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

ЗАТВЕРДЖЕНО
Протокол Вченої ради
ДВНЗ «Ужгородський
національний університет»
28.03. **2024 р. №** 4

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

«Системи технічного захисту інформації»

першого (бакалаврського) рівня вищої освіти

за спеціальністю 125 Кібербезпека та захист інформації

галузі знань 12 Інформаційні технології

кваліфікація: Бакалавр з кібербезпеки та захисту інформації

УВЕДЕНО В ДІЮ
Наказ ректора ДВНЗ
«Ужгородський національний
університет
04.04. **2024 р. №** 250/01-04

Ужгород – 2024

АРКУШ ПОГОДЖЕННЯ
освітньо-професійної програми
«Системи технічного захисту інформації»

1. Ректор **Володимир СМОЛАНКА**

28.03. **2024 р.**

2. Гарант освітньо-професійної програми **Михайло СІЧКА**

21.03 **2024 р.**

3. Декан структурного підрозділу **Володимир ЛАЗУР**

21.03. **2024 р.**

4. Керівник робочої групи **Михайло СІЧКА**

21.03. **2024 р.**

5. Начальник навчальної частини **Анатолій ШТИМАК**

25.03. **2024 р.**

ПЕРЕДМОВА

Освітньо-професійна програма "Системи технічного захисту інформації" підготовки здобувачів першого (бакалаврського) рівня вищої освіти спеціальності 125 Кібербезпека та захист інформації розроблена згідно з вимогами Закону України «Про вищу освіту» та у відповідності до стандарту вищої освіти, затвердженого й уведеного в дію наказом Міністерства освіти і науки України від 04.10.2018 р. № 1074.

Розроблено робочою групою у складі:

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

ЧЛЕНИ РОБОЧОЇ ГРУПИ:

1. Різак Василь Михайлович, доктор фіз.-мат. наук, професор, завідувач кафедри твердотільної електроніки та інформаційної безпеки;

2. Попович Наталія Іванівна, кандидат фіз.-мат. наук, доцент кафедри твердотільної електроніки та інформаційної безпеки;

3. Юрічко Станіслав Володимирович, здобувач вищої освіти.

ЗОВНІШНІЙ СТЕЙКХОЛДЕР: Танчинець Михайло Михайлович, заступник начальника відділу протидії кіберзлочинам в Закарпатській області Департаменту кіберполіції Національної поліції України.

1. Профіль освітньої програми "Системи технічного захисту інформації" зі спеціальності 125 Кібербезпека та захист інформації

1 – Загальна інформація	
Повна назва закладу вищої освіти та структурного підрозділу	Державний вищий навчальний заклад «Ужгородський національний університет», фізичний факультет, кафедра твердотільної електроніки та інформаційної безпеки
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Ступінь вищої освіти: бакалавр. Освітня кваліфікація: бакалавр з кібербезпеки та захисту інформації
Офіційна назва освітньої програми	Системи технічного захисту інформації
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний, 240 кредитів ЄКТС. Термін навчання 3 роки і 10 місяців.
Наявність акредитації	Акредитаційна комісія України Сертифікат про акредитацію серія НД № 0791769 Термін дії сертифікату до 01.07.2024р.
Цикл/рівень	Національна рамка кваліфікацій України – 6 рівень, FQ-EHEA – перший цикл, EQF-LLL – 6 рівень.
Передумови	Наявність повної загальної середньої освіти. Умови вступу визначаються «Правилами прийому до Ужгородського національного університету»
Мова(и) викладання	Українська
Термін дії освітньої програми	До чергового перегляду
Інтернет-адреса постійного розміщення опису освітньої програми	http://www.uzhnu.edu.ua/uk/infocentre/15068
2 – Мета освітньої програми	
Навчання та підготовка висококваліфікованих фахівців, які володіють сучасними загально-науковими й спеціальними знаннями та технологіями інформаційної та/або кібербезпеки, здатних розробляти, використовувати і впроваджувати технології інформаційної безпеки та/або кібербезпеки для вирішення низки актуальних завдань у сфері інформаційної безпеки. Опанування здобувачами вищої освіти знань з основ законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності.	
3 – Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність, спеціалізація(за наявності))	Галузь знань: 12 Інформаційні технології Спеціальність: 125 Кібербезпека та захист інформації

