МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ

Житомирський військовий інститут імені С. П. Корольова

ЗАТВЕРДЖУЮ
Начальник Житомирського військового інституту імені С. П. Корольова
Заслужений діяч науки і техніки України,
доктор військових наук, професор
генерал-майор

О. ЛЕВЧЕНКО

"28". 08 2020 року

ОСВІТНЯ ПРОГРАМА
"КІБЕРБЕЗПЕКА"

Рівень вищої освіти:	*Перший (бакалаврський) рівень*
Ступінь, що присвоюється:	*Бакалавр*
Назва галузі знань	*12 Інформаційні технології*
Назва спеціальності	*125 Кібербезпека*
Обмеження щодо форми навчання:	*Заочна форма навчання*
Освітня кваліфікація:	*Бакалавр з кібербезпеки*
Кваліфікація в дипломі:	*Ступінь вищої освіти – Бакалавр* *Спеціальність – 125 Кібербезпека* *Спеціалізація – 121501 Організація захисту інформації та кібернетичної безпеки в інформаційно-телекомунікаційних системах* *Освітня програма – Кібербезпека*

Житомир-2020

ЛИСТ ПОГОДЖЕННЯ ОСВІТНЬОЇ ПРОГРАМИ “КІБЕРБЕЗПЕКА”

Рівень вищої освіти:	Перший (бакалаврський) рівень
Ступінь, що присвоюється:	Бакалавр
Назва галузі знань:	12 Інформаційні технології
Назва спеціальності:	125 Кібербезпека
Обмеження щодо форми навчання:	Заочна форма навчання
Освітня кваліфікація:	Бакалавр з кібербезпеки
Кваліфікація в дипломі:	Ступінь вищої освіти – Бакалавр Спеціальність – 125 Кібербезпека Спеціалізація – 121501 Організація захисту інформації та кібернетичної безпеки в інформаційно-телекомунікаційних системах Освітня програма – Кібербезпека

РОЗРОБЛЕНО І ВНЕСЕНО
Керівник закладу розробника:
Начальник Житомирського військового інституту імені С. П. Корольова
Заслужений діяч науки і техніки України,
доктор військових наук, професор,
генерал-майор

Олександр ЛЕВЧЕНКО

“ 28 ” 08 2020 р.

Представники стейкхолдерів

ПОГОДЖЕНО
Технічний директор товариства
з обмеженою відповідальністю
науково-виробничого центру
“ІНФОЗАХИСТ”

Ярослав КАЛІНІН

“ 27 ” *серпня* 2020 р.

ПОГОДЖЕНО
Заступник начальника інституту з
навчальної та наукової роботи
кандидат технічних наук,
старший науковий співробітник
полковник

Ігор САЩУК

“ 28 ” 08 2020 р.

ПОГОДЖЕНО
Начальник кафедри охорони державної
таємниці та захисту інформації
факультету охорони держаної таємниці та
інформаційної протиборства
Житомирського військового інституту
імені С. П. Корольова
полковник

Валентин ХОДАКІВСЬКИЙ

“ 28 ” 08 2020 р.

ЛИСТ ПОГОДЖЕННЯ ОСВІТНЬОЇ ПРОГРАМИ “КІБЕРБЕЗПЕКА”
(продовження)

Вчена рада Житомирського військового інституту імені С. П. Корольова.
Протокол від 26 серпня 2020 р. № 14
Секретар вченої ради
працівник Збройних Сил України Сергій ДАВИДОВ

Примітки.

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 освітиі 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"для першого (бакалаврського) рівня вищої освіти, затвердженого наказом Міністерства освітиі науки України від 04.10.2018 № 1074 та інших актів законодавства.

Склад робочої групи з перегляду освітньої програми призначено наказом начальника Житомирського військового інституту імені С. П. Корольова (з основної діяльності) від 27.04.2020 № 160 "Про перегляд освітніх програм підготовки здобувачів вищої освіти на першому (бакалаврському) рівні вищої освіти".

Склад робочої групи з перегляду освітньої програми.

Керівник проєктної групи:

ГРИЩУК Р., заслужений діяч науки і техніки України, д.т.н., професор, полковник.

Члени проєктної групи.

Від науково-педагогічних працівників:

ГУМЕНЮК І., к.т.н., майор;

СТАРОКОНЬ Є., к.психол.н., працівник ЗС України;

НЕЧИПОРУК Н., працівник ЗС України;

ОРЛЮК Є., к.фіз.-мат.н., доцент, працівник ЗС України;

ПЕТРУК М., к.т.н., доцент, працівник ЗС України;

КОЛОС Ю., к.т.н., доцент, працівник ЗС України.

Від здобувачів вищої освіти:

МАНИЛЮК О., студент заочник, старший сержант.

Від замовників та роботодавців:

за згодою.

Склад групи забезпечення освітньої програми призначено наказом начальника Житомирського військового інституту імені С. П. Корольова (з основної діяльності) від 20.08.2020 № 298 "Про призначення групи забезпечення освітніх програм у 2020/2021 навчальному році". Гаранта освітньої програми призначено наказом начальника Житомирського військового інституту імені С. П. Корольова (з основної діяльності) від 20.08.2020 №297 "Про призначення гранатів освітніх програм у 2020/2021 навчальному році".

Керівник робочої групи (гарант освітньої програми):

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.

Зовнішні рецензенти:

1. МОЛОДЕЦЬКА Катерина Валеріївна, доктор технічних наук, професор, професор кафедри комп'ютерних технологій і моделювання систем Поліського національного університету, керівник Лабораторії інжинірингової школи "Noosphere Engineering School", Міністерство освіти і науки України.
2. МИКУСЬ Сергій Анатолійович, начальник кафедри застосування інформаційних технологій та інформаційної безпеки Інституту забезпечення військ (сил) та інформаційних технологій Національного університету оборони України імені Івана Черняховського, Міністерство оборони України.

Освітня програма згідно до стандарту вищої освіти за спеціальністю 125 "Кібербезпека" для першого (бакалаврського) рівня вищої освіти вводиться вперше. Освітня програма є подальшим розвитком освітньо-професійної програми підготовки бакалавра, за якою з 2007 року здійснювалася підготовка студентів очної форм навчання в Житомирському військовому інституті у галузі знань 1701 "Інформаційна безпека" за напрямом підготовки 6.170101 "Безпека інформаційних та комунікаційних систем" спеціальності 7.17010101 "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 телекомунікацій від 26.11.2014, протокол № 14.

Термін перегляду освітньої програми один раз на рік напередодні нового навчального року з обов'язковим урахуванням позицій стейкхолдерів.

Актуалізовано:

Дата перегляду ОП/внесення змін до ОП				
Підстава				
Підпис				
ПІБ гаранта ОП				

І. ПРОФІЛЬ ОСВІТНЬОЇ ПРОГРАМИ
зі спеціальності 125 “Кібербезпека”

1 – Загальна інформація	
Повна назва вищого військового навчального закладу та 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 121501 Організація захисту інформації та кібернетичної безпеки в інформаційно-телекомунікаційних системах
Офіційна назва освітньої програми	Кібербезпека
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний, 240 кредитів ЄКТС, термін навчання 4 роки
Наявність акредитації	Сертифікат про акредитацію, від 09 вересня 2015 р. серія НД-ІІІ, № 0677443.
Цикл/рівень	Перший (бакалаврський) рівень / *QF-EHEA – First cycle qualification,* *EQF for LLL – Level 7,* НРК – 7 рівень
Передумови	Повна загальна середня освіта
Мова(и) викладання	Українська
Термін дії освітньої програми	2025 р.
Інтернет-адреса постійного розміщення опису освітньої програми	*https://www.zvir.zt.ua/osvita/osvitno-profesiini-prohramy*
2 – Мета освітньої програми	
Гарантоване забезпечення умов всебічного розвитку студентів, необхідних для здобуття ними вищої освіти за спеціальністю кібербезпека 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	**<u>Об’єкти професійної діяльності випускників:</u>** – об’єкти інформаційної діяльності (*включаючи комп’ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-довідкові, інформаційно-телекомунікаційні системи військового та подвійного призначення, державні інформаційні ресурси та інформаційні технології*) органів військового управління, військових частин (підрозділів), установ Міністерства оборони України та Збройних Сил України, інших міністерств і відомств сектору безпеки та оборони держави; – технології забезпечення безпеки інформації (*включаючи інформаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання, які спрямовані на забезпечення безпеки інформації державних інформаційних ресурсів, що обробляються (передаються, зберігаються) в інформаційно-телекомунікаційних системах військового та/або подвійного призначення й унеможливлюють або зводять до мінімуму отримання несанкціонованого доступу до таких ресурсів, протидіють*

