МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЖИТОМИРСЬКИЙ ДЕРЖАВНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «КІБЕРБЕЗПЕКА»

Першого рівня вищої освіти
за спеціальністю 125 «Кібербезпека»
галузі знань 12 «Інформаційні технології»
Кваліфікація: бакалавр з кібербезпеки

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ ЖДТУ
Голова Вченої ради
_____ В. В. Євдокимов
(протокол № 7 від «31» 08 2018 р.)

Освітня програма вводиться в дію
з 01 вересня 2018 р.
Ректор ЖДТУ
_____ В. В. Євдокимов
(наказ № 2 від «31» 08 2018 р.)

Житомир – 2018

ПЕРЕДМОВА

Освітньо-професійна програма «Кібербезпека» першого рівня вищої освіти за спеціальністю 125 «Кібербезпека» галузі знань 12 «Інформаційні технології», кваліфікація «бакалавр з кібербезпеки» розроблена робочою групою у складі:

Лобанчикова Н.М.	гарант освітньої програми, к.т.н., ,декан факультету інформаційно-комп'ютерних технологій, доцент, доцент кафедри комп'ютерної інженерії та кібербезпеки
Єфіменко А.А.	к.т.н., завідувач кафедри комп'ютерної інженерії та кібербезпеки
Россінський Ю.М.	к.т.н., доцент, доцент кафедри комп'ютерної інженерії та кібербезпеки

1. Профіль освітньої програми зі спеціальності 125 «Кібербезпека»

1. ПРОФІЛЬ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

1 – Загальна інформація	
Повна назва закладу вищої освіти та структурного підрозділу	Житомирський державний технологічний університет, факультет інформаційно-комп'ютерних технологій
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Перший (бакалаврський) рівень вищої освіти Кваліфікація – «бакалавр з кібербезпеки»
Офіційна назва освітньої програми	Кібербезпека
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний, 240 кредитів ЄКТС, термін навчання 3 роки 10 місяців
Наявність акредитації	Відсутня
Цикл /рівень	НРК України – 6 рівень, FQ-EHEA – перший цикл, EQF-LLL – 6 рівень
Передумови	Повна загальна середня освіта або наявність освітньо-кваліфікаційного рівня «Молодший спеціаліст»
Мова(и) викладання	Українська
Термін дії освітньої програми	Постійно
Інтернет-адреса постійного розміщення опису освітньої програми	https://ztu.edu.ua
2 – Мета освітньої програми	
Професійна підготовка фахівців з кібербезпеки, набуття ними компетентностей в застосуванні принципів, методів та засобів забезпечення кібербезпеки.	
3 – Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність, спеціалізація)	12 – Інформаційні технології 125 – Кібербезпека
Орієнтація освітньої програми	Освітньо-професійна
Основний фокус освітньої програми та спеціалізації	Вища освіта в галузі інформаційних технологій. Програма фокусується на питанням забезпечення кібербезпеки сучасних комп'ютерних систем та мереж. 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 прикладного та системного програмного забезпечення, проходження практичної підготовки з розробки нових і вдосконалення існуючих комп'ютерних та інформаційних систем з подальшим впровадженням науково-практичних розробок у діяльність організацій та установ.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Працевлаштування в організаціях та підприємствах будь-якої форми власності на посадах: І. Згідно ДК 003:2010 3439 (24771). Фахівець із організації інформаційної безпеки. 2149.2 Фахівець (сфера захисту інформації) 1495 Менеджери (управителі) систем з інформаційної безпеки
Подальше навчання	Можливість навчання за програмою другого (магістерського) рівня
5 – Викладання та оцінювання	
Викладання та навчання	Викладання здійснюється на засадах студентоцентрованого навчання, самонавчання, проблемно-орієнтованого навчання тощо
Оцінювання	Поточне опитування, тестовий контроль, презентація індивідуальних завдань, звіти команд, звіти з практики. Підсумковий контроль – екзамени та заліки з урахуванням накопичених балів поточного контролю. Атестація – підготовка та публічний захист кваліфікаційної роботи/проекту
6 - Програмні компетентності	
Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і/або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.
Загальні компетентності (ЗК)	КЗ 1. Здатність застосовувати знання у практичних ситуаціях. КЗ 2. Знання та розуміння предметної області та розуміння професії.

