**Профіль освітньої програми**

**Назва освітньої програми:** *Безпека інформаційних і комунікаційних систем*

**Освітній ступінь:** *Магістр*

**Галузь знань:** *12 Інформаційні технології*

**Спеціальність:** *125 Кібербезпека*

**Спеціалізація:** *Безпека інформаційних і комунікаційних систем*

| **Загальна інформація** | |
|---|---|
| **Повна назва вищого навчального закладу** | Державний вищий навчальний заклад «Ужгородський національний університет» |
| **Ступінь вищої освіти та назва кваліфікації мовою оригіналу** | Ступінь вищої освіти: магістр.<br>Освітня кваліфікація: магістр з кібербезпеки<br>Професійна кваліфікація : професіонал із організації інформаційної безпеки |
| **Офіційна назва освітньої програми** | Безпека інформаційних і комунікаційних систем |
| **Тип диплому та обсяг освітньої програми** | Диплом магістра, одиничний, 90 кредитів ЄКТС.<br>Термін навчання 1 рік і 4 місяців. |
| **Наявність акредитації** | Акредитаційна комісія України<br>Сертифікат про акредитацію серія НД № 0789904<br>Термін дії сертифікату до 01.07.2022р. |
| **Цикл/рівень** | Національна рамка кваліфікацій України – 7 рівень,<br>FQ-EHEA – другий цикл,<br>EQF-LLL – 7 рівень. |
| **Передумови** | Наявність першого (бакалаврського) рівня вищої освіти.<br>Умови вступу визначаються «Правилами прийому до Ужгородського національного університету» |
| **Мова(и) викладання** | Українська |
| **Термін дії освітньої програми** | Відповідно до терміну дії сертифіката про акредитацію |
| **Інтернет-адреса постійного розміщення опису освітньої програми** | http://www.uzhnu.edu.ua/uk/infocentre/15068 |
| **Мета освітньої програми** | |
| Навчання та підготовка професіоналів в області БІКС, які мають базові знання та навички в застосуванні законодавчої бази в галузі інформаційної безпеки, розробці технологій і засобів захисту інформації, застосуванні стандартних і проектуванні нових криптографічних алгоритмів для захисту інформації в комп'ютерних системах і мережах, з метою ефективної боротьби з кібезлочинністю. | |
| **Характеристика освітньої програми** | |
| **Предметна область (галузь знань, спеціальність, спеціалізація(за наявності))** | 12 Інформаційні технології, 125 Кібербезпека, спеціалізація 8.17010201 (Безпека інформаційних і комунікаційних систем).<br>Цикл дисциплін загальної підготовки – 12,5 кредитів ЄКТС, 375 год. З них дисципліни вільного вибору студента – 3,5 кредити ЄКТС, 105 год. |

| | |
|---|---|
| | Цикл дисциплін професійної підготовки – 77,5 кредитів ЄКТС, 2325 год. З них дисципліни вільного вибору студента – 19 кредитів ЄКТС, 570 год. |
| **Орієнтація освітньої програми** | Освітньо-професійна програма орієнтована на поглиблене вивчення дисциплін природничо-наукової підготовки з поглибленим вивченням дисциплін фахової підготовки у тому числі і базових дисциплін суміжних напрямів. |
| **Основний фокус освітньої програми та спеціалізації** | Протягом навчання за програмою «Безпека інформаційних і комунікаційних систем» магістр набуває практичних навичок з організації безпеки операційних систем і баз даних, технічного захисту інформації, антивірусного захисту, безпеки Web-сервісів. |
| **Особливості програми** | Магістри адаптовуються до зростаючих потоків інформації та наслідків науково- технічного прогресу, постійно засвоюють новітні світові науково-технічні досягнення в галузі інформаційної безпеки та захисту інформації, використовують сучасні інформаційні технології, знання фундаментальних законів і понять природничих наук. |
| **Придатність випускників до працевлаштування та подальшого навчання** | |
| **Придатність до працевлаштування** | Професіонал здатний виконувати професійну роботу і може займати первинні посади:<br>– Інженер з комп’ютерних систем<br>– Інженер з програмного забезпечення комп’ютерів<br>– Інженер-дослідник з комп’ютеризованих систем та автоматики<br>– Інженер-програміст<br>– Інженер із застосування комп’ютерів<br>– Інженер електрозв’язку<br>– Інженер засобів радіо та телебачення<br>– Інженер лінійних споруд електрозв’язку та абонентських пристроїв<br>– Інженер мережі стільникового зв’язку<br>– Інженер-електронік<br>– Інженер інформаційно-телекомунікаційних систем<br>– Інженер інформаційно-телекомунікаційних технологій |