	порушенню безпеки, сталого, надійного та штатного режиму функціонування згаданих систем); – процеси управління інформаційною та/або кібербезпекою визначених вище об'єктів інформаційної діяльності, що підлягають захисту. **Цілі навчання:** підготовка висококваліфікованих фахівців, здатних організовувати, використовувати та впроваджувати технології захисту інформації та кібернетичної безпеки в інформаційно-телекомунікаційних системах військового та/або подвійного призначення в інтересах забезпечення кібероборони держави. **Теоретичний зміст предметної області.** *Знання*: – законодавчої, нормативно-правової бази України (*у тому числі відомчої нормативно-правової бази, що не належить до інформації з обмеженим доступом*) та вимог відповідних міжнародних стандартів і передових практик щодо здійснення професійної діяльності; – принципів організації й супроводу систем та комплексів інформаційної та/або кібербезпеки об'єктів інформаційної діяльності; – теорії, моделей та принципів управління доступом до інформаційних ресурсів; – теорії систем управління інформаційною та/або кібербезпекою; – методів та засобів виявлення, управління та ідентифікації ризиків інформаційної та/або кібербезпеки; – методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації; – методів та засобів технічного та криптографічного захисту інформації; – сучасних інформаційно-комунікаційних технологій; – сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій; – автоматизованих систем проектування. *Методи, методики та технології*: – методи, методики та технології забезпечення інформаційної та/або кібербезпеки. *Інструменти та обладнання:* – системи забезпечення, моніторингу та контролю процесів інформаційної та/або кібербезпеки в інформаційно-телекомунікаційних системах; – сучасне програмне, апаратне, програмно-апаратне забезпечення інформаційно-телекомунікаційних систем. **Співвідношення обсягів загальної і професійної складових та вибіркової частини:** Загальний обсяг загальноосвітньої програми бакалавра на базі повної загальної середньої освіти – 240 кредитів ЄКТС, з них: – на забезпечення загальних та спеціальних (фахових) компетентностей за спеціальністю – 180 кредитів ЄКТС (75% обсягу освітньої програми). Цикл: для гуманітарних та соціально-економічних дисциплін складає 19 кредитів ЄКТС; для дисциплін природничо-наукової (фундаментальної) підготовки – 44 кредити ЄКТС; для дисциплін загально-професійної підготовки – 99 ЄКТС; практична підготовка складає 18 кредитів ЄКТС (з них виробнича практика – 4,5 кредити ЄКТС, переддипломна практика – 4,5 кредити ЄКТС, дипломне проектування – 9 кредитів ЄКТС). Вибіркові навчальні дисципліни складають 60 кредитів ЄКТС (25% обсягу освітньої програми).
Орієнтація освітньої програми	**Освітня програма має прикладну орієнтацію.** Прикладна орієнтація програми забезпечується наявністю в складі ЖВІ унікальних, сучасних та одночасно критично важливих для

	набуття практичних навичок навчально-лабораторних комплексів – *навчального кіберполігону, локальної мережної академії CISCO, лабораторії технічного захисту інформації та спецдосліджень, лабораторії радіотехнічних пристроїв спеціального призначення та інших.* **Саме наявність згаданих професійних (спеціалізаційних) акцентів гарантує здійснення прикладно-орієнтованої професійної діяльності** на об'єктах інформаційної діяльності Міністерства оборони України та Збройних Сил України, інших міністерств і відомств сектору безпеки та оборони держави та інших об'єктах професійної діяльності випускників.
Основний фокус освітньої програми та спеціалізації	Спеціальна освіта в галузі кібербезпеки та захисту інформації в інформаційно-телекомунікаційних 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 студентів 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 студентам 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, освітня програма розрахована та адаптована на студентів, які є військовослужбовцями військової служби за контрактом** Збройних Сил України та інших військових формувань, утворених відповідно до чинного законодавства; **е) по-шосте, програма передбачає залучення** (за згодою) **до освітнього процесу стейкхолдерів 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, 100% працевлаштування випускників;** **л) по-восьме, ключовим принципом** програми є **гендерна рівність** у правах та можливостях жінок і чоловіків з числа студентів **у здобутті освіти;** **м) по-дев'яте, потужна та сучасна матеріально-технічна база за місцем постійної дислокації;** **н) по-десяте, спадковість програми,** адже підготовка студентів за очною формою навчання у галузі знань 1701 "Інформаційна безпека" за напрямом підготовки 6.170101 "Безпека інформаційних та комунікаційних систем" спеціальності 7.17010101 "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 телекомунікацій 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 студентів**, які є військовослужбовцями військової служби за контрактом Збройних Сил України та інших військових формувань, утворених відповідно до чинного законодавства, **всі випускники 100% придатні до працевлаштування за військово обліковою спеціальністю (ВОС) 121501** *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 **можуть проходити військову службу за здобутою спеціалізацією на посадах молодшого 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 провожиться 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	**Перед випускником відкриваються можливості щодо здобуття освіти на другому (магістерському) рівні за спеціальністю 125 – Кібербезпека,** або спорідненими спеціальностями в галузі знань 12 – Інформаційні технології **в системі вищої освіти України, а також на "Курсах капітанів" (L-1C), "Курсах лідерства" (L-1B) та "Командно-штабний курсах" (L-2) в системі військової освіти України.**
5 – Викладання та оцінювання	
Викладання та навчання	**В основу викладання покладено студентсько-центричний підхід.** При цьому навчальний матеріал викладається в межах можливостей засвоєння студентами, адекватно поєднуючи в собі прикладну спрямованість та вимоги стандарту вищої освіти за спеціальністю 125 – Кібербезпека. **В основу навчання покладено сучасні дидактичні принципи,** такі як гуманізація та демократизація навчання, принцип нерозривності навчання та національно-патріотичного виховання й всебічного гармонійного розвитку студентів, принцип проблемності та нерозривності теорії з практикою.
Оцінювання	**Підсумкове оцінювання** результатів навчання складається із суми балів, отриманих за виконання індивідуальних завдань та контрольних заходів, передбачених робочою програмою навчальної дисципліни за 100-бальною шкалою 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"; 35 - 49 балів – "незадовільно" з можливістю повторного складання; 1 - 34 балів – "неприйнятно" з обов'язковим повторним вивченням навчальної дисципліни. **Види контролю:** вхідний, поточний, самоконтроль, модульний (рубіжний), семестровий (види семестрового контролю – залік та екзамен), підсумковий (семестровий контроль та атестація на здобуття освітнього ступеня). **Форми контролю:** усне та письмове опитування, тестові завдання, лабораторні звіти, презентації, захист курсових робіт та проєктів, звітів з практик. **Атестація:** захист кваліфікаційної роботи (проєкту). Атестація здійснюється відкрито та публічно з дотриманням вимог законодавства України у сфері охорони державної таємниці та міжнародних принципів академічної доброчесності. 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		
І. Інтегральна компетентність *(визначена стандартом вищої освіти)*	**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
ІІ. Загальні компетентності *(визначені стандартом вищої освіти)*	**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
ІІІ. 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 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
IV. 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 33: вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків
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) системах
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	**ГРИЩУК Руслан Валентинович,** **заслужений діяч науки і техніки України,** **доктор технічних наук (***21.05.01 – Інформаційна безпека держави, ДД № 001980, 2013 р.***), професор (***125 – Кібербезпека, 2018 р. АП № 000589***), начальник кафедри захисту інформації та кібербезпеки факультету охорони державної таємниці та інформаційного протиборства.** ***Освіта:*** – 1998-2003 рр. *золота медаль та диплом з відзнакою* МО № 13597477 Житомирського військового орденів Жовтневої Революції і Червоного Прапора інституту радіоелектроніки імені С. П. Корольова за спеціальністю "Радіоелектронні комплекси, системи та засоби озброєння і військової техніки", кваліфікація – інженер з радіоелектроніки, офіцер управління тактичного рівня; – 2005-2007 рр. очна ад'юнктура (*достроково*) ЖВІ Національного авіаційного університету; – 2020 р. *золота медаль та диплом з відзнакою* ДД № 001980 Національного університету оборони України імені Івана Черняховського за спеціальністю "Забезпечення військ (сил)", *спеціалізація "Управління інформаційною безпекою у Збройних Силах"*, кваліфікація – офіцер оперативно-тактичного рівня. ***Стаж безперервної наукової та науково-педагогічної діяльності в галузі*** більше 15,5 років. Безпосередньо в ЖВІ – 22,5 роки. ***Трудові досягнення і професійна майстерність відмічені на рівні держави:*** Президентом України – Верховним Головнокомандувачем Збройних Сил України (2002 р.), Прем'єр-міністром України (2011 р., 2013 р.), Міністерством оборони України (2008 р., 2014 р., 2018 р.), Міністерством освіти і науки України (2014 р., 2019 р.), Президентом Національної академії наук України (2010 р.). ***Автор та співавтор*** *більше 244 наукових праць*, з яких *більше 100 наукових* статей у фахових виданнях з технічних наук, які індексуються в міжнародних наукометричних базах даних (*Scopus, Web of Science, Index Copernicus, GoogleScholar та ін.*); *5 монографій* (*з них 1 видана за кордоном (Австрія, м. Відень*) іноземною мовою (англійською)). У науковому доробку в галузі кібербезпеки *має 8 патентів України на винаходи та корисні моделі, 4 навчальні посібники та підручники, 28 науково-дослідних робіт.* ***Міжнародне визнання підтверджується***:

