

Міністерство освіти і науки України
Харківський національний університет імені В.Н. Каразіна

Введено в дію наказом від « 08 » 05 2020 р.
№ 0202-1/164

Ректор

Віль БАКІРОВ

« 08 » 2020 р.



Освітньо-професійна програма

Кібербезпека

Спеціальність 125- Кібербезпека

(шифр, назва спеціальності)

Перший (бакалаврський) рівень вищої освіти

Затверджено вченою радою університету « 27 » 04 2020 року,
протокол № 8.

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми

1.1. Вчена рада факультету/інституту: протокол № 8 від « 17 » 03 2020р.

Голова Вченої ради

факультету комп'ютерних наук



Валентин ЛАЗУРИК

1.2. Методична комісія факультету/інституту:

протокол № 6 від « 17 » 02 2020р.

Голова методичної комісії

факультету комп'ютерних наук



Анатолій БЕРДНИКОВ

1.3. Кафедра: протокол № 6 від « 15 » 04 2020р.

Завідувач кафедри безпеки

інформаційних систем і технологій



Сергій РАССОМАХІН

ПЕРЕДМОВА

Розроблено робочою групою у складі:

Прізвище, ім'я, по батькові	Найменування посади (для сумісників – місце основної роботи, посада)	Науковий ступінь, вчене звання, за якою кафедрою (спеціальністю) присвоєно
Керівник робочої групи		
Рассомахін Сергій Геннадійович	Завідувач кафедри безпеки інформаційних систем і технологій	Доктор технічних наук (05.13.06 - Інформаційні технології), доцент за кафедрою автоматизованих систем управління
Члени робочої групи		
Кошман Сергій Олександрович	Професор кафедри безпеки інформаційних систем і технологій	Доктор технічних наук (05.13.05 – Комп'ютерні системи та компоненти), доцент за кафедрою автоматизації та комп'ютерно-інтегрованих технологій
Кузнецов Олександр Олександрович	Професор кафедри безпеки інформаційних систем і технологій	Доктор технічних наук (05.13.21), професор за спеціальністю 20.02.12 - військова кібернетика, системи управління та зв'язок
Колованова Євгенія Павлівна	Доцент кафедри безпеки інформаційних систем і технологій	Кандидат технічних наук (05.13.21)

При розробці Програми враховані вимоги 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.

**1. Профіль освітньої програми «Кібербезпека»
зі спеціальності 125 – Кібербезпека**

1 – Загальна інформація	
Ступінь вищої освіти та назва кваліфікації	Перший (бакалаврський) рівень, бакалавр з кібербезпеки
Тип диплому та обсяг освітньої програми	240 кредитів ЄКТС, 4 роки
Офіційна назва програми	Кібербезпека
Наявність акредитації	Сертифікат про акредитацію серія НД № 2189535, від 17 листопада 2015 р., протокол № 119.
Цикл/рівень	НРК України – 6 рівень, FQ – ENEA – другий цикл, QF – LLL – 6 шостий рівень
Передумови	Наявність повної загальної середньої освіти з терміном навчання 11 років
Мова викладання	державна
Термін дії освітньої програми	до 2024 року
Інтернет-адреса постійного розміщення опису освітньої програми	http://www-csd.univer.kharkov.ua/standarti-osviti/
2 - Мета освітньої програми	
Мета програми	Визначення основних компонент, програмних компетентностей та форм атестації випускників у галузі комплексного захисту складних інформаційних та комунікаційних систем.
3 – Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність, спеціалізація (за наявності))	12 – Інформаційні технології; 125 – Кібербезпека.
Орієнтація освітньої програми	Освітньо-професійна.
Основний фокус освітньої програми та спеціалізації	Безпека інформаційно-комунікаційних систем і технологій.
Особливості програми	Підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки. 75% обсягу освітньої програми спрямовано на забезпечення загальних та спеціальних (фахових) компетентностей за спеціальністю 125.
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.
Подальше навчання	Можливість продовжити навчання за освітньою програмою другого рівня вищої освіти (магістр).
5 – Викладання та оцінювання	
Викладання та навчання	Денна форма навчання. Лекції, лабораторні роботи, семінари, практичні заняття, самостійна робота на основі підручників та конспектів, консультації з викладачами, виробнича та переддипломна практика, написання дипломної роботи.
Оцінювання	Письмові екзамени, звіти з лабораторних та практичних робіт, курсові роботи, поточний контроль, захист кваліфікаційної роботи бакалавра та атестаційний екзамен.
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	КЗ 1. Здатність застосовувати знання у практичних ситуаціях. КЗ 2. Знання та розуміння предметної області та розуміння професії. КЗ 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. КЗ 5. Здатність до пошуку, оброблення та аналізу інформації. КЗ 6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні; КЗ 7. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.
Фахові компетентності	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 і моделей інформаційної безпеки та/або кібербезпеки.

	КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класів та походження. КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.) КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності. КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.
7 – Програмні результати навчання	
Програмні результати навчання	ПРН 1 застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; ПРН 2 організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; ПРН 3 використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; ПРН 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; ПРН 5 адаптуватися в умовах часткої зміни технологій професійної діяльності, прогнозувати кінцевий результат; ПРН 6 критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; ПРН 7 діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки; ПРН 8 готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки; ПРН 9 впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; ПРН 10 виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем; ПРН 11 виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах; ПРН 12 розробляти моделі загроз та порушника; ПРН 13 аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; ПРН 14 вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; ПРН 15 використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; ПРН 16 реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів; ПРН 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; ПРН 18 використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; ПРН 19 застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; ПРН 20 забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від
--	---

	руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах; ПРН 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; ПРН 22 вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної та/або кібербезпеки; ПРН 23 реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; ПРН 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); ПРН 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; ПРН 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; ПРН 27 вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; ПРН 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; ПРН 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; ПРН 30 здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем; ПРН 31 застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем;
--	--

	ПРН 32 вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки; ПРН 33 вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків; ПРН 34 приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; ПРН 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; ПРН 36 виявляти небезпечні сигнали технічних засобів; ПРН 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; ПРН 38 інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації; ПРН 39 проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах; ПРН 40 інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації; ПРН 41 забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур; ПРН 42 впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; ПРН 43 застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; ПРН 44 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;
--	---

	ПРН 45 застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; ПРН 46 здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах; ПРН 47 вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації; ПРН 48 виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; ПРН 49 забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах; ПРН 50 забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); ПРН 51 підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; ПРН 52 використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах; ПРН 53 вирішувати задачі аналізу програмного коду на наявність можливих загроз. ПРН 54 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	
Специфічні характеристики кадрового забезпечення	Викладання фахових дисциплін забезпечує професорсько-викладацький склад кафедри: 9 докторів та 8 кандидатів наук.
Специфічні характеристики матеріально-технічного забезпечення	Для навчання використовуються 8 комп'ютерних класів та навчальна лабораторія факультету комп'ютерних наук, навчально-науковий центр сертифікації ключів ЕЦП, виробнича та переддипломна практика здійснюється на базі ФКН та 6 науково-виробничих підприємств, з якими укладено відповідні договори.
Специфічні характеристики інформаційного та навчально-методичного забезпечення	Використовується навчальний фонд бібліотеки ХНУ, ПЗ дистанційних форм навчання, підручники та навчальні посібники розробки кафедри та провідних світових університетів.
9 – Академічна мобільність	
Національна кредитна мобільність	На основі двосторонніх договорів між Харківським національним університетом ім. В. Н. Каразіна та іншими університетами України. Допускаються індивідуальні угоди про академічну мобільність для навчання та проведення

	досліджень в університетах та наукових установах України. До керівництва науковою роботою здобувачів можуть бути залучені провідні фахівці університетів України на умовах індивідуальних договорів. Кредити, отримані в інших університетах України, перезараховуються відповідно до довідки про академічну мобільність.
Міжнародна кредитна мобільність	Відповідно до «Стратегії гармонізації державного управління країн ЄС та Східного Партнерства», що підписана 28 країнами Європи, в тому числі й Україною, передбачено формування єдиного освітнього простору країн ЄС та Східного Партнерства. Даною загальноєвропейською стратегією передбачено й впровадження міжнародних програм студентського обміну та програм подвійних дипломів між найбільшими українськими університетами та провідними університетами ЄС. Харківський національний університет ім. В. Н. Каразіна є активним учасником даного міжнародного процесу. Міжнародна кредитна мобільність може здійснюватися також на основі двосторонніх договорів між Харківським національним університетом ім. В. Н. Каразіна та закладами вищої освіти зарубіжних країн-партнерів.
Навчання іноземних здобувачів вищої освіти	На загальних умовах. Іноземні здобувачі вищої освіти, що реалізують право на академічну мобільність в рамках договорів про співробітництво між Харківським національним університетом ім. В. Н. Каразіна та іноземними вищими навчальними закладами-партнерами, можуть бути зараховані на навчання за рахунок коштів міжнародних програм та організацій або за рахунок коштів фізичних або юридичних осіб.

