1.3.2.**	**ОК 1.3.3.**	**ОК 1.3.4.**	**ОК 1.3.5.**	**ОК 1.3.6.**	**ОК 1.3.7.**	**ОК 1.3.8.**	**ОК 1.3.9.**	**ОК 1.3.10.**	**ОК 1.3.11.**	**ОК 1.3.12.**	**ОК 1.3.13.**	**ОК 1.3.14.**	**ОК 1.3.15.**	**ОК 1.4.1.**	**ОК 1.4.2.**	**ОК 1.4.3.**	**ВК 2.1.1.**	**ВК 2.1.2.**	**ВК 2.1.3.**	**ВК 2.1.4.**	**ВК 2.1.5.**	**ВК 2.1.6.**	**ВК 2.1.7.**	**ВК 2.1.8.**	**ВК 2.1.9.**	**ВК 2.1.10.**	**ВК 2.1.11**	**ВК 2.1.12.**	**ВК 2.1.13.**	**ВК 2.1.14**
КФ 6	X																X						X				X															
КФ 7																				X			X			X	X															
КФ 8																							X	X			X															
КФ 9																					X		X	X		X	X	X							X							
КФ 10								X	X										X				X			X	X															
КФ 11																					X	X	X		X			X			X				X							
КФ 12						X	X			X														X	X			X															
КФ 13																						X	X						X				X									
КФ 14																																					X					
КФ 15																														X						X	X				
КФ 16												X																		X								X			
КФ 17											X														X																	
КФ 18																																					X	X			X

V. МАТРИЦЯ ЗАБЕЗПЕЧЕННЯ ПРОГРАМНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ ВІДПОВІДНИМИ КОМПОНЕНТАМИ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

	1. ОБОВ`ЯЗКОВІ НАВЧАЛЬНІ ДИСЦИПЛІНИ																																	2. ВИБІРКОВІ НАВЧАЛЬНІ ДИСЦИПЛІНИ													
	ОК 1.1.1.	ОК 1.1.3.	ОК 1.1.4.	ОК 1.1.5.	ОК 1.1.6	ОК 1.2.1.	ОК 1.2.2.	ОК 1.2.3.	ОК 1.2.4	ОК 1.2.5.	ОК 1.2.6.	ОК 1.3.1.	ОК 1.3.2.	ОК 1.3.3.	ОК 1.3.4.	ОК 1.3.5.	ОК 1.3.6.	ОК 1.3.7.	ОК 1.3.8.	ОК 1.3.9.	ОК 1.3.10.	ОК 1.3.11.	ОК 1.3.12.	ОК 1.3.13.	ОК 1.3.14.	ОК 1.3.15.	ОК 1.4.1.	ОК 1.4.2.	ОК 1.4.3.	ВК 2.1.1.	ВК 2.1.2.	ВК 2.1.3.	ВК 2.1.4.	ВК 2.1.5.	ВК 2.1.6.	ВК 2.1.7.	ВК 2.1.8.	ВК 2.1.9.	ВК 2.1.11.	ВК 2.1.12.	ВК 2.1.13.	ВК 2.1.14.	ВК 2.1.15
РН 1		X	X																																						X	
РН 2					X	X				X																X	X	X														
РН 3																										X	X	X														
РН 4								X																							X											
РН 5																											X															
РН 6																										X	X															
РН 7					X																										X										
РН 8			X																																						
РН 9		X																		X					X																X	
РН 10														X		X	X																									
РН 11																						X																				X
РН 12																						X		X										X								X
РН 13																	X																									