	– **цитованістю наукових праць у багатьох державах світу,** *зокрема в США, Іспанії, Південноафриканській Республіці, Республіці Польща, Греції, Китайській Народній Республіці*, *Російській Федерації* та інших державах світу; – **запрошенням міжнародними академічними інституціями до презентації наукових результатів** ***в державах Європейського Союзу****, таких як Республіка Польща та Республіка Болгарія;* – **запрошенням до редагування 41-го випуску міжнародного наукового журналу** "*Information & Security: An International Journal*"; – **є дійсним та запрошеним членом редакційних колегій наукових фахових видань з технічних наук за спеціальністю 125 – Кібербезпека**, які входять до міжнародних наукометричних баз даних: *"Кібербезпека: освіта, наука, техніка"*, *"Сучасний захист інформації"*, *"Захист інформації"* та в галузі знань інформаційні технології *"Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем"*. ***Національне визнання підтверджується***: – **призначенням рішенням МОН України** *головою спеціалізованої вченої ради* К 14.719.01 та СРДФ 14.719.002 ЖВІ, *членом спеціалізованої вченої ради* Д 26.861.06 Державного університету телекомунікацій (*по захисту дисертацій на здобуття наукового ступеня доктора (кандидата) технічних наук за спеціальностями: 21.05.01 – Інформаційна безпека держави (технічні науки); 05.13.21 – Системи захисту інформації (технічні науки)*); – **призначенням офіційним опонентом** 4 докторських та 4 кандидатських дисертацій з технічних наук; – **особистою підготовкою** більше 70 відгуків на автореферати дисертацій на здобуття наукового ступеня; – **керівник та інструктор** *Локальної мережної академії Cisco ЖВІ.* **Засновник в ЖВІ наукової школи з інформаційної та кібернетичної безпеки держави.** *Особисто підготував: 2 докторів технічних наук; 1 кандидата технічних наук; 1 доктора філософії в галузі технічні наук.* Захист ще 1 здобувача наукового ступеня кандидата технічних наук за спеціальністю 21.05.01 – Інформаційна безпека держави заплановано на лютий 2021 р. **САМЧИШИН Олексій Володимирович,** **кандидат технічних наук (***20.02.14 – Озброєння і військова техніка, ДК № 004868, 2012 р.***), професор кафедри захисту інформації та кібербезпеки факультету охорони державної таємниці та інформаційного протиборства.** ***Освіта:*** – 1996-2001 рр. диплом МО № 13579792 Житомирського військового інституту радіоелектроніки імені С. П. Корольова за спеціальністю *"Комплекси, системи та засоби автоматизації управління військами та озброєнням"*, кваліфікація – інженер-системотехнік, офіцер військового управління тактичного рівня; – 2008-2011 рр. очна ад'юнктура ЖВІ. ***Стаж безперервної наукової та науково-педагогічної діяльності в галузі*** більше 12 років. Безпосередньо в ЖВІ – 17 років. **Тривалий період обіймав ключові посади в науковому центі за напрямком кібербезпеки,** зокрема: *наукового співробітника, провідного наукового співробітника та начальника науково-дослідної лабораторії проблем забезпечення кібернетичної безпеки науково-дослідного відділу інформаційної та кібернетичної безпеки наукового центру ЖВІ.* ***Трудові досягнення і професійна майстерність відмічені на рівні держави:***

	МО України, нагороджений пам'ятним знаком "За воїнську доблесть". Учасник бойових дій. ***Автор та співавтор*** *більше 60 наукових праць* (з яких *16* наукових статей у виданнях з технічних наук, включених до переліку наукових фахових видань України) з них: 2 статті без співавторів, 2 наукові статті в міжнародних збірниках акредитованих в наукометричній базі *Scopus*, 3 патенти України на корисну модель. Був виконавцем 12 науково-дослідних робіт (з них у 3 – відповідальним виконавцем). ***Міжнародне визнання підтверджується***: – **цитованістю наукових праць у державах світу,** *зокрема Республіці Польща* та інших державах світу. ***Національне визнання підтверджується***: – **призначенням офіційним рецензентом** на кандидатську дисертацію з технічних наук; – **особистою підготовкою** більше 10 відгуків на автореферати дисертацій на здобуття наукового ступеня; **ГУМЕНЮК Ігор Володимирович,** **кандидат технічних наук (***20.02.14 – Озброєння і військова техніка, ДК № 049434, 2018 р.***), доцент кафедри захисту інформації та кібербезпеки факультету охорони державної таємниці та інформаційного протиборства.** ***Освіта:*** – 2005-2010 рр. *диплом з відзнакою* МО № 13651978 Житомирського військового інституту імені С. П. Корольова Національного авіаційного університету за спеціальністю *"Комплекси, системи та засоби автоматизації управління військами та озброєнням"*, кваліфікація – інженер-системотехнік, офіцер військового управління тактичного рівня; – 2015-2018 рр. очна ад'юнктура ЖВІ. ***Стаж безперервної наукової та науково-педагогічної діяльності в галузі*** більше 5 років. Безпосередньо в ЖВІ – 15,5 роки. Уся педагогічна діяльність пов'язана з посадами на кафедрі захисту інформації та кібербезпеки. ***Автор та співавтор*** *більше 50 наукових праць*, з яких *більше 10 наукових* статей у фахових виданнях з технічних наук, які індексуються в міжнародних наукометричних базах даних (*Index Copernicus, GoogleScholar та ін.*). У науковому доробку в галузі кібербезпеки *має 3 патенти на корисні моделі, 5 свідоцтв про реєстрації авторського права на твір.* ***Національне визнання підтверджується***: – **інструктор** *Локальної мережної академії Cisco ЖВІ;* – **керівник наукової роботи** курсантів, які зайняли *призове (третє) місце* на *І етапі Всеукраїнського конкурсу студентських наукових робіт* з Інформаційних систем та технологій. **ОХРІМЧУК Володимир Васильович,** **старший викладач кафедри захисту інформації та кібербезпеки факультету охорони державної таємниці та інформаційного протиборства.** ***Освіта:*** – 2001-2006 рр. *диплом з відзнакою* МО № 13623685 Житомирського військового орденів Жовтневої Революції і Червоного Прапора інституту радіоелектроніки імені С. П. Корольова за спеціальністю *"Радіоелектронні комплекси, системи та засоби озброєння і військової техніки"*, кваліфікація – інженер з радіоелектроніки, офіцер управління тактичного рівня;

	Стаж безперервної наукової та науково-педагогічної діяльності в галузі більше 8 років. Має великий досвід наукової діяльності на посадах наукових працівників у науково-дослідному відділі інформаційної та кібернетичної безпеки. Безпосередньо в ЖВІ – 19,5 роки. Учасник бойових дій. ***Трудові досягнення і професійна майстерність відмічені на рівні держави:*** ***Автор та співавтор*** *більше 30 наукових праць*, з яких *12 наукових* статей у виданнях з технічних наук, включених до переліку наукових фахових видань України. Одна з наукових статей включена до міжнародної наукометричної бази Scopus. З 2015 року є здобувачем наукового ступеня кандидата технічних наук. ***Національне визнання підтверджується***: – **інструктор** *Локальної мережної академії Cisco ЖВІ.*
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** студентів 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. Студенти мають доступ до української науково-освітньої телекомунікаційної мережі УРАН (*http://www.uran.net.ua/~ukr/uran-members.htm*), а також необмежений доступ до мережі Інтернет.

	Наявний офіційний веб-сайт військового інституту: https://zvir.zt.ua, 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 студентів включає:** навчальні плани і робочі навчальні плани; графіки освітнього процесу; робочі програми навчальних дисциплін; належне навчально-методичне забезпечення з кожної навчальної дисципліни навчального плану; дидактичні матеріали для самостійної та індивідуальної роботи студентів із навчальних дисциплін; методичні вказівки для виконання курсових та бакалаврських 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	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.

