МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «Кібербезпека»

Першого (бакалаврського) рівня вищої освіти
галузі знань F «Інформаційні технології»
спеціальності F5 «Кібербезпека та захист інформації»
Кваліфікація: бакалавр з кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО
Вченою радою Державного університету «Житомирська політехніка»
Голова Вченої ради
_____ Віктор ЄВДОКИМОВ
(протокол від 18 березня 2025 р. № 05)
Освітня програма вводиться в дію з 01 вересня 2025 р.
Ректор
_____ Віктор ЄВДОКИМОВ
(наказ від 18 березня 2025 р. № 68/од)

Житомир – 2025

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійна програми
«Кібербезпека»
Першого (бакалаврського) рівня вищої освіти
галузі знань F «Інформаційні технології»
спеціальності F5 «Кібербезпека та захист інформації»

Гарант освітньо-професійної програми Андрій ЄФІМЕНКО
20.01.2025р

Кафедра комп'ютерної інженерії та кібербезпеки
Протокол від 20 січня 2025р
№ 1

Завідувач кафедри Андрій ЄФІМЕНКО

Вчена рада факультету інформаційно-комп'ютерних технологій
Протокол від 17 лютого 2025р
№ 2

Декан факультету Тетяна НІКІТЧУК

Начальник навчально-методичного відділу Вікторія МЕЛЬНИК-ШАМРАЙ
13.03.2025р

Начальник відділу моніторингу та забезпечення якості Ігор СВІТЛИШИН
13.03.2025р

Науково-методична рада Державного університету «Житомирська політехніка»
Протокол від 14 03 2025р
№ 02

Проректор з науково-педагогічної роботи Андрій МОРОЗОВ
14.03.2025р

ПЕРЕДМОВА

Освітньо-професійну програму розроблено робочою групою у складі:

Керівник робочої групи:

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

Члени робочої групи:

ВОРОТНІКОВ Володимир – професор кафедри комп'ютерної інженерії та кібербезпеки, доктор технічних наук, доцент,

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

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

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

СЕМЕНЕЦЬ Сергій – професор кафедри комп'ютерної інженерії та кібербезпеки, доктор педагогічних наук, професор.

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».

МОСКАЛЕНКО Марія – здобувачка вищої освіти, 3 курс, група КБ-22-3.

ХАРИТОНЮК Юрій – здобувач вищої освіти, 4 курс, група КБ-21-2.

СІНІЦИНА Олександра – випускниця з ОПП 2024 р.; здобувачка вищої освіти, 1 курс, група КБм-24-1.

ГОНЧАРОВ Михайло – випускник з ОПП 2022 р.; аналітик з інцидентів, ТОВ «МЕТІНВЕСТ ДІДЖИТАЛ».

ЛЕЩЕНКО Богдан – випускник з ОПП 2021 р.; адміністратор системи, ТОВ «Сана Комерс Україна».

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	Перший (бакалаврський) рівень вищої освіти
Ступінь вищої освіти	«бакалавр»
Галузь знань	F «Інформаційні технології»
Спеціальність	F5 «Кібербезпека та захист інформації»
Спеціалізація або предметна спеціальність (за наявності)	–
Тип диплома	Диплом бакалавра, одиничний
Найменування партнера за узгодженою спільною освітньою програмою (за наявності)	–
Мова (мови) викладання	Українська
Кількість кредитів ЄКТС, необхідних для виконання програми	240 кредитів ЄТКС
Форми здобуття освіти за освітньою програмою та розрахункові строки виконання освітньої програми за кожною з них	Очна (денна), заочна 3 роки 10 місяців
Освітня кваліфікація	бакалавр з кібербезпеки та захисту інформації
Кваліфікація в дипломі	бакалавр з кібербезпеки та захисту інформації
Вимоги до освіти осіб, які можуть розпочати навчання за програмою	Наявність повної загальної середньої освіти або освітньо-кваліфікаційного рівня «Молодший спеціаліст», освітнього рівня «Молодший бакалавр», на основі освітнього ступеня «фаховий молодший бакалавр»
Наявність акредитації	Національне агентство із забезпечення якості вищої освіти. Сертифікат про акредитацію освітньої програми «Кібербезпека» (за спеціальністю 125 Кібербезпека та захист інформації) № 5694, дійсний до 01.07.2027
Цикл/рівень	НРК України – 6 рівень FQ-EHEA – перший цикл EQF-LLL – 6 рівень
Інтернет адреса постійного розміщення опису освітньої програми	https://learn.ztu.edu.ua/course/view.php?id=3912 https://vstup.ztu.edu.ua/bakalavr/125-kiberbezpeka/
2 – Мета освітньої програми	
Професійна підготовка фахівців з кібербезпеки та захисту інформації, набуття ними компетентностей в застосуванні принципів, методів та засобів забезпечення кібербезпеки та захисту інформації.	

