МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені Ігоря Сікорського»

ЗАТВЕРДЖЕНО
Вченою радою
КПІ ім. Ігоря Сікорського
(протокол №10 від 13.12 2021 р.)
Голова Вченої ради
_____ Михайло ІЛЬЧЕНКО

СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

SYSTEMS OF TECHNICAL PROTECTION OF INFORMATION

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

першого (бакалаврського) рівня вищої освіти

за спеціальністю	**125 Кібербезпека**
галузі знань	**12 Інформаційні технології**
кваліфікація	**Бакалавр з кібербезпеки**

Введено в дію з 2022/2023 навч. року
наказом ректора
КПІ ім. Ігоря Сікорського
від 15.02. 2022 р. № НОМ/75/2022

Київ – 2021

ПРЕАМБУЛА

РОЗРОБЛЕНО проєктною групою:

Керівник проєктної групи:
Новіков Олексій Миколайович,
директор Навчально-Наукового Фізико-Технічного інституту,
д.т.н., професор

Члени проєктної групи:
Ланде Дмитро Володимирович,
завідувач кафедри інформаційної безпеки, д.т.н., професор,

Мачуський Євген Андрійович,
професор кафедри інформаційної безпеки, д.т.н., професор,

Луценко Володимир Миколайович,
доцент кафедри інформаційної безпеки, к.т.н., доцент

Прогонов Дмитро Олександрович,
доцент кафедри інформаційної безпеки, к.т.н., доцент

За підготовку здобувачів вищої освіти за освітньою програмою відповідає кафедра інформаційної безпеки

ПОГОДЖЕНО:

Науково-методичною комісією КПІ ім. Ігоря Сікорського зі спеціальності

125 Кібербезпека

Голова НМКУ зі спеціальності 125 Кібербезпека

_____ Олексій НОВІКОВ
(протокол № 3 від «03» 12 20 21 р.)

Методичною радою КПІ ім. Ігоря Сікорського

Заступник голови Методичної ради

_____ Анатолій МЕЛЬНИЧЕНКО
(протокол № 2 від «09» 12 2021 р.)

ВРАХОВАНО:

фахову експертизу стейкхолдерів:

Представники роботодавців:
Мохонько Олексій Анатолійович, к.ф.-м.н.,
R&D директор з інформаційної безпеки,
ТОВ "Самсунг Електронікс Україна Компані",
український центр досліджень та розробок Samsung

Соловйов Євгеній Валерійович,
Начальник Управління інформаційними технологіями
Служби зовнішньої розвідки України

Авдєєв Ігор Володимирович,
полковник служби цивільного захисту,
Начальник Центру оперативного зв'язку,
телекомунікаційних систем та інформаційних технологій
Державної служби з надзвичайних ситуацій

Представники студентських організацій:
Зібаров Дмитро, в.о. голови Профбюро НН ФТІ,
студент 3 курсу бакалаврату за
спеціальністю 125 Кібербезпека

Городівський Владислав,
виборний представник студентів

Рецензії-відгуки стейкхолдерів додаються.

Освітню програму оновлено у зв'язку з набуттям Фізико-технічним інститутом статусу Навчально-науковий Фізико-технічний інститут. Внесено зміни у склад проєктної групи та склад стейкхолдерів. Внесено корективи щодо придатності до працевлаштування згідно Зміни №10 до Державного класифікатору професій ДК 003:2010. Враховано Постанову від 19 травня 2021 р. № 497 щодо внесення єдиного державного комплексного іспиту зі спеціальності до атестації здобувачів вищої освіти та Постанову Кабінету Міністрів України від 24 березня 2021 р. № 365 «Про внесення змін до постанови Кабінету Міністрів України від 30 грудня 2015 р. № 1187 Про затвердження Ліцензійних умов провадження освітньої діяльності»

Освітню програму обговорено після надходження всіх побажань та пропозицій від роботодавців, здобувачів і випускників освітньої програми. Схвалено на розширеному засіданні кафедри інформаційної безпеки (протокол № 12 від «09» 11 2021 р.).