	КЗ 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. КЗ 5. Здатність до пошуку, оброблення та аналізу інформації. КЗ 6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні; КЗ 7. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.
Спеціальні (фахові, предметні) компетентності (СК)	КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки. КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 6. Здатність відновлювати штатне

	функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.) КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності. КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.
7 - Результати навчання	
РН 1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; РН 2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; РН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; РН 4. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення; РН 5. адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат; РН 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та	

професійній діяльності;
РН 7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки;
РН 8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки;
РН 9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки;
РН 10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем;
РН 11. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах;
РН 12. Розробляти моделі загроз та порушника;
РН 13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних;
РН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень;
РН 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій;
РН 16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів;
РН 17. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент;
РН 18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів;
РН 19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;
РН 20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах;
РН 21. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;
РН 22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційнотелекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки;
РН 23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;
РН 24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових);
РН 25. Забезпечувати введення підзвітності системи управління доступом до

електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту;
РН 26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем;
РН 27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах;
РН 28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки;
РН 29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів;
РН 30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем;
РН 31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем;
РН 32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки;
РН 33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків;
РН 34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації;
РН 35. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки;
РН 36. Виявляти небезпечні сигнали технічних засобів;
РН 37. Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації;
РН 38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації;
РН 39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах;
РН 40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації;
РН 41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур;
РН 42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на

інциденти інформаційної і/або кібербезпеки; РН 43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; РН 44. Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; РН 45. Застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; РН 46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах; РН 47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації; РН 48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; РН 49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах; РН 50. Забезпечувати) функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); РН 51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; РН 52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах; РН 53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз. РН 54. Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	У реалізації даної освітньої програми задіяно 1 доктор наук, професор, 8 кандидатів наук, доцентів, 2 кандидати наук. Таким чином, 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 з підготовки фахівців зі спеціальності 125 «Кібербезпека» відповідає ліцензійним

	вимогам, має актуальний змістовий контент, базується на сучасних інформаційно-комунікаційних технологіях. В університеті функціонують Мережна академія Cisco ресурси якої доступні для студентів (за умови реєстрації).
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 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 повну загальну середню освіту.

2. Перелік компонентів освітньо-професійної/наукової програми

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти/ роботи, практики кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
Обов'язкові компоненти ОП			
ОК1	Іноземна мова	26	1,2,3 – залік, 4 екзамен
ОК2	Основи бібліографії та пошук в інформаційних системах	3	Залік
ОК3	Українська мова професійного спрямування	3	Екзамен
ОК4	Фізика (вибрані розділи)	4	Екзамен
ОК5	Лінійна алгебра та аналітична геометрія	3	Залік
ОК6	Математичний аналіз	8	Залік, Екзамен
ОК7	Теорія ймовірностей і математична статистика	3	Залік
ОК8	Комп'ютерна дискретна математика	3	Екзамен
ОК9	Основи програмування	6	Екзамен
ОК10	Архітектура комп'ютера	4	Екзамен
ОК11	Інженерна та комп'ютерна графіка	3	Екзамен
ОК12	Теорія електричних і магнітних кіл	4	Екзамен
ОК13	Об'єктно-орієнтоване програмування	6	Екзамен, захист КР
ОК14	Веб-дизайн	6	Екзамен
ОК15	Електроніка	6	Залік, екзамен
ОК16	Основи кібербезпеки	3	Екзамен
ОК17	Комп'ютерні мережі	9	Залік, екзамен, захист КП
ОК18	Операційні системи	4	Залік
ОК19	Бази даних	4	Залік
ОК20	Прикладна криптологія	5	Екзамен
ОК21	Адміністрування та захист баз та сховищ даних	4	Екзамен, захист КР
ОК22	Нормативно-правове забезпечення кібербезпеки	4	Залік
ОК23	Теоретичні засади кібербезпеки	3	Залік
ОК24	Системи технічного захисту інформації	6	Екзамен, захист КР
ОК25	Захист інформації в інформаційно-комунікаційних системах	9	Залік, екзамен, захист КП
ОК26	Управління кібербезпекою	4	Екзамен
ОК27	Комплексні системи захисту інформації	3	Екзамен
ОК28	Кібероперації	10	Залік, екзамен, захист КП
Загальний обсяг обов'язкових компонент:		**156**	
Вибіркові компоненти ОП*			
Вибіркові компоненти затверджуються щорічно науково-методичною радою ЖДТУ		**60**	
НП	Навчальна практика	3	
ТП	Технологічна практика	3	
ВП	Виробнича практика	6	
ПП	Переддипломна практика	6	
ДП	Дипломування та захист кваліфікаційної роботи	6	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**240**	

