МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

ЗАТВЕРДЖУЮ
В.о. Ректора НТУ «ХПІ»
_____ Євген СОКОЛ
«30» березня 2026 р.

ОСВІТНЬО-НАУКОВА ПРОГРАМА “КІБЕРБЕЗПЕКА”

Третього (доктора філософії) рівня вищої освіти

за спеціальністю **F5 – Кібербезпека та захист інформації**

галузі знань **F – Інформаційні технології**

кваліфікація **Доктор філософії з кібербезпеки та захисту інформації**

ЗАТВЕРДЖЕНО
ВЧЕНОЮ РАДОЮ НТУ «ХПІ»
Голова вченої ради
_____ / Євген СОКОЛ
Протокол № 4
від «27» березня 2026 р.

Харків 2025 р.

ЛИСТ ПОГОДЖЕННЯ

освітньо-наукової програми «Кібербезпека»

Рівень вищої освіти	Третій (доктор філософії)
Галузь знань	F – Інформаційні технології
Спеціальність	F5 – Кібербезпека та захист інформації
Кваліфікація	Доктор філософії з кібербезпеки та захисту інформації

СХВАЛЕНО
Комісією Методичної ради «Методичне забезпечення підготовки докторів філософії»
Голова комісії

_____ Віктор ШАЙДА
«23» березня 2026 р.

РЕКОМЕНДОВАНО
Методичною радою НТУ «ХПІ»
Заступник голови методичної ради

_____ Руслан МИГУЩЕНКО
Протокол № 3
« 25 » березня 2026 р.

ПОГОДЖЕНО
Робочою групою ОНП із спеціальності «Кібербезпека та захист інформації»
Гарант ОНП

_____ Сергій ПОГАСІЙ
Протокол № 1
« 16 » січня 2026 р.

ПОГОДЖЕНО
Директор навчально-наукового інституту комп'ютерних наук та інформаційних технолгій

_____ Михайло ГОДЛЕВСЬКИЙ
«____»_____2026 р.

ПОГОДЖЕНО
Радою молодих вчених

_____ Дмитро ДАНИЛЬЧЕНКО
«____»_____2026 р.

ПОГОДЖЕНО
Завідувач кафедри кібербезпеки

_____ Сергій ЄВСЕЄВ
Протокол № 12
« 23 » березня 2026 р.

ПОГОДЖЕНО
здобувач вищої освіти
(член робочої групи ОНП)
№ групи А-3523

_____ Сергій ДУНАЄВ
« 23 » березня 2026 р.

ЗАТВЕРДЖЕНО ТА НАДАНО ЧИННОСТІ

Наказом ректора Національного технічного університету «Харківський політехнічний інститут» від « 30 » березня 2026 року № 119 ОД.

РЕЦЕНЗЕНТИ:

Продуктивні зауваження та відгуки на проєкт освітньо-наукової програми одержано від:

1. Дмитро ДАНИЛЬЧЕНКО, голова Ради молодих вчених НТУ “ХПІ”
2. Іван ОПІРСЬКИЙ, доктор технічних наук, професор, завідувач кафедри захисту інформації Інституту комп’ютерних технологій, автоматики та метрології Національного університету «Львівська політехніка»
3. Владислав КОВТУН, кандидат технічних наук, доцент, директор ТОВ “Сайфер”
4. Сергій ГОЛОВАШИЧ, кандидат технічних наук, доцент директор ТОВ “Мікрокрипт Текнолоджіс”
5. Олена ВОЛОЩУК, кандидат технічних наук, керівник освітніх програм ТОВ “Distributed Lab”.
6. Ольга ШАПОВАЛ, виконавчий директор Громадської спілки «Харківський кластер інформаційних технологій»

РЕЦЕНЗІЯ-ВІДГУК

НА ОСВІТНЬО-НАУКОВУ ПРОГРАМУ “КІБЕРБЕЗПЕКА”

третього (доктор філософії) рівня вищої освіти

спеціальності F5 “Кібербезпека та захист інформації”

кафедри кібербезпеки Національного технічного університету

“Харківський політехнічний інститут”

Освітньо-наукова програма за спеціальністю F5 "Кібербезпека та захист інформації", розроблена кафедрою кібербезпеки Національного технічного університету "Харківський політехнічний інститут", є вчасним та відповідним кроком у підготовці фахівців високої кваліфікації для роботи у сфері кібербезпеки. Враховуючи постійне зростання кіберзагроз і важливість забезпечення безпеки на всіх рівнях інформаційних систем, програма є важливим елементом для підготовки кадрів, здатних розв'язувати складні проблеми захисту критичної інфраструктури та інформаційних технологій.

Слід зазначити, що однією з особливостей програми є планомірне та поступове вивчення спеціалізованих предметів та наукова складова підготовки фахівців, здатних використовувати та впроваджувати технології кібербезпеки. Зміст кожної складової програми орієнтується на сучасні наукові дослідження комплексних проблем в галузі захисту інформації, кібербезпеки та інформаційних технологій. Позитивним моментом запропонованої програми є інструменти та обладнання, що залучаються до навчального процесу: системи розробки, забезпечення, моніторингу та контролю процесів кібербезпеки, сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій, спеціалізований клас (кіберполігон) як практичну складову навчальної програми. Такий підхід, дозволить аспірантам на реальних моделях поведінки сторін кіберконфлікту опрацювати наближені до реальності події та застосовувати набуті знання та вміння для розв'язання комплексних проблем в галузі захисту інформації, кібербезпеки та інформаційних технологій.

Важливою особливістю освітньо-наукової програми є акцент на науково-дослідницькій діяльності, що дозволяє аспірантам не лише отримати ґрунтовні знання в галузі кібербезпеки, але й розвивати навички проведення наукових досліджень та впровадження інноваційних технологій у сфері кіберзахисту. Програма також охоплює важливі аспекти програмування, управління проектами та володіння іноземними мовами, що є необхідним для успішної роботи у міжнародному контексті.

Програма орієнтована на формування фахівців, здатних здійснювати висококваліфіковане управління та забезпечення безпеки інформаційних систем, впроваджувати новітні технології захисту, а також здійснювати наукову діяльність у галузі кібербезпеки. Враховуючи сучасні виклики та загрози в галузі кібербезпеки, програма є актуальною і забезпечує якісну підготовку кадрів для роботи в умовах сучасного цифрового середовища.

Загалом, програма за спеціальністю F5 "Кібербезпека та захист інформації" є важливим і своєчасним кроком у підготовці фахівців для наукової, дослідницької та практичної діяльності в галузі кібербезпеки, і вона заслуговує на впровадження в освітній процес для підготовки висококваліфікованих кадрів.

Таким чином, освітньо-наукова програма «Кібербезпека», яка підготовлена кафедрою кібербезпеки Національного технічного університету “Харківський політехнічний інститут”, може бути рекомендована для використання в навчальному процесі для підготовки наукових і науково-педагогічних кадрів за третім (доктор філософії) рівнем вищої освіти зі спеціальності F5 “Кібербезпека та захист інформації”.

Голова Ради
молодих вчених НТУ "ХПІ" _____ Дмитро ДАНИЛЬЧЕНКО

РЕЦЕНЗІЯ-ВІДГУК

НА ОСВІТНЬО-НАУКОВУ ПРОГРАМУ «КІБЕРБЕЗПЕКА»

третього (доктор філософії) рівня вищої освіти

спеціальності F5 “Кібербезпека та захист інформації”

кафедри кібербезпеки Національного технічного університету

“Харківський політехнічний інститут”

Забезпечення інформаційної безпеки сучасної компанії – основа її надійності та конкурентоспроможності у сучасних умовах розвитку інформаційно-телекомунікаційних систем.

Безпека в інформаційній сфері, шифрування важливих даних, протидія кіберзлочинам – все це передбачає глибоке переосмислення наявних та створення нових цілісних знань, якими повинен оволодіти сучасний фахівець, що навчається за спеціальністю F5 “Кібербезпека та захист інформації”. Так, на кафедрі кібербезпеки Національного технічного університету “Харківський політехнічний інститут” розроблено програму за відповідною актуальною спеціальністю та виконується підготовка фахівців з кібербезпеки за третім (доктора філософії) рівнем вищої освіти. Метою освітньо-наукової програми є забезпечення підготовки наукових і науково-педагогічних кадрів у сфері кібербезпеки шляхом здобуття ними компетентностей, достатніх для виконання оригінальних наукових досліджень, результати яких мають наукову новизну, теоретичне та практичне значення, а також їх підтримку в ході підготовки та захисту дисертації в галузі інформаційних технологій за спеціальністю F5 “Кібербезпека та захист інформації”.

Слід відзначити високий рівень підготовки за запропонованою освітньо-науковою програмою, що поєднує навчання та оволодіння професійними компетентностями у галузі кібербезпеки, особливостей програмування, управління проектами, набуття знань з іноземної мови та інші. Однак, безумовно, особливістю програми є планомірне та поступове вивчення спеціалізованих предметів та наукова складова підготовки фахівців, здатних використовувати і впроваджувати технології кібербезпеки. Зміст кожної складової програми орієнтується на сучасні наукові дослідження комплексних проблем в галузі захисту інформації, кібербезпеки та інформаційних технологій.

Аспіранти, що навчаються за спеціальністю F5 “Кібербезпека та захист інформації”, отримають знання та вміння приймати обґрунтовані рішення, бути здатними їх оцінювати та забезпечувати якість виконуваних робіт.

Інструменти й обладнання, що залучаються до навчального процесу: системи розробки, забезпечення, моніторингу та контролю процесів кібербезпеки, сучасне програмно-апаратне забезпечення інформаційно-комунікаційних

технологій, спеціалізований клас (кіберполігон). Особливо слід підкреслити, що кафедра кібербезпеки залучає кіберполігон як практичну складову навчальної програми. Звичайно, такий підхід, дозволяє аспірантам на реальних моделях поведінки атакуючих та сторони, що захищається від кібернападу, опрацювати наближені до реальності події та бути здатними застосувати набуті знання та вміння для вирішення комплексних проблем в галузі захисту інформації, кібербезпеки та інформаційних технологій.

