

**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.Смолянко* В.І.Смолянко

**ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА**

**Підготовки здобувачів першого (бакалаврського) рівня  
вищої освіти**

**ГАЛУЗЬ ЗНАНЬ** 12 Інформаційні технології

**СПЕЦІАЛЬНІСТЬ** 125 Кібербезпека

**НАЗВА ОПП** Системи технічного захисту інформації

Ужгород 2017 р.

Освітньо професійна програма ” Системи технічного захисту інформації” 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:**

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

**1.Профіль освітньої програми зі спеціальності  
№ 125 ”Кібербезпека”(за спеціалізацією ” Системи технічного захисту  
інформації ”)**

<b>Загальна інформація</b>	
<b>Повна назва вищого навчального закладу</b>	Державний вищий навчальний заклад «Ужгородський національний університет»
<b>Ступінь вищої освіти та назва кваліфікації мовою оригіналу</b>	Ступінь вищої освіти: бакалавр. Освітня кваліфікація: бакалавр з кібербезпеки Професійна кваліфікація : фахівець з технічного захисту інформації
<b>Офіційна назва освітньої програми</b>	Системи технічного захисту інформації
<b>Тип диплому та обсяг освітньої програми</b>	Диплом бакалавра, одиничний, 240 кредитів ЄКТС. Термін навчання 3 роки і 10 місяців.
<b>Наявність акредитації</b>	Акредитаційна комісія України Сертифікат про акредитацію серія НД № 0791769 Термін дії сертифікату до 01.07.2024р.
<b>Цикл/рівень</b>	Національна рамка кваліфікацій України – 6 рівень, FQ-EHEA – перший цикл, EQF-LLL – 6 рівень.
<b>Передумови</b>	Наявність повної загальної середньої освіти. Умови вступу визначаються «Правилами прийому до Ужгородського національного університету»
<b>Мова(и) викладання</b>	Українська
<b>Термін дії освітньої програми</b>	Відповідно до терміну дії сертифікату про акредитацію
<b>Інтернет-адреса постійного розміщення опису освітньої програми</b>	<a href="http://www.uzhnu.edu.ua/uk/infocentre/15068">http://www.uzhnu.edu.ua/uk/infocentre/15068</a>
<b>Мета освітньої програми</b>	
Навчання та підготовка фахівців спеціальності 125 ”Кібербезпека”(за спеціалізацією ”Системи технічного захисту інформації”), які розуміються на джерелах загроз та вразливостях об’єктів інформаційної діяльності, технічних каналах витоку інформації, нормативно-правових, організаційних та організаційно-технічних заходах, а також технічних засобах протидії несанкціонованому доступу до інформації з обмеженим доступом. Засвоїти знання з основ законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності.	
<b>Характеристика освітньої програми</b>	
<b>Предметна область (галузь знань, спеціальність, спеціалізація(за наявності))</b>	12 Інформаційні технології, 125 Кібербезпека, спеціалізація (Системи технічного захисту інформації). Обсяг освітньої програми бакалавра: на базі повної загальної середньої освіти з терміном навчання 11 років – 240 кредитів ЄКТС 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 меншим, ніж 120 кредитів.

Об'єкти професійної діяльності випускників:

- об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси і технології;
- 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-комунікаційних (автоматизованих) системах;
- процеси управління інформаційною безпекою та кібербезпекою в інформаційних та інформаційно-комунікаційних (автоматизованих) системах, що підлягають захисту.

Цілі навчання студентів готують до технічного захисту інформації (запобігання витоку інформації) радіоелектронними, віброакустичними і візуально-оптичними каналами; навчають технічних засобів розвідки, елементам економічного і промислового шпигунства, засобів контролю за ефективністю захисту, організації захисту інформації та протидії зловмисникам.

Теоретичний зміст предметної діяльності

Знання:

- законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності;
- принципів забезпечення та супроводу систем та комплексів інформаційної безпеки та\або