3 - Характеристика освітньої програми	
Опис предметної області	***Об'єкти вивчення:*** – технології кібербезпеки та захисту інформації; – процеси управління кібербезпекою та захистом інформації; – об'єкти інформаційної діяльності, в тому числі інформаційні та інформаційно-комунікаційні системи, інформаційні ресурси і технології. ***Цілі навчання:*** підготовка фахівців, здатних використовувати і впроваджувати технології кібербезпеки та захисту інформації та розв'язувати складні задачі у галузі кібербезпеки та захисту інформації. ***Теоретичний зміст предметної області:*** Принципи, концепції, теорії захисту життєво важливих, інтересів людини, суспільства, держави під час використання кіберпростору, за якого забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі. ***Методи, методики та технології:*** методи, методики та технології розв'язання теоретичних і практичних задач кібербезпеки та захисту інформації. ***Інструменти та обладнання*:** засоби, пристрої, мережне устаткування, прикладне та спеціалізоване програмне забезпечення, інформаційні системи та комплекси проектування, моделювання, контролю, моніторингу, зберігання, обробки, відображення та захисту даних.
Основний фокус освітньої програми	Вища освіта в галузі інформаційних технологій. Програма фокусується на питаннях забезпечення кібербезпеки сучасних комп'ютерних систем та мереж. Ключові слова: кібербезпека, комп'ютерна система, комп'ютерна мережа, інформаційна система, інформаційно-комунікаційна 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 нових і вдосконалення існуючих комп'ютерних та інформаційних систем з подальшим впровадженням науково-практичних розробок у діяльність організацій та установ.

4 – Працевлаштування за здобутою освітою	
Працевлаштування випускників	Працевлаштування на посадах у структурних підрозділах установ/підприємств/організацій, які передбачають наявність вищої освіти зі спеціальності F5 Кібербезпека та захист інформації. I. Згідно з ДК 003:2010 та стандарту вищої освіти за спеціальністю для першого (бакалаврського) рівня вищої освіти: 1. Адміністратор безпеки мереж і систем. 2. Фахівець сфери захисту інформації. 3. Фахівець з питань безпеки (інформаційно-комунікаційні технології). 4. Конструктор систем кібербезпеки. 5. Фахівець з підтримки інфраструктури кіберзахисту. 6. Фахівець з реагування на інциденти кібербезпеки. 7. Фахівець з криптографічного захисту інформації. 8. Фахівець з технічного захисту інформації. 9. Фахівець з тестування систем захисту інформації. 10. Аудитор інформаційних технологій (з кібербезпеки). 11. Фахівець з оцінки заходів захисту інформації (кібербезпеки). 12. Кібероператор. II. Згідно з ДК 003:2010: 1. Аналітик з безпеки інформаційно-телекомунікаційних систем. 2. Аналітик з оцінки вразливостей. 3. Аналітик загроз безпеки. 4. Аналітик систем захисту інформації та оцінки вразливостей. 5. Розробник систем захисту інформації. 6. Уповноважений з авторизації безпеки. 7. Фахівець з планування політики та стратегії кібербезпеки. 8. Фахівець із кібердосліджень та розробок систем безпеки. III. 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. Cybersecurity Auditor 8. Cybersecurity Researcher 9. Cybersecurity Risk Manager 10. Digital Forensics Investigator
Подальше навчання (академічні права випускників)	Здобуття освіти на другому (магістерському) рівні вищої освіти. Здобуття або вдосконалення освіти та професійної підготовки в системі освіти дорослих.