Таким чином, освітньо-наукова програма «Кібербезпека», яка підготовлена кафедрою кібербезпеки Національного технічного університету "Харківський політехнічний інститут", може бути рекомендована для використання в навчальному процесі для підготовки наукових і науково-педагогічних кадрів за третім (доктора філософії) рівнем вищої освіти зі спеціальності F5 "Кібербезпека та захист інформації".

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
"ЛЬВІВСЬКА ПОЛІТЕХНІКА"
ПІДПИС ЗАСВІДЧУЮ
НАЧАЛЬНИК ВІДДІЛУ КАДРІВ
Шевцова М.С.
"___" _____ р.

ВІДДІЛ КАДРІВ
02071010

Завідувач кафедри захисту інформації
Інституту комп'ютерних технологій,
автоматики та метрології Національного
університету «Львівська політехніка»,
д.т.н., професор _____ Іван ОПІРСЬКИЙ

CIPHER

Системи захисту інформації
www.cipher.com.ua

ТОВ «САЙФЕР ІТ»
Адреса: 04107, Київ, вул. Нагірна, 25-27
Тел.: +38 044 484 46 12, 484 46 17
E-mail: info@cipher.com.ua

ТОВ «САЙФЕР ІТ»
Адреса: 04107, Київ, вул. Нагірна, 25-27
Тел./Факс: (044) 484-46-17, 484-46-12, 483-03-22
E-mail: info@cipher.com.ua
https://cipher.com.ua

РЕЦЕНЗІЯ-ВІДГУК

НА ОСВІТНЬО-НАУКОВУ ПРОГРАМУ «КІБЕРБЕЗПЕКА»

третього (доктор філософії) рівня вищої освіти

спеціальності F5 "Кібербезпека та захист інформації"

кафедри кібербезпеки Національного технічного університету

"Харківський політехнічний інститут"

Освітньо-наукова програма «Кібербезпека» третього (доктор філософії) рівня вищої освіти, яка розроблена на кафедрі кібербезпеки Національного технічного університету "Харківський політехнічний інститут" за спеціальністю F5 "Кібербезпека та захист інформації" охоплює широкий спектр сучасних методів і технологій для забезпечення кібербезпеки, аналізу загроз та розробки ефективних рішень захисту інформації.

Освітньо-наукова програма підготовки забезпечує здатність розв'язувати комплексні проблеми в галузі кібербезпеки, що передбачає глибоке переосмислення наявних та створення нових цілісних знань та/або професійної практики.

Аспіранти, що навчаються за спеціальністю F5 "Кібербезпека та захист інформації", отримають знання та вміння формувати і аргументовано відстоювати власну думку з різних проблем філософії науки та методології наукового пізнання, бути критичним і самокритичним; поглиблюють знання з іноземної мови для вміння читати оригінальну наукову літературу на іноземній мові, опрацьовувати та оформляти інформацію; вміння та навички критично сприймати та аналізувати існуючі наукові теорії та ідеї, шукати власні шляхи вирішення проблеми та завдань, проводити критичний аналіз власних матеріалів, генерувати власні нові

ідеї, приймати обґрунтовані рішення; вміння демонструвати своєчасність та плановість у науковому дослідженні, спроможність управляти науковими проектами.

Серед обладнання, що залучаються до навчального процесу, особливо слід виділити наявність на кафедрі кібербезпеки кіберполігону. Кіберполігон підсилює практичну складову навчальної програми та дозволяє аспірантам практично перевірити перед захистом дисертаційної роботи отримані наукові результати.

Наукова складова програми забезпечує формування навичок написання наукових статей, патентування розробок та публічних виступів, що є важливим для подальшої академічної або професійної кар'єри.

Освітньо-наукова програма "Кібербезпека", яка підготовлена кафедрою кібербезпеки Національного технічного університету "Харківський політехнічний інститут" за спеціальністю F5 "Кібербезпека та захист інформації", відповідає сучасним вимогам та вимогам Міністерства освіти і науки України.

Здобувачі освіти, що навчаються за освітньо-науковою програмою «Кібербезпека» матимуть необхідні компетенції у предметній області у разі набуття очікуваних результатів навчання. Рекомендуємо освітньо-наукову програму для використання в навчальному процесі для підготовки наукових і науково-педагогічних кадрів за третім (доктор філософії) рівнем вищої освіти зі спеціальності F5 "Кібербезпека та захист інформації".

Директор ТОВ "Сайфер ІТ",
кандидат технічних наук
2026 рік

Владислав КОВТУН

ТОВ «Мікрокрипт Технолоджіс»
E-mail: info@microcrypt.com.ua

«Microcrypt Technologies» LTD.
Web: www.microcrypt.com.ua

ЗАТВЕРДЖУЮ:
Генеральний директор
ТОВ «Мікрокрипт Технолоджіс»
_____ Головашич С.О.
«12» 03 2026 р.

РЕЦЕНЗІЯ-ВІДГУК
НА ОСВІТНЬО-НАУКОВУ ПРОГРАМУ “КІБЕРБЕЗПЕКА”

третього (доктор філософії) рівня вищої освіти
спеціальності F5 “Кібербезпека та захист інформації”
кафедри кібербезпеки Національного технічного університету
“Харківський політехнічний інститут”

На сьогодні підготовка фахівців в галузі кібербезпеки є актуальною задачею. Надзвичайно важливими є дослідження, які спрямовані на розробку математичних моделей, методів і інформаційних технологій призначених для аналізу та розв’язання задач кіберзахисту в умовах складних моделей інформаційно-телекомунікаційної взаємодії. Такі задачі можуть характеризуватися невизначеністю всіх можливих факторів зовнішнього впливу, багатокритеріальністю, неповнотою апріорної та/або апостеріорної інформації, доступної в рамках дослідження, можливими непередбаченими збуреннями в каналах захищеного зв’язку.

Освітньо-наукова програма підготовки докторів філософії “Кібербезпека”, яка розроблена на кафедрі кібербезпеки Національного технічного університету “Харківський політехнічний інститут” за спеціальністю F5 “Кібербезпека та захист інформації”, передбачає підготовку наукових і науково-педагогічних

працівників високого рівня в галузі кібербезпеки на основі попередньо отриманої повної вищої освіти (рівень магістр) за напрямом підготовки в галузі кібербезпеки або споріднених спеціальностей. Ця освітньо-наукова програма регламентує цілі, очікувані результати, зміст, умови та технології реалізації освітнього процесу, оцінку якості підготовки випускників за даною спеціальністю.

Програма охоплює широкий спектр сучасних підходів до забезпечення кібербезпеки, дослідження загроз і розробки захисних рішень.

Освітньо-наукова програма передбачає поєднання освітньої та наукової складових, де наукова діяльність здійснюється протягом усього періоду навчання. Основні компоненти: вивчення інформаційних систем та технологій, що використовуються у кібербезпеці та захисті інформації; аналіз та впровадження сучасних методів і моделей забезпечення інформаційної безпеки; дослідження програмного та апаратного забезпечення засобів кіберзахисту; використання інструментів автоматизованого управління інформаційною безпекою та моніторингу кіберзагроз; проведення наукових досліджень у сфері інформаційних технологій та кібербезпеки.

Програма передбачає ґрунтовну підготовку аспірантів у сфері педагогіки та психології вищої освіти, що є необхідною складовою для майбутніх викладачів. Аспіранти опановують: основи психології навчання дорослих та особливості педагогічної діяльності у закладах вищої освіти; методику розробки навчальних програм, лекційних та практичних занять, що відповідають сучасним стандартам освіти; технології інтерактивного навчання, використання цифрових платформ та онлайн-курсів у викладанні дисциплін з кібербезпеки; методи оцінювання знань студентів, формування тестових завдань, кейс-методів та індивідуальних навчальних траєкторій; розвиток комунікативних та управлінських навичок, необхідних для ефективної роботи у вищих навчальних закладах. Ця складова програми дозволяє аспірантам не лише займатися дослідницькою діяльністю, а й ефективно передавати свої знання майбутнім фахівцям у галузі кібербезпеки.

З результатів вивчення представленої освітньо-наукової програми можна зробити висновок, що вона має високий рівень забезпеченості навчально-методичною літературою та матеріалами.

Освітньо-наукова програма “Кібербезпека” для підготовки докторів філософії за спеціальністю 125 “Кібербезпека та захист інформації” у Національному технічному університеті “Харківський політехнічний інститут” є актуальною, відповідає освітньо-науковим характеристикам і може бути рекомендована до використання у навчальному процесі для підготовки фахівців третього рівня вищої освіти в області кібербезпеки.

Генеральний директор
ТОВ “Мікрокрипт Технолоджіс”,
кандидат технічних наук
2026 рік

Сергій ГОЛОВАШИЧ

РЕЦЕНЗІЯ-ВІДГУК

НА ОСВІТНЬО-НАУКОВУ ПРОГРАМУ “КІБЕРБЕЗПЕКА”

третього (доктора філософії) рівня вищої освіти

спеціальності F5 “Кібербезпека та захист інформації”

кафедри кібербезпеки Національного технічного університету

“Харківський політехнічний інститут”

Освітньо-наукова програма підготовки докторів філософії "Кібербезпека", розроблена на кафедрі кібербезпеки Національного технічного університету "Харківський політехнічний інститут" за спеціальністю F5 "Кібербезпека та захист інформації", спрямована на формування інтегральної компетентності – здатності продукувати нові ідеї, розв’язувати комплексні проблеми професійної та/або дослідницько-інноваційної діяльності у сфері кібербезпеки та захисту інформації, застосовувати методологію наукової та педагогічної діяльності, а також проводити власне наукове дослідження, результати якого мають наукову новизну, теоретичне та практичне значення. Це передбачає глибоке переосмислення наявних знань, створення нових цілісних концепцій та вдосконалення професійної практики.

