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 № 1 від «31» 08 2017 р.)

Освітня програма вводиться в дію
з 01 вересня 2017 р.
Ректор ЖДТУ _____В.В. Євдокимов
(наказ №234 від «31» 08 2017 р.)

Житомир – 2017

1. ПЕРЕДМОВА

1 **Розроблено** проектною групою Житомирського державного технологічного університету.

2 **Ухвалено** Вченою радою Житомирського державного технологічного університету протокол № 1 від 31 серпня 2017 року.

3 **Розробники:**

Лобанчикова Надія Миколаївна – гарант освітньої програми, керівник проектної групи, кандидат технічних наук, доцент, доцент кафедри комп'ютеризованих систем управління та автоматики;

Єфіменко Андрій Анатолійович – член проектної групи, кандидат технічних наук, завідувач кафедри комп'ютерної інженерії;

Казмірчук Світлана Володимирівна – член проектної групи, кандидат технічних наук, доцент, доцент кафедри комп'ютеризованих систем управління та автоматики (докторант денної форми підготовки за державним замовленням Національного авіаційного університету за спеціальністю 125 «Кібербезпека»);

Пількевич Ігор Анатолійович – член проектної групи, доктор технічних наук, професор, Академік Академії інженерних наук України, Заслужений працівник освіти України, професор кафедри комп'ютеризованих систем управління та автоматики (професор кафедри комп'ютерно-інтегрованих технологій та кібербезпеки Житомирського військового інституту імені С.П. Корольова);

Молодецька Катерина Валеріївна – член проектної групи, кандидат технічних наук, доцент, лауреат стипендії Кабінету Міністрів України для молодих учених, доцент кафедри комп'ютеризованих систем управління та автоматики (доцент кафедри комп'ютерних технологій і моделювання систем Житомирського національного агроекологічного університету).

Освітньо-професійна програма підготовки фахівців першого (бакалаврського) рівня вищої освіти за спеціальністю 125 «Кібербезпека» розроблена відповідно до Закону України «Про вищу освіту» від 01.07.2014 р. № 1556-VII, Постанов Кабінету Міністрів України від 23.11.2011 р. «Про затвердження Національної рамки кваліфікацій» від 30.12.2015 р. № 1187, «Про затвердження Ліцензійних умов провадження освітньої діяльності закладів освіти» від 20.12.2015 р., «Про затвердження Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у вищих навчальних закладах (наукових установах)» від 23.03.2016 р. № 261, методичних рекомендацій «Розроблення освітніх програм. Методичні рекомендації» (2014 р.).

Освітньо-професійна програма визначає передумови доступу до навчання, орієнтацію та основний фокус програми, обсяг кредитів ЄКТС, необхідний для здобуття освітнього ступеню бакалавра, перелік загальних та спеціальних (фахових) компетентностей, нормативний і варіативний зміст підготовки фахівця, сформульований у термінах результатів навчання та вимоги до контролю якості вищої освіти.

2. ПРОФІЛЬ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

підготовки бакалаврів в галузі 12 «Інформаційні технології» зі спеціальності

125 «Кібербезпека»

Складові	Опис освітньої програми
1 – Загальна інформація	
Повна назва закладу вищої освіти та структурного підрозділу	Житомирський державний технологічний університет. Кафедра комп'ютеризованих систем управління та автоматики.
Повна назва кваліфікації мовою оригіналу	Бакалавр з кібербезпеки /Bachelor in Cyber Security.
Офіційна назва освітньої програми	Кібербезпека.
Обсяг освітньої програми	Обсяг програми: 240 кредитів ЄТКС/4 роки навчання.
Наявність акредитації	Ліцензується вперше.
Цикл/рівень	Перший (бакалаврський) рівень вищої освіти/ шостий кваліфікаційний рівень Національної рамки кваліфікацій.
Передумови	Умови вступу визначаються «Правилами прийому до Житомирського державного технологічного університету», затвердженими Вченою радою.
Мова(и) викладання	Українська.
Основні поняття та їх визначення	*Галузь знань* – основна предметна область освіти і науки, що включає групу споріднених спеціальностей, за якими здійснюється професійна підготовка (частина перша статті 1 Закону України «Про вищу освіту»). *Європейська кредитна трансферно-накопичувальна система (ЄКТС)* – система трансферу і накопичення кредитів, що використовується в Європейському просторі вищої освіти з метою надання, визнання, підтвердження кваліфікацій та освітніх компонентів і сприяє академічній мобільності здобувачів вищої освіти. Система ґрунтується на визначенні навчального навантаження здобувача вищої освіти, необхідного для досягнення визначених результатів навчання, та обліковується у кредитах ЄКТС (частина перша статті 1 Закону України «Про вищу освіту»).