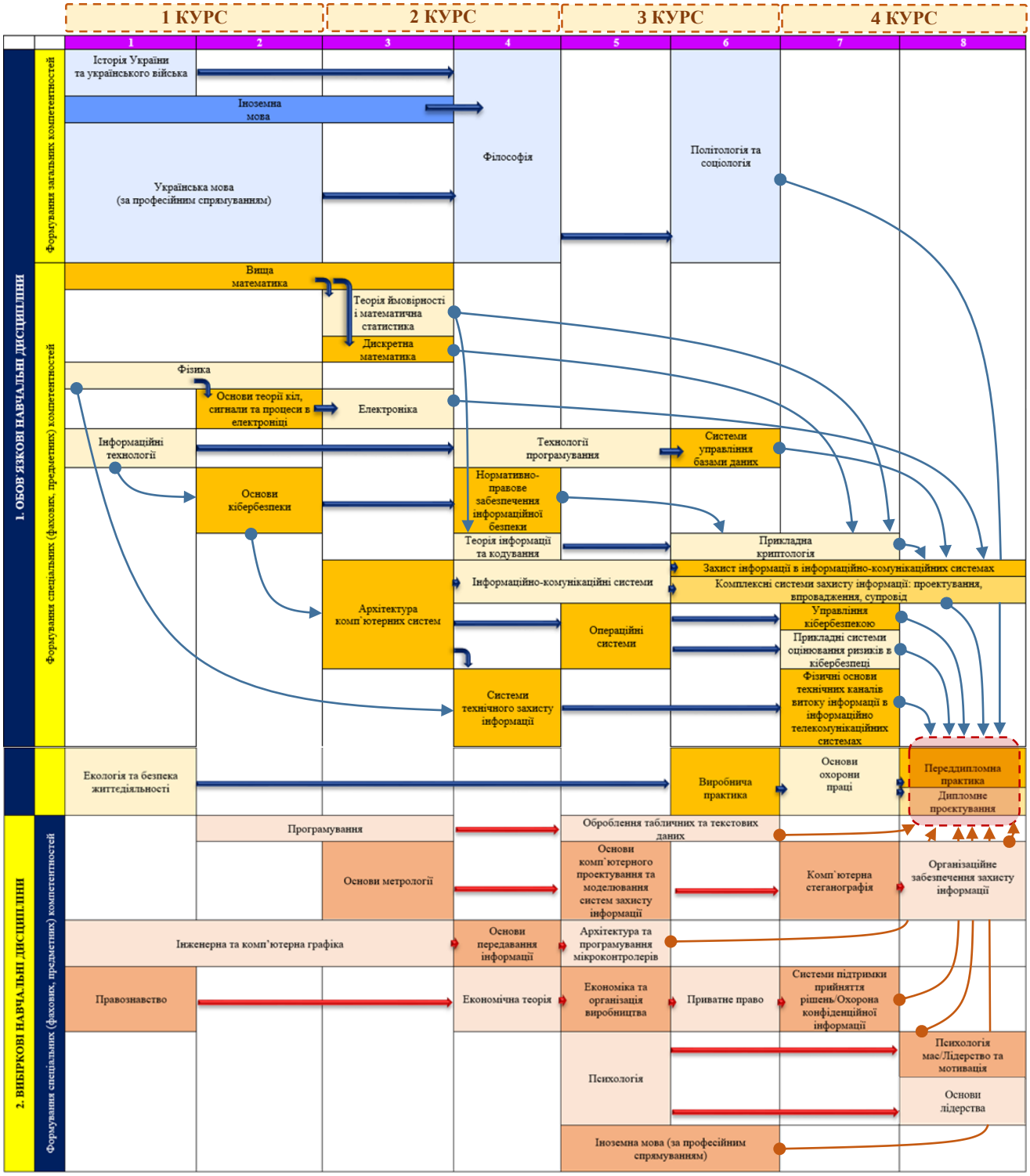
ІІ. ПЕРЕЛІК КОМПОНЕНТ ОСВІТНЬОЇ ПРОГРАМИ ТА ЇХ ЛОГІЧНА ПОСЛІДОВНІСТЬ

2.1. Перелік компонент освітньої програми

Код	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Розподіл годин за курсами і семестрами								Форма підсумкового контролю
			1	2	3	4	5	6	7	8	
1. ОБОВ`ЯЗКОВІ НАВЧАЛЬНІ ДИСЦИПЛІНИ											
Формування загальних компетентностей											
1.1. Гуманітарні та соціально-економічні дисципліни											
ОК 1.1.1.	Історія України та українського війська	3,0	90								*екзамен*
ОК 1.1.2.	Іноземна мова	6,0	60	60	60						*залік, екзамен*
ОК 1.1.3.	Українська мова (за професійним спрямуванням)	3,0	45	45							*залік, екзамен*
ОК 1.1.4.	Філософія	3,0				90					*екзамен*
ОК 1.1.5.	Політологія та соціологія	4,0						120			*екзамен*
	Усього	**19**	**195**	**105**	**60**	**90**		**120**			
Формування спеціальних (фахових, предметних) компетентностей											
1.2. Дисципліни природничо-наукової (фундаментальної) підготовки											
ОК 1.2.1.	Вища математика	19,0	240	210	120						*екзамен*
ОК 1.2.2.	Фізика	11,0	150	180							*екзамен*
ОК 1.2.3.	Теорія ймовірності і математична статистика	4,0			120						*екзамен*
ОК 1.2.4.	Дискретна математика	3,5			105						*залік*
ОК 1.2.5.	Інформаційні технології	4,5	135								*екзамен*
ОК 1.2.6.	Екологія та безпека життєдіяльності	2,0	60								*залік*
	Усього	**44,0**	**585**	**390**	**345**						
1.3. Дисципліни загально-професійної підготовки											
ОК 1.3.1.	Технології програмування	12,5				210	165				*екзамен, ПР*
ОК 1.3.2.	Основи теорії кіл, сигнали та процеси в електроніці	4,0		120							*залік*
ОК 1.3.3.	Операційні системи	4,5					135				*екзамен*
ОК 1.3.4.	Електроніка	3,5			105						*екзамен*
ОК 1.3.5.	Архітектура комп'ютерних систем	4,0			120						*залік*
ОК 1.3.6.	Інформаційно-комунікаційні системи	8,0				135	105				*екзамен*
ОК 1.3.7.	Теорія інформації та кодування	5,0				150					*екзамен*
ОК 1.3.8.	Прикладна криптологія	9,0						135	135		*екзамен, ПР*
ОК 1.3.9.	Нормативно-правове забезпечення інформаційної безпеки	2,0				60					*залік*
ОК 1.3.10.	Системи технічного захисту інформації	4,5				135					*екзамен, ПР*
ОК 1.3.11.	Захист інформації в інформаційно-комунікаційних системах	12,5						120	105	150	*екзамен, КР*
ОК 1.3.12.	Комплексні системи захисту інформації: проектування, впровадження, супровід	11,0						120	105	105	*залік, екзамен*
ОК 1.3.13.	Управління кібербезпекою	3,5							105		*залік*
ОК 1.3.14.	Основи охорони праці	3,0							90		*екзамен*
ОК 1.3.15.	Прикладні системи оцінювання ризиків в кібербезпеці	3,0							90		*залік*

Код	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Розподіл годин за курсами і семестрами								Форма підсумкового контролю
			1	2	3	4	5	6	7	8	
ОК 1.3.16.	Фізичні основи технічних каналів витоку інформації в інформаційно телекомунікаційних системах	3,0							90		*екзамен*
ОК 1.3.17.	Системи управління базами даних	4,0						120			*залік, ПР*
ОК 1.3.18.	Основи кібербезпеки	2,0		60							*екзамен*
	Усього	**99**		**180**	**225**	**690**	**405**	**495**	**720**	**255**	
	1.4. Практична підготовка										
ОК 1.4.1.	Виробнича практика	4,5						135			*залік*
ОК 1.4.2.	Переддипломна практика	4,5								135	*залік*
ОК 1.4.3.	Дипломне проєктування	9,0								270	
	Усього	**18,0**						**135**		**405**	
	Разом за обов'язковою частиною	**180,5**	**780**	**675**	**630**	**780**	**405**	**750**	**735**	**660**	
	2. ВИБІРКОВІ НАВЧАЛЬНІ ДИСЦИПЛІНИ										
	Формування спеціальних (фахових, предметних) компетентностей										
	2.1. Дисципліни вільного вибору										
	Група дисциплін природничо-наукової (фундаментальної) підготовки										
ВК 2.1.1.	Інженерна та комп'ютерна графіка	7,0	60	60	90						*залік*
ВК 2.1.2.	Програмування	8,5		165	90						*залік, екзамен*
	Група дисциплін професійної і практичної підготовки										
ВК 2.1.3.	Економіка та організація виробництва	3,0					90				*залік*
ВК 2.1.4.	Основи метрології	3,0			90						*залік*
ВК 2.1.5.	Основи передавання інформації	2,0				60					*залік*
ВК 2.1.6.	Основи комп`ютерного проектування та моделювання систем захисту інформації	3,5					105				*залік*
ВК 2.1.7.	Організаційне забезпечення захисту інформації	3,0								90	*залік*
ВК 2.1.8.	Комп`ютерна стеганографія	4,0							120		*екзамен*
ВК 2.1.9.	Архітектура та програмування мікроконтролерів	4,0					120				*екзамен*
ВК 2.1.10.	Правознавство	2,0	60								*залік*
ВК 2.1.11.	Психологія	2,0					60				*залік*
ВК 2.1.12.	Економічна теорія	2,0				60					*залік*
	Група дисциплін загально-професійної підготовки (альтернатива військової підготовки)										
ВК 2.1.13.	Оброблення табличних та текстових даних	4,0					75	45			*залік*
ВК 2.1.14.	Системи підтримки прийняття рішень/Охорона конфіденційної інформації	2,0							60		*залік*
ВК 2.1.15.	Іноземна мова (за професійним спрямуванням)	3,0					45	45			*залік*
ВК 2.1.16.	Приватне право	2,0						60			*залік*
ВК 2.1.17.	Основи лідерства	2,5								75	*залік*
ВК 2.1.18.	Соціальний інжиніринг/Основи менеджменту	2,5								75	*залік*
	Разом за вибірковою частиною	**60**	**120**	**225**	**270**	**120**	**495**	**150**	**180**	**240**	
	РАЗОМ ЗА ОСВІТНЬОЮ ПРОГРАМОЮ	**240**	**900**	**900**	**900**	**900**	**900**	**900**	**900**	**900**	

2.2. Структурно-логічна схема освітньої програми



ІІІ. ФОРМА АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Атестація випускників за освітньою програмою “КІБЕРБЕЗПЕКА” спеціальності № 125 – Кібербезпека проводиться у формі захисту бакалаврської роботи.

