МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «КІБЕРБЕЗПЕКА»

Другого (магістерського) рівня вищої освіти
галузі знань F «Інформаційні технології»
спеціальності F5 «Кібербезпека та захист інформації»
Кваліфікація: магістр з кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО
Вченою радою
Державного університету
«Житомирська політехніка»
Голова Вченої ради
_____ Віктор ЄВДОКИМОВ
(протокол від 04 березня 2025 р. № 4)

Освітня програма вводиться в дію з
01 вересня 2025 р.
Ректор
_____ Віктор ЄВДОКИМОВ
(наказ від 04 березня 2025 р. № 58/од)

Житомир – 2025

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми
«Кібербезпека»
Другого (магістерського) рівня вищої освіти
галузі знань F «Інформаційні технології»
спеціальності F5 «Кібербезпека та захист інформації»

Гарант освітньо-професійної програми Володимир ВОРОТНІКОВ
20.01.2025 р

Кафедра комп'ютерної інженерії
та кібербезпеки
Протокол від 20 січня 2025 р
№ 1
Завідувач кафедри Андрій ЄФІМЕНКО

Вчена рада факультету
інформаційно-комп'ютерних технологій
Протокол від 27 січня 2025 р
№ 1
Декан факультету Тетяна НІКІТЧУК

Начальник навчально-методичного
відділу Вікторія МЕЛЬНИК-ШАМРАЙ
14.02.2025 р

Начальник відділу моніторингу
та забезпечення якості Ігор СВІТЛИШИН
14.02.2025 р

Науково-методична рада
Державного університету
«Житомирська політехніка»
Протокол від 18 02 2025 р
№ 01
Проректор
з науково-педагогічної роботи Андрій МОРОЗОВ
18.02.2025 р

ПЕРЕДМОВА

Освітньо-професійну програму розроблено робочою групою у складі:

ВОРОТНІКОВ Володимир – гарант освітньої програми, керівник робочої групи, доктор технічних наук, доцент, професор кафедри комп'ютерної інженерії та кібербезпеки

Члени групи:

ЄФІМЕНКО Андрій. – кандидат технічних наук, доцент, завідувач кафедри комп'ютерної інженерії та кібербезпеки.

ЛОБАНЧИКОВА Надія – кандидат технічних наук, доцент, доцент кафедри інженерії програмного забезпечення.

ШЕЛУХА Олексій – кандидат технічних наук, доцент кафедри комп'ютерної інженерії та кібербезпеки.

ПІРОГ Олександр – кандидат технічних наук, доцент кафедри комп'ютерної інженерії та кібербезпеки.

ТРОКОЗ Єлизавета – старший викладач кафедри комп'ютерної інженерії та кібербезпеки.

ПОКОТИЛО Олександра – старший викладач кафедри комп'ютерної інженерії та кібербезпеки.

КРУЧИНСЬКИЙ Ярослав – представник роботодавця, начальник відділу сервісного обслуговування технічної служби ТОВ «Фрінет».

СІНІЦИНА Олександра – здобувачка вищої освіти, 1 курс, група КБм-24-1

ШЕВЧИК Дарина – здобувачка вищої освіти з ОПП, 2 курс, група КБм-23-1;

ГОНЧАРОВ Михайло – випускник з ОПП 2023 р.; аналітик з інцидентів. ТОВ «МЕТІНВЕСТ ДІДЖИТАЛ»

КУХАРЧУК Максим – випускник з ОПП 2022 р.; адміністратор системи, ТОВ «ПАРТНЕР»

ЛЕЩЕНКО Богдан – випускник з ОПП 2022 р.; адміністратор системи, ТОВ "Сана Комерс Україна"

