**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**Харківський національний університет радіоелектроніки**

# ОСВІТНЬО – ПРОФЕСІЙНА ПРОГРАМА

**«Управління кібербезпекою»**

**першого (бакалаврського) рівня вищої освіти**

**за спеціальністю F5 Кібербезпека та захист інформації**

**галузі знань F Інформаційні технології**

**Кваліфікація: «Бакалавр із кібербезпеки та захисту інформації»**

**ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ ХНУРЕ**
**Голова Вченої ради_____ Ігор РУБАН**
**(протокол від "31" 03 2026 р. № 4)**

**Освітня програма вводиться в дію з 01.09 2026 р.**
**Ректор_____ Ігор РУБАН**

**(наказ від "31" 03 2026 р. № 166)**

Харків 2026 р.

# ЛИСТ ПОГОДЖЕННЯ
## освітньо-професійної програми
## «Управління кібербезпекою»
## спеціальності F5 Кібербезпека та захист інформації
## першого (бакалаврського) рівня вищої освіти

**ПОГОДЖЕНО**
Перший проректор
_____ Андрій ЄРОХІН
«27» 03 2026 р.

Начальник відділу ЛА та ВСЗЯО
_____ Ганна ТУГАЙ
«27» 03 2026 р.

Начальник навчального відділу
_____ Аліна МІХНОВА
«27» 03 2026 р.

Розглянуто на засіданні Вченої ради
Факультету КБ
Протокол від «30» 03. 2026 № 1
Декан факультету ІК
_____ Аркадій СНІГУРОВ

Розглянуто на засіданні кафедри ІКІ
Протокол від «06»03. 2026 № 3
Завідувач кафедри ІКІ
ім.В.В.Поповського
_____ Олександр ЛЕМЕШКО

**Представники роботодавців**
MNC Group _____ Григорій МАЗУР

**Представник студентського самоврядування**
Голова студентського сенату факультету ІК _____ Сергій АЛФЬОРОВ

**РОЗРОБЛЕНО**
**Проектна група:**

керівник проектної групи:
Ляшенко Олексій Сергійович,
кандидат технічних наук, доцент,
декан факультету КІУ ХНУРЕ _____

члени проектної групи:
Сєвєрінов Олександр Васильович,
кандидат технічних наук, доцент,
професор кафедри БІТ ХНУРЕ _____
Євдокименко Марина Олександрівна,
доктор технічних наук, професор,
професор кафедри ІКІ
ім. В.В. Поповського ХНУРЕ _____
Федюшин Олександр Іванович,
кандидат технічних наук, доцент,
доцент кафедри БІТ ХНУРЕ _____

Снігуров Аркадій Владиславович,
кандидат технічних наук, професор,
доцент кафедри ІКІ
ім. В.В. Поповського ХНУРЕ

# ПЕРЕДМОВА

Розроблено проектною групою у складі:

Керівник проектної групи:

Ляшенко Олексій Сергійович, кандидат технічних наук, доцент, декан факультету КІІТ ХНУРЕ.

Члени проектної групи:

Сєвєрінов Олександр Васильович, кандидат технічних наук, доцент, професор кафедри БІТ, факультету КБ ХНУРЕ.

Євдокименко Марина Олександрівна, доктор технічних наук, професор, професор кафедри ІКІ ім. В.В. Поповського факультету КБ ХНУРЕ.

Федюшин Олександр Іванович, кандидат технічних наук, доцент, доцент кафедри БІТ факультету КБ ХНУРЕ.

Снігуров Аркадій Владиславович, кандидат технічних наук, доцент, доцент кафедри ІКІ ім. В.В. Поповського факультету КБ ХНУРЕ.

