МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ

Житомирський військовий інститут імені С. П. Корольова

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

Кібербезпека
(назва)

Перший (бакалаврський) рівень
(рівень вищої освіти)

Галузь знань	F Інформаційні технології
Спеціальність	F5 Кібербезпека та захист інформації
Кваліфікація	Бакалавр з кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО
Вченою радою Житомирського військового інституту імені С. П. Корольова

(протокол від "24" 07 2025 року № 19)

Голова Вченої ради Житомирського військового інституту імені С. П. Корольова
полковник

Андрій СЛЮСАРЕНКО

Введено в дію
наказом начальника Житомирського військового інституту імені С. П. Корольова
від "28" 07 2025 року № 527

Житомир
2025

АРКУШ ПОГОДЖЕННЯ
ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

Кібербезпека

(назва)

Перший (бакалаврський) рівень
(рівень вищої освіти)

Галузь знань	F Інформаційні технології
Спеціальність	F5 Кібербезпека та захист інформації
Кваліфікація	Бакалавр з кібербезпеки та захисту інформації

ПОГОДЖЕНО

Тимчасово виконуючий обов'язки
директора Департаменту військової
освіти і науки Міністерства оборони
України
полковник

Максим КАС'ЯНЕНКО

"09" 04 2025 року

ІНФОРМАЦІЙНИЙ АРКУШ
про внесення змін до освітньо-професійної програми

Кібербезпека
(назва)

Перший (бакалаврський) рівень
(рівень вищої освіти)

Галузь знань	F Інформаційні технології
Спеціальність	F5 Кібербезпека та захист інформації
Кваліфікація	Бакалавр з кібербезпеки та захисту інформації

Зміни внесено відповідно до:
рішення Вченої ради Житомирського військового інституту імені С. П. Корольова (протокол від “___” _____20__ року №__) та введено в дію наказом начальника Житомирського військового інституту імені С. П. Корольова від “___” _____20__ року №___; Освітньо-професійна програма оновлена та викладено із змінами.

ПЕРЕДМОВА

Розроблено робочою групою у складі:

Голова робочої групи-	
Охрімчук Володимир Васильович	кандидат технічних наук, доцент, професор кафедри комп'ютерно-інтегрованих технологій та кібербезпеки
Заступник голови робочої групи	
Чернишук Сергій Вікторович	кандидат технічних наук, доцент кафедри комп'ютерно-інтегрованих технологій та кібербезпеки
Члени робочої групи:	
Жовноватюк Руслан Михайлович	кандидат технічних наук, старший науковий співробітник, начальник кафедри комп'ютерно-інтегрованих технологій та кібербезпеки
Манько Олег Віталійович	кандидат технічних наук, старший науковий співробітник, заступник начальника кафедри комп'ютерно-інтегрованих технологій та кібербезпеки
Гуменюк Ігор Володимирович	кандидат технічних наук, доцент, професор кафедри охорони державної таємниці та захисту інформації
Сметанін Кирило Володимирович	кандидат технічних наук, доцент, професор кафедри радіоелектронної боротьби
Жуков Анатолій Олексійович	старший викладач кафедри комп'ютерно-інтегрованих технологій та кібербезпеки
Кошева Ірина Геннадіївна	викладач кафедри комп'ютерно-інтегрованих технологій та кібербезпеки
Атаманчук Тетяна Йосипівна	викладач кафедри комп'ютерно-інтегрованих технологій та кібербезпеки

Склад робочої групи по розробленню освітньо-професійної програми створено у Житомирському військовому інституті імені С. П. Корольова.

Наказ начальника Житомирського військового інституту імені С. П. Корольова від "13" червня 2025 року №425.

Гарант освітньої програми:

професор кафедри комп'ютерно-інтегрованих технологій та кібербезпеки, кандидат технічних наук, доцент підполковник Охрімчук Володимир Васильович.