	Обсяг освітньої програми бакалавра: – на базі повної загальної середньої освіти з терміном навчання 11 років – 240 кредитів ЄКТС – на базі ступеня «молодший бакалавр» (освітньо-кваліфікаційного рівня «молодший спеціаліст») заклад вищої освіти має право визнати та перезарахувати не більше ніж 120 кредитів ЄКТС, отриманих в межах попередньої освітньої програми підготовки молодшого бакалавра (молодшого спеціаліста). Мінімум 75% 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 ЗВО має право скорочувати обсяг освітньої програми. При цьому програма має забезпечувати набуття визначених стандартом вищої освіти результатів навчання, а її загальний обсяг має бути не меншим, ніж 120 кредитів. Об'єкти професійної діяльності випускників: – системи та комплекси технічного захисту інформації на об'єктах інформаційної діяльності; – системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків); – процеси управління інформаційною безпекою та/або кібербезпекою об'єктів що підлягають захисту. Цілі навчання: підготовка фахівців, здатних розробляти, використовувати і впроваджувати технології інформаційної безпеки та/або кібербезпеки. Теоретичний зміст предметної діяльності Знання: – законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; – принципів супроводу систем та комплексів інформаційної безпеки та/або кібербезпеки; – методів та засобів технічного та криптографічного захисту інформації; – теорії, моделей та принципів управління доступом до інформаційних ресурсів; – теорії систем управління інформаційною та/або кібербезпекою;

	– процесів функціонування системи управління інформаційною безпекою та/або кібербезпекою, а також основ теорії ризиків; – методів та засобів виявлення, управління та ідентифікації ризиків; – методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації; – сучасних інформаційно-комунікаційних технологій; – сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій.
Орієнтація освітньої програми	Програма має освітньо-професійну орієнтацію на здобуття студентами знань, умінь, навичок та інших компетентностей для успішного здійснення професійної діяльності у галузі кібербезпеки; базується на загальновідомих у галузі інформаційних технології наукових результатах, у рамках яких можлива подальші професійна кар'єра і навчання.
Основний фокус освітньої програми та спеціалізації	Загальна вища освіта в галузі знань «Інформаційні технології» з поглибленою спеціалізованою підготовкою в сфері технічного захисту інформації. Ключові слова: технічний захист інформації; інформаційна безпека; кібербезпека,
Особливості програми	Освітньо-професійна програма передбачає: – вивчення законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; – застосування практичних навичок у сфері технічного захисту інформації; – використання теорії, моделей та принципів управління доступом до інформаційних ресурсів; – застосування методів та засобів виявлення, управління та ідентифікації ризиків; – проєктування комплексів технічного захисту інформації; – практичного використання методів та засобів виявлення закладних пристроїв, виявлення та локалізації технічних каналів витоку інформації; – застосування сучасного програмно-апаратного забезпечення та інформаційно-комунікаційних систем і технологій; – використання автоматизованих систем проєктування. Освітня програма враховує вимоги національних роботодавців, міжнародних стандартів інформаційної та кібербезпеки, а також тенденції розвитку IT - галузі.