	Кваліфікація – офіційний результат оцінювання і визнання, який отримано, коли уповноважена установа (компетентний орган) встановила, що особа досягла компетентностей (результатів навчання) за заданими стандартами (частина перша статті 1 Закону України «Про вищу освіту»). *Кваліфікаційна робота* — це навчально-наукова робота, яка може передбачатись на завершальному етапі здобуття певного рівня вищої освіти для встановлення відповідності набутих здобувачами результатів навчання (компетентностей) вимогам стандартів вищої освіти. Форми кваліфікаційної роботи включають (не обмежуючись зазначеним): дипломну роботу, дисертаційне дослідження, публічну демонстрацію (захист), сукупність наукових статей, комбінацію різних форм вище зазначеного тощо. *Кваліфікаційний рівень* – структурна одиниця Національної рамки кваліфікацій, що визначається певною сукупністю компетентностей, які є типовими для кваліфікацій даного рівня. *Компетентність* – динамічна комбінація знань, вмінь і практичних навичок, способів мислення, професійних, світоглядних і громадянських якостей, морально-етичних цінностей, яка визначає здатність особи успішно здійснювати професійну та подальшу навчальну діяльність і є результатом навчання на певному рівні вищої освіти (частина перша статті 1 Закону України «Про вищу освіту»): – Інтегральна компетентність – узагальнений опис кваліфікаційного рівня, який виражає основні компетентністні характеристики рівня щодо навчання та/або професійної діяльності (пункт третій Національної рамки кваліфікацій, затвердженої постановою Кабінету Міністрів України від 23 листопада 2011 р. № 1341). – Загальні компетентності – універсальні компетентності, що не залежать від предметної області, але важливі для успішної подальшої професійної та соціальної діяльності здобувача в різних галузях та для його особистісного розвитку. – Спеціальні (фахові, предметні) компетентності – компетентності, що залежать від предметної області, та є важливими для успішної професійної діяльності за певною спеціальністю. *Кредит Європейської кредитної трансферно-накопичувальної системи* (далі – кредит ЄКТС) – одиниця вимірювання обсягу навчального навантаження здобувача вищої освіти, необхідного для досягнення визначених (очікуваних) результатів навчання. Обсяг одного кредиту ЄКТС становить 30 годин. Навантаження одного навчального року за денною формою навчання становить, як правило, 60 кредитів ЄКТС (частина перша статті 1 Закону України «Про вищу освіту»). *Освітня (освітньо-професійна чи освітньо-наукова) програма* – система освітніх компонентів на відповідному рівні вищої освіти в межах спеціальності, що визначає вимоги до рівня освіти осіб, які можуть розпочати навчання за цією програмою, перелік навчальних дисциплін і логічну послідовність їх вивчення, кількість кредитів ЄКТС, необхідних для виконання цієї програми, а також очікувані результати навчання (компетентності), якими повинен оволодіти здобувач відповідного ступеня вищої освіти (частина перша статті 1 Закону України «Про вищу

	освіту»). *Результати навчання* – сукупність знань, умінь, навичок, інших компетентностей, набутих особою у процесі навчання за певною освітньо-професійною, освітньо-науковою програмою, які можна ідентифікувати, кількісно оцінити та виміряти (частина перша статті 1 Закону України «Про вищу освіту»). *Спеціалізація* – складова спеціальності, що визначається вищим навчальним закладом та передбачає профільну спеціалізовану освітньо-професійну чи освітньо-наукову програму підготовки здобувачів вищої та післядипломної освіти (частина перша статті 1 Закону України «Про вищу освіту»). *Спеціальність* – складова галузі знань, за якою здійснюється професійна підготовка (частина перша статті 1 Закону України «Про вищу освіту».
2 – Мета освітньої програми	
Забезпечити підготовку висококваліфікованих фахівців в галузі інформаційних технологій зі спеціальності 125 «Кібербезпека», здатних вирішувати складні спеціалізовані задачі та практичні проблеми інформаційної безпеки, захищеності інформаційного і кіберпросторів держави в цілому або окремих суб'єктів їх інфраструктури від ризику стороннього кібернетичного впливу.	
3 – Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність)	Галузь знань – 12 «Інформаційні технології»/ 12 «Information technologies». Спеціальність – 125 «Кібербезпека» /125 «Cyber Security».
Орієнтація освітньої програми	Освітньо-професійна.
Основний фокус освітньої програми та спеціалізації	Здобуття вищої освіти в галузі інформаційні технології, спеціальності «Кібербезпека». Акцент на здатності організовувати й підтримувати комплекс заходів щодо забезпечення інформаційної безпеки з урахуванням їхньої правової обґрунтованості, адміністративно-управлінської й технічної реалізації, економічної доцільності, можливих зовнішніх впливів, імовірних загроз і рівня розвитку технологій захисту інформації.
Особливості та відмінності	Інтеграція програмно-апаратних засобів виявлення, моніторингу та забезпечення інформаційної безпеки, сучасних інформаційних технологій захисту інформації в інформаційно-комунікаційних системах, технологій збереження даних в кіберпросторі та інтелектуалізації функцій протидії кіберзлочинності. Високий рівень практичної підготовки фахівців забезпечується розвиненою міжнародною співпрацею в науковій і освітній сферах, наявністю спеціалізованих лабораторій. Фахівці, залучені до професійної підготовки, пройшли стажування у провідних європейських та українських університетах, мають міжнародний досвід освітньої і наукової діяльності. Кафедра комп'ютеризованих систем управління та автоматики: - здійснює реалізацію проекту TEMPUS: EU-PC double degree master program in automation/mechatronics ("Подвійний магістерський ступінь з автоматизації/мехатроніки в ЄС - країнах партнерах"); - виконує науково-дослідну роботу, що фінансуються за кошти державного бюджету, на тему: № 0116U003655

	«Новий приладовий комплекс стабілізатора озброєння легкої броньованої техніки»; - проводить спільні дослідження з науковцями із Przemyslowy Instytut Automatyki і Pomiarow (м. Варшава, Польща) та Технічного університету м. Ліберець (Чехія) та інш. в галузі автоматизації та приладобудування.
4 – Придатність випускників освітньої програми до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Фахівець може займати первинні посади (за ДК 003:2010): 3439 (24771). Фахівець із організації інформаційної безпеки. International Standard Classification of Occupations 2008 (ISCO-08): 2529 Security specialist (ICT).
Подальше навчання	Навчання на другому (магістерському) рівні вищої освіти / сьомий кваліфікаційний рівень Національної рамки кваліфікацій.
5 – Викладання та оцінювання	
Викладання та навчання	Студентоцентроване навчання, технологія проблемного і диференційованого навчання, технологія інтенсифікації та індивідуалізації навчання, технологія програмованого навчання, інформаційна технологія, технологія розвивального навчання, кредитно-трансферна система організації навчання, електронне навчання в системі Moodle, самонавчання, навчання на основі досліджень. Викладання проводиться у вигляді: лекції, мультимедійної лекції, інтерактивної лекції, семінарів, практичних занять, лабораторних робіт, самостійного навчання на основі підручників та конспектів, консультації з викладачами, підготовка кваліфікаційної роботи бакалавра (проекту).
Оцінювання	Оцінювання навчальних досягнень здійснюється за 100-бальною (рейтинговою) шкалою ЕКТС (ECTS), національною 4-х бальною шкалою («відмінно», «добре», «задовільно», «незадовільно») і вербальною («зараховано», «незараховано») системами. Види контролю: поточний, тематичний, періодичний, підсумковий, самоконтроль. Форми контролю: усне та письмове опитування, тестові завдання в тому числі комп'ютерне тестування, лабораторні звіти, презентації, захист курсових робіт та проектів, звітів з практик, захист кваліфікаційної роботи бакалавра.
6 – Програмні компетентності	
Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки, що характеризується комплексністю та неповною визначеністю умов.
Загальні компетентності	КЗ1. Здатність застосовувати знання у практичних ситуаціях. КЗ2. Знання та розуміння предметної області та розуміння професії. КЗ3. Здатність спілкуватися рідною та другою іноземною мовою як усно, так і письмово. КЗ4. Здатність здійснювати професійну діяльність згідно з вимогами санітарно-гігієнічного режиму, охорони праці, техніки безпеки та протипожежної безпеки.