	<p>кібербезпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики безпеки;</p> <ul style="list-style-type: none"> <li>- 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;</li> <li>- процесів функціонування системи управління інформаційною безпекою та\або кібербезпекою та основ теорії ризиків;</li> <li>- методів та засобів виявлення та ідентифікації вразливостей і загроз інформаційній безпеці на об'єктах інформаційної діяльності;</li> <li>- методів та засобів оцінювання та забезпечення відповідного рівня захищеності інформації в інформаційних та інформаційно=комунікаційних (автоматизованих) системах;</li> <li>- методів та засобів технічного та криптографічного захисту інформації із забезпечення інформаційної безпеки і кібербезпеки.</li> </ul> <p><u>Методи, методика та технології:</u> Методи, методика та технології забезпечення інформаційної безпеки та кібербезпеки</p> <p><u>Інструменти та обладнання:</u></p> <ul style="list-style-type: none"> <li>- обладнання, необхідне для моніторингу функціонування і підтримки інформаційно-комунікаційних систем і мереж;</li> <li>- системи забезпечення інформаційної безпеки та кібербезпеки.</li> </ul>
<p><b>Орієнтація освітньої програми</b></p>	<p>Освітньо-професійна програма орієнтована на здобуття студентами професійних знань, умінь, навичок та інших компетентностей для успішного здійснення професійної діяльності у галузі.</p>
<p><b>Основний фокус освітньої програми та спеціалізації</b></p>	<p>Базові знання та навички в застосуванні законодавчої бази в галузі інформаційної та комунікаційної безпеки, проектування і впровадження спеціальних технічних і програмно-математичних засобів захисту інформації,</p>

	забезпечення організаційних і інженерно-технічних заходів захисту інформаційних систем.
<b>Особливості програми</b>	Програма передбачає здобуття комплексних знань та навичок для вирішення низки актуальних завдань у сфері інформаційної безпеки, що передбачають розроблення, впровадження та експлуатацію систем технічного захисту інформації на об'єктах інформаційної діяльності.
<b>Придатність випускників до працевлаштування та подальшого навчання</b>	
<b>Придатність до працевлаштування</b>	Фахівець здатний виконувати наступну професійну роботу: <ul style="list-style-type: none"> <li>– організація захисту інформації з обмеженим доступом;</li> <li>– експлуатація, модернізація та ремонт засобів технічного захисту інформації;</li> <li>– захист інформації в комп'ютерних та інших технічних засобах від копіювання та несанкціонованого доступу;</li> <li>– організація безпеки промислових об'єктів, помешкань і громадських будинків включно з оцінкою їхньої безпеки;</li> <li>– охоронну діяльність, що здійснюється за допомогою механічних та електричних захисних пристроїв;</li> <li>– розслідування та дізнання;</li> <li>– нагляд, охорона та інші види захисту.</li> </ul>
<b>Подальше навчання</b>	Випускник з дипломом бакалавра може продовжити навчання за освітньо-професійною або освітньо-науковою програмою ступеня магістра
<b>Викладання та оцінювання</b>	
<b>Викладання та навчання</b>	Студентсько-центроване навчання, самонавчання, проблемно-орієнтоване навчання, індивідуально-творчий підхід, навчання через виробничу (фахову) та педагогічну практики.
<b>Оцінювання</b>	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;

	Усні та письмові экзамен, заліки, презентації, проектна робота диференційований залік з педагогічної практики, курсова робота.
<b>Програмні компетентності</b>	
<b>Інтегральна компетентність</b>	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки та кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.
<b>Загальні компетентності (ЗК)</b>	<ul style="list-style-type: none"> <li>– Здатність застосовувати знання у практичних ситуаціях. (ЗК1)</li> <li>– Знання та розуміння предметної області та розуміння професії. (ЗК2)</li> <li>– Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово (ЗК3)</li> <li>– Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням (ЗК4)</li> <li>– Здатність до пошуку, оброблення та аналізу інформації з різних джерел. (ЗК5)</li> </ul>
<b>Фахові компетентності (ФК)</b>	<ul style="list-style-type: none"> <li>– 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 кібербезпеки.(ФК1)</li> <li>– Вміння щодо визначення наявності загроз інформації в автоматизованих системах; (ФК2)</li> <li>– Вміння організувати моніторинг стану інформаційної системи для того, щоб аналізувати порушення інформаційної безпеки;ФК3)</li> <li>– Вміння використовувати комплексну систему захисту інформації в організації; (ФК4)</li> <li>– Здатність до здійснення технічного обслуговування, контролю і діагностики комплексної системи захисту інформації в організації; (ФК5)</li> <li>– Здатність до використання програмно-апаратних засобів та криптографічних методів технічного захисту інформації; (ФК6)</li> </ul>

- Здатність до використання засобів захисту програмного забезпечення від несанкціонованого копіювання, впливу комп'ютерних вірусів тощо.; (ФК7)
- Вміння використовувати інформаційні технології для вирішення експериментальних і практичних завдань в галузі професійної діяльності. (ФК8)

### Програмні результати навчання

#### Загальні результати навчання

- Застосувати концептуальні знання з навчальних дисциплін загальної підготовки для засвоєння дисциплін професійної підготовки;(ПРН1)
- Застосувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; (ПРН2)
- Організувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем професійній діяльності, оцінювати їхню ефективність; (ПРН3)
- Використати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності(ПРН4)
- 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)
- 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)



