**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 першого (бакалаврського) рівня вищої освіти**

**ГАЛУЗЬ ЗНАНЬ** 12 Інформаційні технології

**СПЕЦІАЛЬНІСТЬ** 125 Кібербезпека

**НАЗВА ОПП** Безпека інформаційних і комунікаційних систем

Ужгород 2017 р.

Освітньо професійна програма ”Безпека інформаційних і комунікаційних систем” підготовки першого (бакалаврського) рівня вищої освіти спеціальності 125 ”Кібербезпека” розроблена згідно вимог Закону України ”Про вищу освіту”.

Програма відповідає першому циклу вищої освіти та шостому кваліфікаційному рівню за Національною рамкою кваліфікацій України.

**Укладачі програми:**

Різак Василь Михайлович, доктор фіз.-мат. наук професор, завідувач кафедри твердотільної електроніки та інформаційної безпеки (керівник проектної групи);

Січка Михайло Юрійович, кандидат фіз.-мат. наук доцент кафедри твердотільної електроніки та інформаційної безпеки;

Трефілов Юрій Костянтинович, старший викладач 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: бакалавр.<br>Освітня кваліфікація: бакалавр з кібербезпеки<br>Професійна кваліфікація : фахівець із організації інформаційної безпеки |
| **Офіційна назва освітньої програми** | Безпека інформаційних і комунікаційних систем |
| **Тип диплому та обсяг освітньої програми** | Диплом бакалавра, одиничний, 240 кредитів ЄКТС.<br>Термін навчання 3 роки і 10 місяців. |
| **Наявність акредитації** | Акредитаційна комісія України<br>Сертифікат про акредитацію серія НД № 0791769<br>Термін дії сертифікату до 01.07.2024р. |
| **Цикл/рівень** | Національна рамка кваліфікацій України – 6 рівень,<br>FQ-EHEA – перший цикл,<br>EQF-LLL – 6 рівень. |
| **Передумови** | Наявність повної загальної середньої 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 фахівців спеціальності 125 ”Кібербезпека”(за спеціалізацією ”Безпека інформаційних і комунікаційних систем”), здатних розробляти, використовувати і впроваджувати технології інформаційної безпеки і\або кібербезпеки, для вирішення низки актуальних завдань у сфері інформаційної безпеки,. Засвоїти знання з основ законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності. | |
| **Характеристика освітньої програми** | |
| **Предметна область (галузь знань, спеціальність, спеціалізація(за наявності))** | 12 Інформаційні технології, 125 Кібербезпека, спеціалізація (Безпека інформаційних і комунікаційних систем).<br>Обсяг освітньої програми бакалавра:<br>на базі повної загальної середньої освіти з терміном навчання 11 років – 240 кредитів ЄКТС<br>Мінімум 80% обсягу освітньої програми має бути спрямовано на забезпечення загальних та спеціальних (фахових) компетентностей за спеціальністю визначеною стандартом вищої освіти. |

| | |
|---|---|
| | Для здобуття ступеня бакалавра на основі ступеня молодшого бакалавра ВНЗ має право скорочувати обсяг освітньої програми. При цьому програма має забезпечувати набуття визначених цим стандартом результатів навчання, а її загальний обсяг має бути не<br>меншим, ніж 120 кредитів.<br>Об’єкти професійної діяльності випускників:<br>– об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси і технології;<br>– технології забезпечення безпеки інформації об'єктів різного рівня (система, об'єкт системи, компонент об'єкта), що пов'язані з інформаційно-комунікаційними технологіями, що використовуються для забезпечення функціонування об'єктів інформаційної діяльності в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;<br>– процеси управління інформаційною безпекою та\або кібербезпекою в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах, що підлягають захисту.<br>Цілі навчання підготовка фахівців, здатних розробляти, використовувати і впроваджувати технології інформаційної безпеки і\або кібербезпеки .<br>Теоретичний зміст предметної діяльності<br>Знання:<br>– законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності;<br>– принципів забезпечення та супроводу систем та комплексів інформаційної безпеки та\або кібербезпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики безпеки;<br>– теорії та процедури розподілу прав управління доступом, моделей та принципів управління доступом до інформаційних ресурсів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах |

