ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

«КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ»

рівень вищої освіти	перший (бакалаврський)
галузь знань	F Інформаційні технології
спеціальність	F5 «Кібербезпека та захист інформації»
освітня кваліфікація	бакалавр з кібербезпеки та захисту інформації

ЛИСТ ПОГОДЖЕННЯ ОСВІТНЬОЇ ПРОГРАМИ
«КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ»

Первісна редакція

Розроблено робочою групою у складі:

№	ПІБ	Науковий ступінь, вчене звання, найменування посади
1.	Сагайда Павло Іванович	доктор технічних наук, доцент, завідувач кафедри інформаційних технологій та аналітики даних
2.	Кайдан Вадим Петрович	старший викладач кафедри інформаційних технологій та аналітики даних
3.	Костіков Олександр Анатолійович	кандидат фізико-математичних наук, доцент, доцент кафедри інформаційних технологій та аналітики даних
4.	Гетьман Ірина Анатоліївна	кандидат технічних наук, доцент, доцент кафедри інформаційних технологій та аналітики даних
5.	Касьянюк Олександр Сергійович	старший викладач кафедри інформаційних технологій та аналітики даних

Відгуки від стейкхолдерів:

№	ПІБ	Найменування посади
1.	Кудрявцев А.М.	ТОВ «МЕТІНВЕСТ ДІДЖИТАЛ», начальник відділу аналізу даних
2.	Левицький С.І.	ПРАТ ПВНЗ «Запорізький інститут економіки та інформаційних технологій», завідувач кафедри інформаційних технологій, доктор екон. наук, доцент
3.	Лактіонов І.С.	НТУ «Дніпровська політехніка», професор кафедри програмного забезпечення комп'ютерних систем, доктор технічних наук, доцент

Початкова редакція проєкту освітньої програми рекомендована до громадського обговорення на засіданні кафедри інформаційних технологій та аналітики даних

протокол № 4
від 05.05.2026 р.

Керівник департаменту
управління якістю освіти
та акредитації Костянтин МОЙСЕЄНКО

Перший проректор-
проректор з навчальної роботи Наталія РЕКОВА

Затверджено на засіданні Вченої ради ТОВ ТЕХНІЧНИЙ УНІВЕРСИТЕТ «МЕТІНВЕСТ ПОЛІТЕХНІКА» (Протокол №9 від 18.06.2026 р.). Введено в дію: наказ 168/18.06.2026.

Ректор Олександр ПОВАЖНИЙ

І ПРЕАМБУЛА

1.1 Ця освітня програма розроблена на підставі Законів України «Про освіту», «Про вищу освіту», «Про військовий обов'язок і військову службу», «Про основні засади державної політики у сфері утвердження української національної та громадянської ідентичності», «Про інформацію», «Про доступ до публічної інформації», «Про науково-технічну інформацію», «Про основи національного спротиву», «Про охорону праці», Кодексу цивільного захисту, указу Президента України «Про Цілі сталого розвитку України на період до 2030 року», постанов Кабінету Міністрів України «Про затвердження Національної рамки кваліфікацій», «Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти», «Про затвердження Порядку проведення базової загальновійськової підготовки громадян України, які здобувають вищу освіту, та поліцейських», «Про затвердження Порядку здійснення навчання населення діям у надзвичайних ситуаціях», Національного класифікатора України: Класифікатор професій ДК 003:2010, International Standard Classification of Education Fields of education and training 2013 (ISCED-F 2013) – Detailed field descriptions, Статуту ТОВ «ТЕХНІЧНИЙ УНІВЕРСИТЕТ «МЕТІНВЕСТ ПОЛІТЕХНІКА», Положення про організацію освітнього процесу, Положення про концепції освітньої діяльності, освітні програми, робочі програми та силабуси освітніх компонентів у ТОВ «ТЕХНІЧНИЙ УНІВЕРСИТЕТ «МЕТІНВЕСТ ПОЛІТЕХНІКА», Стандарту вищої освіти першого (бакалаврського) рівня за спеціальністю 125 «Кібербезпека та захист інформації» галузі знань 12 «Інформаційні технології», затвердженого наказом Міністерства освіти і науки України від 29.10.2024 р. № 1547, та професійного стандарту «Фахівець сфери захисту інформації», затвердженого наказом Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 25.11.2022 р. № 744.

Освітня програма також враховує міжнародні рекомендації Cybersecurity Curricula 2017 (CSEC2017), розроблені Association for Computing Machinery (ACM), IEEE Computer Society, Association for Information Systems Special Interest Group on Security (AIS SIGSEC) та International Federation for Information Processing (IFIP WG 11.8); положення Cyber Security Body of Knowledge (CyBOK); Workforce Framework for Cybersecurity (NICE Framework, NIST SP 800-181 Rev. 1) Національного інституту стандартів і технологій США (NIST); а також European Cybersecurity Skills Framework (ECSF) Агентства Європейського Союзу з кібербезпеки (ENISA).

