**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**
**ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД**
**«Ужгородський національний університет»**

**ЗАТВЕРДЖЕНО**
Вченою радою ДВНЗ
«Ужгородський національний університет»,
протокол № 6 від 23.05. 2017р.
Голова Вченої ради, ректор
_____В.І.Смоланка

# ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

**Підготовки здобувачів другого (магістерського) рівня вищої освіти**

| | |
|---|---|
| **ГАЛУЗЬ ЗНАНЬ** | 12 Інформаційні технології |
| **СПЕЦІАЛЬНІСТЬ** | 125 Кібербезпека |
| **НАЗВА ОПП** | Системи технічного захисту інформації, автоматизація її обробки |

Ужгород 2017 р.

Освітньо професійна програма ”Системи технічного захисту інформації, автоматизація її обробки ” підготовки другого (магістерського) рівня вищої освіти спеціальності 125 ”Кібербезпека” розроблена згідно вимог Закону України ”Про вищу освіту”.

Програма відповідає другому циклу вищої освіти та сьомому кваліфікаційному рівню за Національною рамкою кваліфікацій України.

**Укладачі програми:**

1. Самохвалов Михайло Прокопович, старший викладач кафедри твердотільної електроніки та інформаційної безпеки
2. Попович Наталія Іванівна, кандидат фіз.-мат. наук доцент кафедри твердотільної електроніки та інформаційної безпеки;
3. Різак Василь Михайлович, доктор фіз.-мат. наук професор, завідувач кафедри твердотільної електроніки та інформаційної безпеки;

## 1.Профіль освітньої програми зі спеціальності № 125 ”Кібербезпека”(за спеціалізацією ”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 захисту інформації з обмеженим доступом. |
| **Офіційна назва освітньої програми** | Системи технічного захисту інформації, автоматизація її обробки |
| **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** | |
| Освітня програма націлена на розвиток професійних і творчих здібностей студентів щодо оволодіння методологією наукової діяльності та їх підготовки до розв’язання проблем в галузі кібербезпеки. | |
| **Характеристика освітньої програми** | |
| **Предметна область (галузь знань, спеціальність, спеціалізація(за наявності))** | 12 Інформаційні технології, 125 Кібербезпека, спеціалізація 8.17010201 (Системи технічного захисту інформації, автоматизація її обробки).<br>Цикл дисциплін загальної підготовки – 16 кредитів ЄКТС, 480 год. З них дисципліни вільного вибору студента – 7 кредитів ЄКТС, 210 год.<br>Цикл дисциплін професійної підготовки – 74 кредити ЄКТС, 2220 год. З них дисципліни вільного вибору студента – 16 кредитів ЄКТС, 480 год. |
| **Орієнтація освітньої програми** | Освітньо-професійна програма орієнтована на отримання студентами необхідних знань щодо |

| | |
|---|---|
| | проявлення технічних каналів витоку інформації, шляхів деструктивного впливу на інформацію та засоби її обробки, застосування заходів та засобів, спрямованих на технічний захист інформації на об'єктах інформаційної діяльності. |
| **Основний фокус освітньої програми та спеціалізації** | Програма спрямована на поєднання інженерного мислення і практики проектування, розробки та експлуатації складових кіберпростору з метою зменшення небажаних наслідків від максимально можливого числа загроз і впливів. |
| **Особливості програми** | Характерною особливістю даної програми є поглиблене вивчення нормативних документів та стандартів з захисту інформації, принципів побудови систем технічного захисту інформації, підходів до управління ризиками, дій для захисту інформаційних ресурсів організацій і користувачів. |
| **Придатність випускників до працевлаштування та подальшого навчання** | |
| **Придатність до працевлаштування** | Професіонал здатний виконувати професійну роботу і може займати первинні посади:<br>– Інженер з організації та управління діяльності служб інформаційної безпеки;<br>– Інженер-проектувальник комплексних систем захисту інформації;<br>– Інженер з експлуатації систем захисту інформації,<br>– Викладач вищого навчального закладу.<br>– 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 виявляти, та вирішувати проблеми у галузі забезпечення інформаційної безпеки, застосовуючи навички використання інформаційних і комунікаційних технологій. |
| **Загальні компетентності (ЗК)** | – Знання та розуміння предметної області та розуміння професійної діяльності; (ЗК 1)<br>– Визначеність і наполегливість щодо поставлених завдань і взятих обов'язків; (ЗК 2)<br>– Здатність до пошуку, оброблення та аналізу інформації з різних джерел.(ЗК 3) |
| **Фахові компетентності (ФК)** | – Здатність до створення інноваційних продуктів в сфері інформаційної та кібернетичної безпеки, заснованої на трансформації наукових досліджень і розробок, провідного досвіду; (ФК 1)<br>– Здатність здійснювати технологічне управління побудовою систем захисту інформації на основі аналізу джерел загроз та засобів їх впливу на об'єкти інформаційної безпеки та ризиків інформаційної безпеки; (ФК 2)<br>– Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та кібернетичної безпеки; (ФК 3)<br>– Здатність проведення атестації та сертифікації технічних засобів та інформаційних ресурсів; (ФК 4) |