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 – Єдиний державний кваліфікаційний іспит, підготовка та публічний захист кваліфікаційної роботи.
6 – Програмні компетентності	
Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі практичні завдання у галузі кібербезпеки та захисту інформації.
Загальні компетентності (К)	***Загальні компетентності, визначені стандартом вищої освіти:*** **ЗК01**. Здатність застосовувати знання у практичних ситуаціях. **ЗК02**. Знання та розуміння предметної області і розуміння професійної діяльності **ЗК03**. Здатність спілкуватися державною мовою як усно, так і письмово. **ЗК04**. Здатність спілкуватися іноземною мовою. **ЗК05**. Здатність вчитися і оволодівати сучасними знаннями. **ЗК06**. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав та свобод людини і громадянина в Україні. **ЗК07**. Здатність ухвалювати рішення й діяти дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності. **ЗК08.** 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. ***Загальні компетентності, визначені за освітньою програмою:*** **ЗК09**. Здатність комунікувати і працювати в команді, а також з замовниками та зовнішніми партнерами. **ЗК10**. Здатність до пошуку, оброблення та аналізу інформації з використанням інформаційних та комуні-каційних технологій.

Спеціальні (фахові, предметні) компетентності	***Спеціальні компетентності, визначені стандартом вищої освіти:*** **СК01.** Здатність застосовувати законодавчу та нормативно-правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності. **СК02.** Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації. **СК03.** Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації. **СК04.** Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації. **СК05.** Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження. **СК06.** Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо.) **СК07.** Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою. **СК08.** Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності. **СК09.** Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності. **СК10.** Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки. ***Спеціальні компетентності, визначені за освітньою програмою:*** **СК11.** Здатність забезпечувати проєктування, розгортання, системне адміністрування, резервування та відновлення функціонування комп'ютерних систем та мереж, а також пристроїв, систем і рішень кібербезпеки та захисту інформації.
7 – Програмні результати навчання	
Результати навчання, визначені стандартом вищої освіти: **РН01**. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків. **РН02**. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації. **РН03.** Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності.	

РН04. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.
РН05. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.
РН06. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.
РН07. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.
РН08. Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення.
РН09. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.
РН10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.
РН11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації.
РН12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.
РН13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та\або інфраструктури організації в цілому.
РН14. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації.
РН15. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.
РН16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.
РН17. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.
РН18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.
РН19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.
РН20. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації.
РН21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.
Результати навчання, визначені за освітньою програмою:
РН22. Здійснювати ефективні міжособистісні та командні комунікації і співпрацю з представниками професійної спільноти, партнерів з приватного, державного та громадського секторів.
РН23. Використовувати різні форми занять фізичною культурою та спортом, а також знання на навички екологічної та безпечної поведінки для забезпечення фізичного здоров'я і професійного довголіття, а також формування і підтримки екологічного та безпечного середовища перебування та діяльності.