Гарант освітньої програми  Аркадій СНІГУРОВ

# 1. Профіль освітньої програми «Управління кібербезпекою» за спеціальністю F5 Кібербезпека та захист інформації

| 1 - Загальна інформація | |
|---|---|
| **Повна назва закладу вищої освіти та структурного підрозділу** | Харківський національний університет радіоелектроніки,<br>Факультет кібербезпеки<br>Кафедра інфокомунікаційної інженерії ім. В.В. Поповського |
| **Ступінь вищої освіти та назва кваліфікації мовою оригіналу** | Бакалавр<br>Бакалавр із кібербезпеки та захисту інформації |
| **Офіційна назва освітньої програми** | Управління кібербезпекою |
| **Тип диплому та обсяг освітньої програми** | Диплом бакалавра, одиничний,<br>240 кредитів ЄКТС,<br>термін навчання 3 роки 10 місяців, 2 роки 10 місяців |
| **Наявність акредитації** | Сертифікат про акредитацію спеціальності УД 21019407. Строк дії сертифікату: до 31.12.2027. |
| **Цикл/рівень** | НРК України –6 рівень, FQ-EHEA – перший цикл,<br>EQF-LLL – 6 рівень |
| **Передумови** | Повна загальна середня освіта (або освітньо-кваліфікаційний рівень молодшого спеціаліста) |
| **Мова(и) викладання** | Українська мова, англійська мова |
| **Термін дії освітньої програми** | До повного завершення періоду навчання або наступного оновлення програми |
| **Інтернет-адреса постійного розміщення опису освітньої програми** | https://nure.ua/abituriyentam/spetsialnosti-ta-spetsializatsiyi/spetsialnist-f5-kiberbezpeka-ta-zakhyst-informatsii/bakalavr-f5-kiberbezpeka-ta-zakhyst-informatsii/upravlinnia-kiberbezpekoiu |
| **2 - Мета освітньої програми** | |
| – підготовка висококваліфікованих та конкурентоспроможних фахівців здатних використовувати та впроваджувати технології інформаційної та/або кібербезпеки;<br>– надання ґрунтовної освіти з інформаційної та/або кібербезпеки із широким доступом до працевлаштування або продовження навчання за другим (освітньо-професійним або освітньо-науковим) рівнем вищої освіти. | |
| | |
| **3 - Характеристика освітньої програми** | |
| **Предметна область (галузь знань, спеціальність)** | F Інформаційні технології.<br>F5 Кібербезпека та захист інформації |
| **Орієнтація освітньої програми** | Освітньо-професійна програма прикладної орієнтації.<br>Акцент програми зроблений на формування фахівців, здатних управляти інформаційною та/або кібербезпекою організацій та підприємств в умовах невизначеностей з використанням сучасних підходів національних та міжнародних стандартів, інноваційних підходів виявлення загроз та вразливостей систем інформаційної та/або кібербезпеки, розроблювати нові та удосконалювати існуючі організаційні, програмно-технічні механізми забезпечення кібербезпеки, оцінювати ризики, виявляти та оброблювати інциденти інформаційної та/або кібербезпеки, проводити аудит та покращення систем інформаційної та/або кібербезпеки, здатних |

| | |
|---|---|
| | генерувати інноваційні зусилля для побудови сталого суспільства. |
| **Основний фокус освітньої програми** | Загальна вища освіта першого (бакалаврського) рівня в галузі F Інформаційні технології за спеціальністю F5 Кібербезпека та захист інформації.<br>Акцент на здатності організовувати й підтримувати комплекс заходів щодо забезпечення кібербезпеки з урахуванням їхньої правової обґрунтованості, адміністративно-управлінської й технічної реалізації, економічної доцільності, можливих зовнішніх впливів, імовірних загроз і рівня розвитку технологій захисту інформації.<br>Ключові слова: кібербезпека, захист інформації, кібератаки, система управління інформаційною безпекою, ідентифікація та аутентифікація користувачів, аудит, менеджмент інцидентів, цифрова криміналістика, криптографічні методи захисту інформації, технічні методи захисту інформації, безпека інформаційно-комунікаційних систем, захист операційних систем, захист систем електронної комерції та банківських систем, кібербезпека проводових та безпроводових мереж |
| **Особливості програми** | Системна інтеграція програмно-апаратних засобів виявлення, моніторингу та забезпечення інформаційної та/або кібербезпеки, сучасних інформаційних технологій захисту інформації в інформаційно-комунікаційних системах, технологій збереження даних в кіберпросторі та інтелектуалізації функцій протидії кіберзлочинності.<br>Особливістю освітньої програми є:<br>- участь в проєкті USAID «Кібербезпека критично важливої інфраструктури в Україні», в якій викладачі кафедри пройшли відповідну підготовку та отримали навчально-методичні матеріали від учасників проекту;<br>- участі та головного реалізатора проекту ERASMUS+ Жан Моне «Інтеграція рамок та політик кібербезпеки ЄС в Україні» (з 2020 року);<br>- участі і головного реалізатора проєкту ERASMUS+ модуль Жан Моне « «Європейський досвід для підвищення стійкості критично важливих об'єктів в Україні» (з 2022 року).<br>- участі і головного реалізатора проєкту ЕРАЗМУС+ модуль Жан Моне «Інтеграція перспективної екосистеми кібербезпеки ЄС в Україні (з 2024 року);<br>- участі у проєкті від Національного фонду досліджень України «Аналіз, дослідження, розробка та впровадження сучасних технологій інформаційної безпеки для глобального моніторингу кібернетичного простору України в умовах кризових та надзвичайних ситуацій»;<br>- участі у проекті CRDF Global в Україні: «Поінформованість України в галузі кібербезпеки: Підтримка низки тренінгів щодо розбудови кіберзахисту та підвищення обізнаності в Україні»;<br>- участі у проєкті ЕРАЗМУС+ "Центр освіти з питань безпеки для уніфікованої стійкості та ефективних комунікацій – Erasmus Secure". |
| **4 - Придатність випускників до працевлаштування та подальшого навчання** | |
| **Придатність до** | Назва професій згідно Національного класифікатора України: |