4 - Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Професійна діяльність в галузі інформаційної та/або кібербезпеки в установах та організаціях різних форм власності.
Подальше навчання	Можливість навчання за програмою другого (магістерського) рівня вищої освіти спеціальності 125 Кібербезпека та захист інформації. Навчання за перехресним вступом та набуття додаткових кваліфікацій в системі післядипломної освіти.
5 - Викладання та оцінювання	
Викладання та навчання	Лекції, практичні та лабораторні заняття, самонавчання, проектно-орієнтоване навчання, консультації із науково-педагогічними працівниками, проведення наукових досліджень. Студентоцентроване 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, спрямовані на опанування навчального навантаження освітньої програми: поточні контроль та оцінювання, поетапний, модульний, підсумковий контроль; екзамени; заліки, презентації, курсовий проект, єдиний державний кваліфікаційний іспит. Проміжкове та підсумкове оцінювання знань відбувається на засадах студентоорієнтованого особистісного підходу з використанням сучасних методик та практик. Оцінювання знань здобувачів вищої освіти відбувається згідно: Положення про організацію освітнього процесу в Державному вищому навчальному закладі «Ужгородський національний університет» https://www.uzhnu.edu.ua/uk/infocentre/get/31357 Положення про порядок та методику проведення семестрових (курсових) екзаменів і заліків в Ужгородському національному університеті https://www.uzhnu.edu.ua/uk/infocentre/get/5952, Положення про атестацію здобувачів вищої освіти та екзаменаційну комісію у Державному вищому навчальному закладі «Ужгородський національний університет» https://www.uzhnu.edu.ua/uk/infocentre/get/11070

	з дотриманням норм академічної доброчесності відповідно до Положення про академічну доброчесність в Ужгородському національному університеті https://www.uzhnu.edu.ua/uk/infocentre/get/12223. Перезарахування кредитів відбувається на основі Положення про визнання (перезарахування) кредитів ЄКТС для учасників програм академічної мобільності у Державному вищому навчальному закладі «Ужгородський національний університет» https://www.uzhnu.edu.ua/uk/infocentre/get/20131. Процедура оцінювання здобувачів вищої освіти також враховує результати неформальної освіти згідно Положення про порядок визнання Державному вищому навчальному закладі «Ужгородський національний університет» результатів навчання, здобутих у неформальній освіті https://www.uzhnu.edu.ua/uk/infocentre/get/22966. Наявна чітка процедура розгляду апеляцій здобувачів вищої освіти, яка описана в Положенні про порядок застосування заходів з врегулювання конфліктів та спорів (суперечок) у діяльності співробітників та здобувачів вищої освіти Державного вищого навчального закладу «Ужгородський національний університет» https://www.uzhnu.edu.ua/uk/infocentre/get/22964 та Положенні про порядок оскарження результатів (апеляція) оцінювання в Державному вищому навчальному закладі «Ужгородський національний університет» https://www.uzhnu.edu.ua/uk/infocentre/get/22967
6 - Програмні компетентності	
Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки та/або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.
Загальні компетентності (ЗК)	– Здатність застосовувати знання у практичних ситуаціях (ЗК1). – Знання та розуміння предметної області та розуміння професії (ЗК2). – Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово (ЗК 3). – Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням (ЗК 4). – Здатність до пошуку, оброблення та аналізу

	інформації (ЗК 5). – Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні (ЗК6). – 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 (ЗК7). – Здатність використовувати технічні засоби захисту та охорони інформаційних ресурсів і баз даних обмеженого доступу (ЗК8).
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 (ФК 1). – Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки (ФК 2). – Здатність до використання програмних та програмно- апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах (ФК 3). – Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної безпеки (ФК 4). – Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної безпеки (ФК 5). – Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження (ФК 6). – Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів,

	процедур, практичних прийомів та ін.) (ФК 7). – Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку (ФК 8). – Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою (ФК 9). – Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності (ФК 10). – Здатність виконувати моніторинг процесів функціонування нформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки (ФК 11). – Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки .(ФК 12). – Здатність оцінювати та визначати фізичні процеси, які висвітлюють характеристики та параметри напівпровідникових активних елементів, а також проводити лінійний та нелінійний аналіз електричних схем, схемотехніки різноманітних підсилювальних каскадів, операційних підсилювачів та елементів логіки (ФК 13). – Здатність виявляти та блокувати канали витоку інформації, методи несанкціонованого доступу до інформації, джерела і способи дестабілізуючого впливу на інформацію, здійснювати пошук закладних пристроїв. (ФК 14).
7 - Програмні результати навчання	
– Застосовувати знання державної та іноземних мов з метою забезпеченн ефективності професійної комунікації (ПРН 1). – Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність (ПРН 2). – Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності (ПРН 3). – 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 (ПРН 4). – Адаптуватися в умовах частої зміни технологій професійної діяльності,	