1.2 Пропозиції щодо удосконалення змісту освітньої програми можна спрямовувати на офіційну юридичну адресу ТОВ «ТЕХНІЧНИЙ УНІВЕРСИТЕТ «МЕТІНВЕСТ ПОЛІТЕХНІКА» або скористуватися

засобами, доступними на офіційному вебсайті Університету за посиланням: Кібербезпека та захист інформації : Polytechnic або за кодом:

ІІ ПРОФІЛЬ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

Загальна інформація	
Назва освітньої програми	Кібербезпека та захист інформації
Ступінь вищої освіти, освітня кваліфікація	Бакалавр, бакалавр з кібербезпеки та захисту інформації
Предметна область	F Інформаційні технології, F5 «Кібербезпека та захист інформації»
Рівень / цикл	– за Національною рамкою кваліфікацій України – 6 рівень; – за Qualifications Framework for the European Higher Education Area (QF-EHEA) – Bachelor's degree (First cycle); – за European Qualifications Framework (EQF-LLL) – Level 6
Тип диплому	– Диплом: одиничний
Форми здобуття освіти та строки виконання програми	Денна очна (з урахуванням вимог безпеки), заочна Обсяг освітньої програми / розрахунковий строк виконання: – з повним терміном навчання – 240 кредитів ЄКТС / 3 роки 10 місяців; – зі скороченим терміном навчання (в разі наявності ступеня «молодший бакалавр», «фаховий молодший бакалавр») – 180 кредитів ЄКТС / 2 роки 10 місяців
Вимоги до освіти осіб, які можуть розпочати навчання за програмою	– з повним розрахунковим терміном навчання: наявність повної загальної середньої освіти (профільної середньої освіти) – 3 (4) рівень НРК, або освітньо-кваліфікаційного рівня молодшого спеціаліста, або освітньо-професійного ступеня фахового молодшого бакалавра, або освітнього ступеня молодшого бакалавра – 5 рівень Національної рамки кваліфікацій; – зі скороченим розрахунковим терміном навчання: наявність освітньо-кваліфікаційного рівня молодшого спеціаліста, або освітньо-професійного ступеня фахового молодшого бакалавра, або освітнього ступеня молодшого бакалавра – 5 рівень Національної рамки кваліфікацій.
Наявність акредитації	-
Мова(и) викладання	Українська, окремі освітні компоненти / матеріали можуть використовувати англійську мову відповідно до внутрішніх положень університету.
Мета і особливості програми	
Мета: підготовка бакалаврів, здатних розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі кібербезпеки та захисту інформації, проєктувати, впроваджувати, експлуатувати і супроводжувати системи захисту, аналізувати загрози та вразливості, застосовувати криптографічні, технічні, програмні й програмно-апаратні засоби захисту, здійснювати моніторинг, реагування на кіберінциденти та управління інформаційною безпекою.	

Предметна область програми	Об’єкт вивчення: технології кібербезпеки та захисту інформації; процеси управління кібербезпекою та захистом інформації; об’єкти інформаційної діяльності, у тому числі інформаційні та інформаційно-комунікаційні системи, інформаційні ресурси і технології; процеси виявлення, попередження, нейтралізації та ліквідації наслідків кіберзагроз і кіберінцидентів. Теоретичний зміст предметної області: принципи, концепції, моделі та теорії кібербезпеки і захисту інформації; принципи забезпечення конфіденційності, цілісності та доступності інформації; закономірності функціонування інформаційних та інформаційно-комунікаційних систем в умовах дії кіберзагроз; теоретичні основи криптографічного, технічного, програмного та програмно-апаратного захисту інформації; методи виявлення вразливостей, оцінювання ризиків, моніторингу подій безпеки та реагування на кіберінциденти. Методи, методики, технології: методи та технології забезпечення кібербезпеки та захисту інформації; методи аналізу загроз, вразливостей і ризиків; методи криптографічного та технічного захисту інформації; методи захисту інформації в інформаційних та інформаційно-комунікаційних системах; методи моніторингу, виявлення несанкціонованого доступу та кіберінцидентів; методики оцінювання захищеності інформаційних систем; технології резервування, відновлення та забезпечення безперервності функціонування інформаційних систем; технології проєктування, впровадження, експлуатації та супроводження комплексних систем захисту інформації. Інструменти та обладнання: комп’ютерні та інформаційно-комунікаційні системи; комп’ютерні мережі та мережеве обладнання; засоби криптографічного, технічного, програмного та програмно-апаратного захисту інформації; системи контролю доступу; засоби моніторингу та аналізу мережевого трафіку; системи виявлення та запобігання вторгненням; засоби аналізу вразливостей і дослідження кіберінцидентів; серверні, хмарні та віртуалізовані середовища; спеціалізоване програмне забезпечення для моделювання, проєктування, контролю, моніторингу та управління кібербезпекою.
Вид програми	Освітньо-професійна
Фокус освітньої програми	Комплексна підготовка фахівців з кібербезпеки та захисту інформації, здатних забезпечувати захист інформаційних та інформаційно-комунікаційних систем на основі поєднання криптографічних, технічних, програмних і програмно-апаратних методів захисту, мережевих технологій, моніторингу кіберзагроз,