| | |
|---|---|
| **працевлаштування** | Класифікатор професій (ДК 003: 2010)<br>2149.2 Фахівець (сфера захисту інформації)<br>3119 Технік (сфера захисту інформації)<br>3439 Фахівець із організації захисту інформації з обмеженим доступом<br>3439 Фахівець із організації інформаційної безпеки<br>2139.2 Аудитор інформаційних технологій (з кібербезпеки)<br>2139.2 Фахівець з оцінки заходів захисту інформації (кібербезпеки)<br>2139.2 Фахівець з реагування на інциденти кібербезпеки<br>2139.2 Фахівець з тестування систем захисту інформації<br>2139.2 Аналітик з безпеки інформаційно-телекомунікаційних систем |
| **Подальше навчання** | Можливість навчання за програмою другого (магістерського) рівня вищої освіти |
| **5 - Викладання та оцінювання** | |
| **Викладання та навчання** | Лекції, практичні заняття, виконання курсової роботи, лабораторні роботи, самостійна робота на основі підручників, навчальних посібників та конспектів лекцій, консультації з викладачами, виробнича та передатестаційна практика, підготовка кваліфікаційної роботи. |
| **Оцінювання** | Оцінювання навчальних досягнень студентів здійснюється за національною шкалою (відмінно, добре, задовільно, незадовільно; зараховано, незараховано); 100-бальною шкалою та шкалою ЄКТС (A, B, C, D, E, FX, F) |
| **6 - Програмні компетентності** | |
| **Інтегральна компетентність** | Здатність розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації |
| **Загальні компетентності (ЗК)** | ЗК1. Здатність застосовувати знання у практичних ситуаціях.<br>ЗК2. Знання та розуміння предметної області і розуміння професійної діяльності.<br>ЗК 3. Здатність спілкуватися державною мовою як усно, так і письмово.<br>ЗК 4. Здатність спілкуватися іноземною мовою.<br>ЗК 5. Здатність вчитися і оволодівати сучасними знаннями.<br>ЗК 6. Здатність реалізувати свої права і обов’язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав та свобод людини і громадянина в Україні.<br>ЗК 7. Здатність ухвалювати рішення й діяти дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності.<br>ЗК 8. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя. |
| **Спеціальні (фахові, предметні)** | СК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні і міжнародні вимоги, практики і стандарти |