РН24. Застосовувати знання й розуміння історичних, культурних, моральних, світоглядних, соціальних та політичних цінностей та досягнень демократичного суспільства для реалізації цілей сталого розвитку держави та світу. **РН25**. Застосовувати сучасні методи, способи та технологій пошуку, збирання, зберігання, оброблення, передавання, аналізу та захисту даних. **РН26**. Виконувати проєктування, розгортання, системне адміністрування, резервування та відновлення функціонування комп'ютерних систем та мереж, а також пристроїв, систем і рішень кібербезпеки та захисту інформації.	
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Для реалізації освітньої програми залучено 6 докторів наук, професорів, або доцентів, або старших наукових співробітників; 15 кандидатів наук, доцентів; 2 кандидатів наук; 1 доктор філософії (PhD), доцент. 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 . Всі НПП, що забезпечують провадження освітнього процесу на освітньо-професійній програмі, за кваліфікацією відповідають профілю і напряму дисциплін, що викладаються, мають необхідний стаж науково-педагогічної роботи. Всі науково-педагогічні працівники мають рівень наукової та професійної активності, який засвідчується виконанням не менше чотирьох видів та результатів ліцензійних вимог. НПП регулярно проходять підвищення кваліфікації на базі ЗВО, ІТ-компаній та сучасних освітніх платформ, а також залучаються до виконання міжнародних грантових проєктів. До організації навчального процесу залучаються професіонали-практики з належними освітою та досвідом.
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 F5 «Кібербезпека та захист інформації» відповідає ліцензійним вимогам, має актуальний змістовий контент, базується на сучасних інформаційно-комунікаційних технологіях. 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. Офіційний веб-сайт https://ztu.edu.ua містить інформацію про освітні програми, освітню, наукову і виховну діяльність, структурні підрозділи, правила прийому, контакти. Всі зареєстровані в університеті користувачі мають необмежений доступ до мережі Інтернет. Матеріали навчально-методичного забезпечення освітньо-професійної програми викладені на освітньому порталі університету: http://learn.ztu.edu.ua

9 – Академічна мобільність	
Національна кредитна мобільність	Індивідуальна академічна мобільність уможливлюється 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 інформаційно-комунікаційних технологій, Національним університетом «Одеська юридична академія» згідно укладених договорів про співпрацю. Кредити, отримані в інших університетах України, перераховуються відповідно до довідки про академічну мобільність.
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.
10 – Форми атестації здобувачів вищої освіти	
Форми атестації здобувачів вищої освіти	Атестація здобувачів вищої освіти з бакалаврської освітньої програми «Кібербезпека» здійснюється у формі здачі Єдиного державного кваліфікаційного іспиту за спеціальністю F5 Кібербезпека та захист інформації та публічного захисту кваліфікаційної роботи.
Вимоги до кваліфікаційної роботи	Кваліфікаційна робота повинна містити результати виконання аналітичних та теоретичних, системотехнічних або експериментальних досліджень одного з актуальних завдань спеціальності F5 «Кібербезпека та захист інформації» в рамках об'єктів професійної діяльності бакалаврів, а також результати проектування, моделювання, імплементації та тестування заданих у завданні до виконання роботи засобів кібербезпеки та захисту інформації та демонструвати досягнення результатів навчання за стандартом та освітньою програмою, здатність автора логічно, на підставі сучасних наукових методів викласти свої погляди за темою роботи, обґрунтувати вибір технічного і програмного забезпечення, робити обґрунтовані висновки і формулювати конкретні пропозиції та рекомендації щодо отриманих результатів. Кваліфікаційні роботи зберігаються на офіційному сайті закладу вищої освіти або його структурного підрозділу і мають бути перевірені (з використанням відповідного програмного забезпечення) на плагіат. Захист кваліфікаційної роботи завершується видачою документу встановленого зразка про присудження йому ступеня бакалавра із присвоєнням кваліфікації: бакалавр з кібербезпеки та захисту інформації.

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 компонентів освітньо-професійної програми