	КЗ5. Вміння виявляти, ставити та вирішувати проблеми. КЗ6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел. КЗ7. Навички міжособистісної взаємодії. КЗ8.Прагнення до збереження навколишнього середовища. КЗ9. Здатність діяти соціально відповідально та громадянсько свідомо. КЗ10. Здатність вчитися і бути сучасно навченим. КЗ11. Здатність приймати обґрунтовані рішення. КЗ12. Здатність до адаптації та дії в новій ситуації. КЗ13. Дотримання та пропагування здорового способу життя. КЗ14. Здатність бути критичним та самокритичним. КЗ15. Креативність, здатність до системного мислення.
Спеціальні (фахові) компетентності	КФ1. Здатність використовувати законодавчу та нормативно-правову бази, а також вимоги відповідних, в тому числі і міжнародних, стандартів та практик щодо здійснення професійної діяльності. КФ2. Здатність до використання інформаційних і комунікаційних технологій. КФ3. Здатність здійснювати проектування (розробку) систем, технологій і засобів інформаційної безпеки. КФ4. Здатність здійснювати протидію несанкціонованому проникненню в ІТ системи і мережі. КФ5. Здатність прогнозувати, виявляти та оцінювати стан інформаційної безпеки об'єктів і систем. КФ6. Здатність відновлювати нормальне функціонування ІТ систем і мереж після здійснення кібернападів, збоїв та відмов. КФ7. Здатність виконувати спеціальні дослідження технічних і програмно-апаратних засобів захисту обробки інформації в ІТС. КФ8. Здатність проводити техніко-економічного аналіз й обґрунтовувати проектні рішення з забезпечення кібербезпеки. КФ9. Здатність формувати комплекс заходів (правил, процедур, практичних прийомів та ін.) для управління інформаційною безпекою. КФ10. Здатність здійснювати управління інцидентами інформаційної та кібербезпеки. КФ11. Здатність здійснювати управління ризиками інформаційної та кібербезпеки. КФ12. Здатність виконувати моніторинг даних, комп'ютерних зловживань та аномалій. КФ13. Здатність прогнозувати, виявляти та оцінювати можливі загрози інформаційному простору держави та дестабілізуючі чинники.

	КФ14. Здатність проводити дослідження у практичній професійній діяльності.
7 – Програмні результати навчання	
Знання	РН1. Знання історії та культури України, періодів розвитку науки та техніки, їх значення та наслідки для розвитку цивілізації. РН2. Виділити та назвати основні загальнофілософські проблеми, явища політичного та соціально-культурного розвитку українського суспільства. РН3. Базові знання фундаментальних наук, в обсязі, необхідному для освоєння навчальних дисциплін професійної підготовки. РН4. Практичне володіння рідною та однією з іноземних мов в обсязі тематики, зумовленої професійними потребами. РН5. Діяти на основі законодавчої, нормативно-правової баз України та вимог відповідних стандартів, тому числі міжнародних. РН6.Знати методи та технології об'єктно-орієнтованого проектування та програмування. РН7. Знати архітектуру комп'ютера, методи дослідження та обслуговування. РН8. Знання методів протидії кібернападам. РН9.Знання теорії інформації та методів кодування. РН10. Знати основи криптології, криптографії та криптографічного аналізу. РН11. Знання стеганографічних методів захисту інформації. РН12.Знати методи вимірювання та принципи роботи сучасних засобів електроніки, передачі сигналів. РН13. Володіння методами цифрової обробки зображень та сигналів. РН14. Знання методів техніко-економічного аналізу й обґрунтування проектних рішень. РН15. Знання методів, засобів та інформаційних технологій для виявлення несанкціонованого доступу на різних ієрархічних рівнях інформаційно-комунікаційної системи. РН16. Знання методів та засобів побудови та захисту сенсорних мереж передачі даних. РН17. Знання способів подання інтелектуальної задачі та методи пошуку рішень. РН18. Знання теорії надійності та методів діагностики працездатності систем. РН19. Знання методологічних та математичних основ комп'ютерного проектування та моделювання систем. РН20. Знання мов програмування мікроконтролерів та контролерів відповідно норм IEC 61131-3. РН21. Знання моделей, методів та засобів побудови та захисту безпровідних мереж передачі даних.
Уміння	РН22. Застосувати концептуальні знання з навчальних дисциплін загальної підготовки для засвоєння навчальних