	реагування на кіберінциденти та управління інформаційною безпекою. Особливий акцент програми спрямовано на практичне застосування сучасних засобів захисту інформації, аналіз вразливостей і загроз, безпеку комп'ютерних мереж та інформаційно-комунікаційних систем, застосування технологій штучного інтелекту і машинного навчання у завданнях кібербезпеки, а також підготовку до роботи з комплексними системами захисту інформації.
Особливості освітньої програми	– орієнтація на підготовку фахівців з розробки та супроводу цифрового підприємства за концепцією Industry 4.0 у межах групи Метінвест, а також на партнерство з науковцями та практиками у сфері диджиталізації; – освітня програма враховує Cybersecurity Curricular Guidelines (CSEC2017) – спільні рекомендації ACM, IEEE Computer Society, AIS SIGSEC та IFIP WG 11.8, Cyber Security Body of Knowledge (CyBOK); NICE Workforce Framework for Cybersecurity, NIST SP 800-181 Rev.1; European Cybersecurity Skills Framework (ECSF), ENISA. – інтерактивне навчання з практичною та академічною складовою, зокрема навчання за матеріалами та із залученням фахівців-практиків від Групи МЕТІНВЕСТ та участь у виконанні досліджень для активів Групи МЕТІНВЕСТ; – можливість викладання окремих курсів англійською мовою та використання англомовних джерел літератури та статистичних даних; – вивчення англійської мови протягом всього періоду навчання, що сприяє успішному складанню ЄВІ з іноземної мови при вступі на магістратуру; – можливість, починаючи з 3 курсу (2 курс зі скороченим терміном навчання) поглиблено працювати над виконанням кваліфікаційної роботи з отриманням постійного зворотного зв'язку від академічного керівника та наставника від бізнесу; – доступ до ресурсів масових онлайн-курсів українських та зарубіжних університетів; – здобувачам освіти доступна стипендіальна програма незалежно від джерела оплати навчання; – здобувачам освіти як членам спільноти групи МЕТІНВЕСТ доступна професіональна психологічна підтримка; – персональний супровід ветеранів; – для здобувачів освіти-громадян України чоловічої статі, які навчаються за денною або дуальною формою здобуття освіти, обов'язковими освітніми компонентами є «Базова загальновійськова підготовка: теоретична частина» та «Базова загальновійськова підготовка: практична частина»; ці компоненти не є обов'язковими для здобувачів освіти чоловічої статі, які визнані за станом здоров'я

	непридатними до військової служби; до набуття громадянства України пройшли військову службу в інших державах; проходили військову службу; мають сертифікат про проходження базової підготовки та здобуття військово-облікової спеціальності, а також для здобувачів освіти жіночої статі, які не виявили добровільного бажання пройти базову загальновійськову підготовку; особи, звільнені від проходження базової загальновійськової підготовки, вивчають освітній компонент «Сучасна воєнно-політична історія України та світу»; – здобувачам освіти доступний курс «Фізичне виховання та особисте здоров'я» як обов'язковий позакредитний.
Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Права випускників на працевлаштування не обмежуються. Після успішного виконання освітньо-професійної програми «Кібербезпека та захист інформації» випускники можуть працювати на таких професійних роботах: – 2132.2 Розробник систем захисту інформації; – 2132.2 Конструктор систем кібербезпеки; – 2139.2 Адміністратор мереж і систем; – 2139.2 Фахівець сфери захисту інформації; – 2139.2 Фахівець з підтримки інфраструктури кіберзахисту; – 2139.2 Фахівець з реагування на інциденти кібербезпеки; – 2139.2 Аналітик з безпеки інформаційно-комунікаційних систем; – 2139.2 Аналітик систем захисту інформації; – 2139.2 Аналітик з оцінки вразливостей; – 2139.2 Фахівець з технічного захисту інформації; – 2139.2 Фахівець з питань безпеки (інформаційно-комунікаційні технології).
Подальше навчання	Можливість продовжити навчання на другому (магістерському) рівні вищої освіти. Набуття додаткових кваліфікацій в системі післядипломної освіти
Викладання та оцінювання	
Викладання і навчання	Студентоцентроване проблемно-орієнтоване навчання, спрямоване на формування наукового і креативного мислення. Основними формами освітньої активності є: онлайн та офлайн лекції-дискусії; семінари-тренінги за участю викладачів-експертів, фахівців-практиків, кейс-технології, творчі завдання, лабораторні роботи з використанням спеціалізованого програмного забезпечення, виконання індивідуальних та групових самостійних завдань, самостійна робота з вивчення оприлюднених на освітній платформі і в репозиторії Університету наукових і навчальних матеріалів, робота з науковими публікаціями у