| | |
|---|---|
| **компетентності** | у професійній діяльності.<br>СК2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації.<br>СК3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації.<br>СК4. Здатність забезпечувати захист Інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації.<br>СК5. Здатність відновлювати функціонування Інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження.<br>СК6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо.)<br>СК7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.<br>СК8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.<br>СК9. Здатність застосовувати методи та засоби технічного захисту Інформації на об'єктах інформаційної діяльності.<br>СК10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки. |
| **7 - Програмні результати навчання** | |
| | РН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків,<br>РН2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.<br>РН3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності.<br>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.<br>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.<br>РН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.<br>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.<br>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.<br>РН10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.<br>РН11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації.<br>РН12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.<br>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.<br>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.<br>РНІ5. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.<br>РН16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах;<br>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.<br>РН18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об’єктах інформаційної діяльності.<br>РН19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.<br>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.<br>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. |
| **8 - Ресурсне забезпечення реалізації програми** | |
| **Кадрове забезпечення** | Реалізація програми забезпечується кадрами високої кваліфікації з науковими ступенями або вченими званнями, які мають досвід навчально-методичної, науково-дослідницької роботи та відповідають кваліфікації відповідно до спеціальності згідно ліцензійних умов |
| **Матеріально-технічне забезпечення** | 1.Забезпеченість приміщеннями для проведення навчальних занять та контрольних заходів.<br>2. Забезпеченість мультимедійним обладнанням для одночасного використання в навчальних аудиторіях.<br>3. Наявність соціально-побутової інфраструктури.<br>4. Забезпеченість здобувачів вищої освіти гуртожитком.<br>5.Забезпеченість комп'ютерними робочими місцями, лабораторіями, полігонами, обладнанням, устаткуванням, необхідними для виконання навчальних планів.<br>Засоби обчислювальної техніки з відповідним програмним забезпеченням, спеціальні радіовимірювальні прилади, засоби ТЗІ, апаратно-програмні комплекси. Високий рівень практичної підготовки фахівців забезпечується розвиненою міжнародною співпрацею в науковій і освітній сферах, наявністю спеціалізованих лабораторій:<br>Навчально-наукова лабораторія кібербезпеки та хмарних технологій (Cybersecurity & cloud laboratory);<br>Навчально-наукова лабораторія маршрутизації та комутації (Routing & switching laboratory);<br>Навчально-наукова лабораторія мережної безпеки та надійності (Network security & resilience laboratory);<br>Навчально-наукова лабораторія радіомоніторингу, технічного захисту інформації та безпеки праці.<br>У 2018 році був введений в експлуатацію кіберполігон для дослідження кібербезпеки хмарних технологій, розгортання якого на кафедрі було профінансовано Європейським Союзом в рамках європейської програми Tempus – підготовки спеціалістів з кібербезпеки наступного покоління.<br>У 2024 р. отримано обладнання та програмного забезпечення від Агентства США з міжнародного розвитку (USAID). Технічна допомога надана USAID через Проєкт USAID «Кібербезпека критично важливої інфраструктури України» включає 13 одиниць комп'ютерного обладнання (Джерела безперебійного живлення, PoE-Інжектори, Сервер HPE ProLiant ML110 Gen10 4LFF CTO, Комутатор, мережні сховища та кріплення), які дають змогу відбудувати та модернізувати освітню IT-інфраструктуру |
| **Інформаційне та навчально-методичне забезпечення** | 1. Забезпеченість бібліотеки вітчизняними та закордонними фаховими періодичними виданнями відповідного або спорідненого профілю, в тому числі в електронному вигляді.<br>2. Наявність доступу до баз даних періодичних наукових видань англійською мовою відповідного або спорідненого профілю.<br>3. Наявність офіційного веб-сайту закладу освіти, на якому розміщена основна інформація про його діяльність (структура, ліцензії та сертифікати про акредитацію, освітня/освітньо-наукова/ видавнича/ атестаційна (наукових кадрів) діяльність, навчальні |

| | |
|---|---|
| | та наукові структурні підрозділи та їх склад, перелік навчальних дисциплін, правила прийому, контактна інформація).<br>4. Наявність електронного ресурсу закладу освіти, який містить навчально-методичні матеріали з дисциплін навчального плану, в тому числі в системі дистанційного навчання.<br>Специфічними характеристиками інформаційного та навчально-методичного забезпечення є:<br>- використання національних стандартів в галузі інформаційної та кібербезпеки,<br>- використання національних та міжнародних наукових видань,<br>- використання міжнародних стандартів в галузі інформаційної та кібербезпеки.<br>- використання навчально-методичних комплексів проєкту USAID «Кібербезпека критично важливої інфраструктури в Україні»;<br>- використання навчально-методичних комплексів проєкту ERASMUS+ Жан Моне «Інтеграція рамок та політик кібербезпеки ЄС в Україні»;<br>- використання навчально-методичних комплексів проєкту ERASMUS+ модуль Жан Моне «Європейський досвід для підвищення стійкості критично важливих об'єктів в Україні»;<br>- використання навчально-методичних комплексів проєкту ЕРАЗМУС+ модуль Жан Моне «Інтеграція перспективної екосистеми кібербезпеки ЄС в Україні. |
| **9 - Академічна мобільність** | |
| **Національна кредитна мобільність** | На основі двосторонніх договорів (угод) між Харківським національним університетом радіоелектроніки та закладами вищої освіти України |
| **Міжнародна кредитна мобільність** | На основі двосторонніх договорів (угод) між Харківським національним університетом радіоелектроніки та закладами вищої іноземних країн |
| **Навчання іноземних здобувачів вищої освіти** | На основі договорів (угод) між Харківським національним університетом радіоелектроніки та закладами вищої освіти іноземних країн |