	дисциплін професійної підготовки. РН23. Застосувати знання державної та однієї з іноземних мов з метою забезпечення ефективності професійної комунікації. РН24. Організувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем професійній діяльності, оцінювати їхню ефективність. РН25. Використати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності. РН26. Здатність до критичного аналізу і креативного синтезу нових ідей кібербезпеки, які можуть сприяти в академічному і професійному контекстах, технологічному, соціальному та культурному прогресу суспільства у сфері захисту інформації та безпечного використання кіберпростору. РН27. Прогнозувати наслідки результатів діяльності людини з метою збереження навколишнього середовища. РН28. 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. РН29. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної безпеки. РН30. Здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій. РН31. Застосувати програмні засоби, навички роботи в телекомунікаційних та комп'ютерних мережах. РН32. Використати спеціалізовані комп'ютерні програми в професійній діяльності. РН33 Обирати відповідну технологію програмування, виконати аналіз специфікації задач. РН34. Виконувати аналіз програмного забезпечення з метою пошуку, ідентифікації, виявлення та усунення помилок програмування. РН35. Виконувати декомпозицію ІТС. РН36. Розробляти структурні схеми з відображенням зв'язків між інформаційними процесами на віддалених системах. РН37. Розробляти модель загроз, розробляти модель порушника. РН38. Розробляти проекти ІТС базуючись на стандартизованих технологіях та протоколах передачі даних. РН39. Вирішувати завдання захисту програм та даних ІТС програмно-апаратними засобами та давати оцінку якості прийнятих рішень. РН40. Обирати основні методи та способи захисту інформації відповідно до вимог сучасних стандартів інформаційної безпеки щодо критеріїв безпеки інформаційних технологій, застосовуючи системний підхід та знання основ теорії інформаційної безпеки.

	РН41. Проектувати та реалізувати комплексні систему захисту інформації АС організації (підприємства) відповідно до вимог нормативних документів системи технічного захисту інформації. РН42. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційних і комунікаційних системах та мережах. РН43. Здійснювати оцінку можливості проникнення в ІТ системи та мережі шляхом експлуатації наявних вразливостей. РН44. Здійснювати оцінку захищеності ІТ систем та мереж. РН45. Використовувати інструментальні засоби оцінки наявних вразливостей. РН46. Оцінювати можливості та ефективність застосування, в тих чи інших умовах, інструментальних засобів оцінки вразливостей ІТ систем та мереж. РН47. Виконувати налаштування інформаційних систем та комунікаційного обладнання. РН48. Виконувати захист інформаційних систем від комп'ютерних вірусів. РН49. Забезпечувати впровадження та дотримання політики кіберзахисту в ІТС, процедур, і правил. РН50. Організовувати процес створення планів неперервності бізнесу. РН51. Приймати участь у розробці планів відновлення, неперервності процесів організації для забезпечення здатності організації продовжувати виконувати необхідну діяльність в період порушення ІТ. РН52. Виявляти небезпечні сигнали технічних засобів. РН53. Вимірювати параметри небезпечних сигналів для технічних каналів витоку інформації та визначати ефективність захисту від витоку інформації відповідно до вимог нормативних документів системи технічного захисту інформації. РН54. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТСМ відповідно до вимог нормативних документів системи технічного захисту інформації. РН55. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах. РН56. Виконувати дослідження, перевірку, аналіз та оцінювання об'єктів щодо їх відповідності вимогам нормативних документів та можливості їх використання для забезпечення інформації. РН57. Аналізувати економічну ефективність заходів інформаційної безпеки. РН58. Визначати особливості організаційної структури та організації робіт. РН59. Використовувати міжнародні та національні специфічні для сектора економіки вимоги та кращі практики. РН60. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.

	РН61. Приймати участь у розробці та впровадженні політики, стандартів та процедур інформаційної безпеки та/ або кібербезпеки. РН62. На основі політики захисту організації розробляти нормативні документи для її реалізації. РН63. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної/кібербезпеки. РН64. Застосовувати національні та міжнародні регулюючі актів в сфері інформаційної безпеки для розслідування внутрішніх та зовнішніх інцидентів інформаційної безпеки. РН65. Розробляти та оцінювати моделі і політику безпеки на основі використання сучасних принципів, способів та методів теорії захищених систем. РН66. Застосовувати політики, що базуються на ризик адаптивному контролі доступу. РН67. Здійснювати аналіз ризиків функціонування ІКС: визначати послідовність аналізу, формувати моделі порушника та загроз, використовувати сучасні методи та методики аналізу ризиків, оцінювання та управління ризиками. РН68. Виконувати конфігурування систем виявлення вторгнень та використовувати компоненти захисту для забезпечення необхідного рівня захищеності ІТС. РН69. Використовувати інструментарій для моніторингу даних в ІТС. РН70.Виконувати аналіз зловмисного програмного коду. РН71.Характеризувати стан інформаційної безпеки особистості, суспільства та держави. РН72. Характеризувати основні форми інформаційного протиборства в умовах входження держави в інформаційне суспільство. РН73. Використовувати теоретичні і практичні методи та методики досліджень у галузі інформаційної безпеки РН74. Застосовувати системний підхід та знання основ теорії інформаційної безпеки. РН75. Володіння основами проектування, експлуатації та технічного обслуговування сучасних архітектур комп’ютерних мереж. РН76. Визначати статичну завадостійкість цифрової форми подання інформації, розраховувати динамічні параметри цифрового сигналу та виконувати аналіз електричних схем логічних елементів. РН77. Впроваджувати системи інтелектуального аналізу даних та прийняття рішень. РН78. Здатність проводити системний аналіз об’єктів захисту від несанкціонованого доступу для побудови оптимальних структур систем захисту інформації. РН79. Спроможність виявляти та виправляти помилки в інформаційних повідомленнях, володіння технологіями кодування інформації. РН80. Володіти технологіями криптографічного перетворення інформації для забезпечення конфіденційності та цілісності інформації в інформаційно-телекомунікаційних системах.