	науково-метричних базах Scopus, Web of Science, на видавничих та інформаційних платформах (SSRN, Wiley Online Library, JSTOR, Researchgate та ін.); підготовка наукових і аналітичних звітів; робота з професійними текстами англійською, проходження практик та підготовка кваліфікаційної роботи.
Оцінювання	Форми оцінювання поточної роботи: тестування, оцінка активності і результатів участі в інтерактивних форматах роботи, постановці та вирішенні проблем; розв'язання аналітично-розрахункових та дослідницьких завдань, підготовка аналітичних звітів; самооцінювання академічного прогресу шляхом визначення ступеню сформованості груп компетентностей; оцінка вчасності та якості підготовки індивідуальних та групових завдань; оцінка якості виконання складових курсових робіт, звітів з практики, кваліфікаційної роботи бакалавра. Форми оцінювання під час підсумкового контролю: тестування, есе, розв'язання аналітично-розрахункових завдань; захист курсових робіт, звітів з практики, кваліфікаційної роботи бакалавра. Підхід до оцінювання: критерієм успішного проходження здобувачем освіти підсумкового оцінювання може бути досягнення ним мінімальних порогових рівнів оцінок за програмними результатами кожного освітнього компоненту під час поточної роботи та/або в ході підсумкового контролю за освітнім компонентом. Оцінювання здійснюється: а) за чотирибальною шкалою: відмінно (рівень досягнення програмного результату навчання 90-100 %, за рівнем – A), добре (75-89 %, B – 82-89%, C – 75-81%), задовільно (60-74 %, D – 67-74%, E – 60-66%), незадовільно (менше 60 %, F – 0-59%); б) за дворівневою шкалою: залік (60-100 %, з відповідним рівнем A-E), незалік (менше 60 % з відповідним рівнем F).
Ресурсне забезпечення програми	
Кадрове забезпечення	– кадрове забезпечення програми здійснюється на основі чинних Ліцензійних умов провадження освітньої діяльності; – для проведення занять, наставництва під час практики запрошуються фахівці з активів Групи МЕТІНВЕСТ, залучені фахівці із закладів вищої освіти та інших партнерів ТОВ «ТЕХНІЧНИЙ УНІВЕРСИТЕТ «МЕТІНВЕСТ ПОЛІТЕХНІКА»
Матеріально-технічне забезпечення та засоби навчання	– навчальні корпуси з тематичними кабінетами, комп'ютерними класами, лабораторіями, актовою залою, пунктом харчування; – полігони і лабораторії на потужностях активів Групи МЕТІНВЕСТ; – спортивний зал, спортивний майданчик;

	– бібліотека з читальним залом, репозиторій, дистанційний доступ до Research4Life, доступ до електронної бібліотеки Kortext; – гуртожиток; – точки бездротового доступу до мережі Інтернет у навчальних корпусах та гуртожитку; – мультимедійне обладнання у лекційних аудиторіях; – ліцензійні пакети програмного забезпечення Microsoft, MathWorks, AutoCAD, програмне забезпечення з відкритою ліцензією; – корпоративний обліковий запис Microsoft із доступом до ліцензійного програмного забезпечення, в т.ч. до центру командної роботи MS Teams, системи управління навчанням Moodle та ін.
Академічна мобільність	
Національна та міжнародна мобільність	Університет стимулюватиме мобільність і визнаватиме кредити, отримані в рамках національної та міжнародної мобільності за дво- і багатосторонніми угодами та програмами, в яких Університет є стороною або учасником
Особливості навчання іноземних громадян та осіб без громадянства	**-**

ІІІ КОМПЕТЕНТНОСТІ ТА ПРОГРАМНІ РЕЗУЛЬТАТИ НАВЧАННЯ

Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації
Загальні компетентності	**ЗК1.** Здатність застосовувати знання у практичних ситуаціях. **ЗК2.** Знання та розуміння предметної області і розуміння професійної діяльності. **ЗК3.** Здатність спілкуватися державною мовою як усно, так і письмово. **ЗК4.** Здатність спілкуватися іноземною мовою. **ЗК5.** Здатність вчитися і оволодівати сучасними знаннями. **ЗК6.** 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. **ЗК7.** Здатність ухвалювати рішення й діяти, дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності. **ЗК8.** 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; здатність до національного спротиву[1].
Фахові компетентності	**СК1.** Здатність застосовувати законодавчу та нормативно-правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності. **СК2.** Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації. **СК3.** Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації. **СК4.** Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації. **СК5.** Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження. **СК6.** Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових,

[1] Елемент «здатність до національного спротиву» додано в 2026 р. з урахуванням змін в законодавстві про національний спротив.