Вибіркові компоненти ОП*			
*Вибірковий блок 1 (за циклом загальної підготовки)**			
Вибіркові компоненти блоку 1 затверджуються щорічно навчально-методичною радою Житомирського державного технологічного університету			
ВК1	**Загальний обсяг вибіркового блоку 1**	**9**	

* *Додаток А*

*Вибірковий блок 2 ** (за циклом професійної та практичної підготовки)*			
ВК2.1	Інтернет-програмування	6	Екзамен
ВК2.2	Операційні системи Unix/Linux	6	Екзамен
ВК2.3	Безпровідні мережі	5	Екзамен
ВК2.4	Системний аналіз та теорія прийняття рішень	4	Екзамен
ВК2.5	Програмування мовою Python	4	Залік
ВК2.6	Теорія ризиків та її застосуванян в кібербезпеці	3	Залік
ВК2.7	Штучний інтелект в задачах кібербезпеки	6	Екзамен
ВК2.8	Адміністрування комп'ютерних систем та мереж	5	Екзамен
ВК2.9	Безпека мобільних та Web-додатків	3	Залік
ВК2.10	Хмарні технології	3	Екзамен
ВК2.11	Тестування на проникнення, виявлення та розслідування інцидентів кібербезпеки	3	Екзамен
ВК2.12	Безпека IoT	3	Залік
*Вибірковий блок 3 ** (за циклом професійної та практичної підготовки)*			
ВК3.1	Інформаційні технології	6	Екзамен
ВК3.2	Системне програмне забезпечення	6	Екзамен
ВК3.3	Безпровідні цифрові мережі	5	Екзамен
ВК3.4	Системи підтримки прийняття рішень	4	Екзамен
ВК3.5	Системне та мережне програмування	4	Залік
ВК3.6	Групова динаміка та комунікації	3	Залік
ВК3.7	Інформаційно-аналітичне забезпечення систем кібербезпеки	6	Екзамен
ВК3.8	Інфраструктура відкритих ключів	5	Екзамен
ВК3.9	Безпека додатків ОС Windows	3	Залік
ВК3.10	Центри обробки даних	3	Екзамен
ВК3.11	Комп'ютерна стеганографія	3	Екзамен
ВК3.12	Технології та засоби сумісної роботи	3	Залік
Загальний обсяг вибіркових компонент:		**60**	