Код ОК	Компоненти освітньої програми (навчальні дисципліни, курсові проєкти/роботи, практики кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1	*2*	*3*	*4*
Обов'язкові компоненти ОП			
ОК 01	Іноземна мова	15	Заліки, екзамен
ОК 02	Українська мова, професійне та академічне письмо	3	Залік
ОК 03	Фізичне виховання	3	Залік
ОК 04	Лінійна алгебра та аналітична геометрія	3	Екзамен
ОК 05	Фізика	4	Екзамен
ОК 06	Математичний аналіз	8	Залік, екзамен
ОК 07	Антикорупція та доброчесність	3	Залік
ОК 08	Розвиток комунікаційних навичок та групова динаміка	3	Залік
ОК 09	Теорія ймовірностей і математична статистика	4	Екзамен
ОК 10	Комп'ютерна дискретна математика	4	Екзамен
ОК 11	Українські історико-культурні та політико-соціальні студії	3	Залік
ОК 12	Екологія, безпека життєдіяльності та охорона праці	3	Залік
ОК 13	Технології та інструменти електронної документації	3	Залік
ОК 14	Архітектура комп'ютера	4	Екзамен
ОК 15	Програмування	9	Залік, екзамен, курсова робота
ОК 16	Теорія кіл та сигналів	5	Екзамен
ОК 17	Теорія інформації та кодування	3	Екзамен
ОК 18	Комп'ютерна електроніка та схемотехніка	4	Залік, екзамен
ОК 19	Операційні системи	7	Залік, екзамен
ОК 20	Комп'ютерні мережі	9	Залік, екзамен, курсовий проєкт
ОК 21	Web-технології	3	Екзамен
ОК 22	Основи кібербезпеки	4	Екзамен
ОК 23	Прикладна криптологія	6	Залік, екзамен
ОК 24	Мережна безпека	9	Залік, екзамен, курсовий проєкт
ОК 25	Бази даних: побудова, адміністрування, захист	4	Екзамен
ОК 26	Теорія ризиків та її застосування в кібербезпеці	3	Екзамен
ОК 27	Системи технічного захисту інформації	4	Екзамен
ОК 28	Теорія кібербезпеки	3	Екзамен
ОК 29	Кібероперації	10	Залік, екзамен, курсовий проєкт

ОК 30	Стандарти та нормативно-правове забезпечення кібербезпеки	3	Екзамен
ОК 31	Управління кібербезпекою	3	Екзамен
ОК 32	Комплексні системи захисту інформації	4	Екзамен
ОК 33	Технологічна практика 1	3	Диф. залік
ОК 34	Технологічна практика 2	3	Диф. залік
ОК 35	Виробнича практика	3	Диф. залік
ОК 36	Переддипломна практика	6	Диф. залік
ОК 37	Кваліфікаційна робота	6	Кваліфікаційна атестація
	Єдиний державний кваліфікаційний іспит	0	Кваліфікаційна атестація
Базова загальновійськова підготовка*			
ОВК 01	Теоретична підготовка БЗВП	3	Диф. залік
Загальний обсяг обов'язкових компонент:		**180**	
Вибіркові компоненти ОП *(обираються навчальні дисципліни загальним обсягом 60 кредитів)*			
ВК 2.01	Дисципліна № 01	4	Залік
ВК 2.02	Дисципліна № 02	4	Залік
ВК 2.03	Дисципліна № 03	4	Залік
ВК 2.04	Дисципліна № 04	4	Залік
ВК 2.05	Дисципліна № 05	4	Залік
ВК 2.06	Дисципліна № 06	4	Залік
ВК 2.07	Дисципліна № 07	4	Залік
ВК 2.08	Дисципліна № 08	4	Залік
ВК 2.09	Дисципліна № 09	4	Залік
ВК 2.10	Дисципліна № 10	4	Залік
ВК 2.11	Дисципліна № 11	4	Залік
ВК 2.12	Дисципліна № 12	4	Залік
ВК 2.13	Дисципліна № 13	4	Залік
ВК 2.14	Дисципліна № 14	4	Залік
ВК 2.15	Дисципліна № 15	4	Залік
Загальний обсяг вибіркових компонент:		**60**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**240**	