| | |
|---|---|
| | згідно встановленої політики інформаційної безпеки і\або кібербезпеки;<br>– процесів функціонування системи управління інформаційною безпекою та\або кібербезпекою та основ теорії ризиків;<br>– методів та засобів виявлення та ідентифікації вразливостей і загроз інформаційній безпеці на об'єктах інформаційної діяльності;<br>– методів та засобів оцінювання та забезпечення відповідного рівня захищеності інформації в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;<br>– методів та засобів технічного та криптографічного захисту інформації із забезпечення інформаційної безпеки і\або кібербезпеки.<br><br><u>Методи, методики та технології:</u><br>Методи, методики та технології забезпечення інформаційної безпеки та/ або кібербезпеки<br><u>Інструменти та обладнання</u>:<br>– обладнання, необхідне для моніторингу функціонування і підтримки інформаційно-телекомунікаційних систем і мереж;<br>системи забезпечення інформаційної безпеки та/ або кібербезпеки. |
| **Орієнтація освітньої програми** | Освітньо-професійна програма орієнтована на здобуття студентами професійних знань, умінь, навичок та інших компетентностей для успішного здійснення професійної діяльності у галузі. |
| **Основний фокус освітньої програми та спеціалізації** | Базові знання та навички в застосуванні законодавчої бази в галузі інформаційної та комунікаційної безпеки, розробці технологій і засобів захисту інформації, застосуванні стандартних і проектуванні нових криптографічних алгоритмів для захисту інформації. |
| **Особливості програми** | Програма передбачає не тільки здобуття базових знань та навичок з комп'ютерних технологій, достатніх для успішної роботи сучасного ІТ-фахівця, але і професійну підготовку в галузі безпеки інформаційних систем і комунікацій. |

| Придатність випускників до працевлаштування та подальшого навчання | |
|---|---|
| **Придатність до працевлаштування** | Фахівець здатний виконувати наступну професійну роботу:<br>– консультування в питаннях безпеки промислових об'єктів, помешкань і громадських будинків з оцінкою їхньої безпеки;<br>– охоронну діяльність, що здійснюється за допомогою комп'ютеризованих захисних пристроїв;<br>– послуги із захисту інформації в комп'ютерних та інших технічних засобах від копіювання та несанкціонованого доступу. |
| **Подальше навчання** | Випускник з дипломом бакалавра може продовжити навчання за освітньо-професійною або освітньо-науковою програмою ступеня магістра |
| **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, курсова робота. |
| **Програмні компетентності** | |
| **Інтегральна компетентність** | Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і\або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов. |
| **Загальні компетентності (ЗК)** | – досягнення необхідних знань і розуміння ролі інформаційних технологій в суспільстві з метою адекватної роботи за майбутніми |

| | |
|---|---|
| | професіями та врахування її впливу на соціальні проблеми (ЗК1)<br>– здатність до абстрактного мислення, аналізу та синтезу на основі логічних аргументів та перевірених фактів (ЗК2)<br>– уміння і здатність до прийняття рішень, навички планування та управління (ЗК3)<br>– здатність постійно підвищувати свою професійну кваліфікацію, світоглядну, громадянську і державницьку позицію шляхом самоосвіти і самовдосконалення (ЗК4)<br>– Здатність застосовувати знання у практичних ситуаціях.(ЗК5)<br>– Знання та розуміння предметної області та розуміння професії.(ЗК6)<br>– Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово(ЗК7)<br>– Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням(ЗК8)<br>– Здатність до пошуку, оброблення та аналізу інформації з різних джерел.(ЗК9) |
| **Фахові компетентності (ФК)** | – Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.(ФК1)<br>– Здатність до використання інформаційно-комунікаційних технологій, сучасних архітектур, методів і моделей безпеки з метою передачі, зберігання, обробки електронних інформаційних ресурсів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах(ФК2)<br>– Здатність до використання програмних та програмно-апаратних комплексів захисту електронних інформаційних ресурсів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі сучасних науково-ємних технологій, а також методів і моделей інформаційної безпеки та/ або кібербезпеки.(ФК3) |