| | |
|---|---|
| | – Професіонал із організації захисту інформації з обмеженим доступом<br>– Професіонал із організації інформаційної безпеки<br>– Асистент |
| **Подальше навчання** | Випускник з дипломом магістра може продовжити навчання в аспірантурі для отримання наукового ступеня доктора філософії.<br>Можливість підвищення кваліфікації та отримання додаткової післядипломної освіти. |
| **Викладання та оцінювання** | |
| **Викладання та навчання** | Студентсько-центроване навчання, самонавчання, проблемно-орієнтоване навчання, індивідуально-творчий підхід, навчання через виробничу та педагогічну практики. |
| **Оцінювання** | Накопичувальна бально-рейтингова система, що передбачає оцінювання студентів за усі види аудиторної та позааудиторної навчальної діяльності, спрямованої на опанування навчального навантаження з освітньої програми: поточний, модульний, підсумковий контроль, комплексний кваліфікаційний екзамен;<br>Усні та письмові екзамени, заліки, презентації, проектна робота диференційований залік з педагогічної практики, переддипломної практики, курсова робота. |
| **Програмні компетентності** | |
| **Інтегральна компетентність** | Здатність розв’язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної та\або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов. |
| **Загальні компетентності (ЗК)** | – Здатність до професійного спілкування іноземною мовою; (ЗК1)<br>– Здатність до здобування нових знань, накопичення наукових та педагогічних вмінь і навичок та їх застосування в практичних ситуаціях; (ЗК2)<br>– Здатність до виявлення, генерування, дослідження та вирішення проблем за професійним спрямуванням;(ЗК3) |

| | |
|---|---|
| **Фахові компетентності (ФК)** | – Здатність до застосування сучасних інформаційних технологій і технологій безпеки у сфері захисту інформації;(ФК1)<br>– Здатність до виявлення уразливостей та забезпечення безпеки проводових і бездротових мереж, розслідування інцидентів інформаційної та кібербезпеки та протидії злоякісному програмному забезпеченню; (ФК2)<br>– Здатність до забезпечення безпеки Web ресурсів, відновлення їх штатного функціонування в результаті збоїв та відмов різних класів і походження; (ФК3)<br>– Здатність до забезпечення безпеки мережевих ресурсів та криптографічного захисту інформації в системах інформаційної та/або кібербезпеки; (ФК4)<br>– Здатність до забезпечення захисту інформації, що обробляється в інформаційно-комунікаційних системах, здійснення адміністрування таких систем та проведення їх експлуатації; (ФК5) |
| **Програмні результати навчання** | |
| **Загальні результати навчання** | – вміти застосовувати знання іноземних мов для забезпечення ефективності професійної комунікації; (ПРН 1)<br>– вміти діагностувати й інтерпретувати ситуації, планувати та здійснювати наукові дослідження, критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; (ПРН 2)<br>– вміти виявляти і формулювати актуальні наукові проблеми, генерувати та інтегрувати нові ідеї та нові знання у сфері захисту інформації, інформаційної та/або кібербезпеки; (ПРН 3) |
| **Фахові результати навчання** | – вміти застосовувати спеціалізовані програмні пакети, сучасні інформаційні та/або безпекові технології у сфері захисту інформації; (ПРН 4)<br>– знати спеціалізоване мережеве обладнання, що застосовується для забезпечення безпеки безпроводових і мобільних мереж; (ПРН 5)<br>– знати методи і способи розробки та тестування програмного забезпечення з виявлення і усунення активності, що загрожує безпеці |