<p><b>Фахові результати навчання</b></p>	<ul style="list-style-type: none"> <li>- Знати основні положення нормативних документів в сфері технічного захисту інформації ; (ПРН8)</li> <li>- Знати проектний менеджмент, менеджмент безпеки трудових ресурсів, маркетинг продуктів та послуг інформаційної безпеки, основні загрози безпеці інформації; (ПРН9)</li> <li>- Здійснювати розроблення і проектування об'єктів, пристроїв і систем технічного захисту інформації ; (ПРН10)</li> <li>- Здійснювати розроблення організаційних механізмів забезпечення інформаційної безпеки, вміти організовувати виконання завдань професійної діяльності, вміти готувати та приймати управлінські рішення ; (ПРН11)</li> <li>- Вміти виконувати діагностичні роботи із засобами та комплексами систем технічного захисту інформації;; (ПРН12)</li> <li>- Вміти проводити атестації технічних засобів та інформаційних ресурсів;; (ПРН13)</li> <li>- Вміти прогнозувати стан інформаційної безпеки підприємства і визначати вплив ефективності задіяних заходів і засобів технічного захисту інформації; (ПРН14)</li> <li>- Здатність контролю безпеки процесів розробки та підтримки; (ПРН15)</li> <li>- Адміністрування доступу до інформації з обмеженим доступом на об'єктах інформаційної діяльності (ПРН16)</li> <li>- Управління та контроль доступу в автоматизованих системах; (ПРН17)</li> <li>- Моніторинг систем, підсистем систем технічного захисту інформації та систем управління інформаційною безпекою.. (ПРН18)</li> </ul>
<p><b>Ресурсне забезпечення реалізації програми</b></p>	
<p><b>Кадрове забезпечення</b></p>	<p>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.</p>

<b>Матеріально-технічне забезпечення</b>	<p>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.</p>
<b>Інформаційне та навчально- методичне забезпечення</b>	<p>-офіційний веб-сайт <a href="http://www.uzhnu.edu.ua">http://www.uzhnu.edu.ua</a> містить інформацію про освітні програми, навчальну, наукову і виховну діяльність, структурні підрозділи, правила прийому, контакти;</p> <ul style="list-style-type: none"> <li>- необмежений доступ до мережі Інтернет;</li> <li>– наукова бібліотека, читальні зали;</li> <li>– навчальні і робочі плани;</li> <li>– графіки навчального процесу;</li> <li>– навчально-методичні комплекси дисциплін;</li> <li>– дидактичні матеріали для самостійної та індивідуальної роботи студентів з дисциплін, програми практик;</li> <li>– методичні вказівки щодо виконання кваліфікаційних робіт.</li> </ul>
<b>Академічна мобільність</b>	
<b>Національна кредитна мобільність</b>	<p>Підвищення кваліфікації (стажування) науково-педагогічних працівників у вітчизняних закладах вищої освіти на основі двосторонніх договорів між Ужгородським національним університетом та університетами України.</p>
<b>Міжнародна кредитна мобільність</b>	<p>Угода щодо семестрового академічного обміну між Поморською Академією у м. Слупськ (Польща) та Ужгородським національним університетом.</p>
<b>Навчання іноземних здобувачів вищої освіти</b>	<p>Можливе навчання іноземних громадян. Навчання іноземних студентів проводиться на загальних умовах або за індивідуальним графіком.</p>

## 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
<b>1 Обов'язкові компоненти ОП</b>			
<b>1.1 Цикл дисциплін гуманітарної та соціально-економічної підготовки</b>			
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
<b>1.2. Дисципліни фундаментальної підготовки</b>			
ОК 1.2.1.	Фізика	16,5	Іспит
ОК 1.2.2.	Вища математика	19	Іспит
ОК 1.2.3.	Інженерна та комп'ютерна графіка	7	Диференційований залік
ОК 1.2.4.	Інформаційні технології	12	Іспит
ОК 1.2.5.	Основи теорії кіл, сигнали та процеси в електроніці	8	Залік, іспит
ОК 1.2.6.	Комп'ютерні мережі	12	Іспит
ОК 1.2.7.	Основи інформаційної безпеки	6	Іспит
ОК 1.2.8.	Метрологія та вимірювання	4,5	Іспит
ОК 1.2.9.	Теорія інформації	5,5	Іспит
ОК 1.2.10.	Правові основи охорони інформації	3	Залік
ОК 1.2.11.	Методи та засоби захисту інформації	10,5	Іспит
ОК 1.2.12.	Організаційно-технічне забезпечення систем захисту інформації	5,5	Іспит
ОК 1.2.13.	Документаційне забезпечення робіт, пов'язаних із захистом інформації	4	Іспит
<b>3. Дисципліни професійної та практичної підготовки</b>			
ОК 1.3.1.	Мікросхемотехніка	10,5	Залік, іспит
ОК 1.3.2.	Апаратні засоби персональних комп'ютерів	8,5	Залік, іспит
ОК 1.3.3.	Основи адміністративного та кримінального права	4	Залік