Програму розроблено групою науково-педагогічних працівників, що складається з висококваліфікованих фахівців, які відповідають вимогам до розробників освітніх програм.

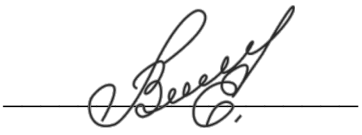
Освітньо-наукова програма забезпечує здатність випускників: до професійного спілкування іноземною мовою; до абстрактного мислення, аналізу та синтезу; до проведення самостійних досліджень; до виявлення та генерування нових ідей; до дослідження й вирішення актуальних проблем у сфері кібербезпеки; до роботи в міжнародному науковому просторі; до розробки та управління науковими проєктами.

Навчальний процес проходить у сучасних аудиторіях і лабораторіях, оснащених передовими комп’ютерними та технічними засобами, зокрема мультимедійним обладнанням і спеціалізованим програмним забезпеченням.

Освітньо-наукова програма "Кібербезпека" забезпечує національну кредитну мобільність на основі двосторонніх договорів між Національним технічним університетом "Харківський політехнічний інститут" та іншими закладами вищої освіти України. Це дозволяє студентам проходити навчання, обмінюватися досвідом, здобувати нові знання й навички в межах спільних освітніх проєктів, академічних обмінів і наукових стажувань.

Освітньо-наукова програма "Кібербезпека", підготовлена кафедрою кібербезпеки Національного технічного університету "Харківський політехнічний інститут", відповідає сучасним вимогам до підготовки фахівців третього (доктора філософії) рівня вищої освіти. Програму рекомендовано для використання в навчальному процесі з підготовки наукових і науково-педагогічних кадрів за спеціальністю F5 "Кібербезпека та захист інформації".

Керівник освітніх програм
Компанії Distributed Lab,
кандитат технічних наук
2026 рік



Олена ВОЛОЩУК

Громадська спілка "Харківський
кластер інформаційних технологій"
вул.Громадянська 11/13,
м.Харків, 61057 Україна
+38 (050) 658-88-46
olga.shapoval@it-kharkiv.com
www.it-kharkiv.com

РЕЦЕНЗІЯ-ВІДГУК

На освітньо-наукову програму «Кібербезпека» за спеціальністю F5 «Кібербезпека та захист інформації» третього (освітньо-наукового) рівня вищої освіти в Національному технічному університеті «Харківський політехнічний інститут»

Освітньо-наукова програма (ОНП) «Кібербезпека» спрямована на підготовку висококваліфікованих фахівців, здатних розв'язувати комплексні завдання у сфері кібербезпеки, які поєднують фундаментальну наукову підготовку з практичною діяльністю. Програма розроблена відповідно до найсучасніших вимог IT-індустрії та включає як теоретичні аспекти захисту інформації, так і практичні інструменти для забезпечення безпеки у складних соціокіберфізичних системах.

ОНП забезпечує здобуття аспірантами компетентностей для виконання інноваційних наукових досліджень, результати яких можуть бути впроваджені як у приватному секторі, так і на державному рівні. Програма відзначається мультидисциплінарним підходом, інтегруючи знання з кібербезпеки, програмування, криптографії, аналізу даних та управління ризиками. Її особливістю є активна співпраця із провідними науковими установами та компаніями, що забезпечує унікальне поєднання академічної освіти та досвіду реальних проєктів.

Проаналізувавши дану ОПП, експерти від IT-компаній роботодавців окреслили її наступні позитивні сторони та надали коментарі й рекомендації, а саме:

- приділена значна увага до сучасних напрямків, таких як постквантова криптографія, DevSecOps, та технології блокчейн;
- наявність лабораторій, партнерств із компаніями та сертифікацій (CISCO);
- участь у конференціях та доступ до міжнародних баз даних;
- індивідуальні освітні траєкторії та вибір дисциплін з урахуванням наукових інтересів здобувачів;

- рекомендовано додати більше тем в навчальні компоненти із застосуванням AI, а саме: штучний інтелект у виявленні кіберзагроз, машинне навчання для аналізу поведінки в мережах;
- рекомендовано підвищити увагу до роботи з великими даними Big Data (додати більше тем в навчальні компоненти щодо аналізу великих даних та кібербезпеки у великих IT-системах);
- рекомендовано розширити спектр soft skills шляхом впровадження курсів з лідерства, управління проєктами, стратегічного мислення у контексті кібербезпеки.

ОНП «Кібербезпека» має потенціал стати лідером у підготовці фахівців найвищого рівня у сфері інформаційних технологій. Запропоновані рекомендації сприятимуть ще більшій актуалізації програми в умовах динамічного розвитку ринку праці IT.

Освітньо-наукова програма «Кібербезпека» відповідає вимогам сучасних роботодавців і може бути рекомендована для підготовки здобувачів вищої освіти третього (освітньо-наукового) рівня вищої освіти спеціальності F5 «Кібербезпека та захист інформації» в Національному технічному університеті «Харківський політехнічний інститут».

Виконавчий директор
ГС «Харківський кластер
інформаційних технологій»
2026 рік

УКРАЇНА
ГРОМАДСЬКА СПІЛКА "ХАРКІВСЬКИЙ КЛАСТЕР ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ" №39887790
місто Харків

Ольга ШАПОВАЛ

ПЕРЕДМОВА

Відповідає Закону України «Про вищу освіту»; постанови Кабінету Міністрів України від 29.04.2015р. № 266 «Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти»; наказу МОН України від 06.11.2015р. № 1151 «Про особливості запровадження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти», постановою Кабінету Міністрів України від 30.12.2015р. № 1187 «Ліцензійні умови провадження освітньої діяльності закладів освіти» та постанови Кабінету Міністрів України від 23.03.2016р. № 261 «Про затвердження Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у вищих навчальних закладах (наукових установах)»; Стандарту вищої освіти третього (доктор філософії) рівня галузі знань F "Інформаційні технології", спеціальності F5 "Кібербезпека та захист інформації", затвердженого та введеного в дію наказом Міністерства освіти і науки України від 29.10.2024 р. № 1543 (https://mon.gov.ua/static-objects/mon/sites/1/vishcha-osvita/zatverdzeni%20standarty/2024/30-10-2024/125-kiberbezpeka-doktor-filosofiyi-1543-vid-29-10-2024.pdf)

Розроблено робочою групою ОНП «Кібербезпека»

Навчально-наукового інституту комп'ютерних наук та інформаційних технолгій Національного технічного університету «Харківський політехнічний інститут» у складі:

Гарант освітньо-наукової програми

Сергій ПОГАСІЙ, доктор технічних наук, доцент, професор кафедри кібербезпеки.

Члени робочої групи ОНП :

1. Сергій ЄВСЕЄВ, доктор технічних наук, професор, завідувач кафедри кібербезпеки.
2. Станіслав МІЛЕВСЬКИЙ, доктор технічних наук, доцент, професор кафедри кібербезпеки.
3. Ольга КОРОЛЬ, кандидат технічних наук, доцент, доцент кафедри кібербезпеки.
4. Сергій ДУНАЄВ, студент групи А-3523.

1. ПРОФІЛЬ ОСВІТНЬО-НАУКОВОЇ ПРОГРАМИ ЗА СПЕЦІАЛЬНІСТЮ F5 КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

1 – ЗАГАЛЬНА ІНФОРМАЦІЯ	
Вищий навчальний заклад та структурний підрозділ	Національний технічний університет "Харківський політехнічний інститут", навчально-науковий інститут комп'ютерних наук та інформаційних технологій, кафедра кібербезпеки
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Ступінь вищої освіти – доктор філософії Освітня кваліфікації – доктор філософії з кібербезпеки та захисту інформації.
Форма навчання	Інституційна (очна (денна, вечірня), заочна)
Професійна кваліфікація	Відсутня
Форма навчання	Очна (денна, вечірня), заочна
Офіційна назва освітньо-наукової програми	Освітньо-наукова програма «Кібербезпека», англійською мовою "Cyber Security"
Тип диплому та обсяг освітньо-наукової програми	Диплом доктора філософії, одиничний, 50 кредитів ЄКТС, термін навчання – 4 роки
Наявність акредитації	Національне агентство із забезпечення якості вищої освіти. Україна. Сертифікат № 9110. термін дії до 01.07.2029р.
Цикл/рівень	Третій (освітньо-науковий) рівень вищої освіти, НРК України – 8 рівень, EQF–LLL – 8 рівень, QF–EHEA – третій цикл.
Передумови	Наявність ступеню вищої освіти «магістр» або освітньо-кваліфікаційного рівня «спеціаліст»
Мова викладання	Українська мова, Англійська мова
Термін дії освітньо-наукової програми	Переглядається щорічно
Посилання на постійне розміщення опису освітньо-наукової програми	https://web.kpi.kharkov.ua/phd/zanyattya/osvitno-naukovi-programi/
2 – МЕТА ОСВІТНЬО-НАУКОВОЇ ПРОГРАМИ	
Забезпечити підготовку наукових і науково-педагогічних кадрів у сфері комп'ютерних наук та кібербезпеки шляхом здобуття ними компетентностей, достатніх для виконання оригінальних наукових досліджень, результати яких мають наукову новизну, теоретичне та практичне значення, а також їх підтримку в ході підготовки та захисту дисертації в галузі інформаційних технологій за спеціальністю F5 "Кібербезпека та захист інформації".	
3 – ХАРАКТЕРИСТИКА ОСВІТНЬО-НАУКОВОЇ ПРОГРАМИ	
Предметна область	**Галузь знань:** F "Інформаційні технології"