Враховано:

1. Закон України від 01.07.2015 №1556 “Про вищу освіту” (зі змінами).
2. Наказ Міністерства освіти і науки України від 29.10.2024 № 1547 “Про внесення змін до стандарту вищої освіти зі спеціальності 125 «Кібербезпека» для першого (бакалаврського) рівня вищої освіти”.
3. Наказ Міністерства освіти і науки України від 15.05.2024 №686 “Про затвердження Положення про акредитацію освітніх програм, за яким здійснюється підготовка здобувачів вищої освіти.
4. Статут Національного агенства із забезпечення якості вищої освіти.
5. Статут Житомирського військового інституту імені С. П. Корольова та інші акти законодавства.
6. Постанова Кабінету Міністрів України від 30 серпня 2024 р. № 1021 “Про внесення змін до переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої та фахової передвищої освіти” та інших актів законодавства.

1. ПРОФІЛЬ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПОГРАМИ

зі спеціальності F5 Кібербезпека та захист інформації

1 – Загальна інформація	
Повна назва закладу вищої освіти та структурного підрозділу	Житомирський військовий інститут імені С. П. Корольова (далі - ЖВІ) факультет інформаційних технологій та інженерії кафедра інформаційних технологій та кібербезпеки
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Ступінь вищої освіти: бакалавр Освітня кваліфікація: бакалавр з кібербезпеки та захисту інформації
Назва освітньої програми	Кібербезпека
Тип освітньої програми	Освітньо-професійна програма, 240 кредитів ЄКТС, термін навчання 4 роки.
Тип диплому	Диплом бакалавра, одиничний.
Наявність акредитації	Акредитована Міністерством освіти і науки України. Сертифікат акредитації від 30 червня 2021 р. № 1925
Рівень з НРК	НРК України – 6 рівень, FQ-EHEA – перший цикл, EQF-LLL – 6 рівень
Передумови	Умови вступу визначаються «Правилами прийому до Житомирського військового інституту імені С. П. Корольова», затвердженими Вченою радою Наявність повної загальної середньої освіти/ освітньо-кваліфікаційного рівня молодшого спеціаліста/ освітньо-професійний ступінь фахового молодшого бакалавра/ освітній ступінь молодший бакалавр
Мова (мови) викладання	Українська
Термін дії освітньої програми	Термін дії освітньої програми до 01 липня 2029 р.
Інтернет-адреса постійного розміщення освітньої програми	https://kzmi.mil.gov.ua/uk/osvita/akredytatsiia-osvitnikh-prohram.html
2 – Цілі 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-комунікаційних системах в інтересах забезпечення кібероборони держави.	
3 – Характеристика освітньої програми	
Предметна область	Об’єкти вивчення: технології кібербезпеки та захисту інформації; процеси управління кібербезпекою та захистом інформації; об'єкти інформаційної діяльності, в тому числі інформаційні та інформаційно-комунікаційні системи, інформаційні ресурси і технології. Теоретичний зміст: принципи, концепції, теорії захисту життєво важливих інтересів людини, суспільства, держави під час використання кіберпростору, за якого забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі. Методи, методики та технології, які використовуються: методи, методики та технології розв'язання теоретичних і практичних задач кібербезпеки та захисту інформації. Інструменти та обладнання, які випускник повинен вміти використовувати: засоби, пристрої, мережне устаткування, прикладне та спеціалізоване програмне забезпечення, інформаційні системи та комплекси проектування, моделювання, контролю, моніторингу, зберігання, обробки, відображення та захисту даних (інформаційних потоків).
Орієнтація ОПП	Освітньо-професійна.
Основний фокус освітньої програми та спеціалізації	Підготовка фахівців, здатних використовувати і впроваджувати технології кібербезпеки та захисту інформації та розв'язувати складні задачі у галузі кібербезпеки та захисту інформації. Програма формує базові компетентності для подальшого професійного розвитку та навчання.
Особливості програми	**а) по-перше, міжнародний вектор спрямованості освітньої програми гарантує:** – 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 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; **д) по-п'яте, <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; **е) по-шосте, <u>100% працевлаштування випускників</u>;** **ж) по-сьоме, <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>** **з) по-восьме, потужна та сучасна матеріально-технічна база за місцем постійної дислокації;** **н) по-десяте, спадковість програми**, адже підготовка здобувачів вищої освіти 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 у Житомирському військовому інституті починаючи з 2007 року.
4 – Можливості 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, всі випускники придатні до працевлаштування за здобутою спеціальністю на посадах, які передбачають наявність вищої випускників освіти зі спеціальності F5 – Кібербезпека та захист інформації.