1. ПРОФІЛЬ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

1 – Загальна інформація	
Повна назва закладу вищої освіти та структурного підрозділу	Державний університет «Житомирська політехніка» Факультет інформаційно-комп'ютерних технологій
Назва освітньої програми	Кібербезпека
Тип освітньої програми	освітньо-професійна
Рівень вищої освіти	Другий (магістерський) рівень вищої освіти
Ступінь вищої освіти	«магістр»
Галузь знань	F «Інформаційні технології»
Спеціальність	F5 «Кібербезпека та захист інформації»
Спеціалізація або предметна спеціальність (за наявності)	–
Тип диплома	Диплом магістра, одиничний
Найменування партнера за узгодженою спільною освітньою програмою (за наявності)	–
Мова (мови) викладання	Українська
Кількість кредитів ЄКТС, необхідних для виконання програми	90 кредитів ЄТКС
Форми здобуття освіти за освітньою програмою та розрахункові строки виконання освітньої програми за кожною з них	Очна (денна, заочна) 1 рік 4 місяці
Освітня кваліфікація	магістр з кібербезпеки та захисту інформації
Кваліфікація в дипломі	магістр з кібербезпеки та захисту інформації
Вимоги до освіти осіб, які можуть розпочати навчання за програмою	На базі освітнього ступеня «бакалавр», «магістр» або освітньо-кваліфікаційного рівня «спеціаліст»
Наявність акредитації	Національне агентство із забезпечення якості вищої освіти. Сертифікат про акредитацію освітньої програми «Кібербезпека» (за спеціальністю 125 Кібербезпека та захист інформації) № 7253, дійсний до 01.07.2029
Цикл/рівень	НРК України – 7 рівень FQ-EHEA – другий цикл EQF-LLL – 7 рівень
Інтернет адреса постійного розміщення опису освітньої програми	https://vstup.ztu.edu.ua/magistr/125-kiberbezpeka/ https://learn.ztu.edu.ua/course/view.php?id=5904
2 – Мета освітньої програми	
Професійна підготовка фахівців з кібербезпеки, набуття ними компетентностей в застосуванні принципів, методів та засобів забезпечення кібербезпеки.	
3 - Характеристика освітньої програми	
Опис предметної області	**Об'єкти вивчення:** – сучасні процеси дослідження, аналізу, створення та забезпечення функціонування інформаційних систем і технологій, інших бізнес-операційних процесів на об'єктах інформаційної діяльності та критичних інфраструктур сфери інформаційної безпеки та/або кібербезпеки;

	– інформаційні системи (інформаційно-комунікаційні, інформаційно-телекомунікаційні, автоматизовані) та технології; – інфраструктура об'єктів інформаційної діяльності та критичних інфраструктур; – системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків); – інформаційні ресурси різних класів (в т.ч. державні інформаційні ресурси); – програмне та програмно-апаратне забезпечення (засоби) кіберзахисту; – системи управління інформаційною безпекою та/або кібербезпекою; – технології, методи, моделі та засоби інформаційної безпеки та/або кібербезпеки. **Цілі навчання:** Підготовка фахівців, здатних розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки. **Теоретичний зміст предметної області** Теоретичні засади наукоємних технологій, фізичні і математичні фундаментальні знання, теорії ідентифікації та прийняття рішень, системного аналізу, складних систем, моделювання та оптимізації процесів, теорія математичної статистики, криптографічного та технічного захисту інформації, теорії ризиків та інших міждисциплінарних теорій і практик у галузі інформаційної безпеки та/або кібербезпеки. **Методи, методики та технології** Методи, моделі, методики та технології створення, обробки, передачі, приймання, знищення, відображення, захисту (кіберзахисту) інформаційних ресурсів у кіберпросторі, а також методи та моделі розробки та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач в галузі інформаційної безпеки та/або кібербезпеки. Технології, методи та моделі дослідження, аналізу, управління та забезпечення бізнес/операційних процесів із застосуванням сукупності нормативно-правових та організаційно-технічних методів і засобів захисту інформаційних ресурсів у кіберпросторі. **Інструменти та обладнання**. Засоби, пристрої, 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), а також методи і моделі теорії ризиків та управління інформаційними ресурсами при дослідженні і супроводженні об'єктів інформаційної діяльності у галузі інформаційної безпеки та/або кібербезпеки.
Основний фокус освітньої програми	Вища освіта в галузі інформаційних технологій. Програма фокусується на питанням забезпечення кібербезпеки та захисту інформації у сучасних комп'ютерних системах та мережах, зокрема, мережній безпеці, тестуванні на проникнення, реагуванню та розслідуванню інцидентів кібербезпеки, організації SOC. Ключові слова: кібербезпека, комп'ютерна система, комп'ютерна мережа, інформаційна система, інформаційно-телекомунікаційна