## 2. Перелік компонент освітньої програми та їх логічна послідовність

2.1. Перелік компонент ОП

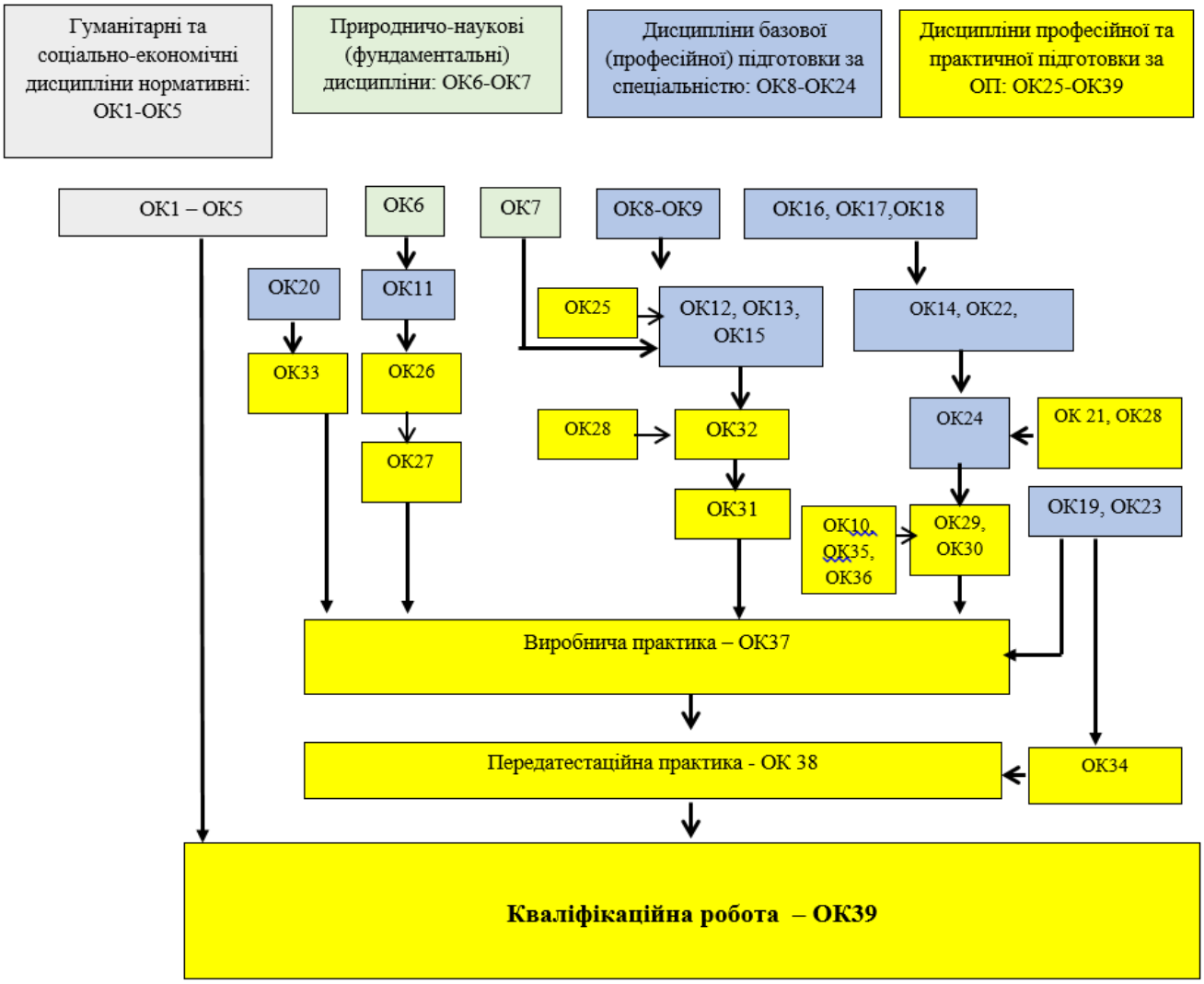
| Код н/д | Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота) | Кількість кредитів | Форма підсумк. контролю |
|---|---|---|---|
| | **ОБОВ'ЯЗКОВІ КОМПОНЕНТИ ОП** | | |
| | **ЦИКЛ ЗАГАЛЬНОЇ ТА СПЕЦІАЛЬНОЇ (ФАХОВОЇ) ПІДГОТОВКИ** | | |
| | **Гуманітарні та соціально-економічні дисципліни (обов'язкові)** | | |
| ОК 1 | Українське фахове мовлення | 4 | Залік |
| ОК 2 | Філософія | 4 | екзамен |
| ОК 3 | Іноземна мова | 8 | екзамен |
| ОК3* | Українська мова як іноземна | 12 | Залік |
| ОК 4 | Основи права | 2 | Залік |
| ОК 5 | Фізичне виховання (за рахунок вільного часу студентів) | 0 | Залік |
| ОК 5* | Українська мова як іноземна (за рахунок вільного часу студентів) | 0 | Залік |
| | Всього: | 18 | |
| | *-для іноземних здобувачів вищої освіти | | |
| | **Дисципліни природничо-наукової (фундаментальної) підготовки за спеціальністю (обов'язкові)** | | |
| ОК 6 | Вища математика | 12 | екзамен |
| ОК 7 | Фізика | 6 | екзамен |
| | Всього: | 18 | |
| | **Дисципліни базової (професійної) підготовки за спеціальністю (обов'язкові)** | | |
| ОК 8 | Безпека життєдіяльності | 3 | Залік |