| | |
|---|---|
| | – Здатність до проектування захищених розподілених комп'ютерних мереж; (ФК 5)<br>– Здатність забезпечувати захист інформаційних потоків даних в інформаційно-телекомунікаційних (автоматизованих) системах, а також безпосередньо в мережах передачі даних різних класів з метою реалізації встановленої політики безпеки; (ФК 6)<br>– Здатність до проведення аудиту інформаційної безпеки на підприємстві та проведення службових розслідувань інцидентів, пов'язаних з порушенням інформаційної безпеки.(ФК 7) |
| **Програмні результати навчання** | |
| **Загальні результати навчання** | – Вміня використовувати методи та правила управління інформацією та роботу з документами за професійним спрямуванням. Володіти методиками та сучасними засобами інформаційних технологій; (ПРН 1)<br>– Знати та розуміти закономірності, методи та підходи творчої та креативної діяльності, системного мислення у професійній сфері; (ПРН 2)<br>– Вміти використовувати методи та методики проведення наукових та прикладних досліджень; (ПРН 3)<br>– Знати методи проведення досліджень та вміти аналізувати складність технічних систем, розуміти складність задач оптимізації цих систем та їх елементів, та вдосконалювати методики їх проведення; (ПРН 4) |
| **Фахові результати навчання** | – Володіння основними методами побудови і аналізу моделей систем захисту інформації, використовувати допоміжні структури (моделі), ієрархічні моделі та моделі взаємодії відкритих систем (OSI/ISO) для забезпечення гарантованого захисту розподілених систем; (ПРН 5)<br>– Володіння актуальними питаннями побудови, інструментальними засобами аналізу, проектування та аналізу вразливостей захищених інформаційних ресурсів, сучасними поглядами і підходами до розв'язання проблем безпеки інформації; (ПРН 6) |

| | |
|---|---|
| | – Вміння забезпечувати послідовність побудови систем захисту інформації, формувати моделі порушника та загроз, використовувати сучасні методи та методики аналізу ризиків, оцінювання та управління ризиками; (ПРН 7)<br>– Вміння проектувати системи захисту для операційних систем та баз даних різної топології, захищених розподілених інформаційних ресурсів; (ПРН 8)<br>– Вміти проводити атестацію та сертифікацію об'єкта інформаційної діяльності спираючись на облік та обстеження виробів, продукції, обладнання об’єкта в тому числі і спеціального призначення з фіксуванням результатів у відповідних документах; (ПРН 9)<br>– Вміння застосовувати апаратне та програмне забезпечення для захисту інформації в розподілених комп’ютерних мережах; (ПРН10)<br>– Вміння аналізувати стан безпеки комп’ютерних систем та мереж, території та об’єктів підприємства, технічних засобів і враховувати можливий спектр загроз та їх наслідки для сервісів систем забезпечення інформаційної та кібернетичної безпеки. (ПРН11) |
| **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. |

## 2. Перелік компонент освітньо-професійної програми та їх логічна послідовність

### 2.1 Перелік компонент ОП

| Код н/д | Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота) | Кількість кредитів | Форма підсумкового контролю |
|---|---|---|---|
| **1** | **2** | **3** | **4** |
| **1 Обов'язкові компоненти ОП** | | | |
| **1.1 Цикл загальної підготовки** | | | |
| ОК 1.1.1 | Охорона праці в галузі | 3 | Іспит |
| ОК 1.1.2. | Методика викладання у вищій школі | 3 | Залік |
| ОК 1.1.3. | Основи наукових досліджень та організація науки | 3 | Залік |
| **1.2. Цикл професійної підготовки** | | | |
| ОК 1.2.1. | Теорія захисту інформаційних ресурсів обмеженого доступу | 7 | Іспит, диференційований залік |
| ОК 1.2.2. | Радіомоніторинг та радіопротидія на об'єктах інформаційної діяльності | 6 | Іспит |
| ОК 1.2.3. | Ліцензування, атестація та сертифікація у сфері безпеки об'єктів інформаційної діяльності | 5 | Залік |
| ОК 1.2.4. | Технології створення та застосування комплексів захисту інформації з обмеженим доступом та охорони об'єктів інформаційної діяльності | 4 | Іспит |
| ОК 1.2.5. | Автоматизація обробки даних з обмеженим доступом | 6 | Іспит |
| ОК 1.2.6. | Педагогічна практика у ВНЗ (2 тижні) | 3 | Диференційований залік |
| ОК 1.2.7. | Науково-дослідна практика (2 тижні) | 3 | Диференційований залік |
| ОК 1.2.8. | Переддипломна практика (3тижні) | 4,5 | Диференційований залік |