	система, операційна система, адміністрування систем, прикладне та системне програмування, вразливість, атака, ризик, компрометація, протидія, захист інформації, тестування на проникнення, моніторинг, розслідування інциденту, міжмережне екранування, система виявлення та попередження вторгнень, кібероперації, спеціальні системи забезпечення кібербезпеки.
Особливості програми	Тісна співпраця з державними та приватними організаціями з метою отримання практичних навичок безпечної експлуатації, адміністрування, забезпечення захисту комп'ютерних систем та мереж, навичок розробки захищеного прикладного та системного програмного забезпечення, проходження практичної підготовки з розробки та забезпечення захисту нових і вдосконалення захисту існуючих комп'ютерних та інформаційних систем з подальшим впровадженням науково-практичних розробок у діяльність організацій та установ.
4 – Працевлаштування за здобутою освітою	
Придатність до працевлаштування	Працевлаштування в організаціях та підприємствах будь-якої форми власності на посадах: I. Згідно ДК 003:2010 (NIST800–181) 1. Розробник систем захисту інформації 2. Адміністратор безпеки мереж і систем 3. Аналітик загроз безпеки 4. Аналітик систем захисту інформації та оцінки вразливостей 5. Аналітик з безпеки інформаційно-телекомунікаційних систем 6. Дізнавач (сфера кібербезпеки та захисту інформації)* 7. Експерт-криміналіст (сфера кібербезпеки та захисту інформації)* 8. Експерт-криміналіст судової експертизи (сфера кібербезпеки та захисту інформації)* 9. Слідчий з кіберзлочинів* 10. Фахівець з криптографічного захисту інформації 11. Фахівець з питань безпеки (інформаційно-комунікаційні технології 12. Фахівець з підтримки інфраструктури кіберзахисту 13. Фахівець з реагування на інциденти кібербезпеки 14. Фахівець з тестування систем захисту інформації 15. Фахівець з технічного захисту інформації 16. Фахівець сфери захисту інформації * може потребувати/потребує додаткового навчання/освіти. II. Згідно ECSF (European Cybersecurity Skills Framework): 1. Chief Information Security Officer (CISO) 2. Cyber Incident Responder 3. Cyber Legal, Policy and Compliance Officer 4. Cyber Threat Intelligence Specialist 5. Cybersecurity Educator 6. Cybersecurity Implementer 7. CybersecurityAuditor 8. Cybersecurity Researcher 9. Cybersecurity Risk Manager 10. Digital Forensics Investigator
Подальше навчання	Можливість отримання освіти за програмами третього (освітньо-наукового) рівня вищої освіти. Можливість набуття додаткових кваліфікацій у системі освіти дорослих.

5 – Викладання та оцінювання	
Викладання та навчання	Викладання здійснюється на засадах студентоцентрованого навчання, самонавчання, проблемно-орієнтованого навчання тощо
Оцінювання	Оцінювання навчальних досягнень здійснюється за 100-бальною (рейтинговою) шкалою ЄКТС. Види контролю: поточний, тематичний, періодичний, підсумковий, самоконтроль. Форми контролю: модульні контрольні роботи за вивченими темами, усне та письмове опитування, комп'ютерне тестування, екзамени та заліки (усні, письмові, у формі тестів в тому числі комп'ютерне тестування), презентація індивідуальних завдань, захист звітів (за результатами практики). Підсумкова атестація – підготовка та публічний захист кваліфікаційної роботи/проекту.
6 – Компетентності	
Інтегральна компетентність	Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.
Загальні компетентності (КЗ)	**КЗ-1**. Здатність застосовувати знання у практичних ситуаціях. **КЗ-2**. Здатність проводити дослідження на відповідному рівні. **КЗ-3**. Здатність до абстрактного мислення, аналізу та синтезу. **КЗ-4**. Здатність оцінювати та забезпечувати якість виконуваних робіт. **КЗ-5**. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
Спеціальні (фахові, предметні) компетентності (КФ)	**КФ-1**. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки. **КФ-2**. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки. **КФ-3.** Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. **КФ-4.** Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог. **КФ-5.** Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. **КФ-6.** Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. **КФ-7**. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління,

	контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. **КФ-8**. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. **КФ-9**. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому. **КФ-10**. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.

7 – Програмні результати навчання

РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.

РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.

РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.

РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.

РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.

РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.

РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.

РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.

РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.
РН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.
РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.
РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.
РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.
РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.
РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.
РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.
РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.
РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

8 – Ресурсне забезпечення реалізації програми

Кадрове забезпечення	У реалізації даної освітньої програми задіяно 5 докторів наук, професорів або доцентів/с.н.с., 6 кандидатів наук, доцентів, 2 кандидати наук/PhD, кожен з яких має виконання не менше 4 пунктів п. 38 Ліцензійних умов провадження освітньої діяльності. Тобто, кадрове забезпечення освітньої програми відповідає ліцензійним вимогам щодо надання освітніх послуг у сфері вищої світи і є достатнім для забезпечення якості освітнього процесу.
Матеріально-технічне забезпечення	Матеріально-технічне забезпечення відповідає ліцензійним вимогам щодо надання освітніх послуг у сфері вищої світи і є достатнім для забезпечення якості освітнього процесу
Інформаційне та навчально-методичне забезпечення	Інформаційне та навчально-методичне забезпечення освітньої програми «Кібербезпека» з підготовки фахівців зі спеціальності 123 «Кібербезпека та захист інформації» відповідає ліцензійним вимогам, має актуальний змістовий контент, базується на сучасних інформаційно-комунікаційних технологіях та засобах забезпечення кібербезпеки та захисту інформації. В університеті функціонують Мережна академія Cisco, Центр підтримки академій Cisco, Центр підготовки інструкторів Cisco, ресурси яких доступні для студентів (за умови реєстрації). Також в університеті реалізуються партнерські академічні програми від компаній IBM, Microsoft, Fortinet, AWS, Oracle та ін. Здобувачам освіти забезпечується доступ до освітніх платформ Udemy, Coursera тощо.

9 – Академічна мобільність

Національна кредитна мобільність	Реалізується в межах спільної діяльності з Національним технічним університетом «КПІ імені Ігоря Сікорського», Хмельницьким національним університетом, Запорізьким національним університетом, Житомирським військовим інститутом імені С.П. Корольова, Житомирським державним університетом імені Івана Франка, Національним університетом водного господарства та природокористування, Харківським національним університетом радіоелектроніки, Харківським національним університетом ім. В. Каразіна, Черкаським державним технологічним університетом, Державним університетом телекомунікацій, Національним університетом «Одеська юридична академія» згідно укладених договорів про співпрацю.
Міжнародна кредитна мобільність	На основі двосторонніх договорів між Державним університетом «Житомирська політехніка» та зарубіжними закладами вищої освіти.
Навчання іноземних здобувачів вищої освіти	На навчання приймаються іноземні громадяни на умовах контракту, які мають документ про отримання першого (бакалаврського) рівня вищої освіти.
10 – Форми атестації здобувачів вищої освіти	
Форми атестації здобувачів вищої освіти	Поточна атестація студентів здійснюється у формі екзаменів, заліків, диференційованих заліків, захисту курсових робіт та проектів. Атестація випускників освітньо-професійної програми «Кібербезпека» за спеціальністю F5 «Кібербезпека та захист інформації» проводиться у формі публічного захисту кваліфікаційного проекту/роботи та завершується видачою документу встановленого зразка про присудження йому освітнього ступеня «магістр» з присвоєнням кваліфікації «магістр з кібербезпеки та захисту інформації».
Вимоги до кваліфікаційної роботи	У кваліфікаційному проекті/роботі не допускається порушень академічної доброчесності, зокрема, наявність академічного плагіату, результатів фабрикації та фальсифікації. Атестація здійснюється відкрито і публічно. Кваліфікаційний проект/робота оприлюднюється у репозитарії закладу вищої освіти.
11 – Система внутрішнього забезпечення якості вищої освіти	

Система внутрішнього забезпечення якості освітньої діяльності та якості вищої освіти відповідає вимогам чинного законодавства України та вимогам міжнародних стандартів якості ISO (ISO 9001 і ISO 21001).

Організація внутрішнього забезпечення якості вищої освіти здійснюється на таких рівнях: університетський; факультетський; кафедральний; викладацький; студентський.

