

ЗАТВЕРДЖЕНО

Вченою радою КПІ ім. Ігоря Сікорського

(протокол № 4 від «23» 04 2017 р.)

Системи технічного захисту інформації

Technical Information Protection Systems

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

другого (магістерського) рівня вищої освіти

за спеціальністю 125 Кібербезпека

галузі знань 12 Інформаційні технології

кваліфікація Магістр з кібербезпеки

Зміни та доповнення погоджено НМКУ 125

(протокол № 3 від «8» 06 2020 р.)

Освітню програму зі змінами та доповненнями

введено в дію з 2020 / 2021 навч. року

(наказ № 1/231 від «08» 07 2020 р.)

ПРЕАМБУЛА

РОЗРОБЛЕНО проєктною групою:

Керівник проєктної групи:

Мачуський Євген Андрійович,
В.о. завідувача кафедри фізико-технічних засобів
захисту інформації, д.т.н., професор

Члени проєктної групи:

Земляк Олександр Михайлович,
професор кафедри фізико-технічних засобів захисту інформації,
д.т.н., професор,

Луценко Володимир Миколайович,
доцент кафедри фізико-технічних засобів захисту інформації,
к.т.н., доцент

Прогонов Дмитро Олександрович,
доцент кафедри фізико-технічних засобів захисту інформації,
к.т.н., доцент

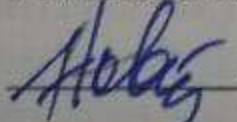
За підготовку здобувачів вищої освіти за освітньою програмою відповідає кафедра фізико-технічних засобів захисту інформації

ПОГОДЖЕНО:

Першу редакцію освітньої програми ухвалено Методичною радою КПП ім. Ігоря Сікорського (протокол № 7 від 30.03.2017 р.)

Зміни та доповнення до освітньої програми погоджені Науково-методичною комісією університету зі спеціальності 125 Кібербезпека (протокол № 3 від «8» 06 2020 р.)

Голова НМКУ зі спеціальності 125 Кібербезпека

 Олексій НОВІКОВ

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

Представники студентських організацій:

Мелько Марія,
голова Профбюро студентів

Михалко Дмитро,
голова Студради ФТІ

Мазурок Валентин,
виборний представник студентів

Назаров Олександр,
виборний представник студентів

Рецензії-відгуки стейкхолдерів додаються.

Освітня програма оновлена у зв'язку з розширенням переліку вибіркового компонентів та залученню нових роботодавців до вдосконалення підготовки здобувачів.

ОП обговорено після надходження всіх побажань та пропозицій від роботодавців, здобувачів і випускників ОП. Схвалено на розширеному засіданні кафедри фізико-технічних засобів захисту інформації (протокол №15/2020 від 15.05.2020).

ЗМІСТ

1. Профіль освітньої програми	5
2. Перелік компонент освітньої програми	12
3. Структурно-логічна схема освітньої програми	13
4. Форма атестації здобувачів вищої освіти	13
5. Матриця відповідності програмних компетентностей компонентам освітньої програми	14
6. Матриця забезпечення програмних результатів навчання відповідними компонентами освітньої програми	14

1. ПРОФІЛЬ ОСВІТНЬОЇ ПРОГРАМИ

«Системи технічного захисту інформації» зі спеціальності 125 Кібербезпека

1 – Загальна інформація	
Повна ЗВО та інституту/ факультету	Національний технічний університет України “Київський політехнічний інститут імені Ігоря Сікорського” Фізико-технічний інститут
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Ступінь – магістр Кваліфікація – магістр з кібербезпеки
Рівень з НРК	НРК України – 8 рівень QF-EHEA – другий цикл EQF-LLL – 7 рівень
Офіційна назва освітньої програми	Системи технічного захисту інформації
Тип диплому та обсяг освітньої програми	Диплом магістра, одиничний, 90 кредитів, термін навчання 1 рік 4 місяці
Наявність акредитації	Сертифікат УД № 11007485 (081836) від 08.01.2019, дійсний до 01.07.2024
Передумови	Наявність ступеня бакалавра
Мова(и) викладання	Українська/англійська
Термін дії освітньої програми	До наступної акредитації
Інтернет-адреса постійного розміщення освітньої програми	http://ptmip.ipt.kpi.ua/ http://ipt.kpi.ua/ https://osvita.kpi.ua/op
2 – Мета освітньої програми	
Підготовка фахівця, здатного професійно аналізувати, формулювати, вирішувати практичні проблеми та розв’язувати складні фізико-технічні та логіко-організаційні задачі кібернетичної безпеки в умовах комплексності та недостатньої визначеності технологічних, екологічних, соціально-економічних та політичних загроз, всебічного професійного, інтелектуального, соціального та творчого розвитку особистості на найвищих рівнях досконалості в освітньо-науковому середовищі.	