** – для здобувачів вищої освіти, звільнених від проходження БЗВП, пропонуються інші дисципліни вільного вибору*

2.2. Структурно-логічна схема освітньо-професійної програми

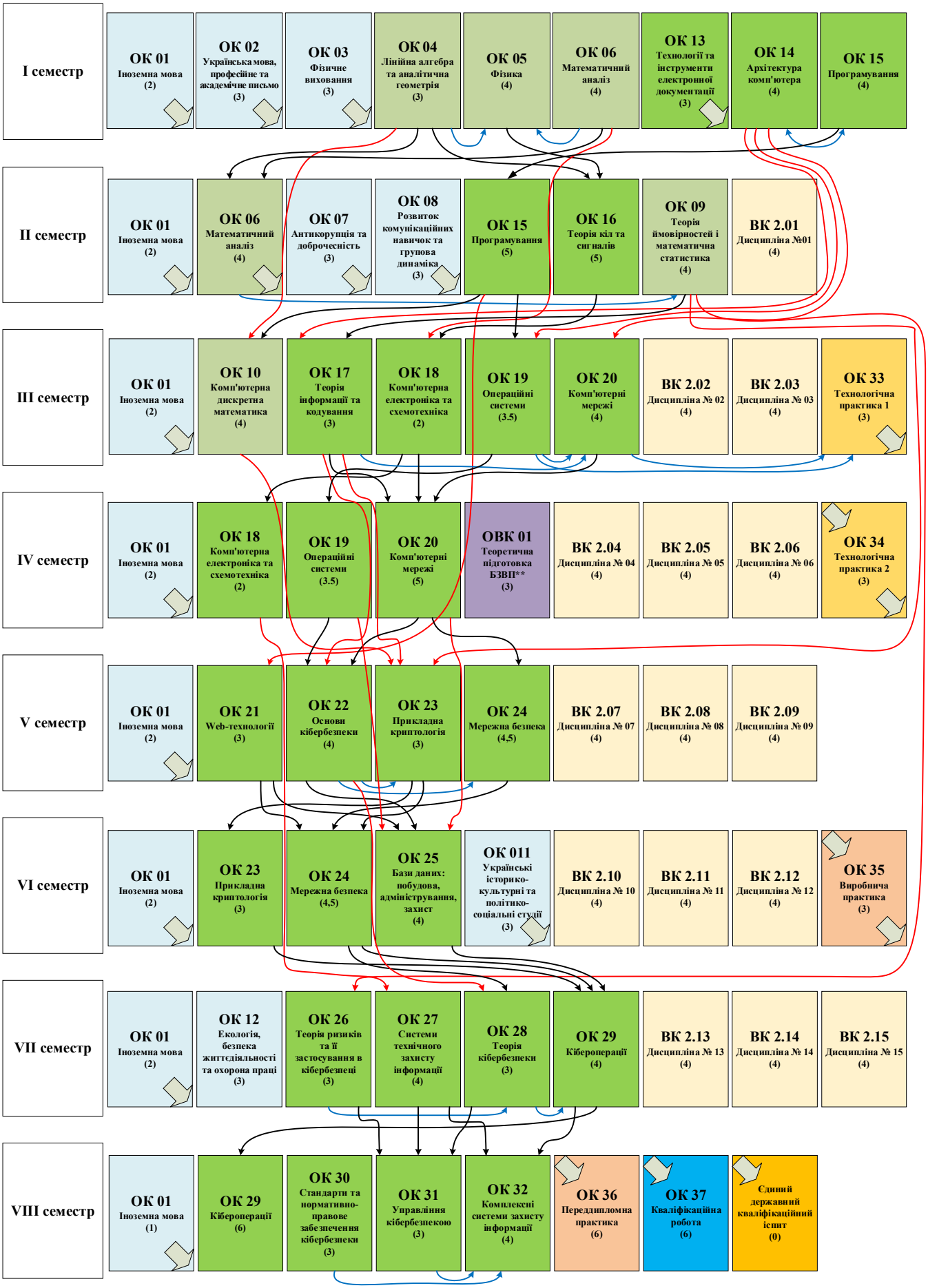
Код ОК	Компоненти освітньої програми (навчальні дисципліни, курсові проєкти/ роботи, практики кваліфікаційна робота)	Кількість кредитів	Загальний обсяг год.	Форма підсумкового контролю
1	*2*	*3*	*4*	*5*
І курс, 1 семестр				
ОК 01	Іноземна мова	2	60	Залік
ОК 02	Українська мова, професійне та академічне письмо	3	90	Залік
ОК 03	Фізичне виховання	3	90	Залік
ОК 04	Лінійна алгебра та аналітична геометрія	3	90	Екзамен
ОК 05	Фізика	4	120	Екзамен
ОК 06	Математичний аналіз	4	120	Залік
ОК 13	Технології та інструменти електронної документації	3	90	Залік
ОК 14	Архітектура комп'ютера	4	120	Екзамен
ОК 15	Програмування	4	120	Залік
	Разом	**30**	**900**	
І курс, 2 семестр				
ОК 01	Іноземна мова	2	60	Залік
ОК 06	Математичний аналіз	4	120	Екзамен
ОК 07	Антикорупція та доброчесність	3	90	Залік
ОК 08	Розвиток комунікаційних навичок та групова динаміка	3	90	Залік
ОК 15	Програмування	5	150	Екзамен, курсова робота
ОК 16	Теорія кіл та сигналів	5	150	Екзамен
ОК 09	Теорія ймовірностей і математична статистика	4	120	Екзамен
ВК 2.01	Дисципліна № 01	4	120	Залік
	Разом	**30**	**900**	
ІІ курс, 1 семестр				
ОК 01	Іноземна мова	2	60	Залік
ОК 10	Комп'ютерна дискретна математика	4	120	Екзамен
ОК 17	Теорія інформації та кодування	3	90	Екзамен
ОК 18	Комп'ютерна електроніка та схемотехніка	2	60	Залік
ОК 19	Операційні системи	3,5	105	Залік
ОК 20	Комп'ютерні мережі	4	120	Залік
ВК 2.02	Дисципліна № 02	4	120	Залік
ВК 2.03	Дисципліна № 03	4	120	Залік
ОК 33	Технологічна практика 1	3	90	Диф. залік
	Разом	**29,5**	**885**	