ЗМІСТ

1. ПРОФІЛЬ ОСВІТНЬОЇ ПРОГРАМИ

«Системи технічного захисту інформації»
зі спеціальності 125 Кібербезпека

1 – Загальна інформація	
Повна назва ЗВО та інституту/ факультету	Національний технічний університет України “Київський політехнічний інститут імені Ігоря Сікорського” Навчально-науковий фізико-технічний інститут
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Ступінь – бакалавр Кваліфікація – бакалавр з кібербезпеки
Рівень з НРК	НРК України – 6 рівень QF-EHEA – перший цикл EQF-LLL – 6 рівень
Офіційна назва освітньої програми	Системи технічного захисту інформації
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний, 240 кредитів, термін навчання 3 роки 10 місяців
Наявність акредитації	Сертифікат акредитації спеціальності УД 11010979, дійсний до 01.07.2028
Передумови	Повна загальна середня освіта
Мова(и) викладання	Українська
Термін дії освітньої програми	До наступної акредитації
Інтернет-адреса постійного розміщення освітньої програми	https://osvita.kpi.ua/node/103, (розділ «Освітні програми»), http://is.ipt.kpi.ua/navchalni-programi-2

2 – Мета освітньої програми

Метою освітньої програми є підготовка фахівців, здатних вирішувати складні задачі в галузі кібернетичної безпеки особистості, спільноти, суспільства та держави, всебічного професійного, інтелектуального, соціального та творчого розвитку особистості на найвищих рівнях досконалості в освітньо-науковому середовищі.

З цією метою освітня програма передбачає:

1. Фундаментальну підготовку фахівців в галузі математики, фізики, філософії природи та суспільства;
2. Гармонізовану спеціалізовану підготовку фахівців в галузі інформаційно-комунікаційних систем різної фізичної природи: від класичної термодинаміки і електродинаміки до квантової гравідинаміки і хромодинаміки;
3. Спеціалізовану гармонізовану підготовку фахівців в галузі континуальної, дискретної та квантової обробки інформації математичними та фізичними методами та засобами;
4. Гармонізовану міждисциплінарну організаційно-економічну та нормативно-правову підготовку фахівців, здатних створювати нові стартапи та успішно конкурувати на високотехнологічних ринках праці;
5. Міждисциплінарну педагогічно-психологічну підготовку фахівців для подальшого саморозвитку і праці в різних галузях освіти, науки та інженерії.

3 – Характеристика освітньої програми	
Предметна область	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; • процеси управління інформаційною та/або кібербезпекою об’єктів, що підлягають захисту. Цілі навчання підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки. Теоретичний зміст предметної області Знання • законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; • принципів супроводу систем та комплексів інформаційної та/або кібербезпеки; • теорії, моделей та принципів управління доступом до інформаційних ресурсів; • теорії систем управління інформаційною та/або кібербезпекою; • методів та засобів виявлення, управління та ідентифікації ризиків; • методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації; • методів та засобів технічного та криптографічного захисту інформації; • сучасних інформаційно-комунікаційних технологій; • сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій; • автоматизованих систем проектування Методи, методики та технології: • Методи, методики та інформаційно-комунікаційні технології ті інші технології забезпечення інформаційної та/або кібербезпеки. Інструменти та обладнання: • системи розробки, забезпечення, моніторингу та контролю процесів інформаційної та/або кібербезпеки; • сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
Орієнтація освітньої програми	Освітньо-професійна

Основний фокус освітньої програми	Основні фокуси програми: 1. Посилена підготовка в галузі дискретної математики та квантової інформатики; 2. Посилена підготовка в галузі механіки, електроніки, радіотехніки, акустики, оптоелектроніки; 3. Посилена підготовка в галузі дискретної обробки інформації логіко-математичними методами та фізико-технічними засобами; 4. Фундаментальна підготовка щодо проектування, розробки, впровадження та супроводу комплексних систем захисту інформації, що циркулює на об'єктах інформаційної діяльності державної та приватної форми власності; 5. Посилена підготовка в галузі міждисциплінарного системного аналізу з метою створення комплексних систем захисту інформаційних потоків у комунікаційних мережах; 6. Силабуси та методичне забезпечення підготовки здобувачів вищої освіти щорічно переглядаються з метою врахування нових науково-технологічних здобутків у галузі кібернетичної безпеки; 7. Широке залучення здобувачів вищої освіти до участі у провідних міжнародних конференціях в галузі кібернетичної безпеки; 8. Проведення щорічних конференцій та олімпіад з нових напрямків кібернетичної безпеки з метою навчання здобувачів вищої освіти розробці індивідуальних стартапів на етапі підготовки кваліфікаційної роботи. Ключові слова: кібернетична безпека, технічні засоби захисту інформації, технічний аудит, проектування та створення комплексів технічного захисту інформації
Особливості програми	1. Перехід від стандартних методів класичної математики та класичної фізики до квантово-механічних та квантово-обчислювальних напрямків розвитку сучасної математичної фізики; 2. Посилена підготовка в галузі природничих наук (математики, фізики), а також технічних наук (програмування, обробки сигналів різної фізичної природи, розробка та оптимізація пристроїв захисту інформації); 3. Фундаментальна підготовка щодо проектування, розробки, впровадження та супроводу комплексних систем захисту інформації, що циркулює на об'єктах інформаційної діяльності державної та приватної форми власності; 4. Проходження практик на провідних підприємствах галузі захисту інформації.