	1. ОБОВ`ЯЗКОВІ НАВЧАЛЬНІ ДИСЦИПЛІНИ																													2. ВИБІРКОВІ НАВЧАЛЬНІ ДИСЦИПЛІНИ													
	ОК 1.1.1.	**ОК 1.1.3.**	**ОК 1.1.4.**	**ОК 1.1.5.**	**ОК 1.1.6**	**ОК 1.2.1.**	**ОК 1.2.2.**	**ОК 1.2.3.**	**ОК 1.2.4**	**ОК 1.2.5.**	**ОК 1.2.6.**	**ОК 1.3.1.**	**ОК 1.3.2.**	**ОК 1.3.3.**	**ОК 1.3.4.**	**ОК 1.3.5.**	**ОК 1.3.6.**	**ОК 1.3.7.**	**ОК 1.3.8.**	**ОК 1.3.9.**	**ОК 1.3.10.**	**ОК 1.3.11.**	**ОК 1.3.12.**	**ОК 1.3.13.**	**ОК 1.3.14.**	**ОК 1.3.15.**	**ОК 1.4.1.**	**ОК 1.4.2.**	**ОК 1.4.3.**	**ВК 2.1.1.**	**ВК 2.1.2.**	**ВК 2.1.3.**	**ВК 2.1.4.**	**ВК 2.1.5.**	**ВК 2.1.6.**	**ВК 2.1.7.**	**ВК 2.1.8.**	**ВК 2.1.9.**	**ВК 2.1.11.**	**ВК 2.1.12.**	**ВК 2.1.13.**	**ВК 2.1.14.**	**ВК 2.1.15**
РН 14																						X		X																			
РН 15														X		X																										
РН 16																							X																			
РН 17															X		X	X																			X					
РН 18																					X																				
РН 19																			X					X									X X								
РН 20		X											X																												X	
РН 21																					X	X																				
РН 22																			X					X									X									
РН 23																				X	X	X															X					
РН 24																			X													X		X								
РН 25									X								X																									
РН 26																	X																									
РН 27																										X																

	1. ОБОВ`ЯЗКОВІ НАВЧАЛЬНІ ДИСЦИПЛІНИ																													2. ВИБІРКОВІ НАВЧАЛЬНІ ДИСЦИПЛІНИ													
	ОК 1.1.1.	ОК 1.1.3.	ОК 1.1.4.	ОК 1.1.5.	ОК 1.1.6	ОК 1.2.1.	ОК 1.2.2.	ОК 1.2.3.	ОК 1.2.4	ОК 1.2.5.	ОК 1.2.6.	ОК 1.3.1.	ОК 1.3.2.	ОК 1.3.3.	ОК 1.3.4.	ОК 1.3.5.	ОК 1.3.6.	ОК 1.3.7.	ОК 1.3.8.	ОК 1.3.9.	ОК 1.3.10.	ОК 1.3.11.	ОК 1.3.12.	ОК 1.3.13.	ОК 1.3.14.	ОК 1.3.15.	ОК 1.4.1.	ОК 1.4.2.	ОК 1.4.3.	ВК 2.1.1.	ВК 2.1.2.	ВК 2.1.3.	ВК 2.1.4.	ВК 2.1.5.	ВК 2.1.6.	ВК 2.1.7.	ВК 2.1.8.	ВК 2.1.9.	ВК 2.1.11.	ВК 2.1.12.	ВК 2.1.13.	ВК 2.1.14.	ВК 2.1.15
РН 28																						X																					
РН 29																							X																				
РН 30																						X	X		X										X								
РН 31																																					X						
РН 32																			X														X									
РН 33																			X	X													X									
РН 34																								X																		
РН 35																							X																				
РН 36							X						X		X						X											X											
РН 37							X						X		X						X											X											
РН 38																				X	X																						
РН 39			X																		X																						
РН 40			X																		X																						
РН 41														X										X																			