ОК 1.3.4.	Криптографічні перетворення	7	Диференційований залік
ОК 1.3.5.	Обчислювальна техніка і програмування	3	Залік
ОК 1.3.6.	Фахова ознайомча практика (1 тиждень)	1,5	Залік
ОК 1.3.7.	Комп'ютерна практика (1 тиждень)	1,5	Залік
ОК 1.3.8.	Схемотехнічна практика (3 тижні)	4,5	Залік
ОК 1.3.9.	Технологічна практика (2 тижні)	3	Залік
ОК 1.3.10.	Складання комплексного державного екзамену	3	Залік
<b>Загальний обсяг обов'язкових компонент:</b>		<b>178 кредитів</b>	
<b>2. Вибіркові компоненти ОП</b>			
<b>2.1. Цикл дисциплін гуманітарної та соціально-економічної підготовки</b>			
ВБ 2.1.1.	Психологія екстремальних стосунків/Екстремальна психологія	3	Залік
ВБ 2.1.2.	Політологія/Актуальні проблеми політичної науки	3	Іспит
ВБ 2.1.3.	Економічна теорія/Соціологія	3	Залік
ВБ 2.1.4.	Основи менеджменту та маркетингу/Основи управління колективом	3	Залік
ВБ 2.1.5.	Основи охорони праці та БЖД/Охорона праці та охорона навколишнього середовища	3	Іспит
<b>2.2. Дисципліни професійної та практичної підготовки</b>			
ВБ 2.2.1.	Спеціальні розділи математики/Теорія функцій комплексної змінної та операційне числення	4	Залік
ВБ 2.2.2.	Основи патентного, авторського та фінансового права/Порівняльне авторське та фінансове право	5	Залік, іспит
ВБ 2.2.3.	Системи обробки текстової, табличної та графічної інформації/Програмне забезпечення обробки інформації	4,5	Іспит
ВБ 2.2.4.	Охорона комерційної таємниці на підприємстві/Комерційна таємниця як об'єкт трудових відносин	5	Залік
ВБ 2.2.5.	Системи банківської безпеки/Захист інформації в банківських та комерційних системах	5	Іспит

ВБ 2.2.6	Основи завадостійкості систем захисту інформації/Завадостійкість та ефективність передачі інформації	5	Іспит
ВБ 2.2.7	Бази даних/Сучасні системи управління базами даних	3	Диференційований залік
ВБ 2.2.8	Технічна графіка/Комп'ютерна техніка	6	Залік
ВБ 2.2.9	Акустoeлектронні пристрої/Фізичні основи акустoeлектроніки	5	Іспит
ВБ 2.2.10	Економічна безпека діяльності підприємств/Управління безпекою бізнесу	4,5	Диференційований залік
<b>2.3. Інші види навчання</b>			
ВБ 2.3.1	Військова підготовка*	30	
<b>Загальний обсяг вибіркового компонента (без військової підготовки):</b>		<b>62 кредитів</b>	
<b>Загальний обсяг освітньої програми (без військової підготовки)</b>		<b>240 кредит</b>	

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
<b>1</b>	1.1.1., 1.1.2., 1.1.6., 1.2.2., 1.2.1., 1.2.3., 1.2.4.,
<b>2</b>	1.1.1., 1.1.2., 1.1.3., 1.2.2., 1.2.1., 1.2.3., 1.2.4., 1.2.5.,
<b>3</b>	1.2.2., 1.2.1., 1.2.5., 1.2.6., 1.3.5., 2.1.4., 2.2.9.
<b>4</b>	1.1.5., 1.2.2., 1.2.6., 1.3.1., 2.2.8.
<b>5</b>	1.2.7., 1.2.8., 1.3.1., 1.3.2., 2.1.3., 2.2.3., 2.2.7.
<b>6</b>	1.3.9., 1.3.10., 1.3.11., 1.3.2., 2.2.1, 2.2.4.,
<b>7</b>	1.1.4., 1.2.12., 1.3.3., 1.3.4., 2.1.4., 2.2.2, 2.2.5.,
<b>8</b>	1.3.11., 1.2.13., 2.1.1., 2.1.2., 2.2.2, 2.2.6., 2.2.10.

## 3. Форма атестації здобувачів вищої освіти

Атестація випускників освітньої програми спеціальності №125 «Системи технічного захисту інформації» 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 з технічного захисту інформації Атестація здійснюється відкрито і публічно.