	РН81. Володіння інформаційними технологіями автоматизації процесів інформаційної діяльності в кіберпросторі для виявлення несанкціонованого доступу на різних ієрархічних рівнях інформаційно-комунікаційної системи. РН82. Володіння програмно-апаратним комплексом для розмежування прав доступу до інформації в кіберпросторі. РН83. Володіння технологіями та інструментальними засобами побудови систем штучного інтелекту для вирішення задач захисту інформації. РН84. Здатність проводити інтелектуальний аналіз даних в системах захисту інформації з використанням навчальної інформації, багатомірного розвідувального аналізу, методів класифікації та прогнозування, пошуку шаблонів даних, OLAP та Data Mining. РН85. Володіння технологіями програмування відповідно норм IEC 61131-3 (Ladder Diagram, Function Block Diagram, Structured Text, Instruction List, Sequential Function Chart). РН86.Володіння технологіями створення безпровідних інформаційно-комунікаційних систем. РН87. Знання та володіння методами моделювання об’єктів захисту, використовуючи системний підхід та сучасні інформаційні технології. РН88. Знання та володіння методами, засобами та інформаційними технологіями автоматизації процесів інформаційної діяльності в кіберпросторі для виявлення несанкціонованого доступу на різних ієрархічних рівнях інформаційно-комунікаційної системи. РН89. Здатність проводити аналіз стану інформаційної та кібербезпеки в умовах виробничої діяльності підприємств та визначати ймовірні загрози та вразливості систем захисту.
Комунікація	РН90. Володіти комунікаційними навичками на рівні вільного спілкування в іншомовному середовищі з фахівцями та нефахівцями щодо захисту інформації та сучасних інформаційних технологій. РН91. Проектувати майбутню професійну діяльність з урахуванням її значущості для громадянина та держави, а також напрямків розвитку інформаційної та кібербезпеки. РН92. Дотримуватись вимог санітарно-гігієнічного режиму, охорони праці, техніки безпеки та протипожежної безпеки при здійсненні професійної діяльності. РН93. Дотримуватись норм міжособистісного спілкування у професійній взаємодії. РН94. Сприймати інформацію, засвоювати її та виробляти професійні рішення в сфері захисту інформації. РН95. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат РН96 Обґрунтування інвестицій в інформаційну безпеку. РН97. Володіння комунікаційними навичками пояснення, переконання та згуртованості. РН98. Розвиток креативного мислення для розробки нових унікальних систем захисту інформації.

Автономія і відповідальність	РН99. Використовувати історичну спадщину та культурні традиції свого народу для професійного зростання, саморозвитку, самовдосконалення. РН100. Вдосконалювати професійний та особистісний розвиток протягом усього життя. РН101. Демонструвати та пропагувати здоровий спосіб життя. РН102. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності. РН103. Дотримуватися етичних норм, враховуючи авторське право та норми академічної доброчесності при проведенні наукових досліджень, розробці програмних продуктів, проектів, презентацій результатів роботи. РН104. Особиста відповідальність за свої дії у питаннях забруднення навколишнього природнього середовища. РН105. Усвідомлення персональної відповідальності за розробку систем захисту інформації, їх впровадження та супровід. РН106. Усвідомлення економічної значимості систем захисту інформації. РН107. Давати якісну оцінку прийнятих рішень.
8 – Ресурсне забезпечення реалізації програми	
Специфічні характеристики кадрового забезпечення	Проектна група: 1 доктор наук, професор, 3 кандидати наук, доценти, 1 кандидат наук. Гарант освітньої програми (керівник проектної групи): доцент кафедри безпеки інформаційних і комунікаційних систем, кандидат технічних наук Лобанчикова Н.М. має стаж науково-педагогічної роботи 15 років, є визнаним професіоналом з досвідом дослідницької діяльності в галузі інформаційних технологій та систем захисту інформації, нагороджена Почесною грамотою Житомирської обласної державної адміністрації, грамотою Виконавчого комітету Богунської районної ради м. Житомира. Член проектної групи, кандидат технічних наук, завідувач кафедри комп'ютерної інженерії Єфіменко А.А. є сертифікованим інструктором Cisco CCNA, керівником локальної мережі академії Cisco, має практичних досвід роботи в сфері захисту інформаційно-комунікаційних систем та мереж (займав посади інженера-програміста, системного адміністратора, завідувача інформаційно-комп'ютерним центром), є визнаним професіоналом в галузі інформаційних технологій та захисту інформації в інформаційно-комунікаційних системах та мережах. Член проектної групи, кандидат технічних наук за спеціальністю «Інформаційна безпека держави», доцент кафедри безпеки інформаційних технологій Казмірчук С.В. є визнаним професіоналом в галузі інформаційних технологій та кібербезпеки. В даний час є докторантом денної форми підготовки за державним замовленням Національного авіаційного університету за спеціальністю 125 «Кібербезпека». Член проектної групи Заслужений працівник освіти України, професор, доктор технічних наук Пількевич І.А. – Академік АІНУ, нагороджений Почесною грамотою Житомирської обласної державної адміністрації, грамотою Виконавчого комітету Богунської районної ради м. Житомира є визнаним професіоналом з досвідом дослідницької діяльності в галузі інформаційних технологій та систем захисту інформації. Член проектної групи, доцент, кандидат технічних наук, лауреат стипендії Кабінету Міністрів України для молодих учених Молодецька К.В. є визнаним професіоналом з досвідом дослідницької діяльності в галузі