| | |
|---|---|
| | – Здатність забезпечувати (штатне \ позаштатне ) функціонування системи управління доступом, а також здійснювати протидію несанкціонованим вторгненням до електронних інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики безпеки.(ФК4)<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.(ФК5)<br>– Здатність відновлювати штатне функціонування інформаційних, інформаційно-комунікаційних систем після реалізації загроз порушником, здійснення кібератак, збоїв та відмов різних класів та походження.(ФК6)<br>– Здатність забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.) для реалізації встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.(ФК7)<br>– Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку з метою реалізації встановленої політики інформаційної та\або кібербезпеки.(ФК8)<br>– Здатність здійснювати професійну діяльність на основі встановленої системи управління інформаційною безпекою згідно вітчизняних та міжнародних вимог і стандартів.(ФК9)<br>– Здатність забезпечувати захист електронних інформаційних ресурсів в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах на основі технологій, методів та засобів |

| | |
|---|---|
| | криптографічного та технічного захисту інформації.(ФК10)<br>– Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем в умовах реалізації загроз різних класів та протидії порушникам.(ФК11)<br>– Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та електронним інформаційним ресурсам .(ФК12) |
| **Програмні результати навчання** | |
| **Загальні результати навчання** | – застосувати концептуальні знання з навчальних дисциплін загальної підготовки для засвоєння дисциплін професійної підготовки;(ПРН1)<br>– застосувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; (ПРН2)<br>– організувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблему професійній діяльності, оцінювати їхню ефективність; (ПРН3)<br>– використати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності(ПРН4)<br>– 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; (ПРН5)<br>– адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат; (ПРН6) |

| | |
|---|---|
| | - критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності(ПРН7) |
| **Фахові результати навчання** | - знати основні положення захисту інформаційних ресурсів та баз даних інформаційно-комунікаційних систем на базі спеціальних програмних і технічних засобів захисту інформації з урахуванням вимог системи нормативно-правових і організаційних заходів; (ПРН8)<br>- знати управління доступом до інформаційно-комунікаційної системи та її послуг на основі положень політики безпеки організації на базі програмних та програмно-апаратних комплексів; (ПРН9)<br>- забезпечення цілісності і конфіденційності баз даних та інформаційних потоків в інформаційно-комунікаційних системах на основі положень політики безпеки організації на базі програмних та програмно-апаратних комплексів; (ПРН10)<br>- знати управління доступом до інформаційних ресурсів та баз даних в інформаційно-комунікаційних системах, в тому числі до програмних бібліотек та додатків; (ПРН11)<br>- основні способи впровадження і супроводження системного, об’єктно-орієнтованого та прикладного програмного забезпечення інформаційно-комунікаційних систем та аналіз його ефективності; (ПРН12)<br>- забезпечення цілісності та конфіденційності системного, об’єктно-орієнтованого та прикладного програмного забезпечення при його впровадженні, використанні чи обміні; (ПРН13)<br>- знати основні положення по розробленню, впровадженню, дослідженню ефективності, супроводженню засобів та комплексів технічного захисту інформації в інформаційно-комунікаційних системах; (ПРН14)<br>- знати методи розроблення окремих складових, впровадження, супроводження та |

| | |
|---|---|
| | дослідження ефективності комплексних систем захисту інформації; (ПРН15)<br>- знати способи обстежень об'єкта інформаційної діяльності, автоматизованої системи та атестації засобів захисту інформаційних ресурсів з визначенням оцінки захищеності інформаційно-комунікаційних систем та їх ресурсів на базі використання спеціальних технічних засобів. (ПРН16)<br>- здатність розробляти та проводити експериментальні дослідження перспективних засобів та комплексів інформаційних та комунікаційних систем, проведення випробувань та обробка результатів експериментів; (ПРН17)<br>- розробляти та проводити роботу для синтезу захищених комп'ютерних та інформаційних систем, а також вміти розробляти документацію для впровадження та використання об'єктів захисту. (ПРН18) |
| **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** | | | |
| **1.1Цикл дисциплін гуманітарної та соціально-економічної підготовки** | | | |
| ОК 1.1.1 | Фізичне виховання | | |
| ОК 1.1.2. | Іноземна мова | 5 | Залік, іспит |