	організаційних та технічних засобів і методів, процедур, практичних прийомів тощо). **СК7.** Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою. **СК8.** Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності. **СК9.** Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності. **СК10.** Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з установленою політикою інформаційної безпеки.
Програмні результати навчання	
РН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків. **РН2.** Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації. **РН3.** Застосовувати принципи неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності. **РН4.** 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. **РН5.** 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. **РН6.** Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат. **РН7.** 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. **РН8.** 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. **РН9.** Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації. **РН10.** Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності. **РН11.** Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахуванням вимог до захисту інформації. **РН12.** Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки. **РН13.** 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.
РН14. 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.
РН15. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.
РН16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.
РН17. 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.
РН18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.
РН19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.
РН20. 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.
РН21. 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.
РН22. *Асоціювати себе як члена громадянського суспільства, розуміти і вміти користуватися власними правами і свободами, визначати і реалізовувати правомірні, й відповідальні способи участі в суспільному житті та національному спротиві*[2]*.*

[2] Програмний результат навчання щодо національного спротиву додано в 2026 р. з урахуванням змін в законодавстві про національний спротив.

IV ПЕРЕЛІК КОМПОНЕНТІВ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ ТА ЇХНЯ ЛОГІЧНА ПОСЛІДОВНІСТЬ

Увага: перелік компонентів може змінюватися в рамках щорічного удосконалення освітніх програм, окрім тих, що вже були опановані здобувачами освіти для відповідного року набору