** *Студент обирає один з вибіркових блоків із запропонованого переліку*

2.2. Структурно-логічна схема ОП

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти/ роботи, практики кваліфікаційна робота)	Кількість кредитів	Загальний обсяг, годин	Форма підсумк. контролю
1	2	3		4
І курс, 1 семестр				
ОК1	Іноземна мова	6,5	195	Залік
ОК3	Українська мова професійного спрямування	3	90	Екзамен
ОК5	Лінійна алгебра та аналітична геометрія	3	90	Залік
ОК5	Математичний аналіз	4	120	Залік
ОК9	Основи програмування	6	180	Екзамен
ОК10	Архітектура комп'ютера	4	120	Екзамен
ОК11	Інженерна та комп'ютерна графіка	3	90	Екзамен
І Курс, 2 семестр				
ОК1	Іноземна мова	6,5	195	Залік
ОК2	Основи бібліографії та пошук в інформаційних системах	3	90	Залік
ОК4	Фізика (вибрані розділи)	4	120	Екзамен
ОК6	Математичний аналіз	4	120	Екзамен
ОК12	Теорія електричних і магнітних кіл	4	120	Екзамен
ОК13	Об'єктно-орієнтоване програмування	6	180	Екзамен, захист КР
НП	Навчальна практика	3	90	Диф. залік
ІІ Курс, 1 семестр				
ОК1	Іноземна мова	6,5	195	Залік
ОК7	Теорія ймовірностей і математична статистика	3	90	Залік
ОК8	Комп'ютерна дискретна математика	3	90	Екзамен
ОК14	Web-дизайн	6	180	Екзамен
ОК15	Електроніка	3	90	Залік
ОК16	Основи кібербезпеки	3	90	Екзамен
ОК17	Комп'ютерні мережі	4	120	Залік
ІІ Курс, 2 семестр				
ОК1	Іноземна мова	6,5	195	Екзамен
ОК15	Електроніка	3	90	Екзамен
ОК17	Комп'ютерні мережі	5	150	Екзамен, захист КП
ОК18	Операційні системи	4	120	Залік
ОК19	Бази даних	4	120	Залік
ВК 2.1	Інтернет-програмування	6	180	Екзамен
ВК 3.1	Інформаційні технології			
ТП	Технологічна практика	3	90	Диф. залік
ІІІ Курс, 1 семестр				
ОК20	Прикладна криптологія	5	150	Екзамен
ОК21	Адміністрування та захист баз та сховищ даних	4	120	Екзамен, захист КР
ОК22	Нормативно-правове забезпечення кібербезпеки	4	120	Залік
ОК23	Теоретичні засади кібербезпеки	3	90	Залік
ВК 2.3	Безпровідні мережі	5	150	Екзамен
ВК 3.3	Безпровідні цифрові мережі			
ВК 2.2	Операційні системи Unix/Linux	6	180	Екзамен
ВК 3.2	Системне програмне забезпечення			
ВК 1.1	Вибіркова дисципліна 1	3	90	Залік
ІІІ Курс, 2 семестр				
ВК 2.4	Системний аналіз та теорія прийняття рішень	4	120	Екзамен
ВК 3.4	Системи підтримки прийняття рішень			
ОК25	Захист інформації в інформаційно-комунікаційних системах	4	120	Залік
ОК24	Системи технічного захисту інформації	6	180	Екзамен, захист КР
ВК 2.6	Теорія ризиків та її застосуванян в кібербезпеці	3	90	Залік
ВК 3.6	Групова динаміка та комунікації			

ВК 2.5	Програмування мовою Python	4	120	Екзамен
ВК 3.5	Системне та мережне програмування			
ВК 1.2	Вибіркова дисципліна 2	3	90	Залік
ВП	Виробнича практика	6	180	Диф. Залік
IV Курс, 1 семестр				
ОК25	Захист інформації в інформаційно-комунікаційних системах	5	150	Екзамен, захист КП
ВК 2.7	Штучний інтелект в задачах кібербезпеки	6	180	Екзамен
ВК 3.7	Інформаційно-аналітичне забезпечення систем кібербезпеки			
ОК26	Управління кібербезпекою	4	120	Екзамен
ВК 2.8	Адміністрування комп'ютерних систем та мереж	5	150	Екзамен
ВК 3.8	Інфраструктура відкритих ключів			
ВК 2.9	Безпека мобільних та Web-додатків	3	90	Залік
ВК 3.9	Безпека додатків ОС Windows			
ОК28	Кібероперації	4	120	Залік
ВК 1.3	Вибіркова дисципліна 3	3	90	Залік
IV Курс, 2 семестр				
ОК28	Кібероперації	6	180	Екзамен, захист КР
ВК 2.10	Хмарні технології	3	90	Екзамен
ВК 3.10	Центри обробки даних			
ВК 2.11	Тестування на проникнення, виявлення та розслідування інцидентів кібербезпеки	3	90	Залік
ВК 3.11	Комп'ютерна стеганографія			
ВК 2.12	Безпека IoT	3	90	Залік
ВК 3.12	Технології та засоби сумісної роботи			
ОК27	Комплексні системи захисту інформації	3	90	Екзамен
ПП	Переддипломна практика	6	180	Диф. залік
ДП	Дипломування та захист кваліфікаційної роботи	6	180	Захист ДП
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**240**	**7200**	

* і ** – Студент має обрати вибірковий блок 2 або вибірковий блок 3 з відповідними вибірковими компонентами.

3. Форма атестації здобувачів вищої освіти

Поточна атестація студентів здійснюється у формі екзаменів, заліків, диференційованих заліків, захисту курсових робіт та проектів.