прогнозувати кінцевий результат (ПРН 5).
- Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності (ПРН 6).
- Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки (ПРН 7).
- Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки (ПРН 8).
- Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки (ПРН 9).
- Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем (ПРН 10).
- Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах (ПРН 11).
- Розробляти моделі загроз та порушника (ПРН 12).
- Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних (ПРН 13).
- Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень (ПРН 14).
- Використовувати сучасне програмно-апаратне забезпечення інформаційно комунікаційних технологій (ПРН 15).
- Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів (ПРН 16).
- Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент (ПРН 17).
- Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів (ПРН 18).
- Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах (ПРН 19).
- Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах (ПРН 20).
- Вирішення задач забезпечення та супроводу (в. т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах (ПРН 21).
- Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно- телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки (ПРН 22).
- Реалізовувати заходи з протидії отриманню несанкціонованого доступу до

інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах (ПРН 23).
- Управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових) (ПРН 24).
- Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів (ПРН 25).
- Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем (ПРН 26).
- Вирішувати задачі захисту потоків даних в інформаційних, інформаційно телекомунікаційних (автоматизованих) системах (ПРН 27).
- Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно- телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки (ПРН 28).
- Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробдяється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів (ПРН 29).
- Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем (ПРН 30).
- Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем (ПРН 31).
- Управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки (ПРН 32).
- Задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків (ПРН 33).
- Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації (ПРН 34).
- Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційх ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизовани3) системах згідно встановленої політики інформаційної і/або кібербезпеки (ПРН 35).
- Виявляти небезпечні сигнали технічних засобів (ПРН 36).
- Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації (ПРН 37).
- Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту

інформації (ПРН 38).
- Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах (ПРН 39).
- Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації (ПРН 40).
- Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур (ПРН 41).
- Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки (ПРН 42).
- Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів (ПРН 43).
- Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами (ПРН 44).
- Застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів (ПРН 45).
- Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах (ПРН 46).
- Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації (ПРН 47).
- Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах (ПРН 48).
- Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах (ПРН 49).
- Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних) (ПРН 50).
- Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах (ПРН 51).
- Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах (ПРН 52).
- Вирішувати задачі аналізу програмного коду на наявність можливих загроз (ПРН 53).
- Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні (ПРН 54).
- Вирішувати задачі проєктування, створення та супроводу комплексів технічного захисту інформації на об'єктах інформаційної діяльності. (ПРН 55).
- Здійснювати вибір і оцінювання систем передачі даних і протоколів, визначати основні параметри каналу зв'язку для подальшої передачі інформації (ПРН 56).

– Визначати потенційні кіберзагрози та оцінювати захищеність інформації на об'єктах інформаційної діяльності (ПРН 57).	
8 - Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Реалізація освітньої програми забезпечується кадрами високої кваліфікації з науковими ступенями та вченими званнями, які мають великий досвід навчально-методичної, науково-дослідної роботи та відповідають Ліцензійним умовам провадження освітньої діяльності на першому (бакалаврському) рівні вищої освіти. Склад групи освітньої програми та професорсько-викладацький склад, що задіяний до викладання навчальних дисциплін, постійно проходять стажування та підвищення кваліфікації, що відповідає Положенню про підвищення кваліфікації та стажування педагогічних та науково-педагогічних працівників ДВНЗ "УжНУ" . https://www.uzhnu.edu.ua/uk/infocentre/get/5950
Матеріально-технічне забезпечення	Відповідає технологічним вимогам щодо матеріально-технічного забезпечення освітньої діяльності у сфері вищої освіти згідно з діючим законодавством України. Існує майже 100% забезпеченість навчальними приміщеннями, комп'ютерними робочими місцями, лабораторіями, мультимедійним обладнанням, устаткуванням, контрольно- вимірювальними приладами необхідними для виконання навчальних планів. Засоби обчислювальної техніки з прикладним та спеціалізованим програмним забезпеченням, спеціальні радіовимірювальні пристрої, засоби технічного захисту інформації, спеціалізовані апаратно-програмні комплекси. Наявна вся необхідна соціально-побутова інфраструктура. 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; – необмежений доступ до мережі Інтернет, фондів та електронних каталогів наукової бібліотеки