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* 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.

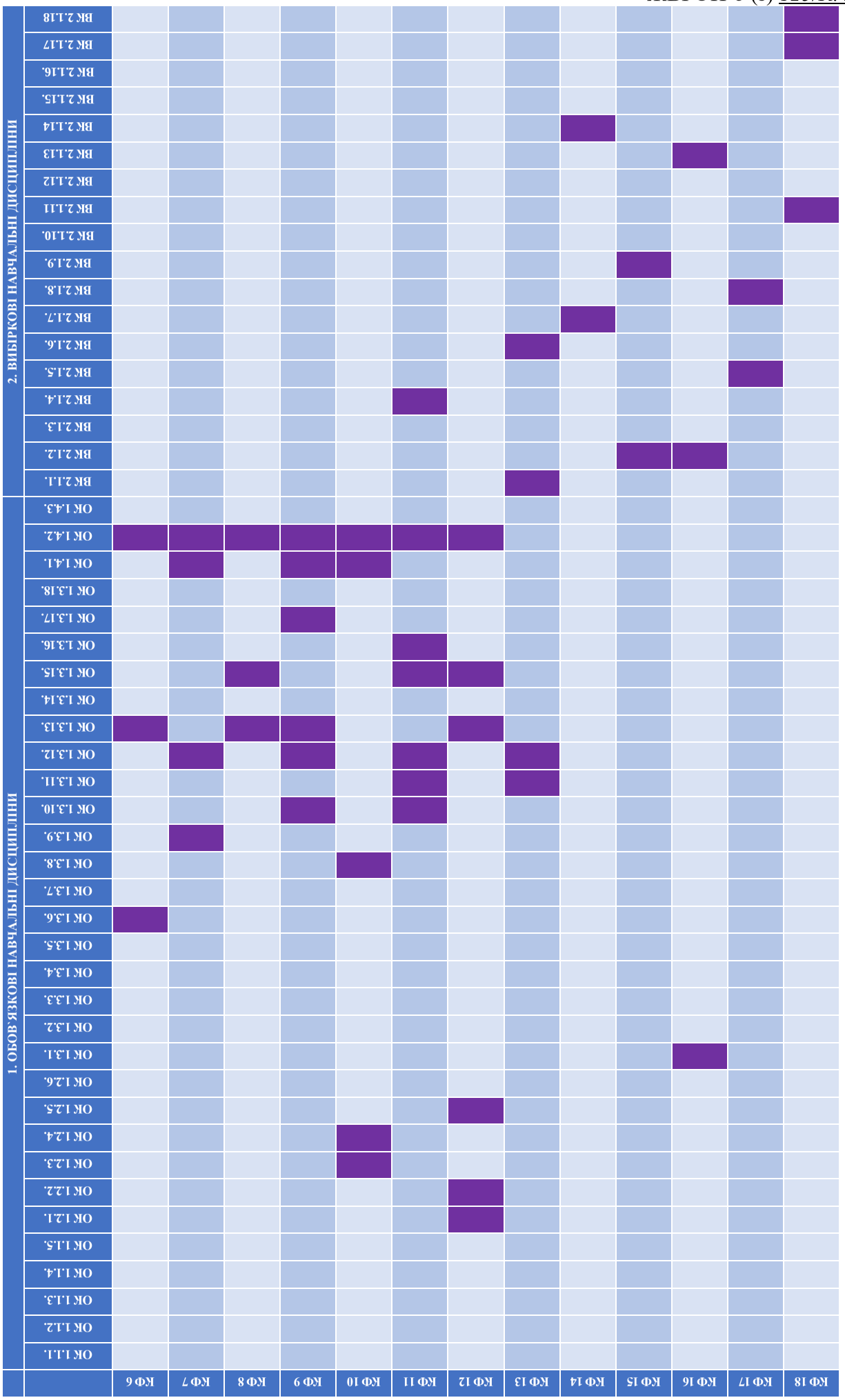
IV. МАТРИЦЯ ВІДПОВІДНОСТІ ПРОГРАМНИХ КОМПЕТЕНТНОСТЕЙ КОМПОНЕНТАМ ОСВІТНЬОЇ ПРОГРАМИ

1. ОБОВ`ЯЗКОВІ НАВЧАЛЬНІ ДИСЦИПЛІНИ

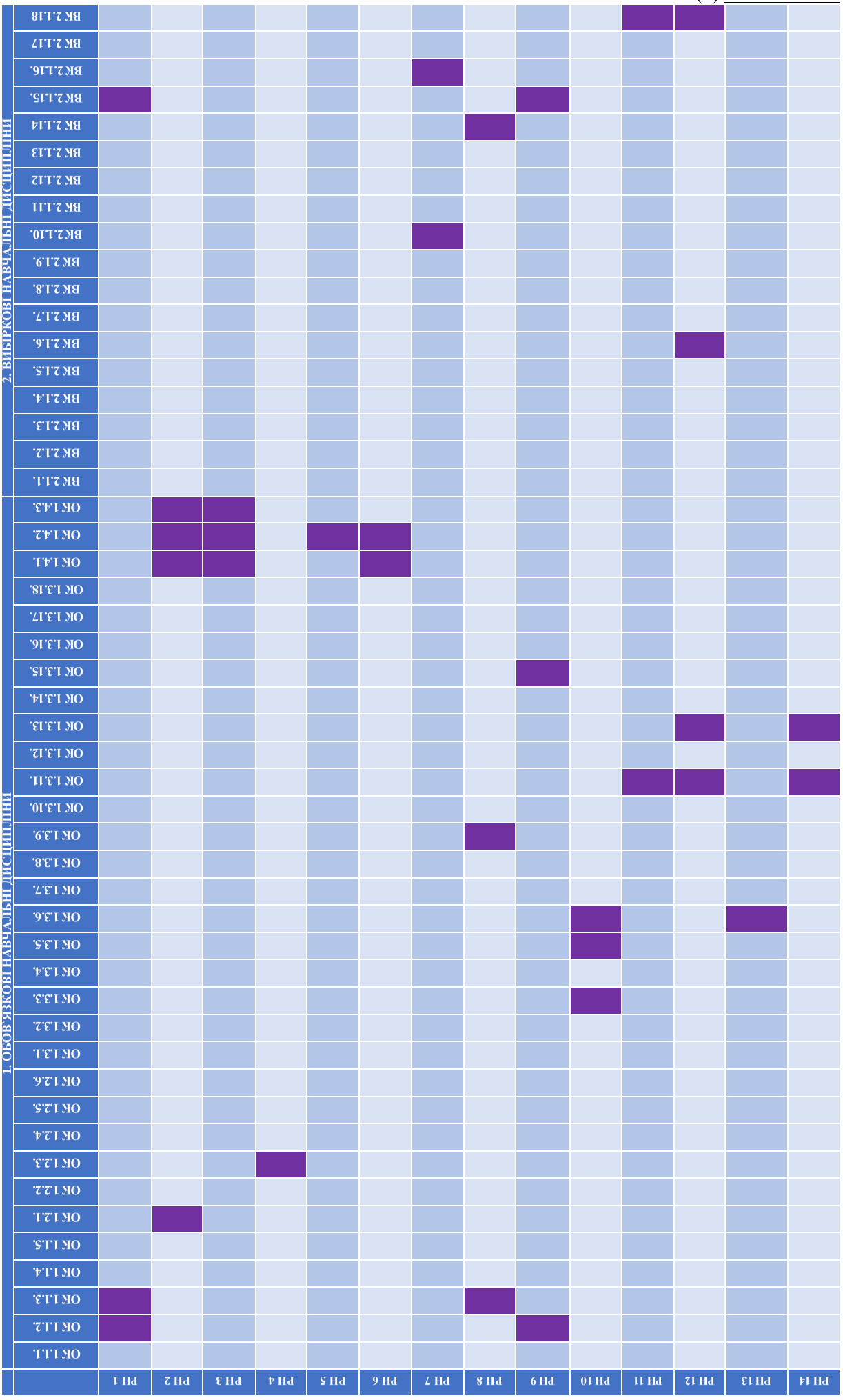
	ОК 1.1.1.	ОК 1.1.2.	ОК 1.1.3.	ОК 1.1.4.	ОК 1.1.5.	ОК 1.2.1.	ОК 1.2.2.	ОК 1.2.3.	ОК 1.2.4.	ОК 1.2.5.	ОК 1.2.6.	ОК 1.3.1.	ОК 1.3.2.	ОК 1.3.3.	ОК 1.3.4.	ОК 1.3.5.	ОК 1.3.6.	ОК 1.3.7.	ОК 1.3.8.	ОК 1.3.9.	ОК 1.3.10.	ОК 1.3.11.	ОК 1.3.12.	ОК 1.3.13.	ОК 1.3.14.	ОК 1.3.15.	ОК 1.3.16.	ОК 1.3.17.	ОК 1.3.18.	ОК 1.4.1.	ОК 1.4.2.	ОК 1.4.3.
КЗ 0	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
КЗ 1		+								+	+	+		+							+	+	+	+	+							
КЗ 2											+								+		+	+	+	+		+			+			
КЗ 3		+	+																													
КЗ 4												+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	+			
КЗ 5								+	+	+		+		+								+		+		+	+	+				
КЗ 6	+		+	+	+															+					+				+			
КЗ 7	+	+	+	+	+																											
КФ 1																				+	+		+	+					+	+	+	
КФ 2																	+			+				+						+	+	
КФ 3																								+		+			+		+	
КФ 4																																
КФ 5																						+									+	