	1. ОБОВ`ЯЗКОВІ НАВЧАЛЬНІ ДИСЦИПЛІНИ																												2. ВИБІРКОВІ НАВЧАЛЬНІ ДИСЦИПЛІНИ													
	ОК 1.1.1.	**ОК 1.1.3.**	**ОК 1.1.4.**	**ОК 1.1.5.**	**ОК 1.1.6**	**ОК 1.2.1.**	**ОК 1.2.2.**	**ОК 1.2.3.**	**ОК 1.2.4**	**ОК 1.2.5.**	**ОК 1.2.6.**	**ОК 1.3.1.**	**ОК 1.3.2.**	**ОК 1.3.3.**	**ОК 1.3.4.**	**ОК 1.3.5.**	**ОК 1.3.6.**	**ОК 1.3.7.**	**ОК 1.3.8.**	**ОК 1.3.9.**	**ОК 1.3.10.**	**ОК 1.3.11.**	**ОК 1.3.12.**	**ОК 1.3.13.**	**ОК 1.3.14.**	**ОК 1.3.15.**	**ОК 1.4.1.**	**ОК 1.4.2.**	**ОК 1.4.3.**	**ВК 2.1.1.**	**ВК 2.1.2.**	**ВК 2.1.3.**	**ВК 2.1.4.**	**ВК 2.1.5.**	**ВК 2.1.6.**	**ВК 2.1.7.**	**ВК 2.1.8.**	**ВК 2.1.9.**	**ВК 2.1.11.**	**ВК 2.1.12.**	**ВК 2.1.13.**	**ВК 2.1.14.**	**ВК 2.1.15**
РН 42																								X																	
РН 43		X	X																X				X																	X	
РН 44		X	X					X																															X	
РН 45																		X															X							
РН 46								X																																	
РН 47									X																													X			
РН 48									X																													X			
РН 49																		X					X	X																
РН 50																																									
РН 51																						X																			
РН 52										X		X							X		X				X					X			X		X						
РН 53																		X												X											
РН 54	X			X							X														X												X	X	X		X
РН 55																						X			X																

	1. ОБОВ`ЯЗКОВІ НАВЧАЛЬНІ ДИСЦИПЛІНИ																													2. ВИБІРКОВІ НАВЧАЛЬНІ ДИСЦИПЛІНИ													
	ОК 1.1.1.	ОК 1.1.3.	ОК 1.1.4.	ОК 1.1.5.	ОК 1.1.6	ОК 1.2.1.	ОК 1.2.2.	ОК 1.2.3.	ОК 1.2.4	ОК 1.2.5.	ОК 1.2.6.	ОК 1.3.1.	ОК 1.3.2.	ОК 1.3.3.	ОК 1.3.4.	ОК 1.3.5.	ОК 1.3.6.	ОК 1.3.7.	ОК 1.3.8.	ОК 1.3.9.	ОК 1.3.10.	ОК 1.3.11.	ОК 1.3.12.	ОК 1.3.13.	ОК 1.3.14.	ОК 1.3.15.	ОК 1.4.1.	ОК 1.4.2.	ОК 1.4.3.	ВК 2.1.1.	ВК 2.1.2.	ВК 2.1.3.	ВК 2.1.4.	ВК 2.1.5.	ВК 2.1.6.	ВК 2.1.7.	ВК 2.1.8.	ВК 2.1.9.	ВК 2.1.11.	ВК 2.1.12.	ВК 2.1.13.	ВК 2.1.14.	ВК 2.1.15
РН 56																																										X
РН 57																							X																			
РН 58																							X																X			X
РН 59																							X																			
РН 60																																X				X						
РН 61																														X												
Н 62																														X												
РН 63																																X										
РН 64																													X					X								
РН 65																																		X								
РН 66																														X					X							
РН 67																																			X							
РН 68														X			X																									
РН 69																																								X		

Технічні зміни
до освітньої програми КІБЕРБЕЗПЕКА за спеціальністю
125 Кібербезпека та захист інформації

Відповідно до постанови Кабінету міністрів України від 16 грудня 2022 р. № 1392 "Про внесення змін до переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти" назву спеціальності 125 Кібербезпека в освітній програмі КІБЕРБЕЗПЕКА замінено на 125 Кібербезпека та захист інформації.

Гарант освітньої програми КІБЕРБЕЗПЕКА за спеціальністю 125 Кібербезпека,
кандидат технічних наук, старший дослідник
полковник Олексій САМЧИШИН