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

2.1 Перелік компонент ОП

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
Обов'язкові компоненти ОП			
ОК 1.	Іноземна мова	6	Екзамен/залік
ОК 2.	Іноземна мова за фахом	3	Залік
ОК 3.	Історія України	3	Екзамен
ОК 4.	Філософія	3	Екзамен
ОК 5.	Вища математика, теорія ймовірностей	24	Екзамен
ОК 6.	Дискретна математика	7	Екзамен/залік
ОК 7.	Інформаційні технології	7	Залік
ОК 8.	Фізика	7	Екзамен/залік
ОК 9.	Безпека життєдіяльності та основи охорони праці	3	Залік
ОК 10.	Вступ до фаху	3	Екзамен
ОК 11.	Електротехніка та електроніка	5	Екзамен
ОК 12.	Комп'ютерні мережі	4	Екзамен

ОК 13.	Основи теорії передачі інформації	4	Екзамен
ОК 14.	Комп'ютерна графіка	3	Залік
ОК 15.	Метрологія та вимірювання, комп'ютерна схемотехніка (КР-1)	6	Екзамен
ОК 16.	Мікропроцесори та їх застосування	3	Екзамен
ОК 17.	Операційні системи	4	Залік
ОК 18.	Оптоінформатика	3	Залік
ОК 19.	Основи інформаційної безпеки держави	3	Залік
ОК 20.	Основи теорії кіл, сигнали та процеси в електроніці		Екзамен
ОК 21.	Спеціалізовані мови програмування та проектування електронних елементів і систем	6	Екзамен/залік
ОК 22.	Стеганографія	6	Екзамен
ОК 23.	Теорія чисел, теорія груп, полів, кілець	7	Екзамен
ОК 24.	Теорія інформації і кодування (КР-1)	5	Екзамен
ОК 25.	Теорія автоматичного управління	4	Екзамен
ОК 26.	Алгоритмізація та програмування	10	Екзамен
ОК 27.	Крос-платформне програмування	3	Залік
ОК 28.	Теорія алгоритмів	3	Залік
ОК 29.	Об'єктно-орієнтоване програмування (КР-1)	10	Екзамен/залік
ОК 30.	Математичні методи та технології тестування і верифікації програмного забезпечення (КР-1)	4	Екзамен
ОК 31.	Спеціальні методи обробки даних в телекомунікаційних системах	6	Екзамен
ОК 32.	Виробнича практика	5	Залік
ОК 33.	Переддипломна практика	5	Залік
ОК 34.	Підготовка кваліфікаційної роботи бакалавра	2	ЗАХИСТ
ОК 35.	Атестаційний екзамен		Екзамен
Загальний обсяг обов'язкових дисциплін		180	
Вибіркові компоненти ОП*			
<i>Вибірковий блок 1</i>			
ВБ 1.1.	Захист інформації в інформаційно-комунікаційних системах (КР-2)	13	Екзамен/залік
ВБ 1.2.	Комплексні системи захисту інформації: проектування, впровадження, супровід (КР-1)	9	Екзамен
ВБ 1.3.	Компоненти складних комп'ютерних мереж	4	Екзамен
ВБ 1.4.	Технології блокчейн	4	Екзамен
ВБ 1.5.	Прикладна криптологія (КР-1)	10	Екзамен
ВБ 1.6.	Системи технічного захисту інформації	4	Екзамен
ВБ 1.7.	Управління інформаційною безпекою	3	Екзамен
ВБ 1.8.	Безпека життєдіяльності та основи охорони праці	3	Залік
<i>Вибірковий блок 2</i>			
ВБ 2.1.	Апаратні засоби захисту інформації та захист програмного забезпечення (КР-2)	13	Екзамен/залік
ВБ 2.2.	Технології проектування та сертифікації захищених ІС	9	Екзамен
ВБ 2.3.	Завадозахищені телекомунікаційні технології та системи	4	Екзамен
ВБ 2.4.	Аналіз та застосування криптовалют	4	Екзамен
ВБ 2.5.	Криптосистеми та криптопротоколи (КР-1)	10	Екзамен
ВБ 2.6.	Захист від технічних розвідок	4	Екзамен