	інформаційних технологій та систем захисту інформації. Переважна більшість науково-педагогічних працівників, залучених до реалізації освітньої складової освітньо-наукової програми мають науковий ступінь та/або вчене звання та є штатними співробітниками ЖДТУ. Всі науково-педагогічні працівники мають підтверджений рівень наукової і професійної активності.
Специфічні характеристики матеріально-технічного забезпечення	Забезпеченість навчальними приміщеннями, комп'ютерними робочими місцями, мультимедійним обладнанням відповідає потребі. Наявна вся необхідна соціально-побутова інфраструктура, кількість місць у гуртожитках відповідає вимогам. Наукові дослідження проводяться у лабораторіях кафедри комп'ютеризованих систем управління та автоматики, кафедри програмного забезпечення систем, кафедри автоматизації та комп'ютерно-інтегрованих технологій імені професора Б.Б. Самотокіна: спеціалізованій комп'ютерній лабораторії електроніки та мікросхемотехніки, спеціалізованій комп'ютерній лабораторії пристроїв та систем передачі інформації, спеціалізованій комп'ютерній лабораторії систем автоматизованого проектування та лабораторії метрології та вимірювальної техніки. В ЖДТУ є 4 локальні комп'ютерні мережі і 12 точок бездротового доступу мережі Інтернет. Користування Інтернет-мережею безлімітне. Для проведення інформаційного пошуку та обробка результатів є спеціалізовані комп'ютерні класи кафедри автоматизованого управління технологічними процесами та комп'ютерних технологій та кафедри комп'ютеризованих систем управління та автоматики, де наявне спеціалізоване програмне забезпечення та необмежений відкритий доступ до Інтернет-мережі.
Специфічні характеристики інформаційно-методичного забезпечення	Офіційний веб-сайт http://www.ztu.edu.ua. містить інформацію про освітні програми, навчальну, наукову і виховну діяльність, структурні підрозділи, правила прийому, контакти. Всі зареєстровані в ЖДТУ користувачі мають необмежений доступ до мережі Інтернет. Матеріали навчально-методичного забезпечення освітньо-наукової програми викладені на освітньому порталі «Навчальні ресурси ЖДТУ»: http://learn.ztu.edu.ua. Фонд наукової бібліотеки ЖДТУ містить 4595 назв (майже 136 тисяч примірників) навчальної, 5293 назв (понад 26 тисяч примірників) наукової літератури, 72 найменування періодичних наукових видань. Електронний архів ЖДТУ містить 8 тисяч найменувань наукових праць. Читальний зал забезпечений бездротовим доступом до мережі Інтернет. Всі ресурси бібліотеки доступні через сайту університету: http://www.ztu.edu.ua. Вільний доступ через сайт ЖДТУ до баз даних періодичних фахових наукових видань (в тому числі, англійською мовою) забезпечується: - участю бібліотеки університету у консорціуму ElibUkr. «Електронна бібліотека України: створення Центрів знань в університетах України», що об'єднує бібліотеки вищих навчальних закладів, національні бібліотеки та інші організації України. Учасникам консорціуму ElibUkr надається доступ до БД електронних журналів, електронних книг – найважливішого ядра світових інформаційних ресурсів, що покривають усі галузі знань (наука, техніка, медицина, соціальні та гуманітарні науки). В рамках проекту було вже надано доступ до БД *«MIPP International»,* «PressReader», «SAGE».

9 – Основні компоненти освітньої програми	
Перелік освітніх компонентів (дисциплін, практик, курсових і кваліфікаційних робіт)	*Освітня компонента:* *1. Цикл загальної підготовки* 1.1. Нормативна частина складає 54 кредити та містить наступні дисципліни: - Іноземна мова – 14 кредитів; - Історія і культура України – 3 кредити; - Українська мова (за професійним спрямуванням) – 3 кредити; - Філософія – 3 кредити; - Політологія – 3 кредити; - Фізика (вибрані розділи) – 4 кредити; - Лінійна алгебра та аналітична геометрія – 3 кредити; - Математичний аналіз – 8 кредитів; - Теорія ймовірностей і математична статистика – 3 кредити; - Комп'ютерна дискретна математика – 4 кредити; - Екологія – 3 кредити; - Економіка та організація виробництва – 3 кредити. 1.2. Варіативна частина містить наступні дисципліни з яких студент має вибирати дисципліни загальним обсягом 9 кредитів з урахуванням тижневого навантаження, допускається заміна на навчальні дисципліни інших спеціальностей: - Історія науки і техніки – 3 кредити; - Релігієзнавство – 3 кредити; - Основи підприємницької діяльності – 3 кредити; - Техноекологія – 3 кредити; - Психологія – 3 кредити; - Основи менеджменту – 3 кредити; - Соціологія – 3 кредити; - Техніко-економічна оцінка проектних рішень – 3 кредити; - Логіка – 3 кредити;

	2. Цикл професійної підготовки 2.1. Нормативна частина складає 108 кредитів та включає наступні дисципліни: - Основи програмування – 7 кредитів; - Архітектура комп'ютера – 4 кредити; - Об'єктно-орієнтоване програмування – 7 кредитів (в т.ч. курсова робота); - Теорія електричних і магнітних кіл – 4 кредити; - Веб-дизайн – 6 кредитів; - Основи та нормативно-правове забезпечення кібербезпеки – 3 кредити; - Електроніка – 8 кредитів (в т.ч. курсова робота); - Бази даних – 6 кредитів; - Інженерна та комп'ютерна графіка – 3 кредити; - Операційні системи – 4 кредити; - Теорія інформації та кодування – 3 кредити; - Комп'ютерні мережі – 9 кредитів; - Прикладна криптологія – 7 кредитів; - Системи технічного захисту інформації в кіберпросторі – 10 кредитів; - Захист інформації в інформаційно-комунікаційних системах – 10 кредитів; - Комплексні системи захисту інформації: проектування, впровадження, супровід – 8 кредитів; - Управління та організаційне забезпечення кібербезпеки – 3 кредити; - Комплексний курсовий проект «Розробка захищеної інформаційно-комунікаційної системи» – 3 кредити; - Комплексний курсовий проект «Розробка комплексу засобів захисту інформаційно-комунікаційних систем» – 3 кредити. 2.2. Варіативна частина містить наступні дисципліни з яких студент має вибирати дисципліни загальним обсягом 51 кредит з урахуванням тижневого навантаження: - Іноземна мова професійного спрямування – 6 кредитів; - Системи підтримки прийняття рішень – 6 кредитів; - Комп'ютерна стеганографія – 6 кредитів; - Мікропроцесори в задачах захисту інформації – 3 кредити;