	ДВНЗ «УжНУ», а також до електронного репозитарію ДВНЗ «УжНУ» (https://dspace.uzhnu.edu.ua/jspui/), де містяться навчально-методичні матеріали з дисциплін навчального плану; – наукова бібліотека, читальні зали; – навчальні і робочі плани; – графіки навчального процесу; – дидактичні матеріали для самостійної та індивідуальної роботи студентів з дисциплін, програми практик; – методичні вказівки щодо виконання кваліфікаційних робіт. – віртуальне навчальне середовище Moodle (https://e-learn..uzhnu.edu.ua/
9 - Академічна мобільність	
Національна кредитна мобільність	Академічна мобільність студентів здійснюється на основі двосторонніх угод, укладених між ДВНЗ «Ужгородським національним університетом» та закладами вищої освіти України.
Міжнародна кредитна мобільність	Відповідно до Положення про академічну мобільність студентів у ДВНЗ «Ужгородський національний університет» https://www.uzhnu.edu.ua/uk/infocentre/get/21269 , встановлено загальний порядок організації академічної мобільності студентів. Здійснюється згідно програми міжнародної академічної мобільності «Еразмус +».
Навчання іноземних здобувачів вищої освіти	До ДВНЗ «УжНУ» приймаються іноземні громадяни, а також особи без громадянства, які проживають на території України на законних підставах. Особливості вступу та навчання визначаються Положенням про навчання іноземних громадян у ДВНЗ «Ужгородський національний університет» https://www.uzhnu.edu.ua/uk/infocentre/get/9378

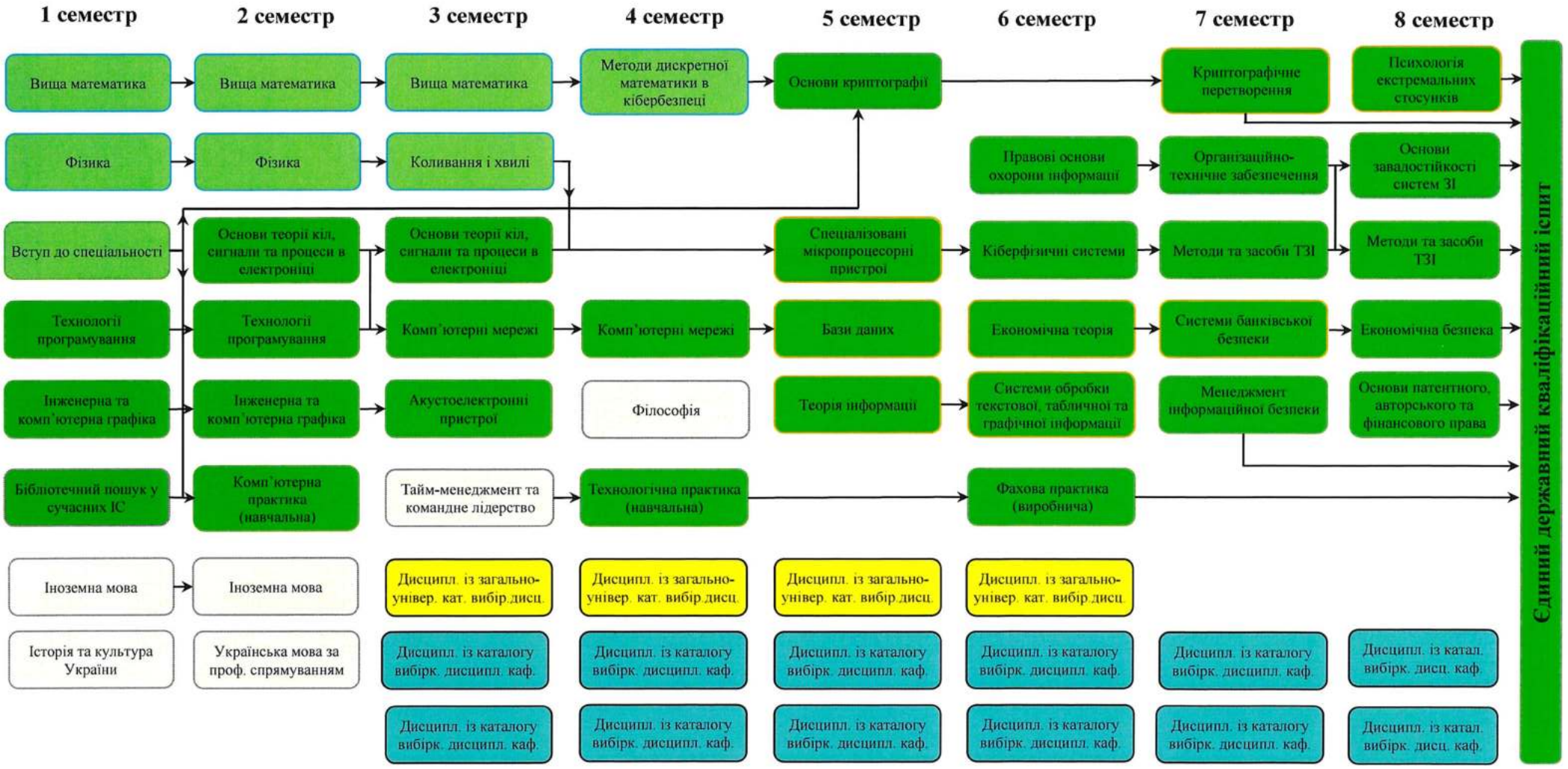
2. Перелік компонент освітньо-професійної програми та їх логічна послідовність