(галузь знань, спеціальність, спеціалізація або предметна спеціальність (за наявності))	**Спеціальність:** F5 “Кібербезпека та захист інформації” ***Об’єкти вивчення та діяльності:*** – інформаційні системи і технології на об’єктах інформаційної діяльності та критичних інфраструктурах сфери кібербезпеки та захисту інформації; – новітні системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення інформації (інформаційних потоків); – сучасні інформаційні ресурси різних класів (у тому числі державні інформаційні ресурси); – програмне та програмно-апаратне забезпечення (засоби) кіберзахисту; – автоматизовані системи управління інформаційною безпекою, кібербезпекою та захистом інформації; – методології, технології, методи, моделі та засоби кібербезпеки та захисту інформації. ***Цілі навчання:*** набуття здатності продукувати нові ідеї, розв’язувати комплексні проблеми професійної та дослідницько-інноваційної діяльності у сфері кібербезпеки та захисту інформації, застосовувати методологію наукової та педагогічної діяльності, та здійснювати власні наукові дослідження, результати яких мають наукову новизну, теоретичне та практичне значення. ***Теоретичний зміст предметної області:*** Принципи, концепції, теорії захисту життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якого забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі. ***Методи, методики та технології:*** Сучасні методи, моделі, методики та технології дослідження та вдосконалення процесів створення, обробки, передачі, приймання, знищення, відображення, захисту (кіберзахисту) інформаційних ресурсів у кіберпросторі, методи статистичного аналізу даних. ***Інструменти та обладнання:*** Програмно-апаратне та програмне забезпечення, інструментальні засоби, комп’ютерна техніка, спеціальні контрольно-вимірювальні прилади, програмно-технічні засоби автоматизації та системи автоматизації проектування, виробництва, експлуатації, контролю, моніторингу, мережні, мобільні, хмарні, технології, мережне устаткування та середовище, прикладне та спеціалізоване програмне забезпечення, автоматизовані системи та комплекси проектування, моделювання, експлуатації, контролю, моніторингу, обробки,

	відображення та захисту даних (інформаційних потоків).
Орієнтація освітньої програми	Освітньо-наукова академічна.
Структура програми	Структура програми передбачає виконання освітньої та наукової складових. Наукова складова виконується під час усього терміну навчання, не переривається на освітню складову, сесію та практику. Зміст кожної складової програми орієнтується на сучасні наукові дослідження комплексних проблем в галузі захисту інформації, кібербезпеки та інформаційних технологій
Основний фокус освітньо-наукової програми та спеціалізації	Спеціальна освіта у галузі інформаційних технологій зі спеціальності F5 "Кібербезпека та захист інформації". Проведення досліджень в галузі F "Інформаційні технології" зі спеціальності F5 "Кібербезпека та захист інформаці" та формування необхідних дослідницьких навиків для наукової кар'єри, викладання дисциплін у галузі інформаційної безпеки та кібербезпеки. Ключові слова: кібербезпека, інформаційна безпека, безпека інформації, захист інформації.
Особливості програми	Програма передбачає вирішення комплексних проблем в галузі захисту інформації, кібербезпеки та інформаційних технологій. Орієнтовано на партнерство із вітчизняними та закордонними закладами освіти та науки, приватним сектором, науковцями та участі в програмах на отримання грантів.
Науковий напрямок програми	Наукова складова ОНП виконується увесь термін навчання в аспірантурі, не переривається на теоретичне навчання та педагогічну практику. Виконання наукової роботи, підготовка наукових публікацій та рукопису дисертації забезпечують формування інтегральної компетентності. Наукова робота проходить під керівництвом одного або двох керівників. Висвітлення результатів наукової роботи передбачає публікацію наукових статей, подачу заявок на патент, виступи на конференціях та після виконання ОНП оформлюється дисертація. Загальний план роботи над дисертацією регламентується сторінкою "**D**". Контроль за виконанням наукової роботи проводиться у рамках проміжної атестації (звітування сторінки "**E**" та річна атестація сторінка "**F**"). З науковим керівником (керівниками) аспірантом обговорюється тема дисертаційної роботи, яка може бути підтримана в напрямку наукових шкіл кафедр, що забезпечують підготовку PhD.
4 – ПРИДАТНІСТЬ ВИПУСКНИКІВ ДО ПРАЦЕВЛАШТУВАННЯ ТА АКАДЕМІЧНІ ПРАВА ВИПУСКНИКІВ	
Придатність до працевлаштування	Працевлаштування на посадах наукових і науково-педагогічних працівників в наукових установах і закладах вищої освіти, посадах працівників найвищої кваліфікації у

	дослідницьких, проектних, конструкторських й т.п. установах і підрозділах підприємств. Назви професій згідно Національного класифікатора України: Класифікатор професій (ДК 003:2010) 1226.2 Начальник відділення (сфера захисту інформації); 1226.2 Керівник структурного підрозділу (сфера захисту інформації); 1229.7 Керівник (директор, начальник та ін.) підрозділу (служби, управління, департаменту та ін.) з безпеки (фінансово-економічної, інформаційної); 2149.2 Професіонал із організації захисту інформації з обмеженим доступом; 2310 Викладачі закладу вищої освіти; 2310.1 Докторант; 2310.1 Доцент закладу вищої освіти.
Академічні права випускників	Можливість навчання в докторантурі, брати участь у постдокторських програмах.
5 – ВИКЛАДАННЯ ТА ОЦІНЮВАННЯ	
Викладання та навчання	Навчання проводиться у формі лекцій, семінарів, практичних лабораторних занять, консультацій, тренінгів, педагогічних практик, самостійного вивчення, виконання самостійного наукового дослідження на основі опрацювання підручників, посібників, монографій, періодичних наукових видань, використання мережі Інтернет тощо.
Оцінювання	Поточний та підсумковий контроль знань (опитування, контрольні та індивідуальні завдання, тестування тощо), заліки та іспити (усні та письмові), звітування, проміжна атестація, презентації, захист звіту з практики, публічний захист дисертаційної роботи.
6 – ПРОГРАМНІ КОМПЕТЕНТНОСТІ	
Інтегральна компетентність	Здатність продукувати нові ідеї, розв’язувати комплексні проблеми професійної та/або дослідницько-інноваційної діяльності у сфері кібербезпеки та захисту інформації, застосовувати методологію наукової та педагогічної діяльності, а також проводити власне наукове дослідження, результати якого мають наукову новизну, теоретичне та практичне значення.
Загальні компетентності	ЗК1. Здатність до абстрактного мислення, аналізу і синтезу. ЗК2. Здатність до пошуку, оброблення та аналізу інформації з різних джерел. ЗК3. Здатність працювати в міжнародному контексті. ЗК4. Здатність розв’язувати комплексні проблеми предметної області на основі системного наукового світогляду та загального культурного кругозору із дотриманням принципів професійної етики та академічної

	доброчесності.
Спеціальні (фахові, предметні) компетентності	СК1. Здатність виконувати оригінальні дослідження, досягати наукових результатів, які створюють нові знання у сфері кібербезпеки та захисту інформації та дотичних міждисциплінарних напрямах і можуть бути опубліковані у провідних наукових виданнях з кібербезпеки та захисту інформації. СК2. Здатність ініціювати, розробляти і реалізовувати комплексні наукові та інноваційні проєкти в сфері кібербезпеки та захисту інформації. СК3. Здатність розв'язувати значущі проблеми у сфері кібербезпеки та захисту інформації, розширювати та переоцінювати наявні знання і професійні практики. СК4. Здатність ефективно застосовувати методи аналізу даних, концептуального, математичного та комп'ютерного моделювання, виконувати натурні та обчислювальні експерименти при проведенні наукових і прикладних досліджень у сфері кібербезпеки та захисту інформації. СК5. Здатність генерувати нові ідеї щодо розвитку теорії та практики кібербезпеки та захисту інформації, виявляти, ставити та вирішувати проблеми дослідницького характеру, оцінювати та забезпечувати якість виконуваних досліджень. СК6. Здатність вільно спілкуватися з питань, що стосуються сфери кібербезпеки та захисту інформації, з колегами, широкою науковою спільнотою, суспільством у цілому з використанням академічної української та англійської мови. СК7. Здатність здійснювати та організовувати наукову та освітню науково-педагогічну діяльність у закладах вищої освіти.
7 – РЕЗУЛЬТАТИ НАВЧАННЯ	
Результати навчання	РН1. Мати передові концептуальні та методологічні знання з кібербезпеки та захисту інформації і на межі предметних галузей, а також дослідницькі навички, достатні для проведення наукових і прикладних досліджень на рівні останніх світових досягнень з кібербезпеки та захисту інформації, отримання нових знань та/або здійснення інновацій. РН2. Планувати і виконувати експериментальні та/або теоретичні дослідження з кібербезпеки та захисту інформації та дотичних міждисциплінарних напрямів з використанням сучасних інструментів та дотриманням норм професійної і академічної етики. РН3. Критично аналізувати результати власних досліджень і результати інших дослідників у контексті усього комплексу сучасних знань щодо досліджуваної проблеми. РН4. Глибоко розуміти загальні принципи та методи