| | | | |
|---|---|---|---|
| ОК 1.2.9. | Виконання магістерської роботи | 16,5 | |
| ОК 1.2.10. | Атестація | 3 | |
| **Загальний обсяг обов`язкових компонент:** | | **67 кредитів** | |
| **2.Вибіркові компоненти ОП** | | | |
| **2.1. Цикл загальної підготовки** | | | |
| ВБ 2.1.1. | Наукові дослідження за темою / НДРС | 7 | Диференційований залік |
| **2.2. Дисципліни професійної ї підготовки** | | | |
| ВБ 2.2.1. | Широкосмугові сигнали в системах ТЗІ /Волоконно-оптичні та бездротові мережі | 6 | Іспит |
| ВБ 2.2.2 | Оптоволоконні комунікаційні системи/ Волоконно-оптичні лінії зв`язку | 5 | Іспит |
| ВБ 2.2.3 | Системи захисту мовної інформації / Захист мовної інформації на об`єктах інформаційної діяльності | 5 | Іспит |
| **Загальний обсяг вибіркових компонент** | | **23 кредити** | |
| **Загальний обсяг освітньої програми** | | **90 кредит** | |

## 2.2 Структурно-логічна схема ОП

| Семестр | Номер дисципліни згідно навчального плану |
|---|---|
| **1** | 1.1.1., 1.1.3., 2.1.1., 1.2.1., 1.2.5., 2.2.1., 2.2.2. |
| **2** | 1.1.2., 2.1.1., 1.2.1., 1.2.2., 1.2.3., 1.2.4., 2.2.3. |
| **3** | 1.2.6., 1.2.7., 1.2.8., 1.2.9. |
| **4** | 1.2.9., 1.2.10. |

## 3. Форма атестації здобувачів вищої освіти

Атестація випускників освітньої програми спеціальності №125 «Кібербезпека», спеціалізація 8.17010201 «Системи технічного захисту інформації, автоматизація її обробки», проводиться у формі захисту кваліфікаційної магістерської роботи та завершується видачею документа встановленого зразка про присудження ступеня магістра із присвоєнням кваліфікації: Магістр з кібербезпеки за спеціалізацією професіонал із організації захисту інформації з обмеженим доступом.

Захист кваліфікаційної (магістерської) роботи відбувається як публічна презентація.

## 4. Матриця відповідності програмних компетентностей компонентам освітньої програми

| | ОК 1.1.1. | ОК 1.1.2. | ОК 1.1.3. | ОК 1.2.1. | ОК 1.2.2. | ОК 1.2.3. | ОК 1.2.4. | ОК 1.2.5. | ОК 1.2.6. | ОК 1.2.7. | ОК 1.2.8. | ОК 1.2.9. | ОК 1.2.10. | ВБ 2.1.1. | ВБ 2.2.1. | ВБ 2.2.2. | ВБ 2.2.3. |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ЗК 1 | + | | | | | | | | | + | | | | + | | | |
| ЗК 2 | | + | | | | | | | + | + | | | | | | | |
| ЗК 3 | | + | + | | | | | | | | + | + | | + | | | |
| ФК 1 | | | + | | | | | | | + | + | | | + | | | |
| ФК 2 | | | | | + | | | + | | | | | | + | | + | |
| ФК 3 | + | | | + | | + | | | | | | | | | | | |
| ФК 4 | | | | | | + | | + | | | | | | | | | + |
| ФК 5 | | | | | | | + | | | | | | | | + | + | |
| ФК 6 | | | | + | | | + | + | | | | | | | | | + |
| ФК 7 | | | | + | + | | + | | | | | | | | | | |

## 1. Матриця забезпечення програмних результатів навчання (ПРН) відповідними компонентами освітньої програми

| | ОК 1.1.1. | ОК 1.1.2. | ОК 1.1.3. | ОК 1.2.1. | ОК 1.2.2. | ОК 1.2.3. | ОК 1.2.4. | ОК 1.2.5. | ОК 1.2.6. | ОК 1.2.7. | ОК 1.2.8. | ОК 1.2.9. | ОК 1.2.10. | ВБ 2.1.1. | ВБ 2.2.1. | ВБ 2.2.2. | ВБ 2.2.3. |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ПРН 1 | + | | | | | + | | | | | | | | | | | |
| ПРН 2 | | + | + | | | | | | | | | | | + | | | |
| ПРН 3 | | | + | | | | | | | + | | + | | | + | | |
| ПРН 4 | | | | | + | | | | + | + | | | | | | | |
| ПРН 5 | | | | | | | | + | | | | + | | + | | | |
| ПРН 6 | | | | + | | | + | | | + | | | | | | | + |
| ПРН 7 | | | | | + | | | | | | + | | | + | | | + |
| ПРН 8 | | | | + | | | + | | | | + | + | | | | + | |
| ПРН 9 | | | | | | + | | | | | | | | | | + | + |
| ПРН 10 | | | | + | | | + | + | | | | | | | | | + |
| ПРН 11 | | | | | + | + | | | | | | | | | | | + |