Міністерство освіти і науки України
Державний вищий навчальний заклад
«Український державний хіміко-технологічний університет»

ОСВІТНЬО–ПРОФЕСІЙНА ПРОГРАМА

Кібербезпека в комп'ютерних мережах

РІВЕНЬ ВИЩОЇ ОСВІТИ **Перший (бакалаврський) рівень**
(назва рівня вищої освіти)

СПЕЦІАЛЬНІСТЬ **125 Кібербезпека**
(код та найменування спеціальності)

ГАЛУЗЬ ЗНАНЬ **12 Інформаційні технології**
(шифр та назва галузі знань)

ОСВІТНЯ КВАЛІФІКАЦІЯ **Бакалавр з кібербезпеки**
(назва ступеня, що присвоюється)

ЗАТВЕРДЖЕНО
Вченою радою ДВНЗ УДХТУ
Протокол № 5 від 29.04. 2021р

ВВОДИТЬСЯ В ДІЮ
з 1.09 2021р.

Ректор Сухий К.М.
Наказ № 71 від 30.04. 2021р.

Дніпро 2021р.

Міністерство освіти і науки України
Державний вищий навчальний заклад
«Український державний хіміко-технологічний університет»

ОСВІТНЬО–ПРОФЕСІЙНА ПРОГРАМА

Кібербезпека в комп'ютерних мережах

РІВЕНЬ ВИЩОЇ ОСВІТИ **Перший (бакалаврський) рівень**
(назва рівня вищої освіти)

СПЕЦІАЛЬНІСТЬ **125 Кібербезпека**
(код та найменування спеціальності)

ГАЛУЗЬ ЗНАНЬ **12 Інформаційні технології**
(шифр та назва галузі знань)

ОСВІТНЯ КВАЛІФІКАЦІЯ **Бакалавр з кібербезпеки**
(назва ступеня, що присвоюється)

ЗАТВЕРДЖЕНО
Вченою радою ДВНЗ УДХТУ
Протокол № 5 від 29.04. 2021р

ВВОДИТЬСЯ В ДІЮ
З 1.09 2021р.

Ректор _____ /Сухий К.М./
Наказ № 42 від 30.04. 2021р.

Дніпро 2021р.

ПЕРЕДМОВА

Розроблено робочою групою у складі:

1. Голова робочої групи (гарант освітньої програми):

Косолап Анатолій Іванович, д-р.фіз-мат. наук, професор

Члени робочої групи:

2. Овчаренко Ольга Вікторівна, к.е.н., доцент, кафедра спеціалізованих комп'ютерних систем

3. Поліщук Юлія Валеріївна, к.т.н., доцент, кафедра теорії неорганічних речовин та екології

4. Завідувач кафедри «Спеціалізованих комп'ютерних систем» Косолап А.І., д-р.фіз-мат. наук, професор

Рецензії відгуки зовнішніх стейкголдерів:

1. Лист-підтримка від начальника відділу ІТ та ЕУ Слобожанской селищної ради

2. Лист-підтримка від Фінансовий директор ТОВ «КІВІСМАРТЮВА»

3. Лист-підтримка від _Приватбанк

4. Лист-підтримка від Публічне акціонерне товариство «Банк-Восток»

Освітня програма розроблена на основі Освітнього стандарту спеціальності 125-«Кібербезпека» для першого (бакалаврського) рівня освіти, що погоджено рішенням Національного агентства із забезпечення якості вищої освіти від 22 травня 2017 р. № 72 та затверджено Наказом МОН України № 1074 від 04.10.2018 р.

І. ПРОФІЛЬ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ БАКАЛАВРА
зі спеціальності 125 -«Кібербезпека»

1. Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	Державний вищий навчальний заклад «Український державний хіміко-технологічний університет». Факультет комп'ютерних наук та інженерії Кафедра спеціалізованих комп'ютерних систем
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Бакалавр Бакалавр, кібербезпека
Офіційна назва освітньої програми	Кібербезпека в комп'ютерних мережах
Тип диплому та обсяг освітньої програми	Диплом бакалавра з кібербезпеки, одиничний (подвійний, спільний при наявності відповідних договорів, програм навчання). 240 кредитів ЄКТС на базі повної загальної середньої освіти; на базі ступеня «молодший бакалавр»/ «фаховий молодший бакалавр» (освітньо-кваліфікаційного рівня «молодший спеціаліст») університет має право визнати та перерахувати кредити ЄТКС, отримані в межах попередньої освітньої програми підготовки молодшого бакалавра/фахового молодшого бакалавра (молодшого спеціаліста), обсягом не більше ніж 120 кредитів ЄТКС.
Наявність акредитації	Акредитаційна комісія МОН України; Строк дії сертифіката про акредитацію до
Цикл/рівень	НРК України – 6 рівень, FQ-EHEA – перший цикл, EQF-LLL – 6 рівень
Передумови	Повна загальна середня освіта або ступінь «молодший бакалавр»/«фаховий молодший бакалавр» (освітньо-кваліфікаційний рівень «молодший спеціаліст»).
Мова(и) викладання	Українська мова
Термін дії освітньої програми	10 років.
Інтернет-адреса постійного розміщення опису освітньої програми	https://udhtu.edu.ua/osvitni-programy
2- Цілі освітньої програми	
Ціль освітньої програми	Підготовка ІТ-професіоналів, здатних проектувати, використовувати та впроваджувати комп'ютерні технології інформаційно-комунікаційної та/або кібербезпеки.
3 Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність)	Галузь знань 12 - інформаційні технології**:** спеціальність 125 - кібербезпека