	кібербезпеки та захисту інформації, а також методологію наукових досліджень, застосувати їх у власних дослідженнях у сфері інформаційних технологій та у викладацькій практиці. РН5. Формулювати і перевіряти гіпотези; використовувати для обґрунтування висновків належні докази, зокрема, результати теоретичного аналізу, експериментальних досліджень і математичного та/або комп'ютерного моделювання, наявні літературні дані. РН6. Вільно презентувати та обговорювати з фахівцями і нефахівцями результати досліджень, наукові та прикладні проблеми кібербезпеки та захисту інформації державною та іноземною мовами усно та письмово, оприлюднювати результати досліджень у наукових публікаціях у провідних вітчизняних та міжнародних наукових виданнях. РН7. Застосовувати загальні принципи та методи математики, інформатики та інших наук, а також сучасні методи та інструменти, цифрові технології та спеціалізоване програмне забезпечення для провадження наукових досліджень у сфері кібербезпеки та захисту інформації. РН8. Розробляти та досліджувати концептуальні, математичні і комп'ютерні моделі процесів і систем, ефективно використовувати їх для отримання нових знань та/або створення інноваційних продуктів у кібербезпеки та захисту інформації та дотичних міждисциплінарних напрямах. РН9. Застосовувати сучасні інструменти і технології пошуку, оброблення та аналізу інформації, зокрема, статистичні методи аналізу даних великого обсягу та/або складної структури, спеціалізовані бази даних та інформаційні системи. РН10. Організовувати і здійснювати освітній процес у сфері кібербезпеки та захисту інформації, його наукове, навчально-методичне та нормативне забезпечення, розробляти і викладати спеціальні навчальні дисципліни у закладах вищої освіти.
8 – РЕСУРСНЕ ЗАБЕЗПЕЧЕННЯ РЕАЛІЗАЦІЇ ПРОГРАМИ	
Кадрове забезпечення	Кадрове забезпечення ОНП відповідає постанові Кабінету Міністрів України від 30.12.2015 р. № 1187 «Про затвердження Ліцензійних умов провадження освітньої діяльності закладів освіти» (зі змінами, внесеними згідно з Постановою КМ від 24.03.2021 р. № 365, додаток 15-16).
Матеріально-технічне забезпечення	Матеріально-технічне забезпечення освітньої програми відповідає постанові Кабінету Міністрів України від 30.12.2015 р. № 1187 «Про затвердження Ліцензійних умов провадження освітньої діяльності закладів освіти» (зі змінами, внесеними згідно з Постановою КМ № 365 від 24.03.2021 До-даток 17).

	Навчальний процес відбувається у аудиторіях та лабораторіях, обладнаних сучасними комп'ютерними та технічними засобами, в тому числі мультимедійними, а також спеціалізованим програмним забезпеченням.
Інформаційне та навчально-методичне забезпечення	Інформаційне та навчально-методичне забезпечення освітньої програми відповідає постанові Кабінету Міністрів України від 30.12.2015 р. № 1187 «Про затвердження Ліцензійних умов провадження освітньої діяльності закладів освіти» (зі змінами, внесеними згідно з Постановою КМ № 365 від 24.03.2021. Додаток 18). Інформаційне та навчально-методичне забезпечення навчального процесу реалізується наявністю необхідної навчальної та методичної літератури: підручники, навчальні посібники, методичні рекомендації до практичних занять, самостійної роботи, силабуси освітніх компонентів (https://cybersecurity.khpi.edu.ua/sylabusy-osvitnikh-komponentiv-f5-doctor-filosofii/). Інформаційні ресурси розміщені у фондах наукової бібліотеки НТУ "ХПІ", сайтах випускових кафедр.
9 – АКАДЕМІЧНА МОБІЛЬНІСТЬ	
Національна кредитна мобільність	Внутрішню академічну мобільність (ступеневу або кредитну), що реалізується здобувачами вищої освіти за освітньо-науковою програмою у вищих навчальних закладах (наукових установах) – партнерах в межах України.
Міжнародна кредитна мобільність	Міжнародна академічна мобільність на основі двосторонніх договорів в рамках проєктів Еразмус КА1 між Національним технічним університетом "Харківський політехнічний інститут" та Університетом ім. Яна Длугоша в м. Ченстохові (Польща), Університетом у Бєльсько-Бялій (Польща).
Навчання іноземних здобувачів освіти	Передбачена можливість навчання іноземних студентів. Наявність сертифікатів професорсько-викладацького складу кафедри: Євсеєв С.П., д.т.н., проф., завідувач кафедри кібербезпеки (B2); Ткачов А.М. к.т.н., с.н.с., доцент кафедри кібербезпеки (B2); Корольов Р.В. к.т.н., доц., доцент кафедри кібербезпеки (B2); Мілевський С.В., д.т.н., доц., професор кафедри кібербезпеки (C1); Погасій С.С. д.т.н., доц., професор кафедри кібербезпеки (B2), Воропай Н.І. к.т.н., доцент кафедри кібербезпеки (B2)

2. ПЕРЕЛІК КОМПОНЕНТІВ ОСВІТНЬО-НАУКОВОЇ ПРОГРАМИ «КІБЕРБЕЗПЕКА» ТА ЇХ ЛОГІЧНА ПОСЛІДОВНІСТЬ

2.1 Перелік компонентів освітньо-наукової програми

Код н/д	Компоненти освітньо-наукової програми (дисципліни, проекти / роботи, практика, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
І. ОСВІТНЯ СКЛАДОВА			
1. Обов'язкові освітні компоненти / Compulsory Educational Components			
1.1 Загальна підготовка / General Training			
ЗП 1	Світоглядні, методологічні та соціокультурні засади наукової діяльності / *Worldview, Methodological and Sociocultural Fundamentals of Scientific Activity*	4,0	Екзамен
ЗП 2	Іноземна мова для комунікації у науково-педагогічному середовищі / *Foreign Languages for Communication in a Scholarly and Pedagogical Environment*	8,0	Екзамен
ЗП 3	Організація науково-дослідної та інноваційної діяльності */ Organization of Scientific Research and Innovation Activities*	4,0	Диф.залік
ЗП 4	Педагогіка і психологія вищої освіти з методикою викладання */ Pedagogy and Psychology of Higher Education with Teaching Methods*	3,0	Диф.залік
1.2 Спеціальна (фахова) підготовка / Special (Professional) Training			
СП 1	Методологія наукової та педагогічної діяльності в науках кіберзахисту */ Methodology of scientific and pedagogical activity in cyber defense sciences*	4,0	Екзамен
СП 2	Оцінка вразливості та захисту інформаційних систем*/ Information systems' vulnerability and protection assessment*	4,0	Екзамен
СП 3	Математичні методи, моделі та інформаційні технології у наукових дослідженнях */ Mathematical methods, models and information technologies in scientific research*	4,0	Екзамен
1.3 Практична підготовка / Practical Training			
ПП 1	Педагогічна практика */ Pedagogical Practice*	3,0	Диф.залік
Загальний обсяг обов'язкових компонентів		**33**	
2. Вибіркові освітні компоненти / Elective Educational Components			
ВП 2.1	Вибіркові освітні компоненти третього семестру	8,0	Екзамен
ВП 2.2	Вибіркові освітні компоненти четвертого семестру	8,0	Диф.залік

Загальний обсяг вибіркових компонентів		**16**	
ІІ. НАУКОВА СКЛАДОВА			
1	Наукові публікації		Статті, поточна атестація
2	Кваліфікаційна наукова праця		Рукопис дисертації
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬО-НАУКОВОЇ ПРОГРАМИ		**50**	

3. РОЗПОДІЛ ЗМІСТУ ОСВІТНЬО-НАУКОВОЇ ПРОГРАМИ ЗА ГРУПАМИ КОМПОНЕНТІВ ТА ЦИКЛАМИ ПІДГОТОВКИ

№ п/п	Цикл підготовки	Обсяг навчального навантаження здобувача вищої освіти (кредитів ECTS / %)		
		Обов'язкові компоненти освітньо-наукової програми	Вибіркові компоненти освітньо-наукової програми	Всього за весь термін навчання
1	Загальна підготовка	19 / 38	–	**19 / 38**
2	Спеціальна (фахова) підготовка	12 / 24	–	**12/ 24**
3	Практична підготовка	3 / 6	–	**3/ 6**
4	Компоненти вільного вибору	–	16 / 32	**16 / 32**
Всього за весь термін навчання		**34 / 68**	**16 / 32**	**50 / 100**

4. ФОРМА АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Поточна атестація	За весь термін навчання аспірант два рази на рік звітує про виконання індивідуального плану (сторінки E та F) на засіданні випускової кафедри, вченій раді інституту і щорічно атестується науковим керівником відповідно до графіку освітнього процесу.
Вимоги до дисертації на здобуття ступеня доктора філософії	Здобувач повинен набути теоретичні знання, уміння, навички та компетентності, визначені стандартом вищої освіти третього (освітньо-наукового) рівня за відповідною спеціальністю, провести власне наукове дослідження, оформлене у вигляді дисертації, та опублікувати основні його наукові результати. Дисертація повинна містити нові науково обґрунтовані результати проведених здобувачем досліджень, які виконують конкретне наукове завдання, що має істотне значення для певної галузі знань. Вимоги щодо оформлення дисертації встановлюються МОН. Максимальний та/або мінімальний обсяг основного тексту дисертації становить 4,5-7 авторських аркушів.
Підсумкова атестація	Науково-дослідна робота аспіранта, яка виконується в рамках теми дисертаційної роботи, є головним елементом у підготовці за освітньо-науковою програмою. За цей час аспірант навчається самостійно виконувати науковий пошук, обрати й обґрунтувати методи дослідження та аналізувати результати своєї роботи. Науково-дослідна робота виконується під керівництвом наукового керівника, який несе повну відповідальність за підготовку аспіранта та своєчасно виконання, подачу дисертаційної роботи. Підготовка дисертаційної роботи та її захист є завершенням навчання на третьому (освітньо-науковому) рівні. Атестація випускників освітньо-наукової програми спеціальності F5 “Кібербезпека та захист інформації” проводиться у формі публічного захисту (демонстрації) кваліфікаційної роботи та завершується видачею документу встановленого зразка про присудження ступеня вищої освіти Доктор філософії з присвоєнням кваліфікації: доктор філософії з кібербезпеки та захисту інформації