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
Обов'язкові компоненти ОПП			
ОК1	Іноземна мова	6	Залік, іспит
ОК2	Історія та культура України	3	Залік
ОК3	Українська мова за професійним спрямуванням	3	Залік
ОК4	Філософія	3	Залік
ОК5	Вступ до спеціальності	3	Залік
ОК6	Фізика	10	Іспит
ОК7	Вища математика	11,5	Іспит
ОК8	Коливання і хвилі	3	Іспит
ОК9	Методи дискретної математики в кібербезпеці	4,5	Іспит
ОК10	Тайм-менеджмент та командне лідерство	3	Залік
ОК11	Бібліотечний пошук у сучасних інформаційних системах	3	Залік
ОК12	Технології програмування	10,5	Іспит
ОК13	Інженерна та комп'ютерна графіка	7	Залік
ОК14	Основи теорії кіл, сигнали та процеси в електроніці	6	Залік, іспит
ОК15	Комп'ютерні мережі	8,5	Залік, іспит
ОК16	Акустоелектронні пристрої	4	Іспит
ОК17	Спеціалізовані мікропроцесорні пристрої	4	Іспит
ОК18	Основи криптографії	3	Іспит
ОК19	Економічна теорія	3	Залік
ОК20	Кіберфізичні системи	4	Іспит
ОК21	Системи обробки текстової, табличної та графічної інформації	3	Іспит
ОК22	Бази даних	5	Іспит
ОК23	Теорія інформації	7	Іспит
ОК24	Правові основи охорони інформації	3	Іспит