Процедури присвоєння професійних кваліфікацій	Присвоєння професійної кваліфікації здійснюється відповідно до вимог Закону України «Про вищу освіту» та стандарту вищої освіти за спеціальністю 125 «Кібербезпека» для першого (бакалаврського) рівня, затвердженого наказом Міністерства освіти і науки України від 29.10.2024 № 1547. Освітньо-професійна програма базується на положеннях стандарту вищої освіти, який визначає обов'язкові компетентності та програмні результати навчання, необхідні для присвоєння кваліфікації. Кваліфікація присвоюється за результатами успішного виконання освітньої програми та успішного складання єдиного державного кваліфікаційного іспиту (захисту кваліфікаційної роботи).
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 в системі військової освіти і підготовки ЗС України.
5 – Викладання та оцінювання	
Викладання та навчання	Освітній процес організовано **на засадах студентоцентрованого підходу** 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. **В основу навчання покладено сучасні дидактичні принципи,** 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 організацію освітнього процесу Житомирського військового інституту імені С. П. Корольова, Положення про контрольні заходи і систему оцінювання результатів навчання здобувачів освіти у Житомирському військовому інституті імені С. П. Корольова, Положення про академічну доброчесність Житомирського військового інституту імені С. П. Корольова 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:** екзамен, залік, усне та письмове опитування, тестові завдання, лабораторні звіти, презентації, захист курсових робіт та проєктів, звітів з практик. **Атестація:** Атестація випускників здійснюється у формі єдиного кваліфікаційного іспиту. Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених стандартом вищої освіти України: перший (бакалаврський) рівень, галузь знань F – Інформаційні технології, спеціальність F5 – 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.

6 – Програмні компетентності	
Інтегральна компетентність (ІК) (визначена стандартом вищої освіти)	Здатність розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації.
Загальні компетентності (ЗК) (визначені стандартом вищої освіти)	ЗК 1. Здатність застосовувати знання у практичних ситуаціях
	ЗК 2. Знання та розуміння предметної області і розуміння професійної діяльності
	ЗК 3. Здатність спілкуватися державною мовою як усно, так і письмово.
	ЗК 4 Здатність спілкуватися іноземною мовою.
	ЗК 5. Здатність вчитися і оволодівати сучасними знаннями.
	ЗК 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 та свобод людини і громадянина в Україні.
	ЗК 7. Здатність ухвалювати рішення й діяти дотримуючись принципу неприпустимості корупції та будь-яких інших | проявів недоброчесності.
	ЗК 8. 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
Спеціальні (фахові, предметні) компетентності (визначені стандартом вищої освіти)	СК 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності.
	СК 2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації.
	СК 3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації.
	СК 4. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних

	системах згідно встановленої політики кібербезпеки й захисту інформації.
	СК 5. Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження.
	СК 6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо).
	СК 7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.
	СК 8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.
	СК 9. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності.
	СК 10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози з інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.
7 – Програмні результати навчання	
Загальна та спеціальна (фахова) підготовка	РН 1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.
	РН 2: Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.
	РН 3: Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності.
	РН 4: Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.
	РН 5: Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

	РН 6: Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.
	РН 7: Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.
	РН 8: Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення.
	РН 9: Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.
	РН 10: Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.
	РН 11: Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації.
	РН 12: Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.
	РН 13: Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та/або інфраструктури організації в цілому.
	РН 14: Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації.

	РН 15: Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.
	РН 16: Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.
	РН 17: Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.
	РН 18: Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.
	РН 19: Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.
	РН 20: Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації.
	РН 21: Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.
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.

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.