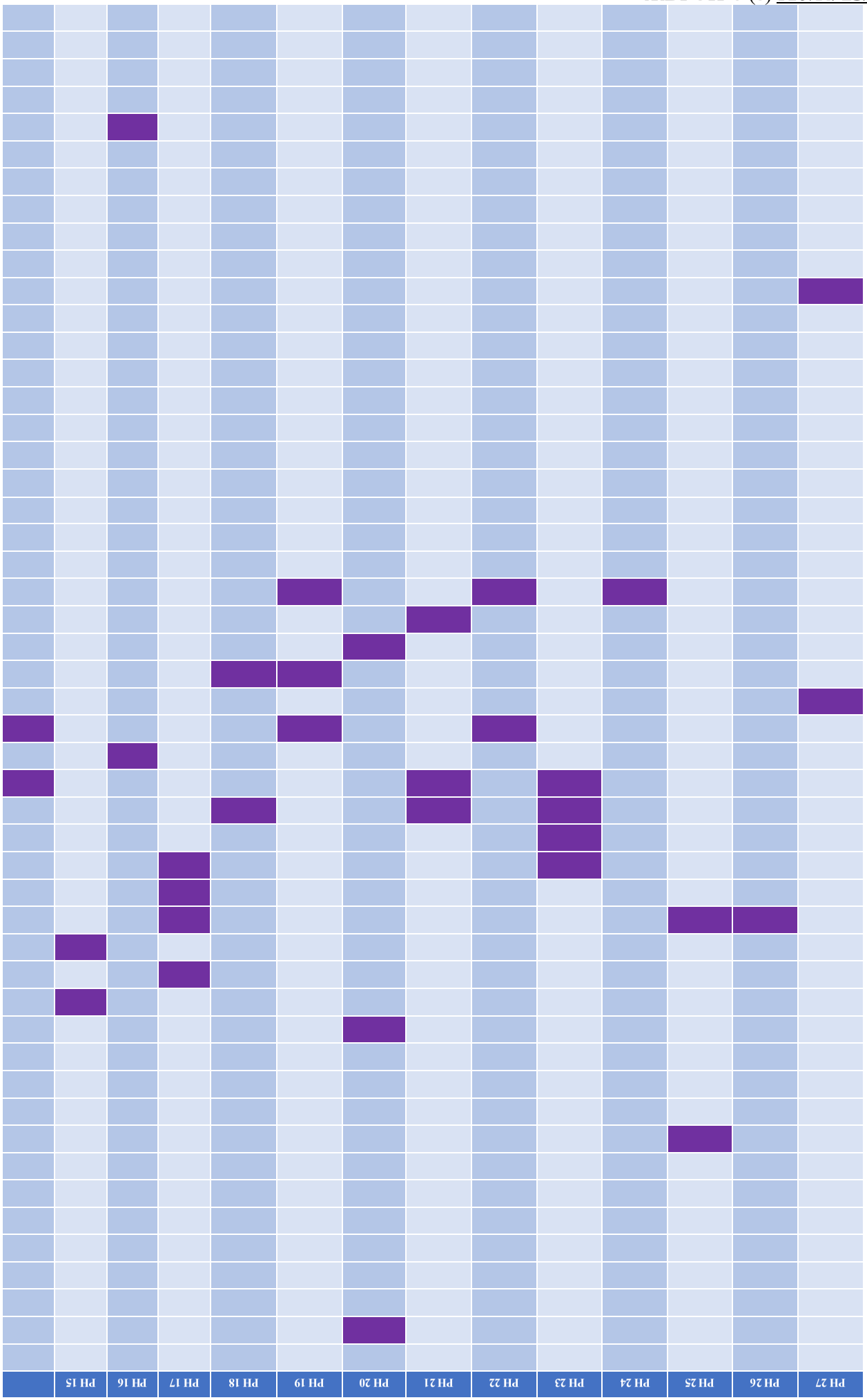
2. ВИБІРКОВІ НАВЧАЛЬНІ ДИСЦИПЛІНИ

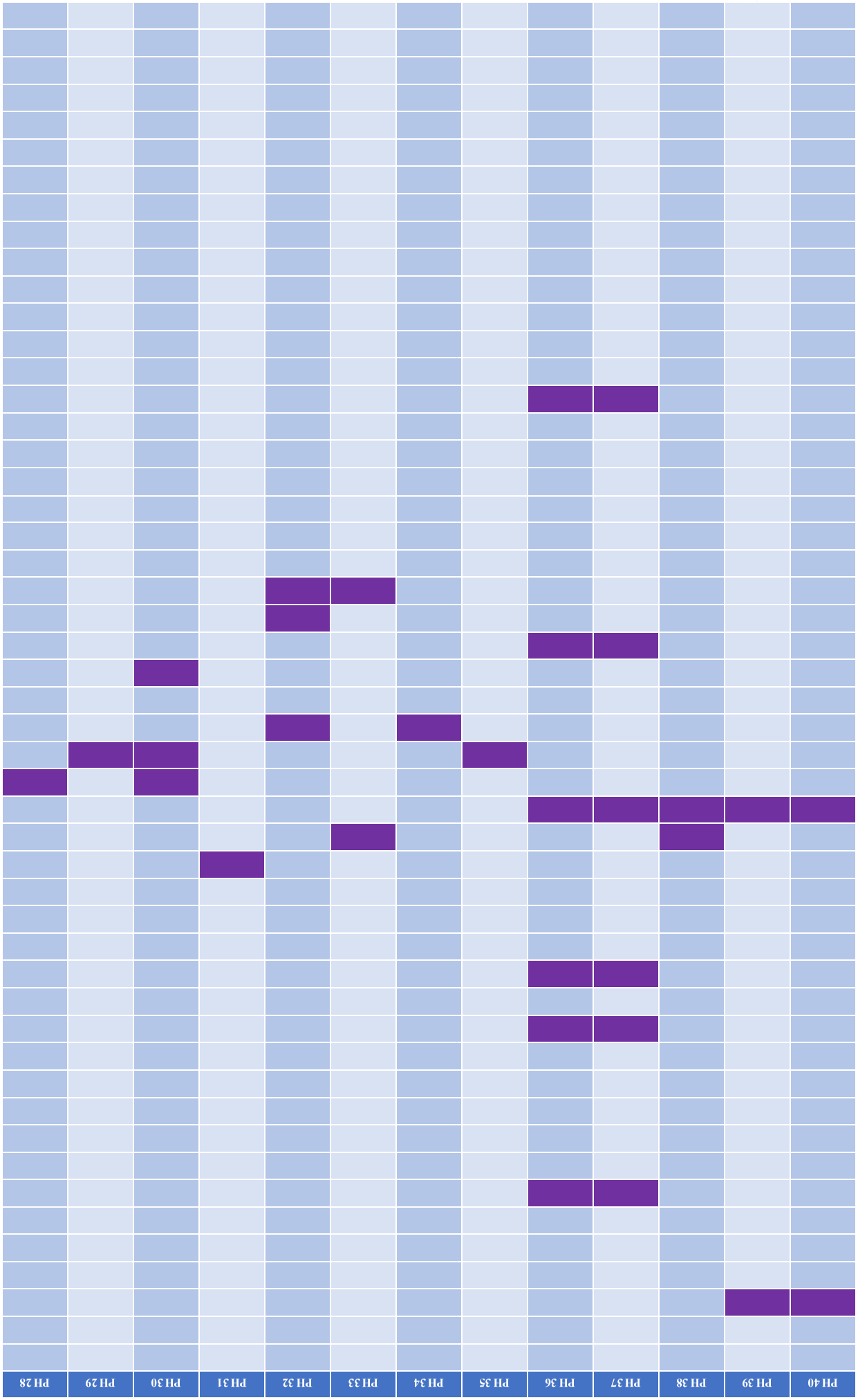
	ВК 2.1.1.	ВК 2.1.2.	ВК 2.1.3.	ВК 2.1.4.	ВК 2.1.5.	ВК 2.1.6.	ВК 2.1.7.	ВК 2.1.8.	ВК 2.1.9.	ВК 2.1.10.	ВК 2.1.11	ВК 2.1.12	ВК 2.1.13	ВК 2.1.14	ВК 2.1.15.	ВК 2.1.16.	ВК 2.1.17	ВК 2.1.18
КЗ 0																		
КЗ 1																		
КЗ 2																		
КЗ 3																		
КЗ 4																		
КЗ 5																		
КЗ 6																		
КЗ 7																		
КФ 1	+		+							+		+			+	+		
КФ 2				+														
КФ 3																		
КФ 4														+				
КФ 5																		