	- Теорія систем та системний аналіз – 6 кредитів; - Сенсорні мережі – 6 кредитів; - Інтелектуальні системи захисту інформації в кіберпросторі – 3 кредити; - Надійність та діагностування систем кіберпростору – 3 кредити; - Інформаційно-аналітичне забезпечення кіберсистем – 6 кредитів; - Комп'ютерне проектування та моделювання кіберсистем – 6 кредитів; - Системи контролю та управління доступом – 6 кредитів; - Мікроконтролери в задачах захисту інформації – 3 кредити; - Адміністрування комп'ютерних систем та мереж – 6 кредитів; - Інтернет-програмування – 9 кредитів; - Інформаційні технології – 9 кредитів; - Цифрова обробка сигналів та зображень – 3 кредити; - Безпровідні мережі – 6 кредитів. 2.3. Практична підготовка складається з 18 кредитів і містить наступні дисципліни: - Навчальна практика – 3 кредити; - Технологічна практика – 3 кредити; - Виробнича практика – 3 кредити; - Переддипломна практика – 3 кредити; - Виконання дипломної роботи – 6 кредитів.
Вимоги до рівня освіти осіб, які можуть розпочати навчання за цією освітньою програмою.	повна загальна середня освіта, молодший спеціаліст, молодший бакалавр.
10 – Академічна мобільність	
Національна кредитна мобільність	Індивідуальна академічна мобільність реалізується у рамках міжуніверситетських договорів про встановлення науково-освітянських відносин для задоволення потреб розвитку освіти і науки з Житомирським національним агроекологічним університетом, Національним технічним університетом «КПІ», 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. До керівництва науковою роботою здобувачів можуть бути залучені провідні фахівці університетів України на умовах індивідуальних договорів. Допускається перезарахування кредитів, отриманих у інших університетах України, за умови відповідності їх набутих компетентностей.
Міжнародна кредитна мобільність	Випускова кафедра та факультет інформаційно-комп'ютерних технологій, до складу якого вона входить, мають договори про співпрацю у рамках проекту TEMPUS: EU-PC double degree master program in automation/mechatronics з Санкт-Петербурзьким державним електротехнічним університетом "ЛЕТІ" (Росія), Технічним університетом м. Ліберець (Чехія), Технічним університетом м. Софія (Болгарія), Університетом ім. Блеза Паскаля (Франція), Саратовським державним технічним університетом (Росія) та інш. Індивідуальна академічна мобільність можлива за рахунок участі у програмах проекту Еразмус + КА107 кредитна мобільність спільно з Господарською академією ім. Д. А. Ценова м. Свіштов (Болгарія), Університетом Південної Богемії (Чеська Республіка); проекту за програмою 545653-EM-1-2013-1-PL-ERA MUNDUS-EMA21 "Ініціатива технічних університетів Кавказького та Атлантичного регіонів в забезпеченні високих освітніх стандартів" кредитна мобільність спільно з Варшавським технологічним університетом (Польща), Університетом м. Тренто (Італія), Університетом Країни Басків (Іспанія), Центральною школою м. Нант (Франція), Університетом м. Саутгемптон (Великобританія), Дублінським технологічним інститутом (Ірландія), Чеським технічним університетом м. Прага (Чехія) та Будапештським університетом технології і економіки (Угорщина).
Навчання іноземних здобувачів вищої освіти	Навчання іноземних здобувачів вищої освіти проводиться на загальних умовах з додатковою мовною підготовкою.

3. АТЕСТАЦІЯ ЗДОБУВАЧА ПЕРШОГО РІВНЯ ВИЩОЇ ОСВІТИ

Атестація здійснюється екзаменаційною комісією відповідно до вимог стандарту вищої освіти після виконання студентом навального плану та завершується видачою диплома встановленого зразка.

На атестацію виноситься увесь нормативний зміст підготовки фахівця.

Термін проведення атестації визначається навчальним планом та графіком освітнього процесу.

Державна атестація освітньої складової освітньо-професійної програми здійснюється шляхом публічного захисту кваліфікаційної роботи/проекту бакалавра перед комісією, склад якої затверджується ректором університету. Захист кваліфікаційної роботи/проекту бакалавра проводиться у терміни, що передбачені навчальним планом.

До атестації допускаються студенти, які виконали всі вимоги освітньої програми та навчального плану.

Результати атестації визначаються оцінками за національною шкалою «відмінно», «добре», «задовільно», «незадовільно».

Кваліфікаційний проект (кваліфікаційна робота) має передбачати розв’язання складного спеціалізованого завдання або практичної проблеми в галузі кібербезпеки, що характеризується комплексністю та невизначеністю умов.

Кваліфікаційний проект (кваліфікаційна робота) – це логічне завершення дослідження певного об’єкту – матеріального (системи, обладнання, пристрою тощо) або нематеріального (певного процесу, програмного продукту або інформаційної технології, інтелектуального твору тощо), його характеристик, властивостей (що є предметом дослідження).

Кваліфікаційний проект (кваліфікаційна робота) – це самостійна індивідуальна робота з елементами дослідництва й інновацій, яка є підсумком теоретичної та практичної підготовки в рамках нормативної та варіативної складових освітньо-професійної програми підготовки бакалавра.

В обов’язковому порядку пояснювальна записка кваліфікаційного проекту (кваліфікаційної роботи) бакалавра повинна містити розроблені студентом алгоритми, моделі, програми, схеми організації баз даних, функціональні та структурні схеми, лістинг програми чи програмного комплексу, інші види технічного опису особистих фахових рішень.

Завдання на кваліфікаційний проект (кваліфікаційну роботу)має відображати систему компетенцій, виробничі функції та типові задачі діяльності, що визначені в освітньо-професійній програмі.

Кваліфікаційний проект (кваліфікаційна робота) має бути перевірений на плагіат. Кваліфікаційний проект (кваліфікаційна робота) має бути розміщений на сайті вищого навчального закладу.