Орієнтація програми	Освітньо-професійна програма має прикладну орієнтацію. Професійні акценти: розробка надійного програмного та апаратного забезпечення комп'ютерних мереж, що забезпечує надійний захист інформації.
Основний фокус програми та спеціалізації	Загальна вища освіта в галузі інформаційних технологій. Здобуття вищої освіти в галузі інформаційні технології, спеціальності 125 „Кібербезпека". Акцент на здатності проектувати та підтримувати комп'ютерні системи та мережі різного призначення, забезпечувати захист інформаційно-комунікаційних мереж та якісне використання обчислювальної техніки у різноманітних галузях виробництва. Ключові слова: кібербезпека, комп'ютерні системи, комп'ютерні мережі, захист інформації, програмування, проектування, адміністрування, мобільні системи.
Особливості та відмінності	Підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки. Орієнтація на здобуття фундаментальних знань та практичних навичок в галузі кібербезпеки в комп'ютерних мережах, які забезпечать не тільки надійний захист інформації, а й ефективне її використання.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Об'єкти професійної діяльності випускників: – об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно- телекомунікаційні системи, інформаційні ресурси і технології; – технології забезпечення безпеки інформації; процеси управління інформаційною та/або кібербезпекою об'єктів, що підлягають захисту. Відповідно до здобутої освітньої кваліфікації бакалавр здатний виконувати професійні роботи за професіями, зазначеними у Національному класифікаторі України КП ДК 003:2010 , а саме: - 312 Технічні фахівці в галузі обчислювальної техніки - 3114 Фахівець інфокомунікацій -3121 Фахівець з розробки та тестування програмного забезпечення - 3439 Фахівець із організації захисту інформації з обмеженим доступом
Подальше навчання	Навчання на другому освітньому рівні за магістерським програмами у галузі інформаційних технологій. НРК України – 7 рівень, QF-EHEA – другий цикл, EQF-LLL – 7 рівень
5 – Викладання та оцінювання	
Викладання та навчання	Комбінація лекцій, практичних та семінарських занять,

	експериментальні дослідження в лабораторіях, написання курсових проектів або робіт, самонавчання, підготовка кваліфікаційної роботи.
Методи оцінювання	Для оцінювання знань здобувачів вищої освіти передбачено: поточний контроль знань; підсумковий контроль знань державна атестація із відповідними методами оцінювання: - письмові контрольні, практичні, розрахунково-графічні роботи, захист лабораторних робіт, рефератів, есе та доповідей, тестові завдання, усне опитування, колоквіуми; заліки, презентації; - письмові та усні екзамени, захист курсових проектів/робіт та звітів з практик; - прилюдний захист бакалаврської кваліфікаційної роботи.
6 – Програмні компетентності	
Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки та\або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.
Загальні компетентності (ЗК)	ЗК1. Здатність застосовувати знання у практичних ситуаціях. ЗК2. Знання та розуміння предметної області та розуміння професії. ЗК3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. ЗК4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. ЗК5. Здатність до пошуку, оброблення та аналізу інформації. 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 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. ЗК8 Здатність працювати в команді.
Спеціальні (фахові) компетентності (ФК)	ФК1. Здатність застосовувати законодавчу та нормативноправову базу, а також державні та міжнародні

	вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки. ФК2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. ФК3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. ФК4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. ФК5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. ФК6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. ФК7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.) ФК8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. ФК9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. ФК10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності. ФК11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. ФК12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.
7 – Програмні результати навчання	
Результати навчання в	ПРН1 застосовувати знання державної та іноземних мов з

когнітивній (пізнавальній) сфері	метою забезпечення ефективності професійної комунікації; ПРН2 організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; ПРН3 використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; ПРН4 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; ПРН5 адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат; ПРН6 критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; ПРН7 діяти на основі законодавчої та нормативноправової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки; ПРН8 готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки; ПРН9 впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; ПРН10 виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем; ПРН11 виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах; ПРН12 розробляти моделі загроз та порушника; ПРН13 аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; ПРН14 вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; ПРН15 використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; ПРН16 реалізовувати комплексні системи захисту

	інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів; ПРН17 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; ПРН18 використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; ПРН19 застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; ПРН20 забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах; ПРН21 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; ПРН22 вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної та\або кібербезпеки; ПРН23 реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; ПРН24 вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); ПРН25 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; ПРН26 впроваджувати заходи та забезпечувати реалізацію

	процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем; ПРН27 вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; ПРН28 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; ПРН29 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; ПРН30 здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем; ПРН31 застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем; ПРН32 вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки; ПРН33 вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків; ПРН34 приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; ПРН35 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; ПРН36 виявляти небезпечні сигнали технічних засобів; ПРН37 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; ПРН38 інтерпретувати результати проведення спеціальних

	вимірювань з використанням технічних засобів, контролю характеристик інформаційнотелекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації; ПРН39 проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах; ПРН40 інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації; ПРН41 забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур; ПРН42 впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; ПРН43 застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; ПРН44 вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; ПРН45 застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризикорієнтованому контролі доступу до інформаційних активів; ПРН46 здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах; ПРН47 вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації; ПРН48 виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; ПРН49 забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах; ПРН50 забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень

	різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); ПРН51 підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; ПРН52 використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах; ПРН53 вирішувати задачі аналізу програмного коду на наявність можливих загроз. ПРН54 усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Відповідає кадровим вимогам щодо забезпечення провадження освітньої діяльності у сфері вищої освіти Ліцензійних умов провадження освітньої діяльності у сфері вищої освіти. Науково-педагогічні працівники обов'язково підвищують свою кваліфікацію за дисциплінами, що викладають, відповідно до нормативних вимог та впроваджують результати стажування і наукової діяльності у освітній процес. Також до освітнього процесу залучаються: представники роботодавців шляхом відкритих лекцій за окремими темами, тематичних семінарів із залученням широкого кола представників підприємств та студентів, керівництва практичною підготовкою, участі у екзаменаційних комісіях з захисту кваліфікаційних робіт здобувачів вищої освіти. Викладання фахових дисциплін забезпечує професорсько викладацький склад кафедри: 3 доктора та 5 кандидатів наук.
Матеріально-технічне забезпечення	Відповідає технологічним вимогам щодо забезпечення провадження освітньої діяльності у сфері вищої освіти Ліцензійних умов провадження освітньої діяльності у сфері вищої освіти. Навчання за ОП здійснюється в предметних аудиторіях, спеціалізованих лабораторіях, комп'ютерних класах та навчальних кабінетах, обладнаних відповідно до змісту навчальних дисциплін. Освітній процес забезпечений комп'ютерною технікою, сучасними програмними засобами, мультимедійним та спеціальним обладнанням; студенти мають безкоштовний доступ до мережі Інтернет та бібліотеки університету з читальними залами. До послуг студентів – гуртожитки, спортивні зали та майданчики, пункти харчування, літній

	оздоровчий табір, актова зала.
Інформаційне та навчально-методичне забезпечення	Відповідає технологічним вимогам щодо забезпечення провадження освітньої діяльності у сфері вищої освіти Ліцензійних умов провадження освітньої діяльності у сфері вищої освіти: Навчально-методичне забезпечення передбачає наявність: затвердженої ОП, навчальних планів, робочих програм з усіх навчальних дисциплін, програм з усіх видів практичної підготовки; методичних матеріалів для проведення підсумкової атестації здобувачів вищої освіти; навчальних планів з обов'язковим вивченням української мови як окремої навчальної дисципліни "Українська мова як іноземна", навчально-методичні комплекси дисциплін із відповідним навчально-методичним контентом. Офіційний веб-сайт https://udhtu.edu.ua (українською та англійською момою) містить інформацію про освітні програми, навчальну, наукову і виховну діяльність, структурні підрозділи, правила прийому, контакти. Ресурси науково-технічної бібліотеки доступні через сайт бібліотеки університету: https://biblioteka.udhtu.edu.ua. Комп'ютерна мережа університету підключена до ресурсів Scopus та Web of Science. Для покращення навчального процесу застосовуються технології електронного навачаня, у тому числі із використанням сайту дистанційного навчання ДВНЗ УДХТУ на платформі http://do.udhtu.edu.ua, де розміщені матеріали навчально-методичного забезпечення ОП.
9 – Академічна мобільність	
Національна кредитна мобільність	Здійснюється на основі двосторонніх договорів між ДВНЗ УДХТУ та відповідними університетами України. Допускається перезарахування кредитів, отриманих у інших закладах освіти України.
Міжнародна кредитна мобільність	на основі двосторонніх договорів між ДВНЗ УДХТУ та іноземними університетами. Допускається перезарахування кредитів, отриманих у іноземних закладах освіти.
Навчання іноземних здобувачів вищої освіти	Навчання іноземних здобувачів вищої освіти проводиться на загальних умовах з додатковою мовною підготовкою.