| ОК 9 | Економіка та бізнес | 3 | Залік |
| ОК 10 | Системи виявлення та протидії атакам | 4 | Залік |
| ОК 11 | Спеціальні розділи математики для кібербезпеки | 4 | Залік |
| ОК 12 | Архітектура комп'ютерних систем | 4 | залік |
| ОК 13 | Схемотехніка | 4 | Залік |
| ОК 14 | Основи IP-мереж | 4 | екзамен |
| ОК 15 | Електрорадіовимірювання | 4 | Залік |
| ОК 16 | Програмування | 10 | екзамен |
| ОК 17 | Об`єктно-орієнтоване програмування | 4 | екзамен |
| ОК 18 | Крос-платформне програмування | 4 | екзамен |
| ОК 19 | Нормативно-правове забезпечення інф. безпеки | 4 | Залік |
| ОК 20 | Операційні системи | 4 | Залік |
| ОК 21 | Введення в спеціальність | 4 | Залік |
| ОК 22 | Теорія інформації та кодування | 5 | екзамен |
| ОК 23 | Управління інформаційною безпекою | 4 | екзамен |
| ОК 24 | Мережна безпека | 9 | екзамен |
| | Всього: | 78 | |
| | **ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ** | | |
| | **Дисципліни професійної та практичної підготовки за освітньою програмою «Управління кібербезпекою» (обов'язкові)** | | |
| ОК 25 | Основи комп'ютерного моделювання | 3 | Залік |
| ОК 26 | Математичні основи криптології | 5,5 | екзамен |
| ОК 27 | Основи криптографічного захисту інформації | 4 | Залік |
| ОК 28 | Безпроводові технології | 4 | залік |