4. ТЕМАТИКА КВАЛІФІКАЦІЙНИХ ПРОЕКТІВ/РОБІТ

- Розробка системи інженерно-технічного захисту інформації в кабінеті керівника підприємства.
- Розробка лабораторної установки для дослідження акустичних каналів витоку інформації.
- Інформаційна система контролю доступу до приміщень військових частин.
- Програмне забезпечення системи контролю зберігання і передачі інформації.
- Підсистема контролю доступу до спеціалізованих приміщень на підприємстві.
- Розробка генератора квазішумових сигналів акустичного діапазону частот.
- Алгоритм і програма візуалізації процесів забезпечення автентичності даних з використанням цифрового підпису Elliptic Curve Digital Signature Algorithm (ECDSA).
- Алгоритм і програма візуалізації процесів забезпечення автентичності даних з використанням цифрового підпису Digital Signature Algorithm (DSA).
- Алгоритм і програма візуалізації процесів забезпечення конфіденційності даних з використанням покращеного алгоритму криптографічного перетворення ГОСТ 28147-89 у режимі простої заміни.
- Алгоритм і програма візуалізації процесів забезпечення конфіденційності даних з використанням шифру "IDEA".
- Програмне забезпечення аутентифікації користувачів веб-сайту.
- Програмне забезпечення клієнт-серверного обміну даними з сеансовим шифруванням.
- Програмне забезпечення віддаленого спостереження та контролю дій працівників ПК локальної мережі.
- Програмне забезпечення обміну та контролю інтернет-трафіку користувачами локальної мережі.
- Розробка системи підтримки прийняття рішень експерта з інформаційної безпеки.
- Розробка автоматизованої системи виявлення конфіденційної інформації в текстових документах.
- Розробка підсистеми оцінки інформаційної безпеки підприємства.
- Розробка проекту модернізації інформаційно-комунікаційної мережі комерційного банку.
- Розробка комплексної системи захисту інформації серверної кімнати комерційного банку.
- Розробка системи захисту інформаційно-комунікаційної мережі.
- Програмне забезпечення контролю встановленого програмного забезпечення.
- Розробка підсистем виявлення динамічної складової у потоках відеоданих.

- Розробка підсистеми захисту інформації приватного підприємства.
- Розробка системи інженерно-технічного захисту інформації.
- Розробка проекту інформаційно-комунікаційної системи відео- контролю територіально-розподілених об’єктів.
- Розробка проекту комплексного захисту готелів та готельних комплексів.
- Розробка комплексної системи захисту вузла Інтернет.
- Розробка імітатора роботи лінії передачі інформації в інфрачервоному діапазоні радіохвиль.
- Алгоритм і програма візуалізації процесів забезпечення конфіденційності даних з використанням стандарту шифрування Advanced Encryption Standard (AES).
- Алгоритм і програма візуалізації процесів забезпечення конфіденційності даних з використанням шифру «Лабіринт».
- Програмне забезпечення пошуку вразливостей комп’ютерів локальної мережі.
- Інформаційна технологія побудови систем підтримки прийняття рішень експертів з інформаційної безпеки.
- Розробка моделей та методів побудови комплексних систем захисту особливо-важливих об’єктів.
- Інформаційна технологія побудови систем моніторингу та оцінки рівня кіберзагроз.
- Розробка підсистеми аутентифікації користувачів інформаційної системи.
- Розробка підсистеми управління доступом в інформаційній системі.
- Розробка підсистеми розмежування доступу до баз даних.
- Розробка захищених інформаційно-комунікаційних систем.
- Розробка автоматизованої системи аудиту стану інформаційної безпеки підприємства відповідно до міжнародного стандарту інформаційної безпеки ISO/IEC 27001.
- Розробка інтелектуальних систем захисту інформації.
- Розробка інтелектуальних систем розпізнавання зображень.
- Розробка інтелектуальних підсистем відображення інформації.
- Розробка складових віртуальної лабораторії із дослідження технологій адміністрування гетерогенних операційних систем.
- Розробка системи підтримки прийняття рішень оператора служби безпеки.
- Розробка систем підтримки прийняття рішень експертів з інформаційної безпеки.
- Розробка підсистеми автоматичного проектування систем захисту інформації.
- Побудова нейромережевих інформаційних систем обробки інформації.

5. ХАРАКТЕРИСТИКА СИСТЕМИ ВНУТРІШНЬОГО ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ПІДГОТОВКИ ЗДОБУВАЧА ТРЕТЬОГО РІВНЯ ВИЩОЇ ОСВІТИ

Система внутрішнього забезпечення вищим навчальним закладом якості вищої освіти складається з таких процедур і заходів, передбачених Законом України «Про вищу освіту»:

1) визначення принципів та процедур забезпечення якості вищої освіти;
2) здійснення моніторингу та періодичного перегляду освітніх програм;
3) щорічне оцінювання здобувачів першого рівня вищої світи, науково-педагогічних працівників вищого навчального закладу та регулярне оприлюднення результатів таких оцінювань на офіційному веб-сайті вищого навчального закладу, на інформаційних стендах тощо;
4) забезпечення підвищення кваліфікації науково-педагогічних працівників;
5) забезпечення наявності необхідних ресурсів для організації освітнього процесу, у тому числі самостійної роботи здобувачів першого рівня вищої освіти, за кожною освітньою програмою;
6) забезпечення наявності інформаційних систем для ефективного управління освітнім процесом;
7) забезпечення публічності інформації про освітні програми, ступені освіти та кваліфікації;
8) забезпечення ефективної системи запобігання та виявлення академічного плагіату у наукових працях працівників вищих навчальних закладів і здобувачів першого рівня вищої освіти.

Гарант освітньої програми,
доцент кафедри
комп'ютерної інженерії та кібербезпеки
к. т. н., доцент Н.М. Лобанчикова

Завідувач кафедри
комп'ютерної інженерії та кібербезпеки
к. т. н. А.А. Єфіменко