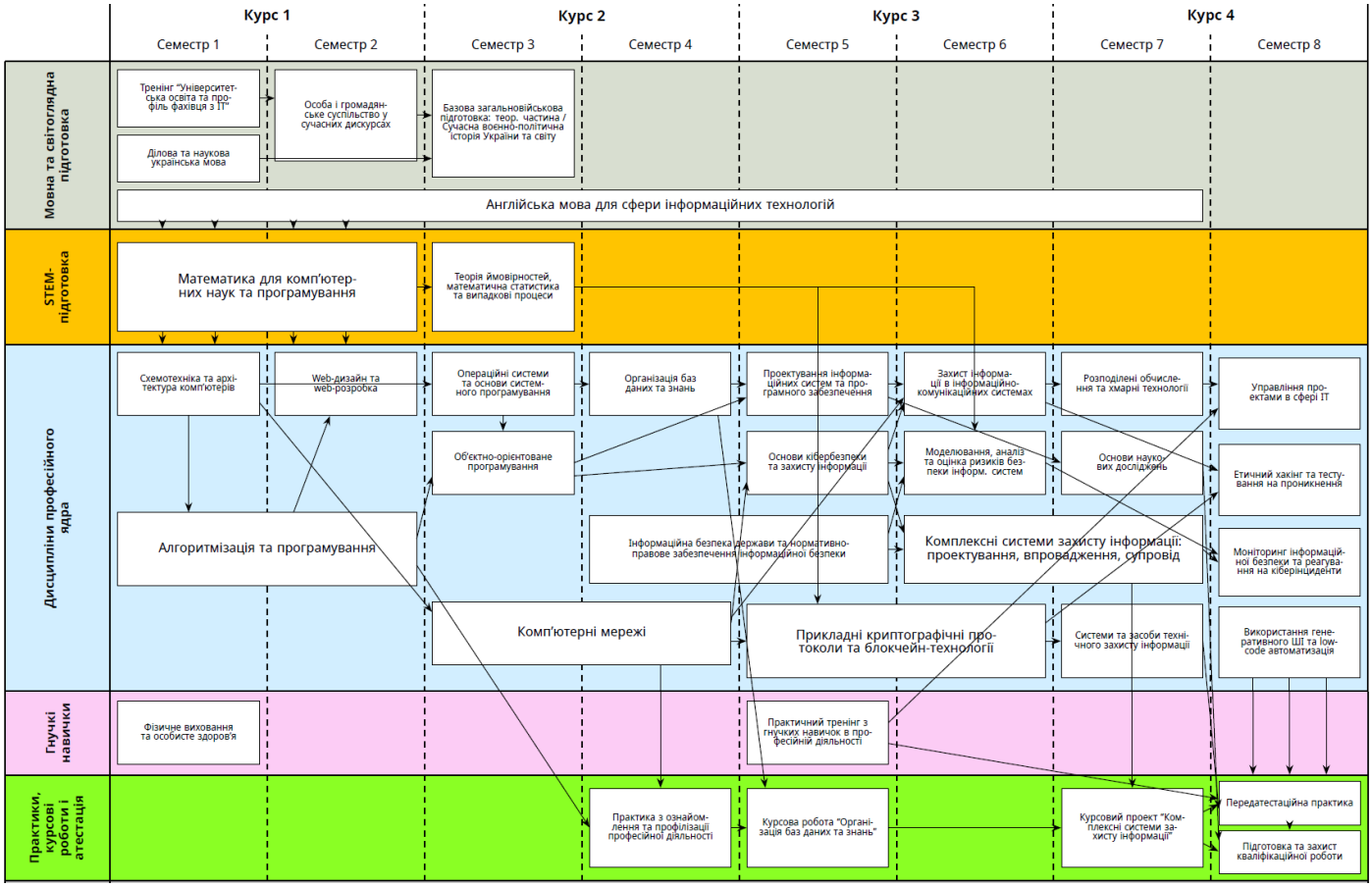
Набір 2026 року

№	Код	*Компоненти освітньої програми (навчальні дисципліни, курсові проекти/роботи, практики, кваліфікаційна робота)*	*Кількість кредитів ЄКТС*	*Форма підсумкового контролю*
	Обов'язкові компоненти			
1.	ОК42209	Тренінг «Університетська освіта та профіль фахівця з кібербезпеки»	1.5	залік
2.	ОК11008	Англійська мова для сфери інформаційних технологій	22	іспит
3.	ОК11010	Ділова та наукова українська мова	4	іспит
4.	ОК11016	Особа і громадянське суспільство у сучасних дискурсах	4	залік
5.	ОК11026	Фізичне виховання та особисте здоров'я	6	залік
6.	ОК15014	Математика для комп'ютерних наук та програмування	12	іспит
7.	ОК42211	Фізичні основи захисту інформації	6	залік
8.	ОК15030	Теорія ймовірностей, математична статистика та випадкові процеси	6	іспит
9.	ОК15019	Методи дослідження операцій	4	іспит
10.	ОК42015	Алгоритмізація та програмування	12	іспит
11.	ОК42212	Архітектура комп'ютерів та комп'ютерна схемотехніка	4	залік
12.	ОК42213	Теорія інформації та кодування, обробка сигналів	4	іспит
13.	ОК42215	Основи інформаційної та кібербезпеки	3.5	залік
14.	ОК42077	Об'єктно-орієнтоване програмування	7	залік
15.	ОК42081	Операційні системи та основи системного програмування	5	іспит
16.	ОК42056	Комп'ютерні мережі	4	іспит
17.	ОК42082	Організація баз даних та знань	4	іспит
18.	ОК42219	Системи штучного інтелекту для захисту інформації в кіберпросторі	9	залік
19.	ОК42221	Безпека інформаційно-комунікаційних систем та мереж	5	іспит
20.	ОК42238	Програмно-апаратні засоби та системи захисту інформації	5.5	залік
21.	ОК42223	Етичний хакінг, основи соціальної інженерії та дослідження загроз	3	залік
22.	ОК42239	Курсовий проєкт «Програмно-апаратні засоби та системи захисту інформації»	2	захист
23.	ОК14018	Основи наукових досліджень	3	залік
24.	ОК40076	Стандарти та методології бізнес-аналізу	3	залік
25.	ОК42118	Розподілені обчислення та хмарні технології	4	іспит

№	Код	*Компоненти освітньої програми (навчальні дисципліни, курсові проекти/роботи, практики, кваліфікаційна робота)*	*Кількість кредитів ЄКТС*	*Форма підсумкового контролю*
26.	ОК42225	Системи виявлення вторгнень та розслідування кіберінцидентів	7	залік
27.	ОК40156	Використання генеративного штучного інтелекту та low-code автоматизація	5	іспит
28.	ОК42218	Управління інформаційною безпекою	3.5	залік
29.	ОК42220	Нормативно-правове забезпечення інформаційної безпеки	3	іспит
30.	ОК14050	Практичний тренінг з гнучких навичок в професійній діяльності	1.5	захист
31.	ОК42155	Практика з ознайомлення та профілізації професійної діяльності	3	захист
32.	ОК42226	Переддипломна практика за ОПП «Кібербезпека та захист інформації»	6	захист
33.	ОК42227	Підготовка та захист кваліфікаційної бакалаврської роботи за ОПП «Кібербезпека та захист інформації»	7.5	атестація
Блок національного спротиву[3]				
34.	ОК11991	Основи національного спротиву	5,0	Залік
35.	ОК11992 / ОК11993	Сучасна воєнно-політична історія України та світу / Тренінг "Робота з ПТСР та тривожними станами в умовах воєнного часу"		Залік
Всього: обсяг освітніх обов'язкових компонентів			**180,0**	
Вибіркові компоненти				
1.	ВК1	Вибірковий компонент	5,0	Залік
2.	ВК2	Вибірковий компонент	5,0	Залік
3.	ВК3	Вибірковий компонент	5,0	Залік
4.	ВК4	Вибірковий компонент	5,0	Залік
5.	ВК5	Вибірковий компонент	5,0	Залік
6.	ВК6	Вибірковий компонент	5,0	Залік
7.	ВК7	Вибірковий компонент	5,0	Залік
8.	ВК8	Вибірковий компонент	5,0	Залік
9.	ВК9	Вибірковий компонент	5,0	Залік
10.	ВК10	Вибірковий компонент	5,0	Залік
11.	ВК11	Вибірковий компонент	5,0	Залік
12.	ВК12	Вибірковий компонент	5,0	Залік
Всього: обсяг вибіркових освітніх компонентів			**60,0**	
ВСЬОГО			**240,0**	

[3] Для денної форми навчання ОК «Основи національного спротиву» (5 кредитів) є обов'язковим компонентом для осіб, які визначені чинним законодавством, інші особи вивчають ОК «Сучасна воєнно-політична історія України та світу» (3 кредити) та Тренінг «Робота з ПТСР та тривожними станами в умовах воєнного часу» (2 кредити). Для заочної форми навчання в блоці національного спротиву компонентами за замовчуванням є «Сучасна воєнно-політична історія України та світу» та Тренінг «Робота з ПТСР та тривожними станами в умовах воєнного часу»; освітній компонент «Основи національного спротиву» може вивчатися за заявою здобувача освіти, однак потребуватиме або присутності на практичних заняттях, або проходження навчання в Центрах підготовки громадян до національного спротиву.