2. Перелік компонент освітньо-професійної програми та їх логічна послідовність

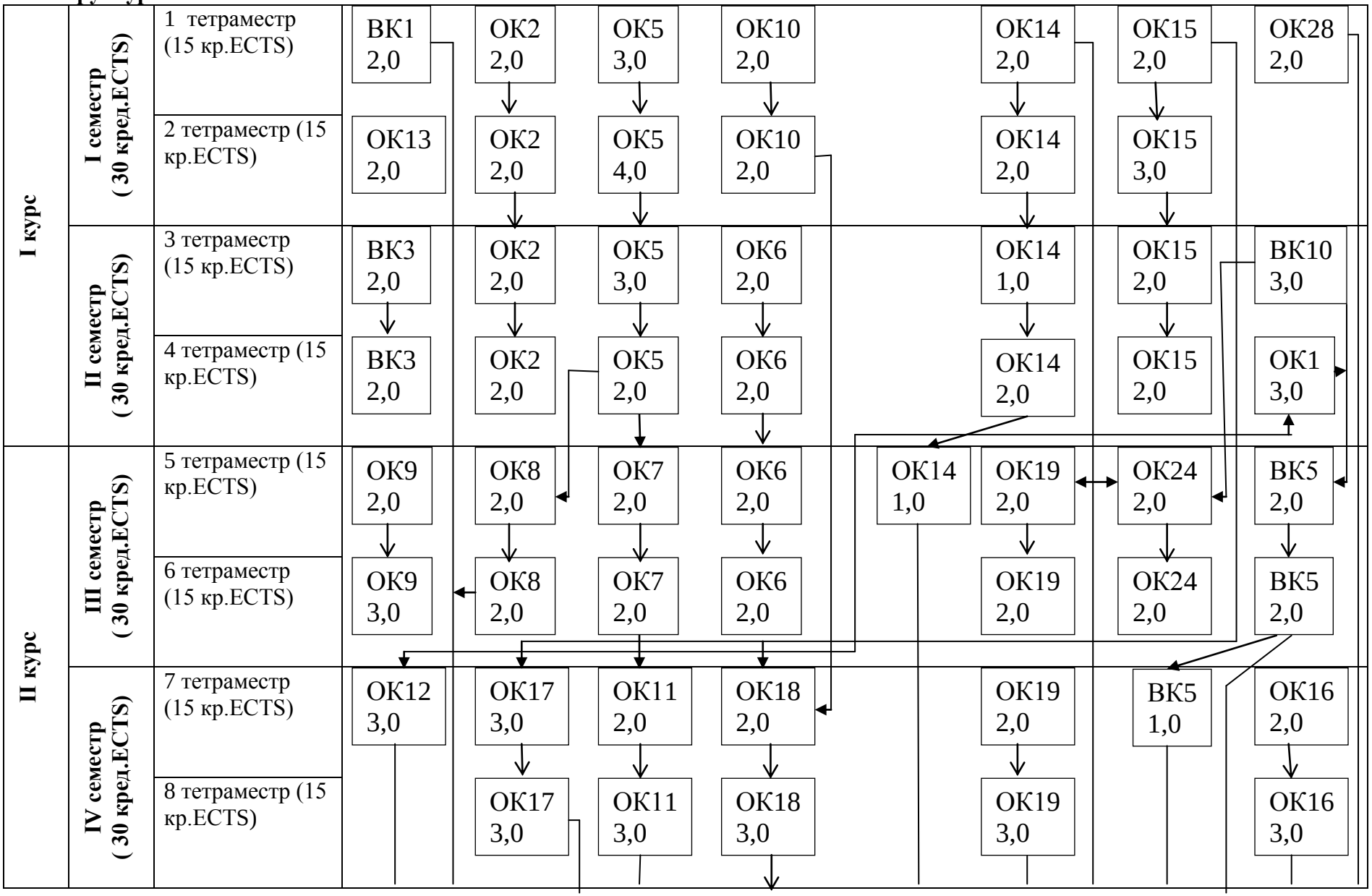
2.1 Перелік компонент ОП

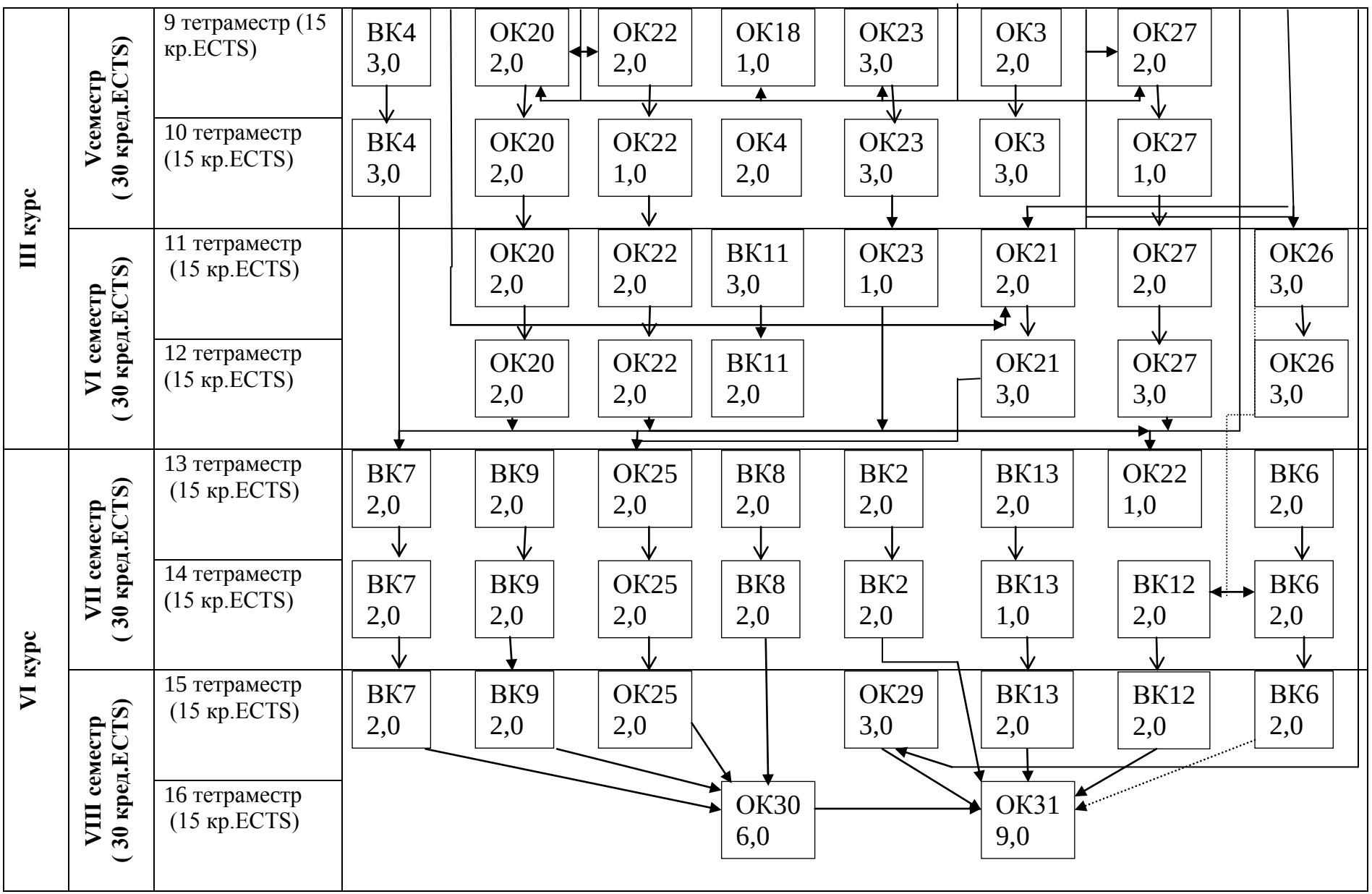
Код к-ти	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1	**2**	**3**	**4**
1. ОБОВ'ЯЗКОВІ КОМПОНЕНТИ			
1.1. Цикл загальної підготовки			
ОК1	Історія України	3,0	екзамен
ОК2	Іноземна мова (за професійним спрямуванням)	8,0	екзамен / залік
ОК3	Філософія	5,0	екзамен
ОК4	Правознавство	2,0	залік
ОК5	Вища математика	12,0	екзамен
ОК6	Фізика	8,0	екзамен
ОК7	Електротехніка та електроніка	4,0	екзамен
ОК8	Теорія ймовірностей, ймовірностні процеси та математична статистика	4,0	екзамен
ОК9	Основи інформаційної безпеки	5,0	екзамен
ОК10	Дискретна математика	4,0	екзамен
ОК11	Комп'ютерна електроніка	5,0	екзамен
ОК12	Українська мова (за професійним спрямуванням)	3,0	екзамен
ОК13	Екологія	2,0	залік
	РАЗОМ за циклом 1.1	**65,0**	
1.2. Цикл професійної підготовки			
ОК14	Алгоритмізація та програмування	8,0	екзамен/дифзалік
ОК15	Комп'ютерна логіка	9,0	залік/екзамен
ОК16	Теорія інформації та кодування	5,0	залік
ОК17	Архітектура комп'ютерів	6,0	екзамен
ОК18	Комп'ютерна схемотехніка	6,0	дифзалік
ОК19	Системне програмування	9,0	залік/екзамен
ОК20	Системне програмне забезпечення	8,0	залік/екзамен
ОК21	Адміністрування та безпека комп’ютерних мереж	5,0	екзамен