ОК25	Організаційно-технічне забезпечення систем захисту інформації	5,5	Іспит
ОК26	Методи і засоби технічного захисту інформації	11,5	Залік, іспит
ОК27	Менеджмент інформаційної безпеки	3	Залік
ОК28	Криптографічне перетворення	4	Залік
ОК29	Системи банківської безпеки	5	Іспит
ОК30	Основи патентного, авторського та фінансового права	3	Іспит
ОК31	Психологія екстремальних стосунків	3	Залік
ОК32	Основи завадостійкості систем захисту інформації	6	Іспит
ОК33	Економічна безпека	3	Залік
ОК34	Комп'ютерна практика (навчальна)	3	Диференційований залік
ОК35	Технологічна практика (навчальна)	6	Диференційований залік
ОК36	Фахова практика (виробнича)	6	Диференційований залік
ОК37	Єдиний державний кваліфікаційний іспит		Кваліфікаційний іспит
Загальний обсяг обов`язкових компонентів:		**180 кредитів**	
Вибіркові компоненти ОПП			
ВБ1	Дисципліна із загальноуніверситетського каталогу вибіркових дисциплін	3	Залік
ВБ2	Дисципліна із загальноуніверситетського каталогу вибіркових дисциплін	3	Залік
ВБ3	Дисципліна із загальноуніверситетського каталогу вибіркових дисциплін	3	Залік
ВБ4	Дисципліна із загальноуніверситетського каталогу вибіркових дисциплін	3	Залік
ВБ5	Дисципліна із каталогу вибіркових дисциплін кафедри	4	Залік
ВБ6	Дисципліна із каталогу вибіркових дисциплін кафедри	4	Залік

ВБ7	Дисципліна із каталогу вибіркових дисциплін кафедри	4	Залік
ВБ8	Дисципліна із каталогу вибіркових дисциплін кафедри	4	Залік
ВБ9	Дисципліна із каталогу вибіркових дисциплін кафедри	4	Залік
ВБ10	Дисципліна із каталогу вибіркових дисциплін кафедри	4	Залік
ВБ11	Дисципліна із каталогу вибіркових дисциплін кафедри	4	Залік
ВБ12	Дисципліна із каталогу вибіркових дисциплін кафедри	4	Залік
ВБ13	Дисципліна із каталогу вибіркових дисциплін кафедри	4	Залік
ВБ14	Дисципліна із каталогу вибіркових дисциплін кафедри	4	Залік
ВБ15	Дисципліна із каталогу вибіркових дисциплін кафедри	4	Залік
ВБ16	Дисципліна із каталогу вибіркових дисциплін кафедри	4	Залік
Загальний обсяг вибіркових компонентів:		**60 кредитів**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ:		**240 кредитів**	

2.2. Структурно-логічна схема освітньо-професійної програми



2.3. Форма атестації здобувачів вищої освіти

Атестація здобувачів першого (бакалаврського) рівня вищої освіти за спеціальністю 125 Кібербезпека та захист інформації в межах освітньо-професійної програми «Системи технічного захисту інформації» здійснюється у формі єдиного державного кваліфікаційного іспиту за умови успішного проходження атестації університет видає документ встановленого зразка про присудження ступеня бакалавра із присвоєнням кваліфікації: бакалавр з кібербезпеки.

Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених стандартом вищої освіти за спеціальністю 125 Кібербезпека та захист інформації, а також освітньо-професійною програмою «Системи технічного захисту інформації».

2.4. Матриця відповідності програмних компетентностей компонентам освітньо-професійної програми

	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ОК14	ОК15	ОК16	ОК17	ОК18	ОК19	ОК20	ОК21	ОК22	ОК23	ОК24	ОК25	ОК26	ОК27	ОК28	ОК29	ОК30	ОК31	ОК32	ОК33	ОК34	ОК35	ОК36	ОК37
ЗК1					+	+	+	+										+		+	+		+	+		+	+	+	+	+	+	+	+	+	+	+	+
ЗК2					+			+							+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ЗК3	+		+					+																													+
ЗК4			+		+										+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ЗК5			+		+		+	+	+	+	+	+	+			+		+		+		+		+		+	+	+		+	+						+
ЗК6		+	+		+																																+
ЗК7		+	+	+	+																																+
ЗК8					+				+				+		+		+			+	+	+	+	+	+	+	+	+	+	+				+	+	+	+
ФК1					+			+					+		+		+				+	+	+	+	+				+	+							+
ФК2					+			+					+		+		+					+	+	+	+				+	+							+
ФК3										+											+																+

ФК4					+								+		+		+					+	+	+	+				+	+						+
ФК5												+							+								+				+			+	+	+
ФК6															+						+		+		+					+		+				+
ФК7																		+			+		+	+			+		+		+			+	+	+	+
ФК8														+							+	+	+		+					+	+		+				+
ФК9													+								+		+		+					+		+		+	+	+	+
ФК10								+							+		+				+	+	+	+					+							+
ФК11												+																				+		+	+	+	+
ФК12																		+															+	+	+	+
ФК13						+						+		+		+																	+				+
ФК14																							+	+		+	+	+	+								+