| Код н/д | Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота) | Кількість кредитів | Форма підсумк. контролю |
|---|---|---|---|
| | **ОБОВ'ЯЗКОВІ КОМПОНЕНТИ ОП** | | |
| ОК 29 | Локальні мережі та їх безпека | 3 | екзамен |
| ОК 30 | Безпека безпроводових мереж | 5 | екзамен |
| ОК 31 | Комплексні системи захисту інформації | 4 | екзамен |
| ОК 32 | Основи технічного захисту інформації | 6 | екзамен |
| ОК 33 | Основи захисту сучасних операційних систем | 4 | екзамен |
| ОК 34 | Основи аудиту інформаційної безпеки | 3 | екзамен |
| ОК 35 | Ідентифікація об'єктів та користувачів | 3,5 | екзамен |
| ОК 36 | Мережна криміналістика | 3 | залік |
| ОК 37 | Виробнича практика | 4,5 | Залік |
| ОК 38 | Передатестаційна практика | 4,5 | Залік |
| ОК 39 | Кваліфікаційна робота | 9 | Екзамен |
| | Всього: | 66 | |
| | **Загальний обсяг обов'язкових компонентів** | **180** | |
| | **ВИБІРКОВІ КОМПОНЕНТИ ОП*** | | |
| | **ЦИКЛ ЗАГАЛЬНОЇ ТА СПЕЦІАЛЬНОЇ (ФАХОВОЇ) ПІДГОТОВКИ** | | |
| | **Гуманітарні та соціально-економічні дисципліни** | 6 | |
| | **Загальний обсяг вибіркових компонентів за циклом** | 6 | |
| | **ЦИКЛ ПРОФЕСІЙНОЇ ПІДГОТОВКИ** | | |
| | **Дисципліни професійної та практичної підготовки за освітньою програмою «Управління кібербезпекою»** | | |
| ВБ 1 | Цифрова розвідка та аналіз відкритих джерел | 3 | залік |
| ВБ 2 | Протидія дезінформації та інформаційним загрозам | 3 | залік |
| ВБ 3 | Проєктування, адміністрування та безпека корпоративних мереж | 6,5 | екзамен |
| ВБ 4 | Захист систем електронної комерції та мультисервісних систем | 4,5 | залік |
| ВБ 5 | Системи управління базами даних | 4 | залік |
| ВБ 6 | Мережне програмування | 6,5 | екзамен |
| ВБ 7 | Інформаційна безпека в операційних системах Unix | 4 | залік |
| ВБ 8 | Основи кібербезпеки в мережах 5G | 4 | екзамен |
| ВБ 9 | Безпека банківських систем | 4 | залік |
| ВБ 10 | Технології транзакцій на основі Blockchain | 4 | екзамен |
| ВБ 11 | Методи моніторингу частотного ресурсу | 4,5 | екзамен |
| ВБ 12 | Основи цифрової криміналістики | 4,5 | залік |
| ВБ 13 | Основи аналізу вразливостей та етичного хакінгу | 4,5 | залік |
| ВБ 14 | Основи Web-безпеки | 4,5 | екзамен |
| ВБ 15 | Безпека кіберінформаційної структури | 4 | екзамен |
| ВБ 16 | Стеганографія | 4 | залік |
| ВБ 17 | Основи інформаційної безпеки телекомунікаційних та хмарних технологій | 4 | екзамен |
| ВБ 18 | Основи побудови та захисту IoT | 4,5 | екзамен |
| ВБ 19 | Основи квантової безпеки та криптографії | 4 | залік |
| ВБ 20 | Штучний інтелект у кібербезпеці | 4 | залік |
| ВБ 21 | Основи DevSecOps у розробці програмного забезпечення | 4,5 | залік |
| | Базова загальна військова підготовка (теоретична частина) | 3 | Диф. залік |

| Код н/д | Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота) | Кількість кредитів | Форма підсумк. контролю |
|---|---|---|---|
| | **ОБОВ'ЯЗКОВІ КОМПОНЕНТИ ОП** | | |
| | Базова загальна військова підготовка (практична частина) | 7 | Диф. залік |
| | **Загальний обсяг вибіркових компонентів за циклом** | **54** | |
| | **Загальний обсяг вибіркових компонентів** | 60 | |
| | **ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ** | **240** | |

* Перелік вибіркових компонентів може бути доповнено у робочому навчальному плані з загального каталогу вибіркових дисциплін Університету – у разі вибору здобувачами вищої освіти

## 2.2 Структурно-логічна схема ОП



## 3. Форма атестації здобувачів вищої освіти

Форма атестації здобувачів вищої освіти за освітньою програмою «Управління кібербезпекою» спеціальності F5 Кібербезпека та захист інформації – захист кваліфікаційної роботи з видачею документу встановленого зразка про присудження здобувачеві ступеня бакалавра із присвоєнням освітньої кваліфікації: «Бакалавр з кібербезпеки та захисту інформації», проведення Єдиного державного кваліфікаційного іспиту.