ІІ курс, 2 семестр				
ОК 01	Іноземна мова	2	60	Залік
ОК 18	Комп'ютерна електроніка та схемотехніка	2	60	Екзамен
ОК 19	Операційні системи	3,5	105	Екзамен
ОК 20	Комп'ютерні мережі	5	150	Екзамен, курсовий проєкт
ОВК 01	Теоретична підготовка БЗВП **	3	90	Диф. залік
ВК 2.04	Дисципліна № 04	4	120	Залік
ВК 2.05	Дисципліна № 05	4	120	Залік
ВК 2.06	Дисципліна № 06	4	120	Залік
ОК 34	Технологічна практика 2	3	90	Диф. залік
	Разом	**30,5**	**915**	
ІІІ курс, 1 семестр				
ОК 01	Іноземна мова	2	60	Залік
ОК 21	Web-технології	3	90	Екзамен
ОК 22	Основи кібербезпеки	4	120	Екзамен
ОК 23	Прикладна криптологія	3	90	Залік
ОК 24	Мережна безпека	4,5	135	Залік
ВК 2.07	Дисципліна № 07	4	120	Залік
ВК 2.08	Дисципліна № 08	4	120	Залік
ВК 2.09	Дисципліна № 09	4	120	Залік
	Разом	**28,5**	**855**	
ІІІ курс, 2 семестр				
ОК 01	Іноземна мова	2	60	Залік
ОК 23	Прикладна криптологія	3	90	Екзамен
ОК 24	Мережна безпека	4,5	135	Екзамен, курсовий проєкт
ОК 25	Бази даних: побудова, адміністрування, захист	4	120	Екзамен
ОК 11	Українські історико-культурні та політико-соціальні студії	3	90	Залік
ВК 2.10	Дисципліна № 10	4	120	Залік
ВК 2.11	Дисципліна № 11	4	120	Залік
ВК 2.12	Дисципліна № 12	4	120	Залік
ОК 35	Виробнича практика	3	90	Диф. залік
	Разом	**31,5**	**945**	