4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Відповідно до Державного класифікатору професій ДК 003:2010 зі Зміною №10 випускники можуть працювати на посадах, що відповідають класифікаційним угрупованням: 2139.2 фахівець з технічного захисту інформації 3121 Фахівець з інформаційних технологій. 3139 Фахівець із організації захисту інформації з обмеженим доступом; Фахівець із організації інформаційної безпеки Можуть працювати фахівцями із захисту інформації в складі інформаційних департаментів підприємств та банків, співробітниками служб захисту інформації; аудиторами інформаційної та кібернетичної безпеки, адміністраторами інформаційної та кібернетичної безпеки, проектувальниками систем захисту інформації в кіберпросторі; розробниками програмних та програмно-апаратних засобів захисту інформації в кіберпросторі, аналітиками кібербезпеки в установах державної та інших форм власності, спеціалістами з забезпечення кібербезпеки в кіберфізичних системах, зокрема, об'єктах критичної інфраструктури.
Подальше навчання	Продовження освіти за другим (магістерським) рівнем вищої освіти
5 – Викладання та оцінювання	
Викладання та навчання	Програмою передбачено студентоцентроване навчання. Викладання проводиться у таких формах: лекції, практичні та семінарські заняття, комп'ютерні практикуми і лабораторні роботи; курсові проекти і роботи; технологія змішаного навчання, практики; виконання дипломного проекту і дипломної роботи
Оцінювання	Оцінювання знань студентів здійснюється у відповідності до Положення про систему оцінювання результатів навчання КПІ ім. Ігоря Сікорського за усіма видами аудиторної та позааудиторної роботи (вхідний, поточний, календарний, підсумковий контроль); екзамени, заліки, індивідуальні завдання тощо.
6 – Програмні компетентності	
Інтегральна Компетентність	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і/або кібербезпеки, що характеризуються комплексністю та неповною визначеністю умов.
Загальні компетентності (КЗ)	
КЗ 1	Здатність застосовувати знання у практичних ситуаціях.
КЗ 2	Знання та розуміння предметної області та розуміння професії.
КЗ 3	Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.
КЗ 4	Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.
КЗ 5	Здатність до пошуку, оброблення та аналізу інформації.
КЗ 6	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;
КЗ 7	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.

Фахові компетентності (КФ)	
КФ 1	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/або кібербезпеки.
КФ 2	Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.
КФ 3	Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.
КФ 4	Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки
КФ 5	Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.
КФ 6	Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класів та походження.
КФ 7	Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)
КФ 8	Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.
КФ 9	Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.
КФ 10	Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.
КФ 11	Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.
КФ 12	Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.
КФ 13	Здатність досліджувати ефективність роботи давачів сигналів різної фізичної природи, проводити їх оптимізацію для заданих умов роботи
КФ 14	Здатність виявляти та локалізувати джерела небезпечних сигналів в умовах обмеженості апріорних даних щодо їх характеристик та фізичної природи
КФ 15	Здатність проводити спеціальні дослідження об’єктів інформаційної діяльності згідно нормативних актів в галузі технічного захисту інформації
7 – Програмні результати навчання	
ПРН 1	Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації
ПРН 2	Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність
ПРН 3	Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач

ПРН 4	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 5	Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат
ПРН 6	Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності
ПРН 7	Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки
ПРН 8	Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки
ПРН 9	Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки
ПРН 10	Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем
ПРН 11	Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах
ПРН 12	Розробляти моделі загроз та порушника
ПРН 13	Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних
ПРН 14	Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень
ПРН 15	Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій
ПРН 16	Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів
ПРН 17	Забезпечувати процеси захисту та функціонування інформаційно- телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; та моделей захисту електронних даних
ПРН 18	Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів
ПРН 19	Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах
ПРН 20	Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах

ПРН 21	Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних системах
ПРН 22	Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно- телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки
ПРН 23	Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах
ПРН 24	Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових)
ПРН 25	Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту
ПРН 26	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 27	Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах
ПРН 28	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 29	Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційних та інформаційно-телекомунікаційних системах, ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів
ПРН 30	Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем
ПРН 31	Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем
ПРН 32	Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки
ПРН 33	Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків
ПРН 34	Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації
ПРН 35	Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно- телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки

ПРН 36	Виявляти небезпечні сигнали технічних засобів
ПРН 37	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 38	Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації
ПРН 39	Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах
ПРН 40	Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації
ПРН 41	Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур
ПРН 42	Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки
ПРН 43	Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів
ПРН 44	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 45	Застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів
ПРН 46	Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах
ПРН 47	Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації
ПРН 48	Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах
ПРН 49	Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах
ПРН 50	Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення втрогнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних)
ПРН 51	Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах
ПРН 52	Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах
ПРН 53	Вирішувати задачі аналізу програмного коду на наявність можливих загроз