ВБ 2.7.	Системний аналіз процесів та систем захисту інформації	3	Екзамен
ВБ 2.8.	Безпека життєдіяльності та основи охорони праці	3	Залік
<i>Міжфакультетські дисципліни</i>			
ВБ 3.1.	Міжфакультетська дисципліна за вибором 1	3	Екзамен/залік
ВБ 3.2.	Міжфакультетська дисципліна за вибором 2	3	Екзамен
ВБ 3.3.	Міжфакультетська дисципліна за вибором 3	3	Екзамен
ВБ 3.4.	Міжфакультетська дисципліна за вибором 4	3	Екзамен
Загальний обсяг вибіркових дисциплін		60	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		240	

2.2 Структурно-логічна схема ОП

Рік навчання	1-й		2-й		3-й		4-й	
Семестр	1	2	3	4	5	6	7	8
ОК 1.								
ОК 2.								
ОК 3.								
ОК 4.								
ОК 5.								
ОК 6.								
ОК 7.								
ОК 8.								
ОК 9.								
ОК 10.								
ОК 11.								
ОК 12.								
ОК 13.								
ОК 14.								
ОК 15.								
ОК 16.								
ОК 17.								
ОК 18.								
ОК 19.								
ОК 20.								
ОК 21.								
ОК 22.								
ОК 23.								
ОК 24.								
ОК 25.								
ОК 26.								
ОК 27.								
ОК 28.								
ОК 29.								
ОК 30.								
ОК 31.								
ОК 32.								

ОК 33.								
ОК 34.								
ОК 35.								
ВБ 1.1.								
ВБ 1.2.								
ВБ 1.3.								
ВБ 1.4.								
ВБ 1.5.								
ВБ 1.6.								
ВБ 1.7.								
ВБ 1.8.								
ВБ 2.1.								
ВБ 2.2.								
ВБ 2.3.								
ВБ 2.4.								
ВБ 2.5.								
ВБ 2.6.								
ВБ 2.7.								
ВБ 2.8.								
ВБ 3.1.								
ВБ 3.2.								
ВБ 3.3.								
ВБ 3.4.								

3. Форма атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація здійснюється експертною комісією відповідно до вимог галузевого стандарту вищої освіти після виконання здобувачем вищої освіти навчального плану. На атестацію виноситься сукупність знань, умінь, навичок, інших компетентностей, набутих особою у процесі навчання за даним стандартом. Термін проведення атестації визначається навчальним планом та графіком освітнього процесу. Атестація здійснюється у формі атестаційного екзамену та публічного захисту кваліфікаційної роботи та за рішенням експертної комісії. До атестації допускаються здобувачі вищої освіти, які виконали всі вимоги програми підготовки.
Вимоги до кваліфікаційної роботи/проекту	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.

4. Матриця відповідності програмних компетентностей компонентам освітньої програми

		КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КЗ 6	КЗ 7	ФК 1	ФК 2	ФК 3	ФК 4	ФК 5	ФК 6	ФК 7	ФК 8	ФК 9	ФК 10	ФК 11	ФК 12
--	--	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	-------	-------	-------