3 – Характеристика освітньої програми	
Предметна область	<p>Об'єкти професійної діяльності випускників:</p> <ul style="list-style-type: none"> • 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. <p>Цілі навчання підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки.</p> <p>Теоретичний зміст предметної області</p> <p>Знання</p> <ul style="list-style-type: none"> • 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 <p>Методи, методики та технології:</p> <ul style="list-style-type: none"> • Методи, методики та інформаційно-комунікаційні технології ті інші технології забезпечення інформаційної та/або кібербезпеки. <p>Інструменти та обладнання:</p> <ul style="list-style-type: none"> • системи розробки, забезпечення, моніторингу та контролю процесів інформаційної та/або кібербезпеки; • сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
Орієнтація освітньої програми	Освітньо-професійна

<p>Основний фокус освітньої програми</p>	<p>Спеціальна освіта в галузі кібербезпеки за освітньою програмою «Системи технічного захисту інформації».</p> <p>Основні фокуси програми:</p> <ol style="list-style-type: none"> 1. Посилена підготовка в галузі новітніх методів отримання, обробки та передавання сигналів різної фізичної природи; 2. Фундаментальна підготовка щодо проектування, розробки, впровадження та супроводу комплексних систем захисту інформації, що циркулює на об'єктах інформаційної діяльності державної та приватної форми власності; 3. Посилена підготовка в галузі міждисциплінарного системного аналізу з метою створення комплексних систем захисту інформаційних потоків у комунікаційних мережах; 4. Робочі плани підготовки здобувачів вищої освіти щорічно переглядаються з метою включення розділів, пов'язаних з розвитком знань у галузі кібернетичної безпеки на основі аналізу нових науково-технологічних здобутків; 5. Розвиток дуальної освіти та міжуніверситетських програм з провідними установами світу, участь у міжнародних конференціях; 6. Проведення щорічних конференцій та олімпіад з нових напрямків кібернетичної безпеки з метою навчання здобувачів вищої освіти розробці індивідуальних стартапів на етапі підготовки кваліфікаційної роботи. <p>Ключові слова: кібернетична безпека, технічні засоби захисту інформації, технічний аудит, проектування та створення комплексів технічного захисту інформації</p>
<p>Особливості програми</p>	<ol style="list-style-type: none"> 1. Посилена підготовка в галузі технічних наук (програмування, обробки сигналів різної фізичної природи, розробка та оптимізація пристроїв захисту інформації); 2. Фундаментальна підготовка щодо проектування, розробки, впровадження та супроводу комплексних систем захисту інформації, що циркулює на об'єктах інформаційної діяльності державної та приватної форми власності; 3. Використання елементів дуальної освіти, зокрема міжуніверситетських програм з провідними установами світу та проходження практик на провідних підприємствах галузі захисту інформації.

4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	<p>Відповідно до Державного класифікатору професій ДК 003:2010 випускники можуть працювати на посадах, що відповідають класифікаційним угрупованням:</p> <p>213 Професіонали в галузі обчислень 2131 Професіонали в галузі обчислювальних систем 2131.2 Розробники обчислювальних систем, адміністратор системи інженер з програмного забезпечення комп'ютерів 2132.2 Розробники комп'ютерних програм, Інженер –програміст, Програміст (бази даних), Програміст прикладний 2149.2 Професіонали із організації інформаційної безпеки</p> <p>Можуть працювати фахівцями із захисту інформації в складі інформаційних департаментів підприємств та банків, розробниками та тестувальниками застосунків, що потребують виконання особливих вимог щодо інформаційної та кібернетичної безпеки; керівниками та 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, консультантами-інструкторами з кібербезпеки, аналітиками кібербезпеки в установах державної та інших форм власності, спеціалістами в галузі кібербезпеки в складі кіберполіції, спеціалістами з забезпечення кібербезпеки в кіберпросторі (зокрема, в соціальних мережах; об'єктах з використанням "інтернету речей", об'єктах критичної інфраструктури (електростанції, водо-, газопостачання тощо)); науковими співробітниками.</p>
Подальше навчання	Продовження освіти за третім (освітньо-науковим) 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 (магістерської дисертації)
Оцінювання	Оцінювання знань студентів здійснюється у відповідності до Положення про рейтингову систему оцінювання результатів навчання студентів КПІ ім. Ігоря Сікорського за усіма видами аудиторної та позааудиторної роботи (вхідний, поточний, рубіжний, підсумковий контроль); екзамени, заліки, індивідуальні завдання тощо.
6 – Програмні компетентності	
Інтегральна компетентність	Здатність професійно аналізувати, формулювати, вирішувати практичні проблеми та розв'язувати складні фізико-технічні та логіко-організаційні задачі кібернетичної безпеки в умовах комплексності та недостатньої визначеності технологічних, екологічних, соціально-економічних та політичних загроз.
Загальні компетентності (ЗК)	
ЗК1	Здатність до абстрактного мислення, аналізу і синтезу
ЗК2	Здатність до навчання та самоаналізу (пошуку, оброблення та аналізу інформації з різних джерел)