Система внутрішнього забезпечення якості включає:

1) визначення та періодичний перегляд принципів і процедур забезпечення якості вищої освіти, формування культури якості;

2) здійснення моніторингу та щорічного перегляду освітньої програми;

3) щорічне оцінювання здобувачів вищої освіти, науково-педагогічних і педагогічних працівників та регулярне оприлюднення результатів таких оцінювань на офіційному веб-сайті університету;

4) забезпечення підвищення кваліфікації педагогічних, наукових і науково-педагогічних працівників;

5) забезпечення наявності необхідних ресурсів для організації освітнього процесу, у тому числі самостійної роботи здобувачів вищої освіти;

6) забезпечення функціонування внутрішніх інформаційних систем («Портал Житомирської політехніки» та «Освітній портал Житомирської політехніки») для ефективного управління освітнім процесом;

7) забезпечення публічності інформації про освітню програму, ступінь вищої освіти та кваліфікацію;

8) забезпечення дотримання академічної доброчесності працівниками та здобувачами вищої освіти, у тому числі шляхом запровадження функціонування ефективної системи запобігання та виявлення академічного плагіату;
9) здійснення щорічного внутрішнього та зовнішнього аудитів процесів забезпечення якості вищої освіти;
10) залучення до процесів забезпечення якості вищої освіти внутрішніх та зовнішніх стейкхолдерів, в тому числі через проведення круглих столів, долучення до проведення навчальних занять, анкетування тощо

2. ПЕРЕЛІК КОМПОНЕНТ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ ТА ЇХ ЛОГІЧНА ПОСЛІДОВНІСТЬ

2.1. Перелік компонент освітньо-професійної програми

Код за ОПП	Компоненти освітньої програми (навчальні дисципліни, курсові проекти/ роботи, практики кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
Нормативна частина			
Дисципліни загальної підготовки			
ОК01	Англійська мова (за професійним спрямуванням)	3	Залік
ОК02	Методологія наукових досліджень	3	Залік
ОК03	Інтелектуальна власність	3	Залік
ОК04	Філософські проблеми наукового пізнання	3	Залік
ОК05	Педагогіка та психологія	3	Залік
ОК06	Цивільний захист	3	Залік
Дисципліни професійної підготовки			
ОК07	Архітектура, проєктування та безпека веб-орієнтованих інформаційних та комп'ютерних систем	4	Екзамен
ОК08	Технології адміністрування та захисту інформаційних систем	4	Екзамен
ОК09	Моніторинг, аудит та управління системами кібербезпеки	4	Екзамен, курсовий проєкт
ОК10	Проектування систем кібербезпеки	3	Залік
ОК11	Хмарна безпека	3	Залік
ОК12	Тестування на проникнення, етичний хакінг та цифрова криміналістика	3	Екзамен, курсова робота
ОК13	Наукова практика	3	Диф. залік
ОК14	Виробнича практика	6	Диф. залік
ОК15	Переддипломна практика	6	Диф. залік
ОК16	Кваліфікаційна робота	12	Кваліфікаційна атестація
Всього:		**66**	
Варіативна частина			
ВК2.1	Дисципліна №1	4	залік
ВК2.2	Дисципліна №2	4	залік
ВК2.3	Дисципліна №3	4	залік
ВК2.4	Дисципліна №4	4	залік
ВК2.5	Дисципліна №5	4	залік
ВК2.6	Дисципліна №6	4	залік
Всього:		**24**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**90**	

2.2. Структурно-логічна схема освітньо-професійної програми

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти/ роботи, практики кваліфікаційна робота)	Кількість кредитів	Загальний обсяг год.	Форма підсумкового контролю
1	2	3	4	
І курс, І семестр				
ОК01	Англійська мова (за професійним спрямуванням)	3	90	Залік
ОК02	Методологія наукових досліджень	3	90	Залік
ОК03	Інтелектуальна власність	3	90	Залік
ОК07	Архітектура, проєктування та безпека веб-орієнтова-них інформаційних та комп'ютерних систем	4	120	Екзамен
ОК08	Технології адміністрування та захисту інформаційних систем	4	120	Екзамен
ОК09	Моніторинг, аудит та управління системами кібербезпеки	4	120	Екзамен, КП
ОК10	Проектування систем кібербезпеки			
ОК11	Хмарна безпека			
ОК13	Наукова практика	3	90	Залік
І курс, ІІ семестр				
ВК2.1	Дисципліна №1	4	120	залік
ВК2.2	Дисципліна №2	4	120	залік
ВК2.3	Дисципліна №3	4	120	залік
ВК2.4	Дисципліна №4	4	120	залік
ВК2.5	Дисципліна №5	4	120	залік
ВК2.6	Дисципліна №6	4	120	залік
ОК14	Виробнича практика	6	180	Диф. залік
ІІ курс, ІІІ семестр				
ОК04	Філософські проблеми наукового пізнання	3	90	Залік
ОК05	Педагогіка та психологія	3	90	Залік
ОК06	Цивільний захист	3	90	Залік
ОК12	Тестування на проникнення, етичний хакінг та цифрова криміналістика	3	90	Екзамен, КР
ОК15	Переддипломна практика	6	180	Диф. залік
ОК16	Кваліфікаційна робота	12	360	Екзамен
	Загальний обсяг:	**90**	**2700**	