| | | | |
|---|---|---|---|
| ОК 1.1.3. | Ділова українська мова | 3 | Залік |
| ОК 1.1.4. | Філософія | 3 | Іспит |
| ОК 1.1.5. | Основи психології і педагогіки | 3 | Залік |
| ОК 1.1.6. | Історія та культура України | 4 | Іспит |
| **1.2. Дисципліни фундаментальної підготовки** | | | |
| ОК 1.2.1. | Фізика | 16.5 | Іспит |
| ОК 1.2.2. | Вища математика | 19 | Іспит |
| ОК 1.2.3. | Дискретна математика | 3 | Іспит |
| ОК 1.2.4. | Нормативно-правове забезпечення ІБ | 4 | Залік |
| **3. Дисципліни професійної та практичної підготовки** | | | |
| ОК 1.3.1. | Теорія інформації і кодування | 3 | Іспит |
| ОК 1.3.2. | Основи теорії кіл, сигнали та процеси в електроніці | 8 | Залік, іспит |
| ОК 1.3.3. | Електроніка | 5 | Залік |
| ОК 1.3.4. | Архітектура і операційне середовище | 11 | Диференційований залік |
| ОК 1.3.5. | Інформаційні технології | 16,5 | Залік, іспит |
| ОК 1.3.6. | Інформаційно-комунікаційні системи | 7,5 | Іспит |
| ОК 1.3.7. | Системи технічного захисту інформації | 4 | Залік |
| ОК 1.3.8. | Технології програмування | 9 | Іспит |
| ОК 1.3.9. | Прикладна криптологія | 7 | Іспит |
| ОК 1.3.10. | Захист інформації в інформаційно-комунікаційних системах | 7 | Залік, іспит |
| ОК 1.3.11. | Комплексні системи захисту інформації: проектування, впровадження, супровід | 8 | Залік, іспит |
| ОК 1.3.12. | Управління інформаційною безпекою | 3 | Залік |
| ОК 1.3.13. | Вступ в інформаційну безпеку | 3 | Диференційований залік |
| ОК 1.3.14. | Інженерна та комп’ютерна графіка | 7 | Диференційований залік |
| ОК 1.3.15. | Комп'ютерна практика (2 тижні) | 3 | Залік |
| ОК 1.3.16. | Технологічна практика (2 тижні) | 3 | Залік |
| ОК 1.3.17. | Фахова практика (2 тижні) | 3 | Залік |
| ОК 1.3.18. | Складання державного екзамену із захистом в ЕК | 3 | |
| **Загальний обсяг обов`язкових компонент:** | | **172 кредити** | |
| **2.Вибіркові компоненти ОП** | | | |

| | | | |
|---|---|---|---|
| **2.1. Цикл дисциплін гуманітарної та соціально-економічної підготовки** | | | |
| ВБ 2.1.1. | Основи менеджменту та маркетингу/Основи управління колективом | 3 | Залік |
| **2.2. Дисципліни професійної та практичної підготовки** | | | |
| ВБ 2.2.1. | Економічна безпека/Управління безпекою бізнесу | 3 | Залік |
| ВБ 2.2.2 | Основи охорони праці та БЖД/Охорона праці та охорона навколишнього середовища | 3 | Іспит |
| ВБ 2.2.3 | Захист інформації в комп'ютерних мережах/Методи захисту даних в сучасних мережах | 7 | Іспит |
| ВБ 2.2.4 | Методи та засоби захисту інформації/Методи та засоби технічного захисту інформації | 9 | Іспит |
| ВБ 2.2.5 | Організація баз даних і знань/Архітектура сучасних баз даних | 7 | Іспит |
| ВБ 2.2.6 | Організація інформаційно-обчислювальних процесів і систем/Інформаційно-обчислювальні системи та мережі | 4 | Іспит |
| ВБ 2.2.7 | Основи інформаційної безпеки/Основи захисту інформації в ІТС | 6 | Іспит |
| ВБ 2. 2.8 | Основи обробки та передачі інформації/Фізичні основи інформаційних процесів | 4,5 | Залік |
| ВБ 2.2.9 | Основи побудови мікропроцесорних систем/Архітектура мікросистем | 4 | Іспит |
| ВБ 2.2.10 | Стеганографія/Методи та засоби стеганографічного захисту інформації | 3 | Залік |
| ВБ 2.2.11 | WEB-програмування/Розробка web-додатків | 3 | Залік |
| ВБ 2.2.12 | Інформаційні банківські технології/Інформаційні системи та технології у банківській сфері | 6 | Іспит |
| ВБ 2.2.13 | Організація та документальне забезпечення проведення робіт, пов'язаних з ЗІ/Організація роботи з секретними документами | 5 | Іспит |
| **2.3. Інші види навчання** | | | |