Підсумкова атестація випускників освітньо-професійної програми «Кібербезпека» за спеціальністю 125 «Кібербезпека» проводиться у формі публічного захисту кваліфікаційного проекту/роботи та завершується видачою документу встановленого зразка про присудження йому освітнього ступеня «бакалавр» з присвоєнням кваліфікації: бакалавр з кібербезпеки

Підсумкова атестація здійснюється відкрито і публічно.

Кваліфікаційний проект/робота оприлюднюється у репозитарії закладу вищої освіти.

4. Матриця відповідності компетентностей компонентам освітньої програми

	КЗ-1	КЗ-2	КЗ-3	КЗ-4	КЗ-5	КЗ-6	КЗ-7	КФ-1	КФ-2	КФ-3	КФ-4	КФ-5	КФ-6	КФ-7	КФ-8	КФ-9	КФ-10	КФ-11	КФ-12
ОК 1	+		+		+			+											
ОК 2					+			+	+	+	+								
ОК 3			+		+			+											
ОК 4					+				+								+		
ОК 5					+				+								+		
ОК 6					+				+										
ОК 7					+				+							+			
ОК 8					+				+								+		
ОК 9					+				+	+							+		+
ОК 10					+				+	+									+
ОК 11					+			+	+	+	+								
ОК 12					+												+		+
ОК 13					+				+	+							+		+
ОК 14					+				+	+							+		+
ОК 15					+				+		+								
ОК 16				+	+		+	+	+			+			+				
ОК 17				+	+				+	+	+	+	+	+	+		+	+	
ОК 18				+	+				+	+	+	+	+	+	+		+	+	
ОК 19					+				+	+	+		+	+					
ОК 20				+	+		+	+	+			+			+				
ОК 21				+	+				+	+	+	+	+	+	+		+		
ОК 22		+		+	+	+		+				+				+	+	+	
ОК 23		+	+	+	+			+	+			+		+		+			+
ОК 24		+	+	+	+			+	+	+	+	+	+	+			+		+
ОК 25		+	+	+	+			+	+	+	+	+	+	+	+				+
ОК 26		+	+	+	+		+	+	+	+	+	+	+	+	+	+			+
ОК 27		+	+	+	+		+	+	+	+	+	+	+	+	+	+			+
ОК 28		+	+	+	+		+	+	+	+	+	+	+	+	+	+			+
НП	+			+	+					+									
ТП	+			+	+			+	+	+			+						
ВП	+			+	+														
ПП	+			+	+			+	+	+	+	+	+	+	+	+	+	+	+
ДП	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+

5. Матриця забезпечення результатів навчання відповідними компонентами освітньої програми

	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	РН-24	РН-25	РН-26	РН-27
ОК 1			+	+	+		+	+	+																		
ОК 2								+	+	+	+	+	+		+			+	+		+				+		
ОК 3	+						+	+																			
ОК 4										+	+																
ОК 5										+	+	+															
ОК 6										+	+	+														+	
ОК 7										+	+	+															
ОК 8										+	+	+															
ОК 9										+	+	+			+			+		+							
ОК 10										+	+		+		+			+	+	+							
ОК 11								+	+	+	+	+	+		+			+	+		+				+		
ОК 12																										+	
ОК 13										+	+	+			+			+		+						+	
ОК 14										+	+		+		+				+	+						+	
ОК 15			+		+					+	+	+									+		+	+			
ОК 16	+	+	+	+	+	+	+			+	+	+		+								+					
ОК 17		+	+	+						+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	
ОК 18		+	+	+						+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ОК 19										+	+		+		+	+		+	+	+	+			+	+		
ОК 20	+	+	+	+	+	+	+			+	+	+		+								+					
ОК 21		+	+	+						+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	
ОК 22		+	+	+		+	+	+	+																	+	
ОК 23		+	+	+		+	+		+	+	+	+															
ОК 24		+	+	+		+	+		+	+	+		+		+	+		+			+	+		+			+
ОК 25		+	+	+		+	+			+	+		+	+	+		+	+		+	+	+	+	+	+		+
ОК 26		+	+	+		+	+	+	+	+	+	+	+		+	+	+	+	+		+				+		+
ОК 27		+	+	+		+	+	+	+	+	+	+	+		+	+	+	+	+		+				+		+
ОК 28		+	+	+		+	+	+	+	+	+	+	+		+	+	+	+	+		+				+		+
НП		+	+	+	+										+												
ТП		+	+	+	+		+			+	+	+	+		+												
ВП		+	+	+	+		+		+	+	+	+	+	+	+		+	+	+				+				+
ПП		+	+		+		+	+	+	+	+	+	+		+	+	+		+	+	+		+	+	+		
ДП	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+