ЗК3	Здатність застосовувати знання на практиці
ЗК4	Готовність до вільного усного та письмового спілкування українською мовою, здатність спілкуватися, читати та писати іноземною мовою
ЗК5	Готовність до міжособистісних комунікацій
ЗК6	Готовність до користування інформаційних і комунікаційних технологій
ЗК7	Здатність розв'язування поставленої задачі та приймати відповідні рішення
ЗК8	Здатність оцінювати та забезпечувати якість виконуваних робіт
ЗК9	Здатність працювати як індивідуально, так і в команді
ЗК10	Готовність застосовувати на практиці базові дослідницькі навички і уміння
ЗК11	Здатність виявляти наукову сутність проблем у професійній сфері, знаходити адекватні шляхи щодо їх розв'язання
ЗК12	Здатність до самостійного освоєння нових методів дослідження, зміні наукового і науково-виробничого профілю своєї діяльності
ЗК13	Здатність керувати проектами, організовувати командну роботу, проявляти ініціативу з удосконалення роботи
ЗК14	Здатність генерувати нові ідеї й нестандартні відходи до їх реалізації (креативність)
Фахові компетентності спеціальності (ФК)	
ФК1	Здатність використовувати управлінсько-організаційні, математичні, технічні та правові методи, засоби й заходи для реалізації проектних рішень з побудови систем забезпечення інформаційної та кібернетичної безпеки.
ФК2	Здатність проводити патентні дослідження з метою забезпечення патентної чистоти та патентоздатності нових проектних рішень та визначення показників технічного рівня продукції, засобів технічного та інформаційного забезпечення
ФК3	Здатність застосовувати вітчизняні та міжнародні методичні й нормативні документи, пропозиції та проводити заходи щодо реалізації розроблених проектів і програм
ФК4	Здатність проектувати та моделювати інформаційні системи різного виду та призначення.
ФК5	Здатність використовувати управлінсько-організаційні, математичні, технічні та правові методи забезпечення інформаційної та кібернетичної безпеки
ФК6	Здатність здійснювати планування, виконання проектних дій та прийняття проектних рішень в процесі управління проектуванням інформаційних систем, їх розгортанням, впровадженням, ефективною експлуатацією та розвитком
ФК7	Здатність організовувати роботу колективів виконавців, приймати управлінські рішення, визначати порядок виконання робіт, вибирати оптимальні рішення при створенні систем забезпечення інформаційної та кібернетичної безпеки, систематизувати й узагальнювати результати роботи.
ФК8	Здатність до роботи в багатонаціональних колективах, у тому числі при роботі над міждисциплінарними й інноваційними проектами, створювати в колективах відносини ділового співробітництва.
ФК9	Здатність проводити системні дослідження та застосовувати їх в керуванні проектами для забезпечення інформаційної та кібербезпеки.
ФК10	Здатність володіти технологіями розроблення комплексів захисту інформації.