ОК22	Комп'ютерні системи	8,0	залік/екзамен
ОК23	Комп'ютерні мережі	7,0	залік/екзамен
ОК24	Організація баз даних та знань	4,0	залік
ОК25	Управління телекомунікаційними системами та мережами	6,0	залік /екзамен
ОК26	Розробка надійного програмного забезпечення	6,0	залік
ОК27	Програмування на мові Java	8,0	залік /екзамен
ОК28	Безпека життєдіяльності	2,0	залік
ОК29	Основи охорони праці	3,0	екзамен
ОК30	Виробнича практика	6,0	дифзалік
ОК31	Підготовка кваліфікаційної бакалаврської роботи та державна атестація (ДА)	9,0	-
	РАЗОМ за циклом 1.2	**115,0**	
	ОБОВ'ЯЗКОВІ КОМПОНЕНТИ РАЗОМ	**180,0**	
2. ВИБІРКОВІ КОМПОНЕНТИ			
2.1. Цикл загальної підготовки			
ВК1	**Дисципліни гуманітарної підготовки**	2,0	дифзалік
ВК2	**Дисципліни економічної підготовки**	4,0	залік
ВК3	**Дисципліни природничо-наукової підготовки**	4,0	залік
	РАЗОМ за циклом 2.1	**10,0**	
Вибірковий блок 1 – Оптимізація захисту даних			
ВК4	Системний аналіз	6,0	екзамен
ВК5	Інтернет-технології	5,0	залік
ВК6	Оптимізація захисту та використання інформації в комп’ютерних мережах	6,0	залік /екзамен
ВК7	Системи управління ризиками в кібербезпеці	6,0	залік/екзамен
ВК8	Методи верифікації та тестування програмного забезпечення	4,0	екзамен
ВК9	Мережеве програмування	6,0	залік/екзамен
	Один з модулів	**17,0**	
	Модуль 1		
ВК10	Офісні комп'ютерні технології	3,0	залік
ВК11	Прикладна криптографія	5,0	залік
ВК12	Захист банківських операцій	4,0	залік
ВК13	Проектування систем штучного	5,0	залік /екзамен

	інтелекту		
	Модуль 2		
ВК14	Комп'ютерна графіка	3,0	залік
ВК15	Управління інформаційною безпекою	5,0	залік
ВК16	Технології клієнт-сервер	4,0	залік
ВК17	Мультимедійні системи	5,0	залік /екзамен
Вибірковий блок 2 – Системний аналіз захисту інформації			
ВК18	Вступ в спеціальність	6,0	залік /екзамен
ВК19	Інтернет-технології	5,0	залік
ВК20	Аналіз даних	6,0	залік /екзамен
ВК21	Методи верифікації та тестування програмного забезпечення	6,0	екзамен
ВК22	Системи технічного захисту інформації	4,0	залік
ВК23	Інженерія програмного забезпечення	6,0	залік/екзамен
	Один з модулів	**17,0**	
	Модуль 1		
ВК24	Комп'ютерна графіка	3,0	залік
ВК25	Стеганографія	5,0	залік
ВК26	Системи управління мобільними пристроями	4,0	залік /екзамен
ВК27	Проектування систем штучного інтелекту	5,0	залік
	Модуль 2		
ВК28	Офісні комп'ютерні технології	3,0	залік
ВК29	Технології клієнт-сервер	5,0	залік
ВК30	Аналіз та застосування криптовалют	4,0	залік/екзамен
ВК31	Мультимедійні системи	5,0	залік
	РАЗОМ за циклом 2.2	**50,0**	
	ВИБІРКОВІ КОМПОНЕНТИ РАЗОМ	**60,0**	
	ЗАГАЛЬНИЙ ОБСЯГ	**240,0**	