5. ВИМОГИ ДО НАЯВНОСТІ СИСТЕМИ ВНУТРІШНЬОГО ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ВИЩОЇ ОСВІТИ

Принципи та процедури забезпечення якості освіти	Принципи: – відповідність європейським і національним стандартам якості вищої освіти; – автономія закладу вищої освіти, який відповідає за забезпечення якості освітньої діяльності та якості вищої освіти; – системний підхід, який передбачає управління якістю на всіх рівнях освітнього процесу; – здійснення моніторингу якості освіти; – залучення аспірантів, роботодавців та інших зацікавлених сторін до процесу забезпечення якості; – відкритість інформації на всіх етапах забезпечення якості. Процедури: – удосконалення планування освітньо-наукової діяльності; – затвердження, моніторинг і періодичний перегляд освітньо-наукових програм; – підвищення якості підготовки контингенту здобувачів вищої освіти; – посилення кадрового потенціалу Університету; – забезпечення наявності необхідних ресурсів для організації освітнього процесу та підтримки здобувачів вищої освіти; – розвиток інформаційних систем з метою підвищення ефективності управління освітнім процесом; – забезпечення публічності інформації про діяльність Університету; – створення ефективної системи запобігання та виявлення академічного плагіату в наукових працях викладачів та здобувачів вищої освіти.
Моніторинг та періодичний перегляд програм	Регулярний моніторинг, перегляд і оновлення освітньо-наукових програм мають на меті гарантувати відповідний рівень надання освітніх послуг, а також створює сприятливе й ефективне навчальне середовище для здобувачів вищої освіти. Це передбачає оцінювання: змісту програми, гарантуючи відповідність програми сучасним вимогам; потреб суспільства, що змінюються; навчального навантаження здобувачів вищої освіти, їх досягнень і результатів завершення освітньо-наукової програми; ефективності процедур оцінювання аспірантів; очікувань, потреб і задоволеності здобувачів вищої освіти змістом та процесом навчання; навчального середовища відповідності меті і змісту програми; якості сервісних послуг для здобувачів вищої освіти. Програми регулярно переглядають і оновлюють після завершення повного циклу підготовки до початку нового навчального року.
Оцінювання здобувачів вищої освіти	Оцінювання результатів навчання аспірантів здійснюється під час проведення контрольних та моніторингових заходів.

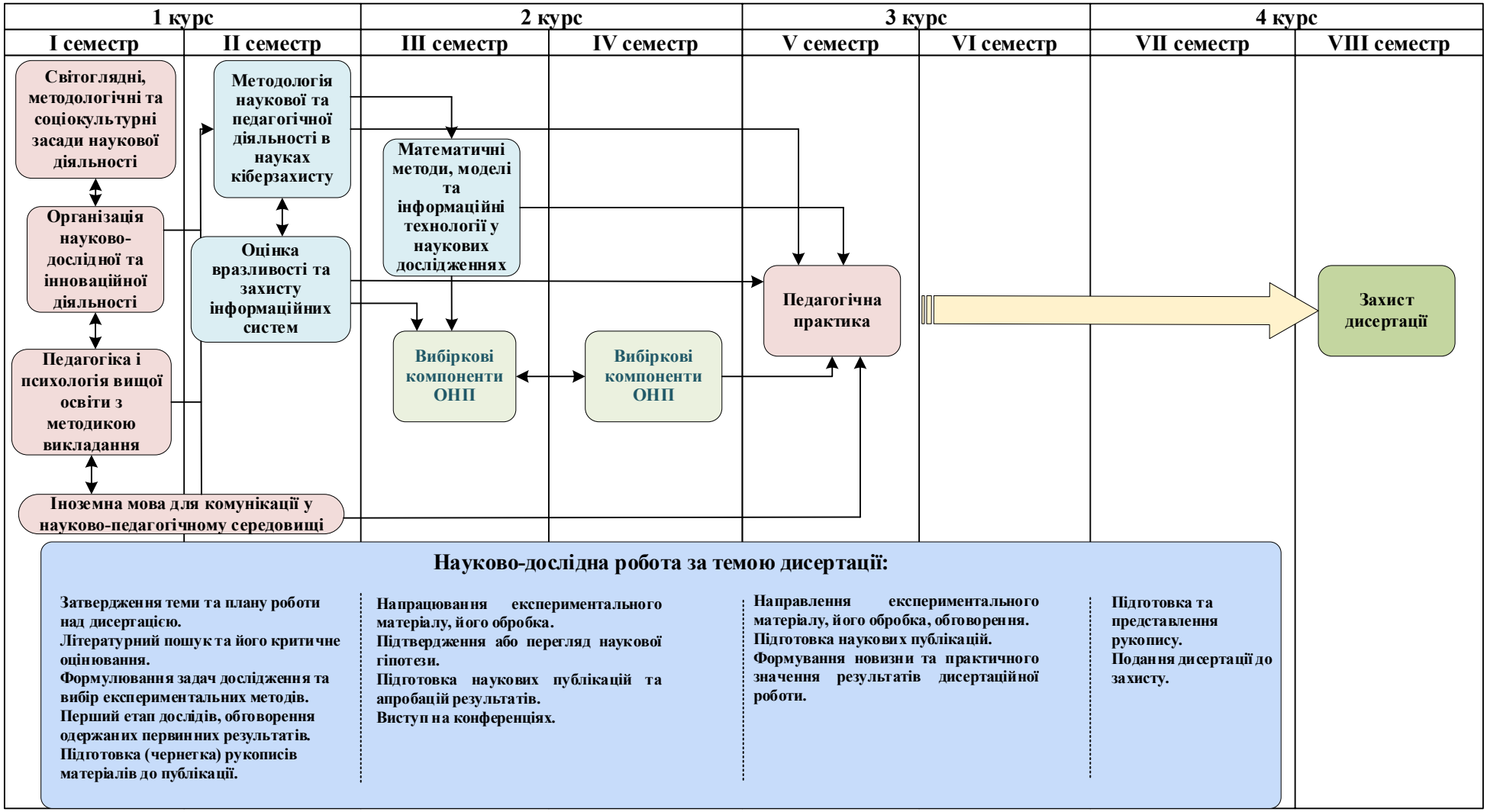
	Заходи передбачають поточний і семестровий контроль, звітування та атестація. Завданням поточного контролю є перевірка розуміння і засвоєння певного матеріалу, вироблених навичок проведення розрахункових робіт, умінь самостійно опрацьовувати тексти, публічно чи письмово представляти певний матеріал тощо. Формами поточного контролю є: виконання індивідуальних завдань; виконання тестових завдань; виконання контрольних робіт, які виконуються в аудиторії або під час самостійної роботи; написання і захист рефератів; захист лабораторних робіт. Підсумковий контроль проводиться з метою оцінки результатів навчання на відповідному освітньому рівні або на окремих його завершальних етапах. Підсумковий контроль включає семестровий контроль (екзамен, диференційований залік з конкретної навчальної дисципліни) та атестацію аспіранта. Семестровий контроль проводиться у формі семестрового екзамену або заліку з конкретної навчальної дисципліни в обсязі навчального матеріалу, визначеного навчальною програмою, і в терміни, встановлені навчальним планом. Навчальні дисципліни, з яких заплановано проведення моніторингових контрольних робіт, терміни проведення контрольних заходів визначаються графіком навчального процесу. Оцінювання результатів навчання аспірантів Університету проводиться методами, що відповідають специфіці конкретної навчальної дисципліни. Моніторинг успішності аспиранту здійснюється за допомогою 100-бальної системи оцінювання з обов'язковим переведенням оцінок до національної шкали та шкали ECTS.
Підвищення кваліфікації науково-педагогічних, педагогічних та наукових працівників	Система підвищення кваліфікації науково-педагогічних, педагогічних та наукових працівників розробляється у відповідності до діючої нормативної бази та будується на наступних принципах: обов'язковості та періодичності проходження стажування і підвищення кваліфікації; прозорості процедур організації стажування та підвищення кваліфікації; моніторингу відповідності змісту програм підвищення кваліфікації задачам професійної діяльності; обов'язковості впровадження результатів підвищення кваліфікації в наукову та педагогічну діяльність; оприлюднення результатів стажування та підвищення кваліфікації.
Наявність необхідних ресурсів для організації освітнього процесу	Наявне кадрове, матеріально-технічне, навчально-методичне та інформаційне забезпечення зі спеціальності відповідає вимогам діючих Ліцензійних умов провадження освітньої діяльності закладів освіти та забезпечує реалізацію державних вимог до фахівця з вищою освітою.

Наявність інформаційних систем для ефективного управління освітнім процесом	З метою управління освітніми процесами розроблено ефективну політику в сфері інформаційного менеджменту та відповідну інтегровану інформаційну систему управління освітнім процесом. Дана система передбачає автоматизацію основних функцій управління освітнім процесом, зокрема: забезпечення проведення вступної компанії, планування та організація навчального процесу; доступ до навчальних ресурсів; обліку та аналізу успішності здобувачів вищої освіти; адміністрування основних та допоміжних процесів забезпечення освітньої діяльності; моніторинг дотримання стандартів якості. Для управління якістю освітньої діяльності в Університеті створена інформаційна система АСУ НП.
Публічність інформації про освітньо-наукові програми, ступені вищої освіти та кваліфікації	Інформації про ОНП, ступені вищої освіти та кваліфікації розміщена у відкритому доступі на сайті НТУ «ХПІ».
Дотримання академічної доброчесності працівниками Університету та здобувачами вищої освіти	В Університеті працівниками та здобувачами вищої освіти здійснюється дотримання академічної доброчесності. Система забезпечення дотримання академічної доброчесності учасниками освітнього процесу базується на таких принципах: дотримання загальноприйнятих принципів моралі; демонстрація поваги до Конституції і законів України, дотримання їхніх норм; повага до всіх учасників освітнього процесу незалежно від їхнього світогляду, соціального стану, релігійної та національної приналежності; дотримання норм законодавства про авторське право; посилання на джерела інформації у разі запозичень ідей, тверджень, відомостей; самостійне виконання індивідуальних завдань.
Система запобігання та виявлення академічного плагіату	Здійснюється перевірка на плагіат згідно з вимогами нормативних документів Університету.