Структурно-логічна схема послідовності вивчення (виконання) обов’язкових освітніх компонент ОПП, набір 2026 року



V ФОРМА АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Випускна атестація здобувачів вищої освіти за освітньо-професійною програмою спеціальності F5 «Кібербезпека та захист інформації» проводиться у формі публічного захисту (демонстрації) кваліфікаційної бакалаврської роботи. Кваліфікаційна робота має передбачати теоретичне, системотехнічне або експериментальне дослідження складного спеціалізованого завдання або практичної проблеми в галузі кібербезпеки та захисту інформації, яке характеризується комплексністю та невизначеністю умов і потребує застосування теорій та методів інформаційних технологій. У кваліфікаційній роботі не може бути академічного плагіату, фальсифікації та списування.

Кваліфікаційна робота може виконуватися на матеріалах одного з Активів Групи МЕТІНВЕСТ. Оцінка результатів публічного захисту роботи здійснюється екзаменаційною комісією з урахуванням оцінки керівника і рецензента.

Кваліфікаційні роботи, що не містять комерційної таємниці, оприлюднюються у репозиторії Університету. Оприлюднення кваліфікаційних робіт, що містять інформацію з обмеженим доступом, здійснюється шляхом оприлюднення версії з виключенням відповідної інформації.

VI МАТРИЦЯ ЗАБЕЗПЕЧЕННЯ ПРОГРАМНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ КОМПОНЕНТАМИ ОП

Рік набору 2026

№ з/п	Назва ОК	Шифр ОК	Програмні результати навчання																					
			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	РН 22
1.	Тренінг «Університетська освіта та профіль фахівця з кібербезпеки»	ОК42209				+	+	+			+	+												
2.	Англійська мова для сфери інформаційних технологій	ОК11008		+																				
3.	Ділова та наукова українська мова	ОК11010	+			+																		
4.	Особа і громадянське суспільство у сучасних дискурсах	ОК11016			+		+																	+
5.	Фізичне виховання та особисте здоров'я	ОК11026				+																		+
6.	Математика для комп'ютерних наук та програмування	ОК15014							+	+		+												
7.	Фізичні основи захисту інформації	ОК42211							+	+												+		
8.	Теорія ймовірностей, математична статистика та випадкові процеси	ОК15030							+	+									+				+	
9.	Методи дослідження операцій	ОК15019				+	+			+		+												
10.	Алгоритмізація та програмування	ОК42015				+						+			+									
11.	Архітектура комп'ютерів та комп'ютерна схемотехніка	ОК42212										+		+	+							+		
12.	Теорія інформації та кодування, обробка сигналів	ОК42213							+	+										+	+	+		
13.	Основи інформаційної та кібербезпеки	ОК42215									+	+		+					+				+	
14.	Об'єктно-орієнтоване програмування	ОК42077				+						+			+									
15.	Операційні системи та основи системного програмування	ОК42081										+		+	+	+							+	
16.	Комп'ютерні мережі	ОК42056										+		+	+								+	
17.	Організація баз даних та знань	ОК42082										+		+	+								+	
18.	Системи штучного інтелекту для захисту інформації в кіберпросторі	ОК42219						+				+					+						+	
19.	Безпека інформаційно-комунікаційних систем та мереж	ОК42221												+	+	+	+						+	
20.	Програмно-апаратні засоби та системи захисту інформації	ОК42238												+	+			+				+	+	
21.	Етичний хакінг, основи соціальної інженерії та дослідження загроз	ОК42223			+		+				+						+						+	
22.	Курсовий проєкт «Програмно-апаратні засоби та системи захисту інформації»	ОК42239												+	+			+				+	+	
23.	Основи наукових досліджень	ОК14018				+	+	+									+							
24.	Стандарти та методології бізнес-аналізу	ОК40076											+						+					
25.	Розподілені обчислення та хмарні технології	ОК42118										+		+	+	+								
26.	Системи виявлення вторгнень та розслідування кіберінцидентів	ОК42225														+	+		+				+	
27.	Використання генеративного штучного інтелекту та low-code автоматизація	ОК40156						+				+											+	
28.	Управління інформаційною безпекою	ОК42218									+		+						+					
29.	Нормативно-правове забезпечення інформаційної безпеки	ОК42220			+						+										+			
30.	Практичний тренінг з гнучких навичок в професійній діяльності	ОК14050	+	+		+	+	+																
31.	Практика з ознайомлення та профілізації професійної діяльності	ОК42155				+	+				+	+		+									+	
32.	Переддипломна практика за ОПП «Кібербезпека та захист інформації»	ОК42226				+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	
33.	Підготовка та захист кваліфікаційної бакалаврської роботи за ОПП «Кібербезпека та захист інформації»	ОК42227	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
34.	Основи національного спротиву / альтернативні компоненти відповідно до чинного порядку	ОК11991			+		+																	+
35.	Сучасна воєнно-політична історія України та світу / Тренінг "Робота з ПТСР та тривожними станами в умовах воєнного часу"	ОК11992 / ОК11993			+		+																	+