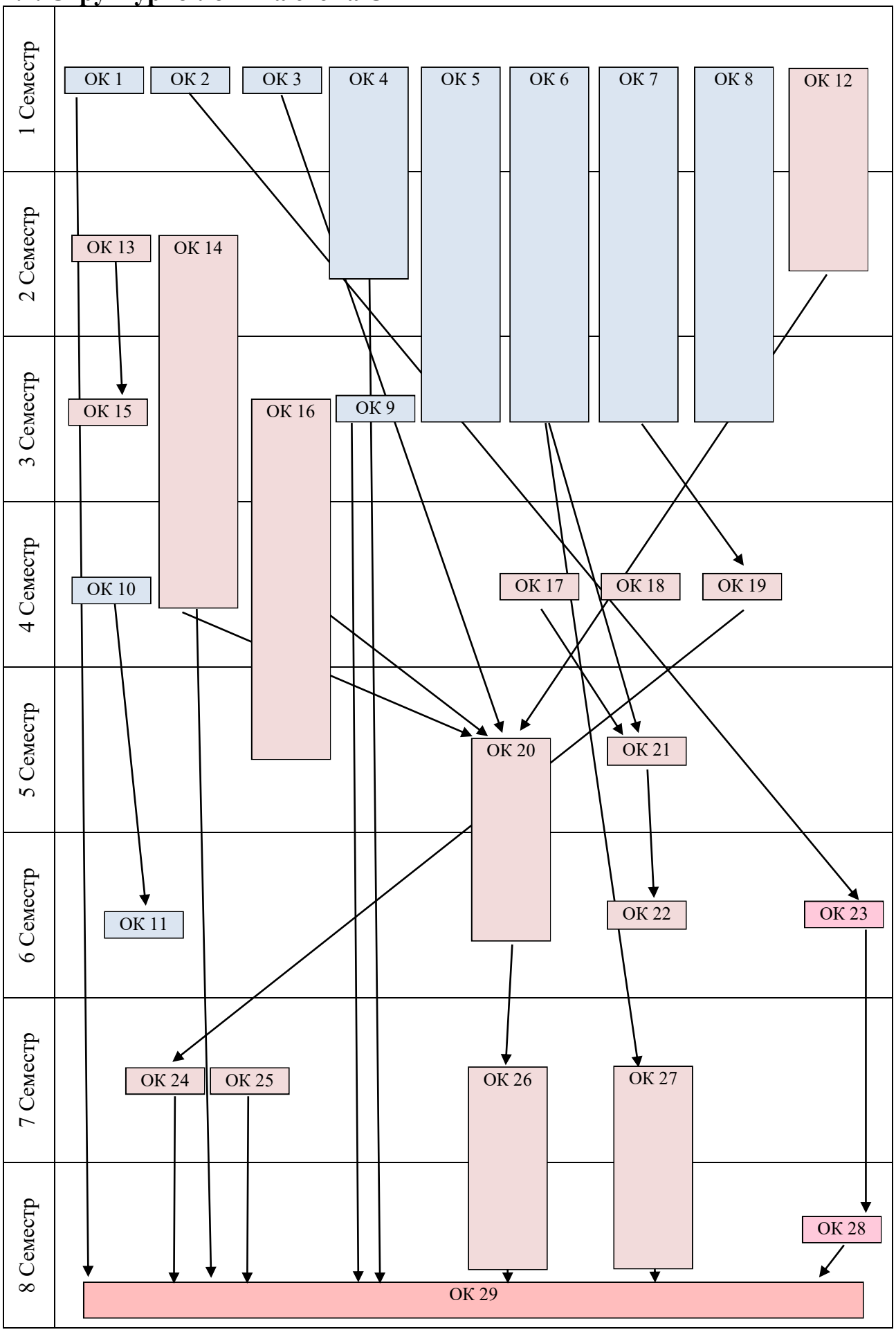
2. ПЕРЕЛІК ОБОВ'ЯЗКОВИХ КОМПОНЕНТ ЇХ ЛОГІЧНА ПОСЛІДОВНІСТЬ

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 ОПП			
Цикл загальної підготовки			
ОК 1	Історія України та українського війська	3,0	екзамен
ОК 2	Екологія та безпека життєдіяльності	2,0	залік
ОК 3	Інформаційні технології	3,0	залік
ОК 4	Українська мова (за професійним спрямуванням)	3,0	залік, екзамен
ОК 5	Іноземна мова	6,0	залік, екзамен
ОК 6	Вища математика	19,0	залік, екзамен
ОК 7	Загальна фізика	13,0	екзамен
ОК 8	Інженерна та комп`ютерна графіка	6,0	залік
ОК 9	Лідерство в професійній діяльності	3,0	залік
ОК 10	Філософія	3,0	екзамен
ОК 11	Політологія та соціологія	4,0	екзамен
Обсяг загальної підготовки		**65**	
Цикл професійної підготовки			
ОК 12	Архітектура комп'ютерних та операційних систем	6,0	екзамен, залік
ОК 13	Основи теорії кіл, сигнали та процеси в кібербезпеці	2,5	залік
ОК 14	Основи алгоритмізації та програмування в кібербезпеці	14,0	залік, екзамен, КР
ОК 15	Електроніка і мікросхемотехніка засобів технічного захисту інформації	3,0	залік
ОК 16	Комп'ютерні мережі	12,0	залік, екзамен, КР
ОК 17	Спеціальні розділи математики	4,0	залік
ОК 18	Теорія інформації та кодування	5,0	екзамен
ОК 19	Системи технічного захисту інформації	5,5	екзамен, КР
ОК 20	Кібербезпека ІКС	14,0	залік, екзамен
ОК 21	Прикладна криптологія	5,0	залік
ОК 22	Криптографічний захист інформації в ІКС	5,0	екзамен
ОК 23	Виробнича практика	4,5	залік
ОК 24	Проєктування комплексних системи захисту інформації	4,0	екзамен
ОК 25	Основи охорони праці	3,0	екзамен
ОК 26	Управління кібербезпекою	7,0	залік, екзамен
ОК 27	Теорія ризиків в кібербезпеці	7,0	залік, екзамен, КР
ОК 28	Переддипломна практика	4,5	залік

ОК 29	Атестація (Дипломне проєктування)	9,0	ЄДКІ (захист кваліфікаційної роботи)
Обсяг професійної підготовки		**115**	