6. МАТРИЦЯ ВІДПОВІДНОСТІ ВИЗНАЧЕНИХ СТАНДАРТОМ КОМПЕТЕНТНОСТЕЙ ДЕСКРИПТОРАМ НРК

Класифікація компетентностей за НРК	**Знання** **Зн1.** Концептуальні та методологічні знання в галузі чи на межі галузей знань або професійної діяльності.	**Уміння/Навички** **Ум1.** Спеціалізовані уміння/навички і методи, необхідні для розв'язування задач ц сфері професійної діяльності, науки та/або інновацій, розширення та переоцінки вже існуючих знань і професійної практики. **Ум2.** Започаткування, планування, реалізація та коригування послідовного процесу грунтовного наукового дослідження з дотриманням належної академічної доброчесності. **Ум3.** Критичний аналіз, оцінка і синтез нових та комплексних ідей.	**Комунікація** **К1.** Вільне спілкування з питань, що стосуються сфери наукових та екпертних заннь, з колегами, широкою науковою спільнотою, суспільством в цілому. **К2.** Використання академічної державної та іноземної мови у професійній діяльності та дослідженнях.	**Відповідальність і автономія** **АВ1.** Демонстрація значної авторитетності, інноваційність, високий ступінь самостійності, академічна та професійна доброчесність, послідовна відданість розвитку нових ідей або процесів у передових контекстах професійної та наукової діяльності. **АВ2.** Здатність до безперервного саморозвитку та самовдосконалення.
ЗАГАЛЬНІ КОМПЕТЕНТНОСТІ				
ЗК-1		Ум1		АВ1, АВ2
ЗК-2	Зн1	Ум1, Ум3	К2	АВ2
ЗК-3			К1, К2	АВ1, АВ2
ЗК-4	Зн1	Ум2	К2	АВ1, АВ2
СПЕЦІАЛЬНІ (ФАХОВІ, ПРЕДМЕТНІ) КОМПЕТЕНТНОСТІ				
СК-1	Зн1	Ум1, Ум2, Ум3	К1, К2	АВ1, АВ2
СК-2			К1, К2	АВ1, АВ2
СК-3			К1	АВ2
СК-4	Зн1	Ум1, Ум2, Ум3		
СК-5	Зн1	Ум1, Ум2, Ум3		АВ2
СК-6		Ум2, Ум3	К1	АВ1
СК-7		Ум1, Ум2, Ум3	К1, К2	АВ2

7.СТРУКТУРНО-ЛОГІЧНА СХЕМА



8. ГРАФІК ОСВІТНЬОГО ПРОЦЕСУ

Місяць	Жовтень					Листопад					Грудень				Січень					Лютий				Березень				Квітень				Травень				Червень				Липень				Серпень				Вересень			
кінець тижня	05	12	19	26	02	09	16	23	30	07	14	21	28	04	11	18	25	01	08	15	22	01	08	15	22	29	05	12	19	26	03	10	17	24	31	07	14	21	28	05	12	19	26	02	09	16	23	30	06	13	20	27
початок тижня	29	06	13	20	27	03	10	17	24	01	08	15	22	29	05	12	19	26	02	09	16	23	02	09	16	23	30	06	13	20	27	04	11	18	25	01	08	15	22	29	06	13	20	27	03	10	17	24	31	07	14	21	28
пн		06	13	20	27	03	10	17	24	01	08	15	22	29	05	12	19	26	02	09	16	23	02	09	16	23	30	06	13	20	27	04	11	18	25	01	08	15	22	29	06	13	20	27	03	10	17	24	31	07	14	21	28
вт		07	14	21	28	04	11	18	25	02	09	16	23	30	06	13	20	27	03	10	17	24	03	10	17	24	31	07	14	21	28	05	12	19	26	02	09	16	23	30	07	14	21	28	04	11	18	25	01	08	15	22	29
ср	01	08	15	22	29	05	12	19	26	03	10	17	24	31	07	14	21	28	04	11	18	25	04	11	18	25	01	08	15	22	29	06	13	20	27	03	10	17	24	01	08	15	22	29	05	12	19	26	02	09	16	23	30
чт	02	09	16	23	30	06	13	20	27	04	11	18	25	01	08	15	22	29	05	12	19	26	05	12	19	26	02	09	16	23	30	07	14	21	28	04	11	18	25	02	09	16	23	30	06	13	20	27	03	10	17	24	
пт	03	10	17	24	31	07	14	21	28	05	12	19	26	02	09	16	23	30	06	13	20	27	06	13	20	27	03	10	17	24	01	08	15	22	29	05	12	19	26	03	10	17	24	31	07	14	21	28	04	11	18	25	
сб	04	11	18	25	01	08	15	22	29	06	13	20	27	03	10	17	24	31	07	14	21	28	07	14	21	28	04	11	18	25	02	09	16	23	30	06	13	20	27	04	11	18	25	01	08	15	22	29	05	12	19	26	
нд	**05**	**12**	**19**	**26**	**02**	**09**	**16**	**23**	**30**	**07**	**14**	**21**	**28**	**04**	**11**	**18**	**25**	**01**	**08**	**15**	**22**	**01**	**08**	**15**	**22**	**29**	**05**	**12**	**19**	**26**	**03**	**10**	**17**	**24**	**31**	**07**	**14**	**21**	**28**	**05**	**12**	**19**	**26**	**02**	**09**	**16**	**23**	**30**	**06**	**13**	**20**	**27**	
Категорія тижня	I	II	I	II	I	II	I	II	I	II	I	II	I	II	I	II	I	II	I	II	I	II	I	II	I	II	I	II	I	II	I	II	I	II	I	II	I	II	I	II	I	II	I	II	I	II	I	II	I	II	
I курс	Т Т Т Т Т Т Т Т Т Т Н Н Н Н Н Н Н Н Н Н	С	Н	Н	Н Н Н Н Н Н Н Н Н Н	Т Т Т Т Т Т Т Т Т Т Н Н Н Н Н Н Н Н Н Н	3 Н	Т Т Н	С	Н	Н	К К К К К К К К	Н	Н	Н	А Н
II курс	Т Т Т Т Т Т Т Т Т Т Н Н Н Н Н Н Н Н Н Н	С	Н	Н	Н Н Н Н Н Н Н Н Н Н	Т Т Т Т Т Т Т Т Т Т Н Н Н Н Н Н Н Н Н Н	3 Н	Т Т Н	С	Н	Н	К К К К К К К К	Н	Н	Н	А Н
* III курс	П П П П П П П П П П Н Н Н Н Н Н Н Н Н Н	Н	Н	Н	Н Н Н Н Н Н Н Н Н Н	П П П П П П П П П П Н Н Н Н Н Н Н Н Н Н	3 Н	Н Н	Н	Н	Н	К К К К К К К К	Н	Н	Н	А Н
** III курс	П П П П П П П П П П Н Н Н Н Н Н Н Н Н Н	Н	Н	Н	Н Н Н Н Н Н Н Н Н Н	Н Н Н Н Н Н Н Н Н Н	3 Н	Н Н	Н	Н	Н	К К К К К К К К	Н	Н	Н	А Н
IV курс	Н Н Н Н Н Н Н Н Н Н	Н	А	А	Д Д Д Д Д Д Д Д Д Д	Д Д Д Д Д Д Д Д Д Д	Д	Д Д Д	Д	Д	Д	К К К К К К К К	Д	Д	Д	Д

Т	Теоретичне навчання
Н	Науково-дослідна робота
С	Екзаменаційна сесія
З	Звіт
П	Практика
Д	Підготока та захист дисертації
К	Канікули
А	Атестація

* III курс усіх спеціальності, крім **

** III курс спеціальностей: "011-Освітні, педагогічні науки"; "054-Соціологія"; "105-Прикладна фізика та наноматеріали"; "123-Комп'ютерна інженерія"; "132-Матеріалознавство"; "133-Галузеве машинобудування"; "141-Електроенергетика, електротехніка та електромеханіка"; "144-Теплоенергетика"; "171-Електроніка"; "172-Електронні комунікації та радіотехніка"; "175-Інформаційно-вимірювальні технології"; "255-Озброєння та військова техніка"; 281-"Публічне управління та адміністрування"

9. МАТРИЦЯ ВІДПОВІДНОСТІ ВИЗНАЧЕНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ, КОМПЕТЕНТНОСТЕЙ ТА ОСВІТНІХ КОМПОНЕНТІВ

Результати навчання	**Компетентності**										
	Інтегральна компетентність: Здатність розв'язувати комплексні проблеми в галузі професійної та/або дослідницько-інноваційної діяльності у сфері кібербезпеки та захисту інформації, що передбачає глибоке переосмислення наявних та створення нових цілісних знань та/або професійної практики										
	Загальні компетентності				**Спеціальні (фахові) компетентності**						
	ЗК-1	ЗК-2	ЗК-3	ЗК-4	СК-1	СК-2	СК-3	СК-4	СК-5	СК-6	СК-7
РН-1			ЗП2, ЗП3, ЗП4, ПП1		СП2 СП3 ПП1					ЗП2 ЗП3 ЗП4 СП1 ПП1	
РН-2	ЗП1 ЗП2 ЗП3 ЗП4 СП2 СП3 ПП1	ЗП1 ЗП2 ЗП3 ЗП4 СП1 СП2 СП3 ПП1		ЗП1 СП1 СП2 СП3 ПП1	СП2 СП3 ПП1	СП1 СП2 ПП1	ЗП1 СП1 ПП1			ЗП2 ЗП3 ЗП4 СП1 ПП1	ЗП2 ЗП3 ЗП4 СП1 СП3 ПП1
РН-3			ЗП2, ЗП3, ЗП4, ПП1	ЗП1 СП1 СП2 СП3 ПП1	СП2 СП3 ПП1			СП1 СП2 СП3 ПП1			
РН-4		ЗП1 ЗП2 ЗП3 ЗП4				СП1 СП2 ПП1		СП1 СП2 СП3 ПП1			ЗП2 ЗП3 ЗП4 СП1