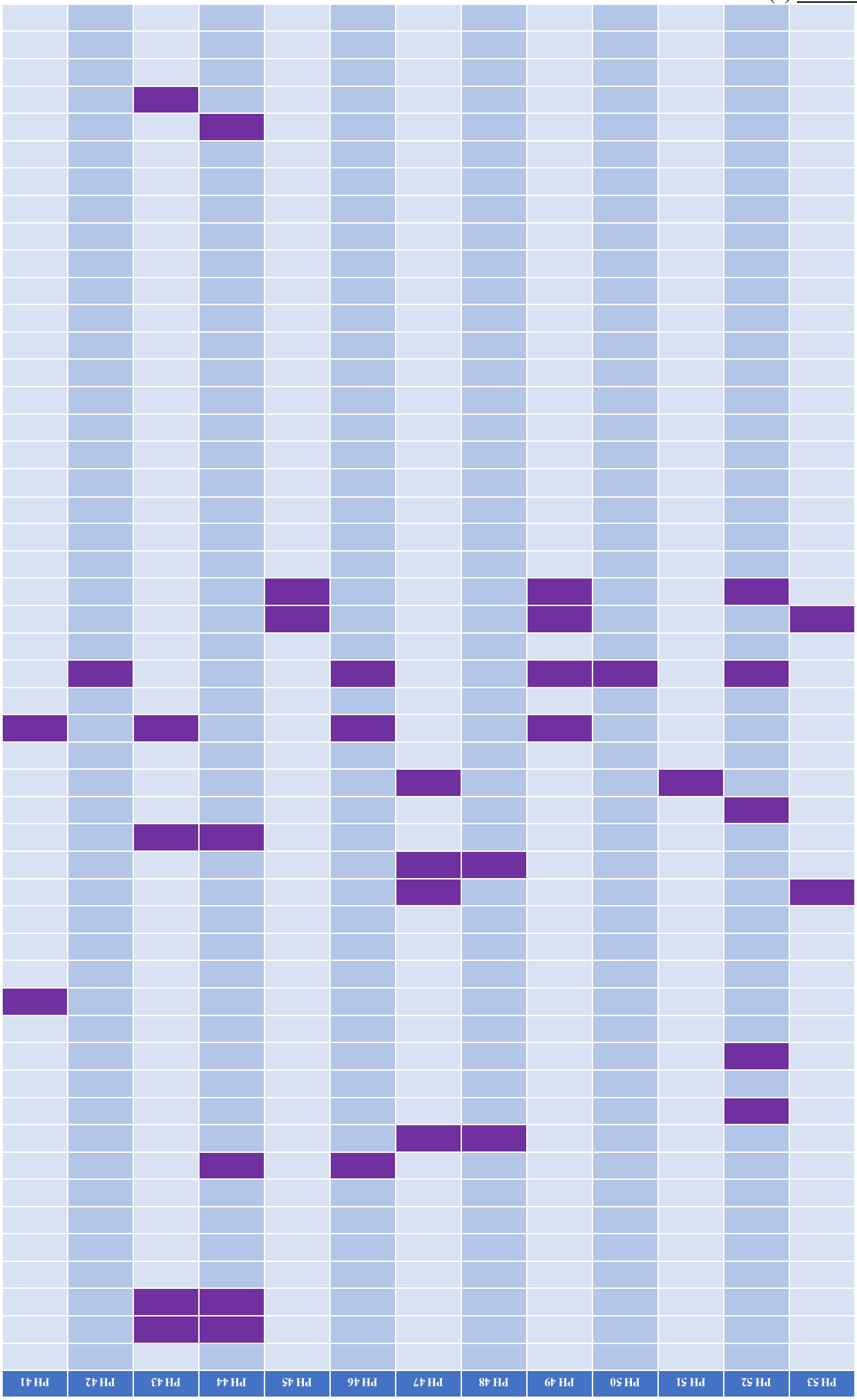

1. ОБОВ'ЯЗКОВІ НАВЧАЛЬНІ ДИСЦИПЛІНИ
2. ВИБІРКОВІ НАВЧАЛЬНІ ДИСЦИПЛІНИ
ОК 1.1.
ОК 1.2.
ОК 1.3.
ОК 1.4.
ОК 1.5.
ОК 2.1.
ОК 2.2.
ОК 2.3.
ОК 2.4.
ОК 2.5.
ОК 2.6.
ОК 3.1.
ОК 3.2.
ОК 3.3.
ОК 3.4.
ОК 3.5.
ОК 3.6.
ОК 3.7.
ОК 3.8.
ОК 3.9.
ОК 3.10.
ОК 3.11.
ОК 3.12.
ОК 3.13.
ОК 3.14.
ОК 3.15.
ОК 3.16.
ОК 3.17.
ОК 3.18.
ОК 4.1.
ОК 4.2.
ОК 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.
ВК 2.1.15.
ВК 2.1.16.
ВК 2.1.17.
ВК 2.1.18.
КФ 6
КФ 7
КФ 8
КФ 9
КФ 10
КФ 11
КФ 12
КФ 13
КФ 14
КФ 15
КФ 16
КФ 17
КФ 18

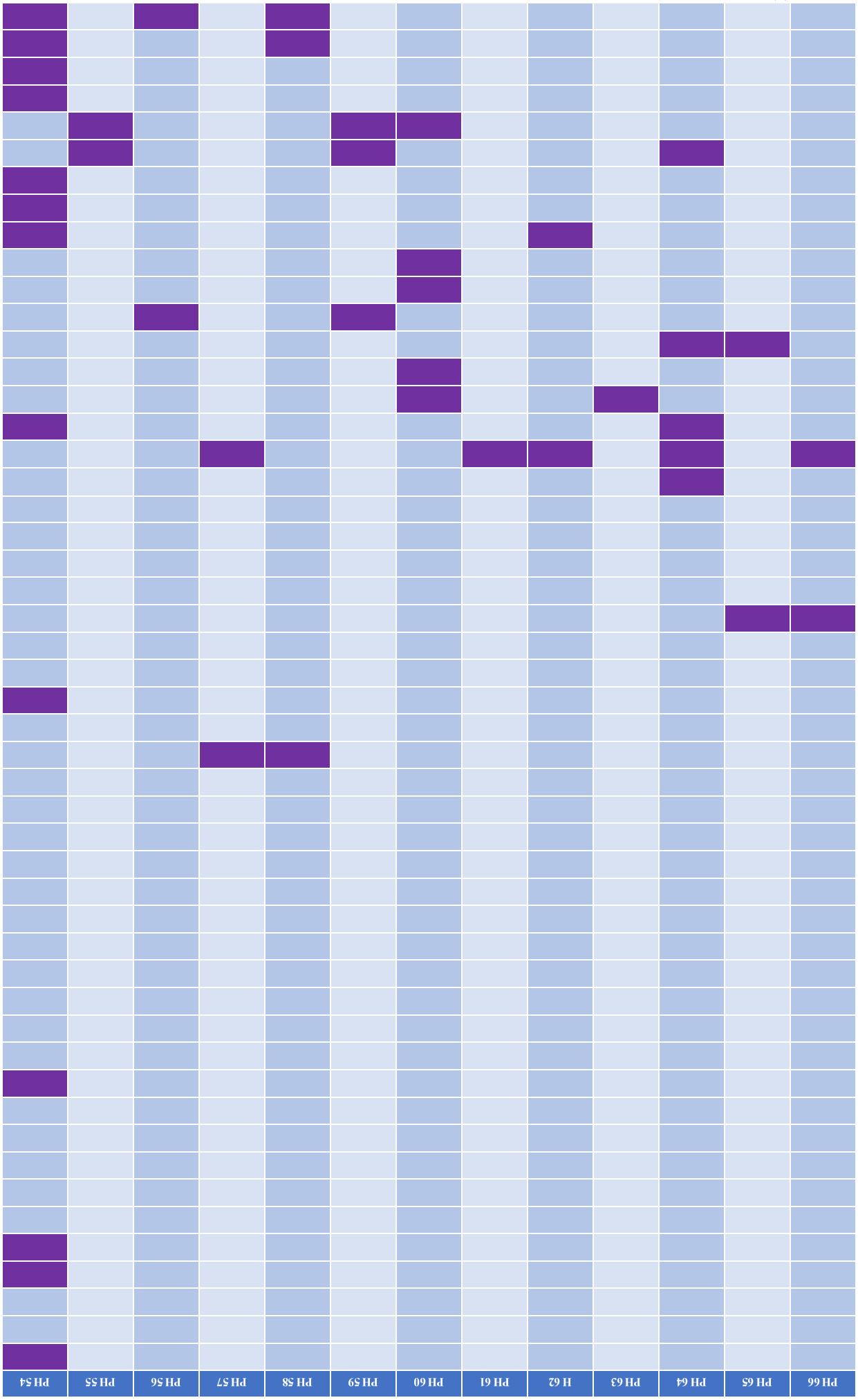
V. МАТРИЦЯ ЗАБЕЗПЕЧЕННЯ ПРОГРАМНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ (ПРН) ВІДПОВІДНИМИ КОМПОНЕНТАМИ ОСВІТНЬОЇ ПРОГРАМИ