| | | | |
|---|---|---|---|
| ВБ 2.3.1 | Військова підготовка* | 30 | |
| **Загальний обсяг вибіркових компонент( без військової підготовки):** | | **69 кредитів** | |
| **Загальний обсяг освітньої програми (без військової підготовки)** | | **241 кредит** | |

Примітка* Військова підготовка: Відповідно Наказу Міністерства оборони України, Міністерства освіти і науки України № 719/1289 від 14 грудня 2015 року "Про затвердження Інструкції про організацію військової підготовки громадян України за програмою підготовки офіцерів запасу"

## 2.2 Структурно-логічна схема ОП

| Семестр | Номер дисципліни згідно навчального плану |
|---|---|
| **1** | 1.1.1., 1.1.2., 1.1.6., 1.2.1., 1.2.2., 1.3.8., 1.3.13., 1.3.14. |
| **2** | 1.1.1., 1.1.2., 1.1.3., 1.2.1., 1.2.2., 1.3.2., 1.3.8., 1.3.14., 1.3.15. |
| **3** | 1.2.1., 1.2.2., 1.3.2., 1.3.4., 1.3.5., 1.3.6. |
| **4** | 1.1.5., 1.2.2., 1.2.3., 1.3.3., 1.3.4., 1.3.5., 1.3.16. |
| **5** | 1.2.4., 1.3.9., 2.2.5, 2.2.7, 2.2.9, 2.2.12. |
| **6** | 1.3.1., 1.3.5., 1.3.9., 1.3.17., 2.1.1., 2.2.4, 2.2.6, 2. 2.8. |
| **7** | 1.1.4., 1.3.7., 1.3.10., 1.3.11., 1.3.12., 1.3.18., 2.2.1., 2.2.2, 2.2.3, 2.2.4, |
| **8** | 1.3.10., 1.3.11., 2.2.3, 2.2.10, 2.2.11, 2.2.13. |

## 3. Форма атестації здобувачів вищої освіти

Атестація випускників освітньої програми спеціальності №125 «Безпека інформаційних і комунікаційних систем» здійснюється у формі складання комплексного екзамену, та завершується видачею документу встановленого зразка про присудження йому ступеня бакалавра із присвоєння кваліфікації: Бакалавр з кібербезпеки за спеціалізацією фахівець із організації інформаційної безпеки.

Атестація здійснюється відкрито і публічно.