Загальний обсяг обов'язкових компонент:		**180**	
ВИБІРКОВІ КОМПОНЕНТИ ОПП			
ВК 1.1	Вибіркова дисципліна 1	3,0	залік
ВК 1.2	Вибіркова дисципліна 2	3,0	залік
ВК 2.1	Вибіркова дисципліна 3	3,0	залік
ВК 2.2	Вибіркова дисципліна 4	3,0	залік
ВК 3.1	Вибіркова дисципліна 5	4,0	залік
ВК 3.2	Вибіркова дисципліна 6	4,0	залік
ВК 4.1	Вибіркова дисципліна 7	4,0	екзамен
ВК 4.2	Вибіркова дисципліна 8	4,0	екзамен
ВК 5.1	Вибіркова дисципліна 9	6,5	залік
ВК 5.2	Вибіркова дисципліна 10	6,5	залік
ВК 6.1	Вибіркова дисципліна 11	3,0	залік
ВК 6.2	Вибіркова дисципліна 12	3,0	залік
ВК 7.1	Вибіркова дисципліна 13	3,0	залік
ВК 7.2	Вибіркова дисципліна 14	3,0	залік
ВК 8.1	Вибіркова дисципліна 15	8,0	екзамен, КР
ВК 8.2	Вибіркова дисципліна 16	8,0	екзамен
ВК 9.1	Вибіркова дисципліна 17	4,0	залік
ВК 9.2	Вибіркова дисципліна 18	4,0	залік
ВК 10.1	Вибіркова дисципліна 19	7,5	екзамен
ВК 10.2	Вибіркова дисципліна 20	7,5	екзамен
ВК 11.1	Вибіркова дисципліна 21	11,0	залік, екзамен, КР
ВК 11.2	Вибіркова дисципліна 22	11,0	залік, екзамен, КР
ВК 12.1	Вибіркова дисципліна 23	3,0	залік
ВК 12.2	Вибіркова дисципліна 24	3,0	залік
Загальний обсяг вибіркових компонент		**60,0**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**240**	

2.2. Структурно-логічна схема ОПП



3. ФОРМА (ФОРМИ) АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Атестація випускників за освітньою програмою “КІБЕРБЕЗПЕКА” спеціальності F5 – 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 F – Інформаційні технології, спеціальність F5 – 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 F5 – 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.

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 та захисту інформації”* за спеціальністю *F5 Кібербезпека та захист інформації*, 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.