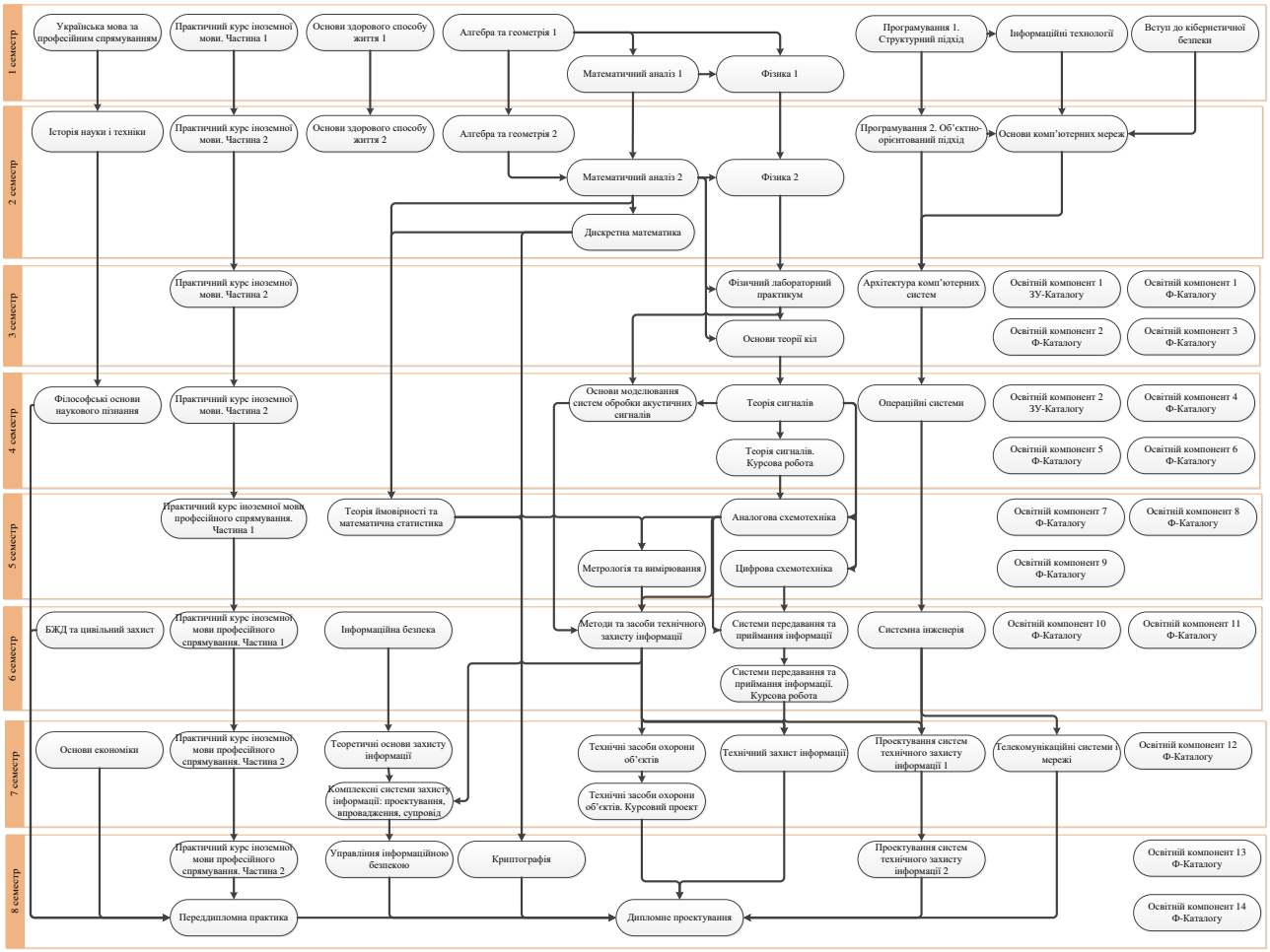
ПРН 54	Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні
ПРН 55	Вирішувати задачі розробки, впровадження та супроводу систем моніторингу джерел небезпечних сигналів різної фізичної природи
ПРН 56	Здійснювати аналіз та обробку сигналів різної фізичної природи з використанням новітніх методів статистичного, спектрального та структурного аналізу
ПРН 57	Застосовувати нормативні документи в галузі технічного захисту інформації при вирішенні задач розробки, впровадження та супроводу комплексних систем захисту інформації
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Відповідно до кадрових вимог щодо забезпечення провадження освітньої діяльності для відповідного рівня ВО, затверджених Постановою Кабінету Міністрів України від 30.12.2015 р. № 1187 (в чинній редакції).
Матеріально-технічне забезпечення	Відповідно до технологічних вимог щодо матеріально-технічного забезпечення освітньої діяльності відповідного рівня ВО, затверджених Постановою Кабінету Міністрів України від 30.12.2015 р. № 1187 (в чинній редакції). Використання обладнання для проведення лекцій у форматі презентацій, мережевих технологій, зокрема на платформі дистанційного навчання Sikorsky.
Інформаційне та навчально-методичне забезпечення	Відповідно до технологічних вимог щодо навчально-методичного та інформаційного забезпечення освітньої діяльності відповідного рівня ВО, затверджених Постановою Кабінету Міністрів України від 30.12.2015 р. № 1187 (в чинній редакції). Користування Науково-технічною бібліотекою КПІ ім. Ігоря Сікорського.
9 – Академічна мобільність	
Національна кредитна мобільність	Участь студентів в програмах академічної мобільності, можливість укладення угод одержання студентами подвійних дипломів
Міжнародна кредитна мобільність	Можливість укладення угод про міжнародну академічну мобільність, про подвійне дипломування, про тривалі міжнародні проекти
Навчання іноземних здобувачів вищої освіти	Навчання іноземних здобувачів ВО, які опановують ОП за програмами міжнародної академічної мобільності, навчання може проводитись англійською або українською мовою, за умови володіння здобувачем мовою навчання на рівні не нижче В2.