2.2 Структурно-логічна схема




III курс
VI курс
Vсеместр (30 кред.ECTS)
VI семестр (30 кред.ECTS)
VII семестр (30 кред.ECTS)
VIII семестр (30 кред.ECTS)
9 тетраместр (15 кр.ECTS)
10 тетраместр (15 кр.ECTS)
11 тетраместр (15 кр.ECTS)
12 тетраместр (15 кр.ECTS)
13 тетраместр (15 кр.ECTS)
14 тетраместр (15 кр.ECTS)
15 тетраместр (15 кр.ECTS)
16 тетраместр (15 кр.ECTS)
ВК4 3,0
ОК20 2,0
ОК22 2,0
ОК18 1,0
ОК23 3,0
ОК3 2,0
ОК27 2,0
ВК4 3,0
ОК20 2,0
ОК22 1,0
ОК4 2,0
ОК23 3,0
ОК3 3,0
ОК27 1,0
ОК20 2,0
ОК22 2,0
ВК11 3,0
ОК23 1,0
ОК21 2,0
ОК27 2,0
ОК26 3,0
ОК20 2,0
ОК22 2,0
ВК11 2,0
ОК21 3,0
ОК27 3,0
ОК26 3,0
ВК7 2,0
ВК9 2,0
ОК25 2,0
ВК8 2,0
ВК2 2,0
ВК13 2,0
ОК22 1,0
ВК6 2,0
ВК7 2,0
ВК9 2,0
ОК25 2,0
ВК8 2,0
ВК2 2,0
ВК13 1,0
ВК12 2,0
ВК6 2,0
ВК7 2,0
ВК9 2,0
ОК25 2,0
ОК29 3,0
ВК13 2,0
ВК12 2,0
ВК6 2,0
ОК30 6,0
ОК31 9,0

3. Форма атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація за освітньою програмою Кібербезпека в комп'ютерних мережах спеціальності 125 - кібербезпека здійснюється відкрито у формі публічного захисту кваліфікаційної роботи. На атестацію виноситься сукупність знань, умінь, навичок, інших компетентностей, набутих особою у процесі навчання за даним стандартом. До атестації допускаються студенти, які виконали всі вимого програми підготовки.
Вимоги до кваліфікаційної роботи (за наявності)	Кваліфікаційна робота має передбачати розв'язання спеціалізованої задачі в галузі інформаційної безпеки та кібербезпеки. Кваліфікаційна робота має бути перевірена на плагіат з оприлюдненням на сайті. Кваліфікаційна робота має бути розміщена на сайті або у репозитарії університету.
Документи, які отримує випускник	Випускник отримує документ встановленого зразка про присудження йому ступеня бакалавр із присвоєнням кваліфікації: бакалавр, Кібербезпека.

4. Матриця відповідності програмних компетентностей навчальним компонентам освітньої програми кібербезпека в комп'ютерних мережах (обов'язкові компоненти)

	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ОК14	ОК15	ОК16	ОК17	ОК18	ОК19	ОК20	ОК21	ОК22	ОК23	ОК24	ОК25	ОК26	ОК27	ОК28	ОК29	ОК30	ОК31
ЗК1		+			+	+			+	+				+			+		+										+	+
ЗК2							+		+		+			+	+	+	+	+	+	+	+	+	+		+					+	+
ЗК3	+	+										+																			
ЗК4					+			+							+	+				+	+		+		+	+	+			+	+
ЗК5																								+							
ЗК6	+			+																											
ЗК7	+		+										+															+	+		
ЗК8																							+					+	+		
ФК1				+					+																+						+
ФК2																+					+										
ФК3																										+	+				
ФК4				+																											
ФК5																										+	+				
ФК6																			+	+		+	+								
ФК7									+																						
ФК8																															+
ФК9																														+	
ФК10																								+							
ФК11																							+		+				+		
ФК12																						+									+

4. Матриця відповідності програмних компетентностей навчальним компонентам освітньої програми кібербезпека в комп'ютерних мережах (вибіркові компоненти)

	Блок 1																		Блок 2																	
	ВК1	ВК2	ВК3	ВК4	ВК5	ВК6	ВК7	ВК8	ВК9	ВК10	ВК11	ВК12	ВК13	ВК14	ВК15	ВК16	ВК17	ВК18	ВК19	ВК20	ВК21	ВК22	ВК23	ВК24	ВК25	ВК26	ВК27	ВК28	ВК29	ВК30	ВК31
ЗК1					+			+		+		+		+		+			+			+		+		+		+		+	
ЗК2						+	+	+												+	+	+									
ЗК3	+																														
ЗК4								+														+									
ЗК5			+	+														+													
ЗК6		+																													
ЗК7	+																														
ЗК8										+				+										+				+			
ФК1										+				+										+				+			
ФК2						+														+											
ФК3					+								+				+		+								+				+
ФК4		+																													
ФК5											+				+										+				+		
ФК6												+				+										+				+	
ФК7												+				+										+				+	
ФК8							+				+				+						+				+				+		
ФК9										+				+										+				+			
ФК10											+				+										+				+		
ФК11								+	+													+	+								
ФК12				+	+													+	+												

5. Матриця забезпечення програмних результатів навчання (ПРН) відповідними компонентами освітньої програми кібербезпека в комп'ютерних мережах (обов'язкові компоненти)