	РН-28	РН-29	РН-30	РН-31	РН-32	РН-33	РН-34	РН-35	РН-36	РН-37	РН-38	РН-39	РН-40	РН-41	РН-42	РН-43	РН-44	РН-45	РН-46	РН-47	РН-48	РН-49	РН-50	РН-51	РН-52	РН-53	РН-54
ОК 1																											
ОК 2				+																	+			+		+	
ОК 3																											
ОК 4				+					+	+	+																
ОК 5				+						+	+																
ОК 6				+																							
ОК 7				+													+			+							
ОК 8				+						+	+						+			+							
ОК 9		+		+																	+			+			
ОК 10				+																			+			+	
ОК 11				+																	+			+		+	
ОК 12									+	+	+													+			
ОК 13		+		+																	+			+			
ОК 14		+	+	+																	+		+	+		+	
ОК 15				+																							
ОК 16				+								+															
ОК 17				+	+			+						+	+							+	+		+		
ОК 18				+	+			+						+	+							+	+		+		
ОК 19				+	+			+															+				
ОК 20				+								+															
ОК 21	+			+	+	+		+						+			+	+		+		+			+		
ОК 22																	+										+
ОК 23	+	+	+			+	+										+		+								
ОК 24				+				+	+	+			+	+						+							
ОК 25				+	+			+										+									
ОК 26				+		+		+						+	+	+		+		+	+		+	+		+	
ОК 27				+		+		+						+	+	+		+		+	+		+	+		+	
ОК 28				+		+		+						+	+	+		+		+	+		+	+		+	
НП																										+	
ТП				+																							
ВП		+	+	+			+	+					+	+						+							
ППП	+			+	+	+	+	+				+											+			+	
ДП	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+

Додаток А

Вибіркові компоненти блоку 1 (ВК1) складаються з варіативних дисциплін циклу загальної підготовки. Затверджуються щорічно навчально-методичною радою Житомирського державного технологічного університету

*Вибірковий блок 1 (дисципліни за циклом загальної підготовки на 2018-2019 н.р.)**			
ВК1.1	HR-менеджмент (Human Resources Management)	3	Залік
ВК1.2	Екологічна безпека	3	Залік
ВК1.3	Комп'ютерний аналіз та синтез механізмів	3	Залік
ВК1.4	Комп'ютерне моделювання теплофізичних процесів	3	Залік
ВК1.5	Комунікативний менеджмент	3	Залік
ВК1.6	Основи податкової грамотності	3	Залік
ВК1.7	Основи програмування на мові Go	3	Залік
ВК1.8	Польська мова	3	Залік
ВК1.9	Пошуки та розвідка родовищ корисних копалин	3	Залік
ВК1.10	Тайм-менеджмент	3	Залік
ВК1.11	Теорія корупції та антикорупційні діяльність	3	Залік
ВК1.12	Управління конфліктами	3	Залік
ВК1.13	Управління фінансами та стратегічний менеджмент за програмою IFA	3	Залік
ВК1.14	Social English Studies	3	Залік
ВК1.15	Управління бізнесом	3	Залік
ВК1.16	Бухгалтерський облік з використанням інформаційних технологій	3	Залік
ВК1.17	Ораторське мистецтво	3	Залік
ВК1.18	Веб-дизайн	3	Залік
ВК1.19	Кримінальне право	3	Залік
ВК1.20	Основи кібербезпеки	3	Залік
ВК1.21	Національне та міжнародне оподаткування	3	Залік
ВК1.22	Основи мережевих IT технологій	3	Залік
ВК1.23	Логістика	3	Залік
ВК1.24	Політичні системи та менеджмент сучасних країн	3	Залік
ВК1.25	Страхування	3	Залік
ВК1.26	Ділові комунікації	3	Залік
ВК1.27	Коштовне та декоративне каміння	3	Залік
ВБ1	**Загальний обсяг вибіркового блоку 1**	9	

* Студент обирає 3 дисципліни із запропонованого переліку (по одній дисципліні в 5, 6 і 7 семестрі)