2. ПЕРЕЛІК КОМПОНЕНТ ОСВІТНЬОЇ ПРОГРАМИ

Код н/д	Компоненти освітньої програми (навчальні дисципліни, практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
1. НОРМАТИВНІ освітні компоненти			
1.1. Цикл загальної підготовки			
ЗО 1	Українська мова за професійним спрямуванням	2	Залік
ЗО 2	Історія науки та техніки	2	Залік
ЗО 3	Основи здорового способу життя	3	Залік
ЗО 4.1	Практичний курс іноземної мови. Частина 1	3	Залік
ЗО 4.2	Практичний курс іноземної мови. Частина 2	3	Залік
ЗО 5	Основи економіки	2	Залік
ЗО 6	БЖД та цивільний захист	2	Залік
ЗО 7.1	Математичний аналіз. Частина 1	6,5	Екзамен
ЗО 7.2	Математичний аналіз. Частина 2	5,5	Екзамен
ЗО 8.1	Фізика. Частина 1	4,5	Залік
ЗО 8.2	Фізика. Частина 2	5,5	Екзамен
ЗО 9	Теорія ймовірності та математична статистика	2,5	Залік
ЗО 10	Дискретна математика	4,5	Екзамен
ЗО 11.1	Програмування. Частина 1. Структурний підхід	4,5	Екзамен
ЗО 11.2	Програмування.Частина 2. Об’єктно-орієнтований підхід	3,5	Залік
ЗО 12.1	Алгебра та геометрія. Частина 1	4,5	Екзамен
ЗО 12.2	Алгебра та геометрія. Частина 2	3	Залік
ЗО 13	Вступ до кібернетичної безпеки	2	Залік
ЗО 14	Інформаційні технології	3	Залік
ЗО 15	Основи комп'ютерних мереж	3	Залік
ЗО 16	Архітектура комп’ютерних систем	4	Екзамен
ЗО 17	Операційні системи	4	Екзамен
ЗО 18	Теоретичні основи захисту інформації	4	Екзамен
ЗО 19	Системна інженерія	6,5	Залік
ЗО 20	Криптографія та стеганографія	3,5	Залік
ЗО 21	Комплексні системи захисту інформації: проектування, впровадження, супровід	4	Екзамен
ЗО 22	Управління інформаційною безпекою	2	Залік
ЗО 23.1	Практичний курс іноземної мови професійного спрямування. Частина 1	3	Залік
ЗО 23.2	Практичний курс іноземної мови професійного спрямування. Частина 2	3	Екзамен
ЗО 24	Філософські основи наукового пізнання	2	Залік
ЗО 25	Інформаційна безпека	2	Залік
ЗО 26	Переддипломна практика	6	Залік
ЗО 27	Дипломне проектування	6	Залік
1.2. Цикл професійної підготовки			
ПО 1	Фізичний лабораторний практикум	3	Залік
ПО 2	Основи теорії кіл	7,5	Екзамен