2.5. Матриця забезпечення програмних результатів навчання (ПРН) відповідними компонентами освітньо-професійної програми

	ОК1	**ОК2**	**ОК3**	**ОК4**	**ОК5**	**ОК6**	**ОК7**	**ОК8**	**ОК9**	**ОК10**	**ОК11**	**ОК12**	**ОК13**	**ОК14**	**ОК15**	**ОК16**	**ОК17**	**ОК18**	**ОК19**	**ОК20**	**ОК21**	**ОК22**	**ОК23**	**ОК24**	**ОК25**	**ОК26**	**ОК27**	**ОК28**	**ОК29**	**ОК30**	**ОК31**	**ОК32**	**ОК33**	**ОК34**	**ОК35**	**ОК36**	**ОК37**
ПРН1	+							+													+						+							+	+	+	+
ПРН2			+					+							+			+				+			+			+		+	+			+	+	+	+
ПРН3					+			+					+			+					+						+		+						+	+	+
ПРН4			+		+															+				+							+				+	+	+
ПРН5					+											+			+							+									+	+	+
ПРН6					+										+						+				+		+					+			+	+	+
ПРН7					+															+				+						+							+

ПРН8																		+					+		+				+			+					+
ПРН9					+										+				+										+				+				+
ПРН10																	+	+			+		+			+		+				+					
ПРН11															+				+			+				+	+			+	+	+					+
ПРН12														+		+				+			+					+						+	+	+	+
ПРН13																		+			+	+	+			+		+						+		+	+	
ПРН14																			+													+						+
ПРН15																				+	+		+					+								+	+	+
ПРН16					+				+		+			+					+				+		+		+	+				+		+			+	
ПРН17													+										+					+								+	+	+
ПРН18														+					+		+		+					+			+					+		
ПРН19			+			+		+														+	+	+			+	+									+
ПРН20															+					+										+				+		+		+
ПРН21																	+	+			+		+			+		+				+					
ПРН22							+		+						+				+			+				+	+				+	+			+	+	+
ПРН23														+		+				+			+					+							+	+	
ПРН24																	+			+	+	+			+		+						+		+	+	+
ПРН25				+				+		+				+				+		+																	+
ПРН26																							+					+	+			+			+	+	+
ПРН27		+			+		+							+				+		+															+		
ПРН28																							+					+	+			+			+		+
ПРН29														+				+		+																	+
ПРН30																+				+		+			+		+					+		+	+	+	+
ПРН31													+									+	+				+	+								+	
ПРН32							+		+											+				+		+											+
ПРН33															+				+		+				+							+		+		+	+

ПРН34															+							+					+					+				+		+
ПРН35															+				+			+				+			+	+				+			+		+
ПРН36																+				+			+					+										+
ПРН37																	+			+	+	+			+		+									+		
ПРН38																		+		+																	+	+
ПРН39																							+					+	+			+				+		
ПРН40																		+		+																	+		+
ПРН41																							+					+	+			+				+		+
ПРН42																		+		+																			+
ПРН43																+				+		+			+		+					+			+		
ПРН44												+				+			+				+		+	+		+		+						+	+
ПРН45													+				+			+																		
ПРН46														+			+	+	+			+					+									+	+	+
ПРН47								+							+		+															+						+
ПРН48								+												+				+		+				+					+	+	+
ПРН48															+		+																					+
ПРН49																				+				+		+				+					+	+	+
ПРН50															+		+																			+	+	+
ПРН51													+				+		+			+				+	+								+	+	+
ПРН52													+									+	+				+	+									+
ПРН53																	+				+			+							+		+	+	+	+	+
ПРН54		+	+															+				+			+		+										+
ПРН55																			+			+	+	+			+	+	+						+	+	+
ПРН56																				+		+					+								+	+	+
ПРН57																									+							+		+		+	+