## 4. Матриця відповідності програмних компетентностей компонентам освітньої програми

| | ОК 1.1.1 | ОК 1.1.2 | ОК 1.1.3 | ОК 1.1.4 | ОК 1.1.5 | ОК 1.1.6 | ОК 1.2.1. | ОК 1.2.2. | ОК 1.2.3. | ОК 1.2.4. | ОК 1.3.1. | ОК 1.3.2. | ОК 1.3.3. | ОК 1.3.4. | ОК 1.3.5. | ОК 1.3.6. | ОК 1.3.7. | ОК 1.3.8 | ОК 1.3.9. | ОК 1.3.10. | ОК 1.3.11. | ОК 1.3.12. | ОК 1.3.13. | ОК 1.3.14. | ОК 1.3.15. | ОК 1.3.16. | ОК 1.3.17. | ОК 1.3.18. | ВБ 2.1.1. | ВБ 2.2.1. | ВБ 2.2.2 | ВБ 2.2.3. | ВБ 2.2.4. | ВБ 2.2.5. | ВБ 2.2.6. | ВБ 2.2.7. | ВБ 2.2.8. | ВБ 2.2.9. | ВБ 2.2.10 | ВБ 2.2.11. | ВБ 2.2.12. | ВБ 2.2.13. | ВБ 2.3.1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ЗК1 | ■ | | | | ■ | | | | ■ | | | | | | | | | | | | | | | | | | | | ■ | | ■ | | | | | | | | | | | | |
| ЗК2 | | | | ■ | | | ■ | ■ | | | ■ | | | | | | | | ■ | | | | ■ | | | | | | ■ | | | | | | | | | | | | | | |
| ЗК3 | | ■ | | | ■ | | | | | | | | ■ | | | ■ | | | | | | | | | | | | | ■ | | ■ | | | | | | | | | | | | |
| ЗК4 | ■ | | | ■ | | ■ | | | | | | | | | ■ | | | | | ■ | | | | | | | | | | | | | | | | | | | | | | | |
| ЗК5 | | | | | | | ■ | | | | ■ | | | ■ | | | | ■ | | | | | | | ■ | ■ | ■ | | | | | | | | | | | | | | | | |
| ЗК6 | | ■ | | | | | | | | ■ | | ■ | | | | | ■ | | ■ | | | | | | | | | | | | | | | | | | | | | | | |
| ЗК7 | | | | | | | | ■ | | | | | | | | ■ | | | | | ■ | | | | | | | | | | | | | | | | | | | | | |
| ЗК8 | | ■ | ■ | | | | | | ■ | | | | ■ | | | | | | | ■ | | | ■ | | | | ■ | | | | | | | ■ | ■ | | | | | | | |
| ЗК9 | | | | | | ■ | | | | | ■ | | | | ■ | ■ | | | ■ | | | | | | ■ | | | | | | | | | | | | | | | | | |
| ФК1 | | | | ■ | | | | | | ■ | | | | ■ | | | | | | | | ■ | | ■ | | | | | ■ | | | | | | | | | | | | ■ | |
| ФК2 | | | | | | | | ■ | | | | | | | | | ■ | | | | | | | | | | | | | | | | | | ■ | | ■ | | ■ | | | | |
| ФК3 | | | ■ | | | | | | | | | ■ | | | | | | ■ | | | ■ | | | | ■ | | ■ | | | | | ■ | | | | | | | | | | |
| ФК4 | | | | | | | | | | | ■ | | | ■ | | | ■ | | | ■ | | | | | | | | | | | ■ | ■ | | | | | | | | | | |
| ФК5 | | | | | | | | | | | | | | | ■ | | | | | ■ | ■ | ■ | ■ | | | | | | | ■ | | | | ■ | | | | | ■ | | |
| ФК6 | | | | | | | | | | | | ■ | ■ | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ФК7 | | | | | | | | | | ■ | | | | ■ | | | | ■ | ■ | | | | | ■ | | | | | | | | | | | ■ | | | | | | |
| ФК8 | | | | | | | | | | | | | | | | ■ | | | | | | ■ | | | | ■ | | | | | | | | | | | | ■ | | ■ | |
| ФК9 | | | | | | | | | ■ | | | | | | ■ | | | | | | | | | | | | | | ■ | | | | ■ | | | | | | | | |
| ФК10 | | | | | | | | | | | | | | | | | | | | | | ■ | | | | | | | | | | | | | | ■ | | | | | |
| ФК11 | | | | | | | | | | | | | | | | | ■ | | ■ | | ■ | | | | | | | | | | ■ | | | | | | | | | | |
| ФК12 | | | | | | | | | | | | | | | | | | | | | ■ | | | | | | | | | | ■ | | | | ■ | | | | | | |