1	2	3	4
ПО 3	Теорія сигналів	4,5	Екзамен
ПО 4	Теорія сигналів. Курсова робота	1	Залік
ПО 5	Основи моделювання систем обробки акустичних сигналів	3	Залік
ПО 6	Аналогова схемотехніка	4	Екзамен
ПО 7	Цифрова схемотехніка	5	Екзамен
ПО 8	Метрологія та вимірювання	5	Екзамен
ПО 9	Системи передавання та приймання інформації	5	Екзамен
ПО 10	Системи передавання та приймання інформації. Курсова робота	1	Залік
ПО 11	Методи та засоби технічного захисту інформації	4	Екзамен
ПО 12	Технічний захист інформації	3	Залік
ПО 13	Телекомунікаційні системи і мережі	3	Залік
ПО 14	Технічні засоби охорони об’єктів	4	Екзамен
ПО 15	Технічні засоби охорони об’єктів. Курсовий проект	1,5	Залік
ПО 16.1	Проектування систем технічного захисту інформації. Частина 1	3	Залік
ПО 16.2	Проектування систем технічного захисту інформації. Частина 2	3	Екзамен
2. ВИБІРКОВІ освітні компоненти			
2.1. Цикл загальної підготовки (Вибіркові освітні компоненти з загально університетського Каталогу)			
ЗВ 1	Освітній компонент 1 ЗУ-Каталогу	2	Залік
ЗВ 2	Освітній компонент 2 ЗУ-Каталогу	2	Залік
2.2. Цикл професійної підготовки (Вибіркові освітні компоненти з міжфакультетського/факультетського/ кафедрального Каталогів)			
ПВ 1	Освітній компонент 1 Ф-Каталогу	4	Залік
ПВ 2	Освітній компонент 2 Ф-Каталогу	4	Залік
ПВ 3	Освітній компонент 3 Ф-Каталогу	4	Залік
ПВ 4	Освітній компонент 4 Ф-Каталогу	4	Залік
ПВ 5	Освітній компонент 5 Ф-Каталогу	4	Залік
ПВ 6	Освітній компонент 6 Ф-Каталогу	4	Залік
ПВ 7	Освітній компонент 7 Ф-Каталогу	4	Залік
ПВ 8	Освітній компонент 8 Ф-Каталогу	4	Залік
ПВ 9	Освітній компонент 9 Ф-Каталогу	4	Залік
ПВ 10	Освітній компонент 10 Ф-Каталогу	4	Залік
ПВ 11	Освітній компонент 11 Ф-Каталогу	4	Залік
ПВ 12	Освітня компонента 12 Ф-Каталогу	4	Залік
ПВ 13	Освітня компонента 13 Ф-Каталогу	4	Залік
ПВ 14	Освітня компонента 14 Ф-Каталогу	4	Залік
Загальний обсяг **обов’язкових компонент:**		**180**	
Загальний обсяг **вибіркових компонент:**		**60**	
Обсяг освітніх компонентів, що забезпечують здобуття компетентностей, визначених СВО		**180**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**240**	

3. СТРУКТУРНО-ЛОГІЧНА СХЕМА ОСВІТНЬОЇ ПРОГРАМИ



4. ФОРМА АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Атестація здобувачів вищої освіти за освітньо-професійною програмою «Системи технічного захисту інформації» здійснюється у формі публічного захисту кваліфікаційного проекту/роботи та виконання єдиного державного кваліфікаційного іспиту за спеціальністю. Атестація завершується видачею документу встановленого зразка про присвоєння кваліфікації бакалавра з кібербезпеки.

На атестацію виноситься сукупність знань, умінь, навичок, інших компетентностей, набутих особою у процесі навчання. До атестації допускаються студенти, які виконали всі вимоги програми підготовки.

Кваліфікаційна робота перевіряється на плагіат та після захисту розміщується в репозиторії науково-технічної бібліотеки університету для вільного доступу.