ОК 1.	Іноземна мова			+															
ОК 2.	Іноземна мова за фахом	+		+															
ОК 3.	Історія України			+			+	+											
ОК 4.	Філософія	+					+	+											
ОК 5.	Вища математика, теорія ймовірностей	+							+										
ОК 6.	Дискретна математика								+	+									
ОК 7.	Інформаційні технології	+			+	+			+										
ОК 8.	Фізика																		
ОК 9.	Безпека життєдіяльності та основи охорони праці	+					+	+	+										
ОК 10.	Вступ до фаху		+		+				+		+							+	
ОК 11.	Електротехніка та електроніка	+																	
ОК 12.	Комп'ютерні мережі					+			+										
ОК 13.	Основи теорії передачі інформації								+										
ОК 14.	Комп'ютерна графіка	+				+													
ОК 15.	Метрологія та вимірювання, комп'ютерна схемотехніка	+																	
ОК 16.	Мікропроцесори та їх застосування				+														
ОК 17.	Операційні системи	+							+										
ОК 18.	Оптоінформатика								+										
ОК 19.	Основи інформаційної безпеки держави	+	+		+				+			+					+	+	+
ОК 20.	Основи теорії кіл, сигнали та процеси в Ел.								+										
ОК 21.	Спеціалізовані мови програмування та проектування ЕЕС	+				+													
ОК 22.	Стеганографія		+		+				+										
ОК 23.	Теорія чисел, теорія груп, полів, кілець		+		+												+		
ОК 24.	Теорія інформації і кодування		+		+				+										
ОК 25.	Теорія автоматичного управління	+	+		+														
ОК 26.	Алгоритмізація та програмування																		
ОК 27.	Крос-платформне програмування	+				+		+											
ОК 28.	Теорія алгоритмів								+										
ОК 29.	Об'єктно-орієнтоване програмування	+							+										
ОК 30.	Математичні методи та технології Т і В ПЗ					+			+	+	+	+							
ОК 31.	Спеціальні методи обробки даних					+			+	+		+				+			
ОК 32.	Виробнича практика	+			+				+	+						+	+		+
ОК 33.	Переддипломна практика				+	+			+						+		+		
ОК 34.	Підготовка бакалаврської роботи				+				+						+	+			+
ОК 35.	Атестаційний екзамєн				+				+						+	+	+		
ВБ 1.1.	Захист інформації в ІКС		+		+				+	+	+	+	+	+			+		+
ВБ 1.2.	Комплексні системи захисту інформації: проектування, впровадження, супровід	+	+		+				+	+	+	+	+	+					+
ВБ 1.3.	Компоненти складних комп'ютерних мереж		+		+				+		+			+				+	
ВБ 1.4.	Технології блокчейн		+		+				+	+	+						+		

ВБ 1.5.	Прикладна криптологія		+		+							+	+		+	+		+	+	+	+
ВБ 1.6.	Системи технічного захисту інформації	+	+		+							+	+	+		+					+
ВБ 1.7.	Управління інформаційною безпекою	+	+		+				+			+	+		+	+	+			+	+
ВБ 1.8.	Безпека життєдіяльності та основи охорони праці	+			+					+					+						
ВБ 2.1.	Апаратні засоби захисту інформації та захист ПЗ		+		+						+	+	+	+		+				+	
ВБ 2.2.	Технології проектування та сертифікації захищених ІС		+		+						+		+	+		+					+
ВБ 2.3.	Заводозахищені телекомунікаційні Т і С	+	+		+						+	+	+		+					+	
ВБ 2.4.	Аналіз та застосування криптовалют		+		+						+			+				+	+		
ВБ 2.5.	Криптосистеми та криптопротоколи	+	+		+						+		+					+		+	
ВБ 2.6.	Захист від технічних розвідок	+	+		+							+	+	+	+	+			+		
ВБ 2.7.	Системний аналіз процесів та систем ЗІ	+	+		+						+	+	+	+		+	+		+	+	+
ВБ 2.8.	Безпека життєдіяльності та основи охорони праці	+			+						+				+						

5. Матриця забезпечення програмних результатів навчання (ПРН) відповідними компонентами освітньої програми

	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ОК 10	ОК 11	ОК 12	ОК 13	ОК 14	ОК 15	ОК 16	ОК 17	ОК 18	ОК 19	ОК 20	ОК 21	ОК 22	ОК 23	ОК 24	ОК 25	ОК 26	ОК 27	ОК 28	ОК 29	ОК 30	ОК 31	ОК 32	ОК 33	ОК 34	ОК 35	ВБ 1	ВБ 2	ВБ 3	ВБ 4	ВБ 5	ВБ 6	ВБ 7	ВБ 8				
ПРН 1	+	+																																													
ПРН 2			+	+																																											
ПРН 3					+		+																									+															
ПРН 4						+																																				+					
ПРН 5				+	+				+	+																		+			+																
ПРН 6				+	+							+																						+						+	+						
ПРН 7																											+			+											+	+					
ПРН 8																								+												+											
ПРН 9																+		+				+																									
ПРН 10									+																									+											+		
ПРН 11											+						+																													+	
ПРН 12							+			+																		+		+																	
ПРН 13																+						+														+											
ПРН 14											+																								+	+											
ПРН 15										+											+									+												+	+				
ПРН 16																											+								+												
ПРН 17											+																					+															
ПРН 18									+						+	+												+																			
ПРН 19																						+											+			+											
ПРН 20																		+	+															+													
ПРН 21				+				+	+										+				+																								
ПРН 22							+				+		+																+			+								+							
ПРН 23																																	+						+								
ПРН 24																									+											+				+						+	
ПРН 25								+												+	+															+											
ПРН 26			+				+									+																+															
ПРН 27							+																+															+				+					
ПРН 28																					+													+						+							

[illegible]