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

| | ОК 1.1.1 | ОК 1.1.2 | ОК 1.1.3 | ОК 1.1.4 | ОК 1.1.5 | ОК 1.1.6 | ОК 1.2.1. | ОК 1.2.2. | ОК 1.2.3. | ОК 1.2.4. | ОК 1.3.1. | ОК 1.3.2. | ОК 1.3.3. | ОК 1.3.4. | ОК 1.3.5. | ОК 1.3.6. | ОК 1.3.7. | ОК 1.3.8 | ОК 1.3.9. | ОК 1.3.10. | ОК 1.3.11. | ОК 1.3.12. | ОК 1.3.13. | ОК 1.3.14. | ОК 1.3.15. | ОК 1.3.16. | ОК 1.3.17. | ОК 1.3.18. | ВБ 2.1.1. | ВБ 2.2.1. | ВБ 2.2.2 | ВБ 2.2.3. | ВБ 2.2.4. | ВБ 2.2.5. | ВБ 2.2.6. | ВБ 2.2.7. | ВБ 2.2.8. | ВБ 2.2.9. | ВБ 2.2.10 | ВБ 2.2.11. | ВБ 2.2.12. | ВБ 2.2.13. | ВБ 2.3.1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ПРН1 | ■ | | ■ | | ■ | ■ | ■ | | | | | | | | | | | | | | | | | | | | | | | | ■ | | | | | | | | | | | | |
| ПРН2 | | ■ | ■ | | | | | | | | | | | | | | | | | | | | | | ■ | ■ | ■ | | | | | | | | | | | | | | | | |
| ПРН3 | ■ | | | ■ | ■ | | | | | ■ | | | ■ | | | | | | | | | | | | | | | | ■ | ■ | | | | | | | | | ■ | | ■ | |
| ПРН4 | | | | | | | | | | | | | | | ■ | ■ | ■ | | ■ | ■ | | | | | | | | | | | ■ | ■ | | | | | | | | | | ■ | |
| ПРН5 | | | | | | | | ■ | ■ | | | | | | | | | | | | | ■ | | | ■ | ■ | ■ | | | | | | ■ | | ■ | | | | | | | |
| ПРН6 | | | | | ■ | | | | | | | | | | | | | ■ | | | | | ■ | | | | | | | | | | | | | | | | | | | |
| ПРН7 | | | | ■ | | | | | | | | ■ | | | | | | | ■ | | | | | | | | | | ■ | | ■ | | | | | | | | | | ■ | | |
| ПРН8 | | | | | | | | | | ■ | | | ■ | | | ■ | ■ | | | ■ | ■ | | | | | | | | | | | ■ | ■ | ■ | | | | | ■ | | ■ | |
| ПРН9 | | | | | | | | | | | | | | ■ | | | | | | | | ■ | ■ | | | | | | | | | | | ■ | | | | | ■ | | | |
| ПРН10 | | | | | | | | | | | | | | ■ | | | | | | | | ■ | ■ | | | | | | | | | | | | ■ | ■ | | | | ■ | ■ | |
| ПРН11 | | | | | | | | | | | | | | ■ | | | | ■ | | | ■ | ■ | | | | | | | | | | | | | | | | | | | | |
| ПРН12 | | | | | | | | | | | | | | | | ■ | | | | | | ■ | | | | | | | | | | | | | ■ | | | | | ■ | | |
| ПРН13 | | | | | | | | | | | | | | | ■ | | | | | | ■ | | | | | | | | | | | | | | | ■ | | | | | | |
| ПРН14 | | | | | | | | | | ■ | | | | | | | ■ | | ■ | | | | | | | | | | | | | ■ | ■ | | | | | | ■ | | | |
| ПРН15 | | | | | | | | | | | | | | | | | | | | | | ■ | | | | | | | | ■ | | | | | ■ | | | ■ | | ■ | | |
| ПРН16 | | | | | | | | | | | ■ | | | | | | | ■ | | | ■ | | | | | | | | | | | | | | | ■ | | | | ■ | | |
| ПРН17 | | | | | | | | | | | | | | ■ | | | | | | ■ | | | | | | | | | | | | | | | ■ | | | ■ | ■ | | | |
| ПРН18 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | ■ | | | | ■ | | | | | | ■ | | |