**Форми атестації**

Атестація здійснюється у формі публічного захисту кваліфікаційної роботи та проведення Єдиного державного кваліфікаційного іспиту.

**Вимоги до кваліфікаційної роботи**

Кваліфікаційна робота має передбачати розв'язок спеціалізованого завдання теоретичного або практичного спрямування в галузі кібербезпеки та захисту інформації. У кваліфікаційній роботі не повинно бути академічного плагіату, фальсифікації та фабрикації. Кваліфікаційна робота має бути оприлюднена (за виключенням робіт, що містять інформацію з обмеженим доступом) на офіційному сайті закладу вищої освіти або його структурного підрозділу, або у репозиторії закладу вищої освіти.

## 4. Матриця відповідності компетентностей компонентам освітньої програми

Матриця відповідності загальних та фахових компетентностей обов'язковим компонентам (ОК) освітньої програми

| | ОК 1 | ОК2 | ОК3 | ОК4 | ОК5 | ОК 6, ОК 7 | ОК 8, ОК 9 | ОК10 | ОК24, ОК29 | ОК30 | 0К11 | ОК26, ОК27 | 0К12, ОК13, ОК15 | ОК31 | ОК32 | ОК21 | 0К14, ОК22, ОК28 | 0К16, ОК17, ОК18, ОК25 | ОК19 | ОК23, ОК34 | ОК20, ОК33 | ОК35 | ОК.36 | 0К37, 0К38, 0К39 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **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** | | | | | | | | | + | + | | | | | | | | | | | | | + | + |

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

Матриця забезпечення ПРН обов’язковими компонентами (ОК) освітньої програми

| | **ОК 1** | **ОК2** | **ОК3** | **ОК4** | **ОК5** | **ОК 6, ОК 7** | **ОК 8, ОК 9** | **ОК10** | **ОК24, ОК29** | **ОК30** | **0К11** | **ОК26, ОК27** | **0К12, ОК13, ОК15** | **ОК31** | **ОК32** | **ОК21** | **0К14, ОК22, ОК28** | **0К16, ОК17, ОК18, ОК25** | **ОК19** | **ОК23, ОК34** | **ОК20, ОК33** | **ОК35** | **ОК.36** | **0К37, 0К38, 0К39** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **РН – 1** | + | | | | | | | | | | | | | | | | | | | | | | | + |
| **РН – 2** | | | | | | | | | | | | | | | | | | | | | | | | + |
| **РН – 3** | | | + | | | | | | | | | | | | | | | | | | | | | + |
| **РН – 4** | | | | + | | | | | | | + | | | | | + | | | | | | | | + |
| **РН – 5** | | + | | | | + | + | + | + | | | + | | | + | + | | | + | + | + | | | + |
| **РН – 6** | | | | | | | | | | | | | | | | | | | | | | | | + |
| **РН – 7** | | | | | | | | | + | + | | | | | | | | | | | | | | + |
| **РН – 8** | | | | | | | | | | | | | + | | | | + | | | | | | | + |
| **РН – 9** | | | | | | | | | | | | | | | | | | | + | + | | | | + |
| **РН – 10** | | | | | | | | | + | + | | | | | | | + | + | | | | | + | + |

| | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **PH – 11** | | | | | | | | | | | | | | | | | | | | + | | | + |
| **PH – 12** | | | | | | | | | + | + | | | | | | | | | | | + | | + |
| **PH – 13** | | | | | | | | + | + | + | | | | | | | | | | | | | + |
| **PH – 14** | | | | | | | | | + | + | | | | | | | | | | | | + | + |
| **PH – 15** | | | | | | | | + | + | + | | | | | | | | | | | | + | + |
| **PH – 16** | | | | | | | | | | | | | | + | | | | | | | | | + |
| **PH – 17** | | | | | | | | | | | | | | | | | | | | + | | | + |
| **PH – 18** | | | | | | | | | | | + | + | | | | | | | | | | | + |
| **PH – 19** | | | | | | | | | | | + | + | | | | | | | | | | | + |
| **PH – 20** | | | | | | | | | | | | | + | | + | | | | | | | | + |
| **PH – 21** | | | | | | | | | + | + | | | | + | | | | | | | | | + |