| | |
|---|---|
| | системи (антивіруси, firewalls, сніфери, сканери портів); (ПРН 6)<br>– вміти проводити семантичний аналіз файлів;( ПРН 7)<br>– вміти виявляти злоякісне програмне забезпечення й файли за їх структурою та поведінкою; (ПРН 8)<br>– вміти відновлювати пошкоджену інформацію;(ПРН 9)<br>– вміти моделювати уразливості ПЗ та використовувати шаблони проектування для захисту ПЗ; (ПРН 10)<br>– знати існуючі уразливості Web ресурсів (sql ін'єкції, брутфорс, xss й т.д) та способи боротьби з ними на етапі розробки та в процесі експлуатації, знати шаблони проектування безпечних Web додатків; (ПРН 11)<br>– знати методи і способи тестування мережевих ресурсів на наявність уразливостей безпеки, вміти знаходити шляхи для їх усунення;(ПРН 12)<br>– вміти проектувати перспективні криптосистеми та застосовувати сучасні технології криптографічного захисту інформації в системах інформаційної та/або кібербезпеки. (ПРН 13)<br>– знати уразливості й методи їх застосування в різних телекомунікаційних технологіях, знати способи боротьби з даними уразливостями, а також спеціалізоване мережеве обладнання, що застосовується для забезпечення безпеки корпоративних мереж; (ПРН 14) |
| **Ресурсне забезпечення реалізації програми** | |
| **Кадрове забезпечення** | Склад проектної групи освітньої програми, професорсько-викладацький склад, що задіяний до викладання навчальних дисциплін за спеціальністю відповідають Ліцензійним умовам провадження освітньої діяльності на першому (бакалаврському) рівні вищої освіти. |

| | |
|---|---|
| **Матеріально-технічне забезпечення** | Забезпеченість навчальними приміщеннями, комп'ютерними робочими місцями, мультимедійним обладнанням відповідає потребам. Наявна вся необхідна соціально-побутова інфраструктура, кількість місць в гуртожитку відповідає вимогам. Для проведення практичних і лабораторних робіт, інформаційного пошуку та обробки результатів наявні спеціалізовані комп'ютерні класи факультету з необхідним програмним забезпеченням та необмежено відкритим доступом до Інтернет-мережі. |
| **Інформаційне та навчально- методичне забезпечення** | -офіційний веб-сайт http://www.uzhnu.edu.ua містить інформацію про освітні програми, навчальну, наукову і виховну діяльність, структурні підрозділи, правила прийому, контакти;<br>-необмежений доступ до мережі Інтернет;<br>− наукова бібліотека, читальні зали;<br>− навчальні і робочі плани;<br>− графіки навчального процесу;<br>− навчально-методичні комплекси дисциплін;<br>− дидактичні матеріали для самостійної та індивідуальної роботи студентів з дисциплін, програми практик;<br>− методичні вказівки щодо виконання кваліфікаційних робіт. |
| **Академічна мобільність** | |
| **Національна кредитна мобільність** | Підвищення кваліфікації (стажування) науково-педагогічних<br>працівників у вітчизняних закладах вищої освіти на основі двосторонніх договорів між Ужгородським національним університетом та університетами України. |
| **Міжнародна кредитна мобільність** | Угода щодо семестрового академічного обміну між Поморською Академією у м. Слупськ (Польща) та Ужгородським національним університетом. |
| **Навчання іноземних здобувачів вищої освіти** | Можливе навчання іноземних громадян. Навчання іноземних студентів проводиться на загальних умовах або за індивідуальним графіком. |

**Гарант освітньої програми:** старший викладач Трефілов Ю. К.

(науковий ступінь, вчене звання, прізвище, ініціали гаранта ОП)