Результати навчання	**Компетентності**										
	Інтегральна компетентність: Здатність розв'язувати комплексні проблеми в галузі професійної та/або дослідницько-інноваційної діяльності у сфері кібербезпеки та захисту інформації, що передбачає глибоке переосмислення наявних та створення нових цілісних знань та/або професійної практики										
	Загальні компетентності				**Спеціальні (фахові) компетентності**						
	ЗК-1	ЗК-2	ЗК-3	ЗК-4	СК-1	СК-2	СК-3	СК-4	СК-5	СК-6	СК-7
		СП1 СП2 СП3 ПП1									СП3 ПП1
РН-5	ЗП1 ЗП2 ЗП3 ЗП4 СП2 СП3 ПП1			ЗП1 СП1 СП2 СП3 ПП1		СП1 СП2 ПП1					
РН-6	ЗП1 ЗП2 ЗП3 ЗП4 СП2 СП3 ПП1		ЗП2 ЗП3 ЗП4 ПП1		СП2 СП3 ПП1		ЗП1 СП1 ПП1		ЗП1 ЗП2 ЗП3 ЗП4 СП2 ПП1	ЗП2 ЗП3 ЗП4 СП1 ПП1	ЗП2 ЗП3 ЗП4 СП1 СП3 ПП1
РН-7				ЗП1 СП1 СП2 СП3 ПП1		СП1 СП2 ПП1			ЗП1 ЗП2 ЗП3 ЗП4 СП2 ПП1		

Результати навчання	**Компетентності**										
	Інтегральна компетентність: Здатність розв'язувати комплексні проблеми в галузі професійної та/або дослідницько-інноваційної діяльності у сфері кібербезпеки та захисту інформації, що передбачає глибоке переосмислення наявних та створення нових цілісних знань та/або професійної практики										
	Загальні компетентності				**Спеціальні (фахові) компетентності**						
	ЗК-1	ЗК-2	ЗК-3	ЗК-4	СК-1	СК-2	СК-3	СК-4	СК-5	СК-6	СК-7
РН-8	ЗП1 ЗП2 ЗП3 ЗП4 СП2 СП3 ПП1	ЗП1 ЗП2 ЗП3 ЗП4 СП1 СП2 СП3 ПП1			СП2 СП3 ПП1		ЗП1 СП1 ПП1				ЗП2 ЗП3 ЗП4 СП1 СП3 ПП1
РН-9	ЗП1 ЗП2 ЗП3 ЗП4 СП2 СП3 ПП1	ЗП1 ЗП2 ЗП3 ЗП4 СП1 СП2 СП3 ПП1	ЗП2 ЗП3 ЗП4 ПП1					СП1 СП2 СП3 ПП1	ЗП1 ЗП2 ЗП3 ЗП4 СП2 ПП1		
РН-10	ЗП1 ЗП2 ЗП3 ЗП4 СП2 СП3 ПП1		ЗП2 ЗП3 ЗП4 ПП1					СП1 СП2 СП3 ПП1			

10. РЕЗУЛЬТАТИ ОБГОВОРЕННЯ ОСВІТНЬОЇ ПРОГРАМИ

Стейкхолдери (вказати ПІБ та посаду, місце роботи)	Зауваження/Рекомендація	враховано / частково враховано / не враховано	Примітка
Зав. аспірантурою НТУ «ХПІ» к.пед.н., доц. О.М. Лапузіна, проректор з наукової роботи НТУ «ХПІ» проф. А.П. Марченко (на підставі листа Національного агентства із забезпечення якості вищої освіти за № 672 від 03.09.2021 р. «Про забезпечення володіння випускниками ОНП доктора філософії методологією педагогічної діяльності»)	До обов'язкових компонент додати нову дисципліну загальної підготовки «Педагогіка і психологія вищої освіти з методикою викладання» (3 кредити). Вилучити проходження аспірантами докторського іспиту.	Враховано.	Додано дисципліну «Педагогіка і психологія вищої освіти з методикою викладання» (3 кредити).
Гарант ОНП, д.т.н., проф. Погасій С.С. завідувач кафедри, д.т.н., професор Євсеєв С.П. Члени робочої групи ОПП	Зміна шифру спеціальності та галузі знань (згідно з постановою Кабінету Міністрів України від 30 серпня 2024 р. No 1021).	Враховано.	Зміни внесено.
Шаповал О. С., виконавчий директор Громадської спілки «Харківський кластер інформаційних технологій»	Підвищити увагу до роботи з великими даними Big Data (додати більше тем в навчальні компоненти щодо аналізу великих даних та кібербезпеки у великих IT-системах). Розширити спектр soft skills шляхом впровадження курсів з лідерства, управління проєктами, стратегічного мислення у контексті кібербезпеки	Враховано.	До переліку вибіркових освітніх компонент додано: Дисципліна «Інформаційні технології обробки великих даних» (4 кредити), «Управління науковими проєктами та дослідженнями» (4 кредити), «Методологія і логіка науково-педагогічної

			діяльності у вищій технічній школі (4 кредити)
Гарант ОНП, д.т.н., проф. Погасій С.С. завідувач кафедри, д.т.н., професор Євсеєв С.П. Члени робочої групи ОПП	З метою приведення у відповідність до сучасної термінології та стандартів вищої освіти оновити назви окремих дисциплін освітньої програми.	Враховано.	У межах періодичного перегляду освітньої програми з урахуванням рекомендацій стейкхолдерів, сучасних тенденцій розвитку галузі та актуалізації термінології було оновлено назви окремих навчальних дисциплін. Зміни мають редакційний характер і не впливають на зміст дисциплін, результати навчання, обсяг кредитів ЄКТС та структуру освітньої програми.
Волощук О. Б., к. т. н., керівник освітніх програм ТОВ “Distributed Lab”	Позитивний відгук. Без зауважень.	-	-
Опірський І.Р., доктор технічних наук, професор, завідувач кафедри захисту інформації Інституту комп’ютерних технологій, автоматики та метрології Національного університету «Львівська політехніка»	Позитивний відгук. Без зауважень.	-	-

Ковтун В. Ю., кандидат технічних наук, доцент, директор ТОВ “Сайфер”	Позитивний відгук. Без зауважень.	-	-
Головашич С. О., кандидат технічних наук, доцент директор ТОВ “Мікрокрипт Текнолоджіс”	Позитивний відгук. Без зауважень.	-	-

Завідувач кафедри кібербезпека _____ Сергій ЄВСЕЄВ

Гарант освітньої програми _____ Сергій ПОГАСІЙ

11. ПЛАН ВРАХУВАННЯ ЗАУВАЖЕНЬ/РЕКОМЕНДАЦІЙ ЗА РЕЗУЛЬТАТАМИ АКРЕДИТАЦІЙНОЇ ЕКСПЕРТИЗИ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

Рекомендації, надані під час останньої акредитації	Період врахування (короткостроковий/ довгостроковий/не доцільно враховувати)	Заходи, що спрямовані на врахування рекомендацій/Обгрунтування щодо недоцільності впровадження рекомендації	Терміни впровадження заходів/відповідальні особи
Загальні рекомендації Експертної групи та Галузевої експертної ради (по кафедрі, галузі, інституту, університету)			
Рекомендація 1 Залучення студентів до обговорення та оновлення ОНП.	Довгостроковий	Провести зустріч членів робочої групи з представниками студентського самоврядування. Розглянуто на засіданні кафедри, протокол № 1 від 26.03.2025р.	Період часу до наступної акредитації ОП. Відповідальні: гарант ОП, завідувач кафедри.
Рекомендація 2 Привести у відповідність кількість кредитів по кожній ОК.	Довгостроковий	Переглянути збалансованість, раціональне призначення і кількість кредитів (не менше 3-х кредитів – кожна ОК) Змінено кількість кредитів ОК «Педагогічна практика» з 2 на 3 кредити. Розглянуто на засіданні кафедри, протокол № 12 від 14.03.2025р.	Період часу до наступної акредитації ОП. Відповідальні: гарант ОП, завідувач кафедри.
Рекомендація 3 Визначити передумови вивчення дисциплін як в силабусах, так і в структурно-логічній схемі самої ОНП.	Довгостроковий	Проаналізувати і виправити силабуси освітніх компонент. Розглянуто на засіданні кафедри, протокол № 12 від 14.03.2025р.	Період часу до наступної акредитації ОП. Відповідальні: гарант ОП, завідувач кафедри, викладачі кафедри.

Рекомендація 4 Залучити здобувачів ВО даної ОНП до міжнародної й внутрішньої академічної мобільності.	Довгостроковий	Виконати аналіз аналогічних ОНП іноземних ЗВО з метою можливості залучення аспірантів до програм академічної мобільності. Розглянуто на засіданні кафедри, протокол № 12 від 14.03.2025р.	Період часу до наступної акредитації ОП. Відповідальні: гарант ОП, завідувач кафедри.
Рекомендація 5 Запровадити систему особистого зобов'язання дотримання норм академічної доброчесності здобувачем ВО та НПП.	Довгостроковий	Проводится постійно під час проведення лекційних занять з дисципліни «Методологія наукової та педагогічної діяльності в науках кіберзахисту». Розглянуто на засіданні кафедри, протокол № 12 від 14.03.2025р.	Період часу до наступної акредитації ОП. Відповідальні: гарант ОП, завідувач кафедри, викладачі кафедри.
Рекомендація 6 Залучати до проведення лекційних занять, вітчизняних та закордонних фахівців-практиків у галузі кібербезпеки. Мотивувати та залучати НПП до участі у міжнародних проєктах (грантах) та конференціях.	Довгостроковий	Участь НПП у міжнародних проєктах (грантах) та конференціях. Розглянуто на засіданні кафедри, протокол № 12 від 14.03.2025р.	Період часу до наступної акредитації ОП. Відповідальні: гарант ОП, завідувач кафедри, викладачі кафедри.

Директор навчально-наукового інституту
комп'ютерних наук та інформаційних технологій _____ Михайло ГОДЛЕВСЬКИЙ

Гарант освітньої програми _____ Сергій ПОГАСІЙ