	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ОК14	ОК15	ОК16	ОК17	ОК18	ОК19	ОК20	ОК21	ОК22	ОК23	ОК24	ОК25	ОК26	ОК27	ОК28	ОК29	ОК30	ОК31
ПРН1		+										+																			+
ПРН2																														+	
ПРН3					+	+		+																+					+	+	+
ПРН4										+															+	+					+
ПРН5					+	+		+																	+						
ПРН6					+	+		+							+						+		+			+					+
ПРН7									+					+								+				+			+			
ПРН8																												+			
ПРН9																						+				+						
ПРН10																										+		+				
ПРН11																								+	+							
ПРН12										+														+		+						
ПРН13																							+	+								
ПРН14							+				+							+	+								+	+				
ПРН15							+		+		+															+		+				
ПРН16										+				+																		
ПРН17																							+									
ПРН18													+			+	+	+	+	+		+	+		+	+	+			+		
ПРН19															+						+				+							
ПРН20																+				+												
ПРН21					+	+		+													+					+						
ПРН22										+	+					+				+			+									

ПРН23																									+						
ПРН24																+			+	+							+				
ПРН25																+				+							+				
ПРН26		+																	+					+	+						
ПРН27									+		+											+	+		+						+
ПРН28															+									+	+	+					+
ПРН29									+												+				+		+				+
ПРН30															+	+			+	+	+						+				
ПРН31										+				+								+	+	+	+						+
ПРН32																+			+	+				+	+	+					
ПРН33				+																											
ПРН34																														+	
ПРН35										+																+	+				+
ПРН36									+		+				+	+			+	+											
ПРН37				+			+		+										+		+	+									+
ПРН38									+	+					+							+									
ПРН39							+				+		+				+	+			+										
ПРН40										+									+			+									
ПРН41						+		+								+				+				+							
ПРН42										+	+								+			+									+
ПРН43																					+										+
ПРН44																															+
ПРН45																					+										
ПРН46									+					+																	+
ПРН47						+	+	+		+	+										+										+
ПРН48							+								+										+						+
ПРН49													+			+	+	+	+	+			+									+

ПРН50																			+								+				+
ПРН51																+			+	+					+						
ПРН52																+			+	+	+		+			+	+				
ПРН53													+				+	+									+	+			
ПРН54	+		+		+		+			+	+																				+

5. Матриця забезпечення програмних результатів навчання (ПРН) відповідними компонентами освітньої програми кібербезпека в комп'ютерних мережах (вибіркові компоненти)

				Блок 1														**Блок 2**													
	ВК1	**ВК2**	**ВК3**	**ВК4**	**ВК5**	**ВК6**	**ВК7**	**ВК8**	**ВК9**	**ВК10**	**ВК11**	**ВК12**	**ВК13**	**ВК14**	**ВК15**	**ВК16**	**ВК17**	**ВК18**	**ВК19**	**ВК20**	**ВК21**	**ВК22**	**ВК23**	**ВК24**	**ВК25**	**ВК26**	**ВК27**	**ВК28**	**ВК29**	**ВК30**	**ВК31**
ПРН1	+																													
ПРН2												+	+			+	+								+	+			+	+
ПРН3						+														+										
ПРН4											+	+	+		+	+	+							+	+	+		+	+	+
ПРН5						+	+													+	+									
ПРН6			+			+	+	+												+	+	+								
ПРН7							+														+									
ПРН8							+				+	+			+	+					+			+	+			+	+	
ПРН9							+	+													+	+								
ПРН10							+		+												+		+							
ПРН11					+																									
ПРН12							+				+	+			+	+					+			+	+			+	+	
ПРН13									+																					
ПРН14					+			+	+										+			+	+						
ПРН15					+			+				+				+			+			+				+			+	

ПРН16										+				+										+				+			
ПРН17						+																+									
ПРН18								+	+			+				+						+	+			+				+	
ПРН19							+					+				+					+					+				+	
ПРН20								+	+													+	+								
ПРН21						+		+	+											+		+	+								
ПРН22							+					+				+					+					+				+	
ПРН23							+														+										
ПРН24									+		+																				
ПРН25										+				+										+				+			
ПРН26												+				+										+				+	
ПРН27									+																						
ПРН28							+														+										
ПРН29							+		+												+		+								
ПРН30												+				+										+				+	
ПРН31							+				+				+							+				+			+		
ПРН32									+																						
ПРН33		+					+					+				+					+					+				+	
ПРН34							+			+	+	+		+	+	+					+			+	+	+		+	+	+	
ПРН35											+																				
ПРН36																						+									
ПРН37				+	+													+	+												
ПРН38													+				+											+				+
ПРН39					+														+												
ПРН40																						+									
ПРН41						+														+											
ПРН42							+														+										

ПРН43												+																			
ПРН44										+		+		+		+								+		+		+		+	
ПРН45												+				+										+				+	
ПРН46												+				+										+				+	
ПРН47					+	+					+				+				+	+					+				+		
ПРН48					+						+	+			+	+			+						+	+			+	+	
ПРН49											+				+										+				+		
ПРН50								+														+									
ПРН51							+																								
ПРН52															+																
ПРН53								+	+													+	+								
ПРН54	+	+			+														+												

,