Структурно-логічна схема ОП

Вихідна стрілка, яка розміщена в правому нижньому кутку, показує, що ОК забезпечує решту ОК поточного і наступних семестрів;
Вхідна стрілка, яка розміщена у лівому верхньому кутку, показує, що ОК забезпечується ОК попередніх та поточного семестрів.

Вихідна стрілка, яка розміщена в правому нижньому кутку показує, що ОК забезпечує ОК професійного спрямування поточного та наступних семестрів.
Вхідна стрілка, яка розміщена у лівому верхньому кутку, показує, що ОК забезпечується ОК професійного спрямування поточного та попередніх семестрів.

3. ВІДПОВІДНІСТЬ ПРОГРАМНИХ КОМПЕТЕНТНОСТЕЙ КОМПОНЕНТАМ ОСВІТНЬОЇ ПРОГРАМИ

3.1. Матриця відповідності компетентностей обов'язковим компонентам

	Загальні компетентності (КЗ)					Спеціальні (фахові, предметні) компетентності (КФ)									
	КЗ-1	КЗ-2	КЗ-3	КЗ-4	КЗ-5	КФ-1	КФ-2	КФ-3	КФ-4	КФ-5	КФ-6	КФ-7	КФ-8	КФ-9	КФ-10
ОК 1	+				+										
ОК 2		+	+			+				+		+			
ОК 3	+			+	+										+
ОК 4	+		+												
ОК 5	+														+
ОК 6	+				+										
ОК 7	+					+							+		
ОК 8	+					+		+			+		+	+	
ОК 9	+	+					+	+	+	+	+			+	
ОК 10	+	+		+		+	+	+	+						
ОК 11	+					+				+	+				
ОК 12	+	+					+	+		+		+	+		
ОК 13	+	+	+	+	+	+		+	+	+		+	+	+	+
ОК 14	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ОК 15	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ОК 16	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+

4. ЗАБЕЗПЕЧЕНІСТЬ ПРОГРАМНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ ВІДПОВІДНИМИ КОМПОНЕНТАМИ ОСВІТНЬОЇ ПРОГРАМИ

4.1. Матриця забезпечення програмних результатів навчання обов'язковими компонентами

	РН-1	РН-2	РН-3	РН-4	РН-5	РН-6	РН-7	РН-8	РН-9	РН-10	РН-11	РН-12	РН-13	РН-14	РН-15	РН-16	РН-17	РН-18	РН-19	РН-20	РН-21	РН-22	РН-23
ОК 1	+														+								
ОК 2		+		+		+		+				+				+				+	+	+	+
ОК 3			+		+		+								+	+	+		+	+			
ОК 4	+	+			+															+		+	
ОК 5	+														+		+	+					
ОК 6	+															+							
ОК 7		+	+	+		+		+			+		+			+			+	+	+		+
ОК 8		+		+		+	+	+		+	+		+	+		+				+	+		+
ОК 9		+	+	+	+	+	+	+	+	+	+	+		+		+			+	+	+	+	+
ОК 10		+	+	+	+	+	+	+				+	+		+	+			+	+	+	+	+
ОК 11		+	+	+		+	+	+		+	+		+	+		+			+	+	+		+
ОК 12		+	+	+	+	+	+	+		+		+	+			+			+	+	+	+	+
ОК 13	+		+					+				+	+							+	+	+	
ОК 14	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ОК 15	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ОК 16	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+