5. МАТРИЦЯ ВІДПОВІДНОСТІ ПРОГРАМНИХ КОМПЕТЕНТНОСТЕЙ КОМПОНЕНТАМ ОСВІТНЬОЇ ПРОГРАМИ

	ЗО 1	ЗО2	ЗО3	ЗО 4	ЗО 5	ЗО 6	ЗО 7	ЗО 8	ЗО 9	ЗО 10	ЗО 11	ЗО 12	ЗО 13	ЗО 14	ЗО 15	ЗО 16	ЗО 17	ЗО 18	ЗО 19	ЗО 20	ЗО 21	ЗО 22	ЗО 23	ЗО 24	ЗО 25	ЗО 26	ЗО 27	ПО 1	ПО 2	ПО 3	ПО 4	ПО 5	ПО 6	ПО 7	ПО 8	ПО 9	ПО 10	ПО 11	ПО 12	ПО 13	ПО 14	ПО 15	ПО 16
КЗ 1							+	+	+	+	+				+	+	+	+	+	+	+	+				+	+	+		+		+									+	+
КЗ 2											+		+					+	+	+	+	+							+	+			+	+	+	+		+	+	+	+		
КЗ 3	+			+																			+																				
КЗ 4																		+	+		+	+										+	+	+	+	+	+	+	+	+	+		
КЗ 5																			+		+	+		+	+							+							+		+		+	
КЗ 6		+				+																			+																		
КЗ 7	+	+	+	+	+	+																	+	+																			
КФ 1																		+			+	+																						
КФ 2							+		+	+	+	+		+	+	+	+																+										+
КФ 3											+			+	+	+	+		+		+							+	+	+	+		+	+	+	+	+	+	+	+	+	+	+
КФ 4																		+			+	+																						+
КФ 5															+	+	+				+															+	+			+				
КФ 6															+	+	+				+												+	+						+			
КФ 7																		+	+		+	+																				+	+	+
КФ 8																		+			+	+																+						

КФ 15	КФ 14	КФ 13	КФ 12	КФ 11	КФ 10	КФ 9	
							ЗО 1
							ЗО2
							ЗО3
							ЗО 4
							ЗО 5
							ЗО 6
							ЗО 7
	+	+					ЗО 8
	+	+					ЗО 9
							ЗО 10
							ЗО 11
							ЗО 12
+							ЗО 13
							ЗО 14
				+			ЗО 15
				+			ЗО 16
				+			ЗО 17
+			+			+	ЗО 18
						+	ЗО 19
					+		ЗО 20
			+	+		+	ЗО 21
						+	ЗО 22
							ЗО 23
							ЗО 24
							ЗО 25
						+	ЗО 26
						+	ЗО 27
+	+	+					ПО 1
+	+	+					ПО 2
+	+	+					ПО 3
+	+	+					ПО 4
+	+	+					ПО 5
+		+					ПО 6
+		+					ПО 7
+	+	+					ПО 8
+	+	+					ПО 9
+	+	+					ПО 10
			+		+	+	ПО 11
+					+	+	ПО 12
				+			ПО 13
					+		ПО 14
					+		ПО 15
			+			+	ПО 16

6. МАТРИЦЯ ЗАБЕЗПЕЧЕННЯ ПРОГРАМНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ КОМПОНЕНТАМИ ОСВІТНЬОЇ ПРОГРАМИ

	ЗО 1	ЗО2	ЗО3	ЗО 4	ЗО 5	ЗО 6	ЗО 7	ЗО 8	ЗО 9	ЗО 10	ЗО 11	ЗО 12	ЗО 13	ЗО 14	ЗО 15	ЗО 16	ЗО 17	ЗО 18	ЗО 19	ЗО 20	ЗО 21	ЗО 22	ЗО 23	ЗО 24	ЗО 25	ЗО 26	ЗО 27	ПО 1	ПО 2	ПО 3	ПО 4	ПО 5	ПО 6	ПО 7	ПО 8	ПО 9	ПО 10	ПО 11	ПО 12	ПО 13	ПО 14	ПО 15	ПО 16
ПРН 1	+			+																			+				+																
ПРН 2					+	+	+	+		+	+	+	+						+	+						+	+		+	+		+	+	+		+		+	+		+		+
ПРН 3				+			+	+		+	+	+	+	+	+			+	+			+	+	+	+	+		+	+		+	+	+		+		+	+	+	+		+
ПРН 4							+	+	+	+	+	+		+	+	+	+	+	+	+	+	+		+		+		+	+		+	+	+		+		+	+	+	+		+
ПРН 5				+	+		+	+	+	+	+	+	+	+	+	+	+	+		+		+	+	+			+		+	+		+	+	+		+		+	+	+			+
ПРН 6		+				+	+	+	+	+	+	+	+	+		+	+	+	+		+	+				+	+		+	+		+											
ПРН 7																			+			+			+	+	+											+	+		+	+	+	+
ПРН 8																						+			+		+																	
ПРН 9				+														+	+			+	+		+													+	+				+
ПРН 10											+		+			+	+	+	+		+	+			+	+										+	+	+	+				+
ПРН 11											+		+		+	+	+	+			+	+			+	+												+	+				+
ПРН 12									+				+					+			+	+			+	+																	+
ПРН 13																+			+			+				+	+													+			+