4. МАТРИЦЯ ВІДПОВІДНОСТІ ПРОГРАМНИХ КОМПЕТЕНТНОСТЕЙ КОМПОНЕНТАМ ОСВІТНЬ-ПРОФЕСІЙНОЇ ПРОГРАМИ

4.1 Обов'язкові компоненти

	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6.	ОК 7	ОК 8	ОК 9	ОК 10	ОК 11	ОК 12	ОК 13	ОК 14	ОК 15	ОК 16	ОК 17	ОК 18	ОК 19	ОК 20	ОК 21	ОК 22	ОК 23	ОК 24	ОК 25	ОК 26	ОК 27	ОК 28	ОК 29
ІК	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ЗК1		+							+	+			+	+				+		+			+					+	+
ЗК 2		+							+	+													+		+			+	+
ЗК 3	+			+																									
ЗК 4					+																								
ЗК 5						+	+										+												
ЗК 6	+										+																		
ЗК 7	+										+																		
ЗК 8		+											+	+				+		+					+				
СК 1											+																		
СК 2			+					+						+															
СК 3																				+						+			
СК 4												+				+			+	+									
СК 5												+								+									
СК 6																								+					
СК 7																										+	+		
СК 8																					+	+							
СК 9															+				+										
СК 10																							+						

4.2 Вибіркові компоненти

	ВК 1	ВК 2	ВК 3	ВК 4	ВК 5	ВК 6	ВК 7	ВК 8	ВК 9	ВК 10	ВК 11	ВК 12	ВК 13	ВК 14	ВК 15	ВК 16	ВК 17	ВК 18	ВК 19	ВК 20	ВК 21	ВК 22	ВК 23	ВК 24
ІК	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ЗК1										+		+										+		+
ЗК 2						+						+						+						+
ЗК 3																								
ЗК 4							+												+					
ЗК 5																								
ЗК 6			+												+									
КЗ 7																								
ЗК 8						+				+								+				+		
СК 1			+												+									
СК 2																								
СК 3		+			+									+			+							
СК 4				+				+								+				+				
СК 5								+												+				
СК 6									+												+			
СК 7																								
СК 8																								
СК 9	+												+											
СК 10											+												+	

5. МАТРИЦЯ ЗАБЕЗПЕЧЕННЯ ПРОГРАМНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ ВІДПОВІДНИМИ КОМПОНЕНТАМИ ОСВІТНЬ-ПРОФЕСІЙНОЇ ПРОГРАМИ

5.1 Обов'язкові компоненти

	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6.	ОК 7	ОК 8	ОК 9	ОК 10	ОК 11	ОК 12	ОК 13	ОК 14	ОК 15	ОК 16	ОК 17	ОК 18	ОК 19	ОК 20	ОК 21	ОК 22	ОК 23	ОК 24	ОК 25	ОК 26	ОК 27	ОК 28	ОК 29
РН 1	+			+																									
РН 2					+																								
РН 3	+										+																		
РН 4		+							+														+					+	
РН 5										+																			+
РН 6		+																							+				
РН 7													+	+				+		+									
РН 8						+	+										+												
РН 9											+																		
РН 10			+					+						+															
РН 11																				+						+			
РН 12																+			+	+									
РН 13												+				+				+									
РН 14												+								+									
РН 15																				+									
РН 16																								+					
РН 17																										+	+		
РН 18																					+	+							
РН 19																					+	+							
РН 20															+				+										
РН 21																							+						

5.2 Вибіркові компоненти

	ВК 1	ВК 2	ВК 3	ВК 4	ВК 5	ВК 6	ВК 7	ВК 8	ВК 9	ВК 10	ВК 11	ВК 12	ВК 13	ВК 14	ВК 15	ВК 16	ВК 17	ВК 18	ВК 19	ВК 20	ВК 21	ВК 22	ВК 23	ВК 24
РН 1																								
РН 2							+												+					
РН 3																								
РН 4																								
РН 5												+												+
РН 6						+												+						
РН 7										+												+		
РН 8																								
РН 9			+												+									
РН 10																								
РН 11		+			+									+			+							
РН 12								+												+				
РН 13				+												+								
РН 14								+												+				
РН 15								+												+				
РН 16									+												+			
РН 17																								
РН 18																								
РН 19																								
РН 20	+												+											
РН 21											+												+	

РЕЦЕНЗІЯ-ВІДГУК
на освітньо-професійну програму

Кібербезпека

(назва)

Перший (бакалаврський) рівень
(рівень вищої освіти)

За спеціальністю F5 Кібербезпека та захист інформації