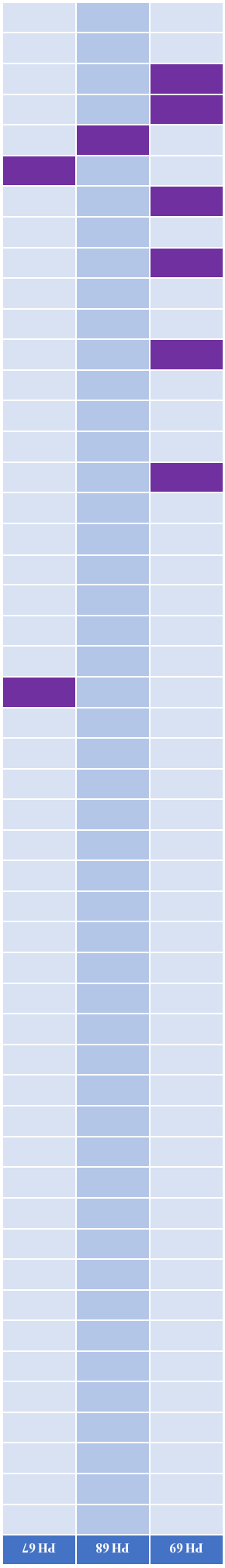



РН 15
РН 16
РН 17
РН 18
РН 19
РН 20
РН 21
РН 22
РН 23
РН 24
РН 25
РН 26
РН 27


PH 28
PH 29
PH 30
PH 31
PH 32
PH 33
PH 34
PH 35
PH 36
PH 37
PH 38
PH 39
PH 40


PH 41
PH 42
PH 43
PH 44
PH 45
PH 46
PH 47
PH 48
PH 49
PH 50
PH 51
PH 52
PH 53


РН 54
РН 55
РН 56
РН 57
РН 58
РН 59
РН 60
РН 61
Н 62
РН 63
РН 64
РН 65
РН 66


Pr 67
Pr 68
Pr 69

VI. ПЕРЕЛІК ОСНОВНИХ НОРМАТИВНИХ ДОКУМЕНТІВ, НА ЯКИХ БАЗУЄТЬСЯ ОСВІТНЯ ПРОГРАМА

1. *Закон України "Про вищу освіту"* [Електронний ресурс] // Відомості Верховної Ради (ВВР) № 37-38, ст. 2004. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/1556-18#Text.
2. *Закон України "Про основні засади забезпечення кібербезпеки України"*. [Електронний ресурс] // Відомості Верховної Ради (ВВР), 2017, № 45, ст.403. – Режим доступу: http:// zakon.rada.gov.ua/laws/show/2163-19.
3. *Указ Президента України* від 15 березня 2016 року № 96/2016 "Стратегія кібербезпеки України". https://zakon.rada.gov.ua/laws/show/96/2016. (дата звернення: 02.03.2020).
4. *Стандарт вищої освіти України: перший (бакалаврський) рівень, галузь знань 12 – Інформаційні технології, спеціальність 125 – Кібербезпека* [Електронний ресурс] // МОН України. – 2018. – Режим доступу до ресурсу: https://mon.gov.ua/storage/app/media/vishcha-osvita/zatverdzeni%20standarty/12/21/125-kierbezpeka-bakalavr.pdf.
5. *Постанова КМ України від 29 квітня 2015 р. № 266 "Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти"* [Електронний ресурс] // КМ України – Режим доступу до ресурсу: https://www.kmu.gov.ua/npas/248149695.
6. *Рашкевич Ю. М.* Методичні рекомендації щодо опису освітньої програми в контексті нових стандартів вищої освіти [Електронний ресурс] / Ю. М. РАШКЕВИЧ // Higher Education Reform Experts Team – Ukraine. – 2015. – Режим доступу до ресурсу: https://webcache.googleusercontent.com/search?q=cache:AdBrxkfoTQ4J:https://erasmusplus.org.ua/korysna-informatsiia/korysni-materialy/category/3-materialy-natsionalnoi-komandy-ekspertiv-shchodo-zaprovadzhennia-instrumentiv-bolonskoho-protsesu.html%3Fdownload%3D285:metodychni-rekomendatsii-shchodo-opysu-osvitnoi-prohramy-v-konteksti-novykh-standartiv-vyshchoi-osvity+&cd=1&hl=uk&ct=clnk&gl=ua.
7. *Наказ МОН України* від 11.07.2019 № 977 "Про затвердження Положення про акредитацію освітніх програм, за якими здійснюється підготовка здобувачів вищої освіти" [Електронний ресурс] // МОН України. – 2019. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/z0880-19#Text.
8. *Наказ МО України від 05 березня 2020 р. № 250/34533* "Про затвердження Положення про особливості організації освітньої діяльності у вищих військових навчальних закладах Міністерства оборони України та військових навчальних підрозділах закладів вищої освіти" [Електронний ресурс] // МОН України. – 2020. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/z0880-19#Text.
9. *Постанова КМ України від 25 червня 2020 р. № 519 "Про внесення змін у додаток до постанови Кабінету Міністрів України від 23 листопада 2011 р. № 1341"* [Електронний ресурс] // КМ України. – 2020. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/519-2020-%D0%BF#Text.
10. *Національний класифікатор України: Класифікатор професій ДК 003:2010* [Електронний ресурс] // Державний комітет України з питань технічного регулювання та споживчої політики. – 2010. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/rada/show/va327609-10#Text.
11. *Наказ МО України від 09.09.2015 № 472 "Про затвердження Положення про екзаменаційні комісії вищих військових навчальних закладів та військових навчальних підрозділів вищих навчальних закладів"* [Електронний ресурс] // МО України. – 2015. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/z1141-15#Text.
12. *Освітньо-професійна програма* "Системи, технології та математичні методи кібербезпеки" [Електронний ресурс] // НТУ України "КПІ". – 2020. – Режим доступу до ресурсу: https://drive.google.com/file/d/1O6hImxhQdZZlSgGaIBmUbNemKyXlk2ca/view.
13. *Освітньо-професійна програма* "Кібербезпека" [Електронний ресурс] // КНУ ім. Тараса Шевченка. – 2018. – Режим доступу до ресурсу: http://fit.univ.kiev.ua/wp-content/uploads/2019/07/%D0%9E%D0%9F%D0%9F_%D0%B1%D0%B0%D0%BA_%D0%9AI%D0%91%D0%95%D0%A0%D0%91_%D0%9A%D0%91_2017_3n.pdf.
14. *Освітньо-професійна програма* 125.00.01 "Безпека інформаційних та комунікаційних систем першого (бакалаврського) рівня вищої освіти [Електронний ресурс] // КУ ім. Бориса Грінченка. – 2018. – Режим доступу до ресурсу: https://kubg.edu.ua/images/stories/Departaments/vstupnikam/fitu/2020/bach/opp_%D0%9A%D0%91_%D0%91%D0%86%D0%9A%D0%A1.pdf.
15. *Cybersecurity: A Generic Reference Curriculum (RC).* Dear Partners, NATO Members, 4500-1 (OSEM PED) October 2016, 73 p.
16. *Наказ МО 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"* [Електронний ресурс] // МО України. – 2020. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/z0188-20#Text.