ПРН 28	ПРН 27	ПРН 26	ПРН 25	ПРН 24	ПРН 23	ПРН 22	ПРН 21	ПРН 20	ПРН 19	ПРН 18	ПРН 17	ПРН 16	ПРН 15	ПРН 14	
															ЗО 1
															ЗО2
															ЗО3
															ЗО 4
															ЗО 5
															ЗО 6
															ЗО 7
															ЗО 8
															ЗО 9
															ЗО 10
								+		+			+	+	ЗО 11
															ЗО 12
															ЗО 13
								+		+			+		ЗО 14
	+	+	+	+	+								+		ЗО 15
											+				ЗО 16
		+	+	+	+	+	+	+		+	+	+	+	+	ЗО 17
+		+			+		+		+		+	+		+	ЗО 18
													+		ЗО 19
	+				+						+	+	+		ЗО 20
+		+													ЗО 21
+			+	+	+	+	+		+		+			+	ЗО 22
															ЗО 23
															ЗО 24
												+			ЗО 25
	+	+			+		+	+		+			+		ЗО 26
+	+	+			+		+		+	+	+	+	+	+	ЗО 27
															ПО 1
															ПО 2
															ПО 3
															ПО 4
															ПО 5
															ПО 6
															ПО 7
															ПО 8
													+		ПО 9
													+		ПО 10
		+			+				+	+		+	+	+	ПО 11
		+			+				+	+		+	+	+	ПО 12
+								+	+		+		+	+	ПО 13
					+							+			ПО 14
					+							+			ПО 15
+	+	+	+	+	+		+		+	+	+	+	+	+	ПО 16

ПРН 43	ПРН 42	ПРН 41	ПРН 40	ПРН 39	ПРН 38	ПРН 37	ПРН 36	ПРН 35	ПРН 34	ПРН 33	ПРН 32	ПРН 31	ПРН 30	ПРН 29	
															ЗО 1
															ЗО2
															ЗО3
+															ЗО 4
										+					ЗО 5
										+					ЗО 6
															ЗО 7
			+		+	+	+								ЗО 8
													+	+	ЗО 9
															ЗО 10
															ЗО 11
															ЗО 12
	+														ЗО 13
															ЗО 14
															ЗО 15
															ЗО 16
		+						+			+	+			ЗО 17
+								+	+	+		+	+	+	ЗО 18
				+											ЗО 19
															ЗО 20
											+	+	+	+	ЗО 21
+	+	+						+	+	+	+	+	+	+	ЗО 22
+															ЗО 23
															ЗО 24
															ЗО 25
+			+		+	+	+	+					+	+	ЗО 26
+								+		+		+	+	+	ЗО 27
			+		+	+	+								ПО 1
			+		+	+									ПО 2
			+		+	+									ПО 3
			+		+	+									ПО 4
															ПО 5
			+	+	+	+	+								ПО 6
			+	+	+	+	+								ПО 7
			+		+	+	+								ПО 8
				+		+	+								ПО 9
				+		+	+								ПО 10
	+		+	+	+	+	+	+	+	+		+	+	+	ПО 11
	+		+	+	+	+	+	+	+	+		+	+	+	ПО 12
											+	+	+	+	ПО 13
	+		+	+	+				+			+	+		ПО 14
	+		+	+	+				+			+	+		ПО 15
									+	+		+	+	+	ПО 16

ПРН 57	ПРН 56	ПРН 55	ПРН 54	ПРН 53	ПРН 52	ПРН 51	ПРН 50	ПРН 49	ПРН 48	ПРН 47	ПРН 46	ПРН 45	ПРН 44	
			+											ЗО 1
			+											ЗО2
			+											ЗО3
			+											ЗО 4
			+										+	ЗО 5
			+											ЗО 6
														ЗО 7
	+	+												ЗО 8
	+	+									+	+		ЗО 9
														ЗО 10
				+	+	+	+	+						ЗО 11
														ЗО 12
+					+		+				+			ЗО 13
				+	+	+	+							ЗО 14
					+	+	+	+						ЗО 15
					+					+				ЗО 16
				+	+	+	+	+						ЗО 17
+								+			+	+	+	ЗО 18
						+								ЗО 19
									+	+				ЗО 20
+					+						+		+	ЗО 21
					+	+	+	+			+	+	+	ЗО 22
			+											ЗО 23
														ЗО 24
+			+										+	ЗО 25
				+	+	+	+	+	+	+				ЗО 26
				+	+					+	+	+	+	ЗО 27
+	+	+												ПО 1
+	+	+												ПО 2
+	+	+												ПО 3
+	+	+												ПО 4
+	+	+												ПО 5
+		+												ПО 6
+		+												ПО 7
+	+	+												ПО 8
+	+	+												ПО 9
+	+	+												ПО 10
						+	+	+						ПО 11
+						+	+	+						ПО 12
														ПО 13
						+								ПО 14
						+								ПО 15
					+	+	+	+					+	ПО 16