IV курс, 1 семестр				
ОК 01	Іноземна мова	2	60	Залік
ОК 12	Екологія, безпека життєдіяльності та охорона праці	3	90	Залік
ОК 26	Теорія ризиків та її застосування в кібербезпеці	3	90	Екзамен
ОК 27	Системи технічного захисту інформації	4	120	Екзамен
ОК 26	Теорія кібербезпеки	3	90	Екзамен
ОК 29	Кібероперації	4	120	Залік
ВК 2.13	Дисципліна № 13	4	120	Залік
ВК 2.14	Дисципліна № 14	4	120	Залік
ВК 2.15	Дисципліна № 15	4	120	Залік
	Разом	**31**	**930**	
IV курс, 2 семестр				
ОК 01	Іноземна мова	1	30	Екзамен
ОК 29	Кібероперації	6	180	Екзамен, курсовий проєкт
ОК 30	Стандарти та нормативно-правове забезпечення кібербезпеки	3	90	Залік
ОК 31	Управління кібербезпекою	3	90	Залік
ОК 32	Комплексні системи захисту інформації	4	120	Екзамен
ОК 36	Переддипломна практика	6	180	Диф. залік
ОК 37	Кваліфікаційна робота	6	180	Кваліфіка-ційна атестація
	Єдиний державний кваліфікаційний іспит	0	0	Кваліфіка-ційна атестація
	Разом	**29**	**870**	
	Загальний обсяг:	**240**	**7200**	

*** – для здобувачів вищої освіти, звільнених від проходження БЗВП та заочної форми навчання, пропонуються інші дисципліни вільного вибору*

СТРУКТУРНО-ЛОГІЧНА СХЕМА



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 решту ОК поточного і наступних семестрів.

3. ВІДПОВІДНІСТЬ ПРОГРАМНИХ КОМПЕТЕНТНОСТЕЙ КОМПОНЕНТАМ ОСВІТНЬОЇ ПРОГРАМИ

Матриця відповідності компетентностей обов'язковим компонентам

	ЗК01	ЗК02	ЗК03	ЗК04	ЗК05	ЗК06	ЗК07	ЗК08	ЗК09	ЗК10	СК01	СК02	СК03	СК04	СК05	СК06	СК07	СК08	СК09	СК10	СК11
ОК 01				+					+												
ОК 02			+			+	+		+												
ОК 03								+													
ОК 04	+	+			+																
ОК 05	+	+			+														+		
ОК 06	+	+			+			+													
ОК 07						+	+	+	+												
ОК 08	+	+	+					+	+												
ОК 09	+	+			+			+		+											
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	+	+			+			+				+	+								
ОК 29	+	+			+			+		+	+	+	+	+	+	+		+		+	+
ОК 30	+	+									+		+			+					
ОК 31	+	+						+			+		+		+	+	+				
ОК 32	+	+						+			+		+		+	+	+			+	
ОК 33	+	+	+	+	+	+	+	+	+	+		+		+	+						+
ОК 34	+	+	+	+	+	+	+	+	+	+		+		+	+						+
ОК 35	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ОК 36	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ОК 37	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+

4. ЗАБЕЗПЕЧЕНІСТЬ ПРОГРАМНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ ВІДПОВІДНИМИ КОМПОНЕНТАМИ ОСВІТНЬОЇ ПРОГРАМИ

Матриця забезпечення програмних результатів навчання обов'язковими компонентами

	РН 01	РН 02	РН 03	РН 04	РН 05	РН 06	РН 07	РН 08	РН 09	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
ОК 01		+																				+				
ОК 02	+		+																			+				
ОК 03																							+			
ОК 04				+	+			+																		
ОК 05				+	+			+												+						
ОК 06				+	+		+	+																		
ОК 07			+																			+		+		
ОК 08	+			+		+																+				
ОК 09				+	+		+	+																	+	
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				+	+	+	+	+		+	+															
ОК 29				+	+	+	+	+	+	+	+	+	+	+	+			+	+		+				+	+
ОК 30				+	+				+		+					+										
ОК 31				+	+	+			+		+			+			+									
ОК 32				+	+	+			+		+			+		+	+				+					
ОК 33	+	+	+	+	+	+	+	+		+		+	+	+								+			+	+
ОК 34	+	+	+	+	+	+	+	+		+		+	+	+	+							+			+	+
ОК 35	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ОК 36	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ОК 37	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+