VII МАТРИЦЯ ВІДПОВІДНОСТІ ПРОГРАМНИХ КОМПЕТЕНТНОСТЕЙ КОМПОНЕНТАМ ОСВІТНЬОЇ ПРОГРАМИ

Рік набору 2026

№ з/п	Назва ОК	Шифр ОК	Загальні компетентності								Фахові (спеціальні) компетентності									
			ЗК 1	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
1.	Тренінг «Університетська освіта та профіль фахівця з кібербезпеки»	ОК42209	+	+			+				+	+								
2.	Англійська мова для сфери інформаційних технологій	ОК11008				+	+													
3.	Ділова та наукова українська мова	ОК11010			+		+													
4.	Особа і громадянське суспільство у сучасних дискурсах	ОК11016						+	+	+										
5.	Фізичне виховання та особисте здоров'я	ОК11026								+										
6.	Математика для комп'ютерних наук та програмування	ОК15014	+	+			+					+								
7.	Фізичні основи захисту інформації	ОК42211	+	+															+	
8.	Теорія ймовірностей, математична статистика та випадкові процеси	ОК15030	+				+					+								+
9.	Методи дослідження операцій	ОК15019	+				+					+								
10.	Алгоритмізація та програмування	ОК42015	+	+			+					+		+						+
11.	Архітектура комп'ютерів та комп'ютерна схемотехніка	ОК42212	+	+								+		+					+	
12.	Теорія інформації та кодування, обробка сигналів	ОК42213	+	+								+						+	+	
13.	Основи інформаційної та кібербезпеки	ОК42215	+	+							+	+		+			+		+	
14.	Об'єктно-орієнтоване програмування	ОК42077	+	+			+					+		+						+
15.	Операційні системи та основи системного програмування	ОК42081	+	+								+		+	+	+				+
16.	Комп'ютерні мережі	ОК42056	+	+								+	+	+	+					+
17.	Організація баз даних та знань	ОК42082	+	+								+		+	+					+
18.	Системи штучного інтелекту для захисту інформації в кіберпросторі	ОК42219	+	+			+					+					+			+
19.	Безпека інформаційно-комунікаційних систем та мереж	ОК42221	+	+										+	+				+	+
20.	Програмно-апаратні засоби та системи захисту інформації	ОК42238	+	+										+		+			+	+
21.	Етичний хакінг, основи соціальної інженерії та дослідження загроз	ОК42223	+	+			+		+											+
22.	Курсовий проєкт «Програмно-апаратні засоби та системи захисту інформації»	ОК42239	+	+			+							+		+			+	+
23.	Основи наукових досліджень	ОК14018	+	+			+					+								+
24.	Стандарти та методології бізнес-аналізу	ОК40076	+	+			+						+				+			
25.	Розподілені обчислення та хмарні технології	ОК42118	+	+			+					+		+	+					
26.	Системи виявлення вторгнень та розслідування кіберінцидентів	ОК42225	+	+			+								+					+
27.	Використання генеративного штучного інтелекту та low-code автоматизація	ОК40156	+	+			+					+								+
28.	Управління інформаційною безпекою	ОК42218	+	+			+						+				+			
29.	Нормативно-правове забезпечення інформаційної безпеки	ОК42220		+				+	+		+									
30.	Практичний тренінг з гнучких навичок в професійній діяльності	ОК14050	+	+	+	+	+				+	+	+	+	+					
31.	Практика з ознайомлення та профілізації професійної діяльності	ОК42155	+	+	+	+	+				+	+		+						+
32.	Переддипломна практика за ОПП «Кібербезпека та захист інформації»	ОК42226	+	+	+	+	+	+	+		+	+	+	+	+	+	+	+	+	+
33.	Підготовка та захист кваліфікаційної бакалаврської роботи за ОПП «Кібербезпека та захист інформації»	ОК42227	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
34.	Основи національного спротиву / альтернативні компоненти відповідно до чинного порядку	ОК11991	+					+	+	+										
35.	Сучасна воєнно-політична історія України та світу / Тренінг "Робота з ПТСР та тривожними станами в умовах воєнного часу"	ОК11992 / ОК11993	+					+	+	+										