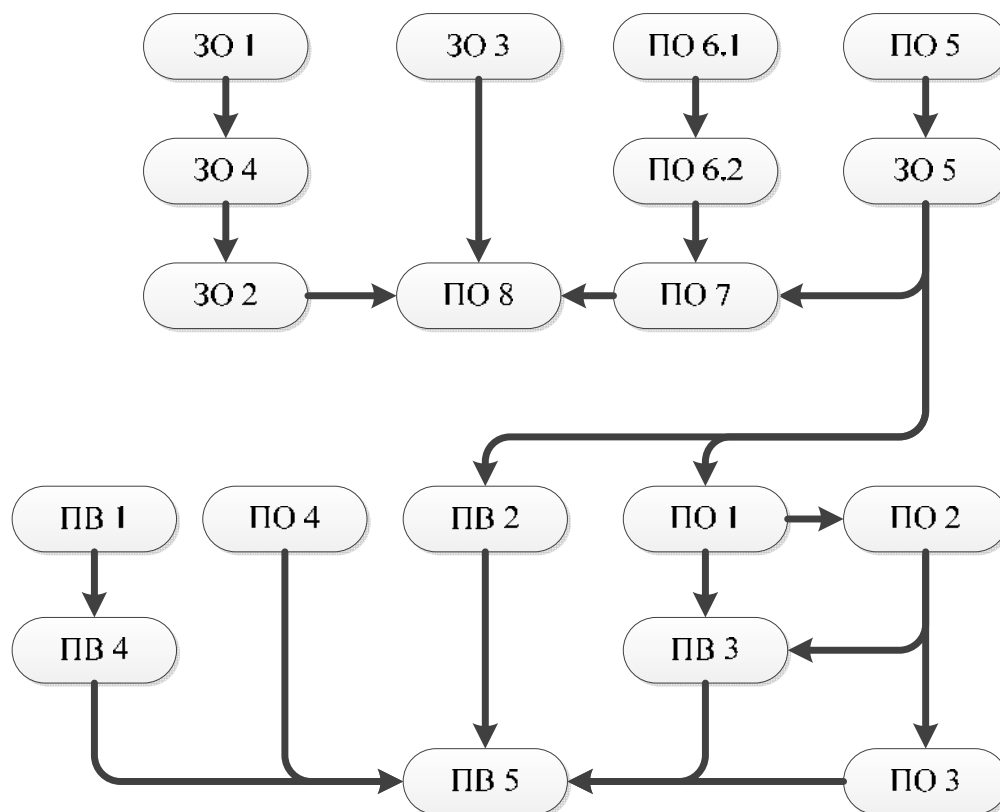
ФК 11	Здатність до застосування математичного та комп'ютерного моделювання для вирішення широкого спектру задач інформаційної та кібернетичної безпеки.
7 – Програмні результати навчання	
ПРН 1	впливу технічних рішень в суспільному, економічному, соціальному і екологічному контексті
ПРН 2	основ інтелектуальної власності та патентознавства
ПРН 3	основ теорії сталого розвитку суспільства
ПРН 4	основ менеджменту
ПРН 5	іноземної мови
ПРН 6	основ педагогіки
ПРН 7	основ наукових досліджень
ПРН 8	теорії інтелектуальних систем
ПРН 9	технологій проектування систем
ПРН 10	системно мислити та застосовувати творчі здібності до формування принципово нових ідей.
ПРН 11	ефективно працювати як індивідуально, так і у складі команди
ПРН 12	поєднувати теорію і практику, а також приймати рішення та виробляти стратегію для вирішення завдань спеціальності з урахуванням загальнолюдських цінностей, суспільних, державних та виробничих інтересів.
ПРН 13	виконувати експериментальні дослідження за професійною тематикою.
ПРН 14	оцінювати отримані результати та аргументовано захищати прийняті рішення.
ПРН 15	спілкуватися, включаючи усну та письмову комунікацію українською мовою та однією з іноземних мов (англійською, німецькою, італійською, французькою, італійською)
ПРН 16	використовувати інформаційні технології та інші методи для ефективного спілкування на професійному та соціальному рівнях
ПРН 17	усвідомлювати необхідність навчання впродовж усього життя з метою поглиблення набутих та здобуття нових фахових знань, удосконалення креативного мислення
ПРН 18	відповідально ставитися до виконання роботи та досягти поставленої мети з дотриманням вимог професійної етики.
ПРН 19	здійснювати патентний пошук
ПРН 20	застосовувати знання для ідентифікації, формулювання і розв'язування технічних задач в галузі кібербезпеки, використовуючи відомі методи
ПРН 21	застосовувати знання для розв'язування задач аналізу та синтезу апаратних засобів захисту інформації
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Відповідно до кадрових вимог щодо забезпечення провадження освітньої діяльності у сфері вищої та післядипломної освіти (пункти 28-32 Постанови Кабінету Міністрів України № 1187 від 30.12.2015 р.) за текстом постанови Кабінету Міністрів України від 10.05.2018 р. № 347, п. 28-32)

Матеріально-технічне забезпечення	Відповідно до технологічних вимог щодо забезпечення започаткування та провадження освітньої діяльності у сфері вищої та післядипломної освіти для осіб з вищою освітою (пункти 33-38 Постанови Кабінету Міністрів України № 1187 від 30.12.2015 р.) за текстом постанови Кабінету Міністрів України від 10.05.2018 р. № 347, п. 34-35)
Інформаційне та навчально-методичне забезпечення	Відповідно до організаційних вимог щодо провадження освітньої діяльності у сфері вищої та післядипломної освіти для осіб з вищою освітою (пункти 39-45 Постанови Кабінету Міністрів України № 1187 від 30.12.2015 р.) , за текстом постанови Кабінету Міністрів України від 10.05.2018 р. № 347, п.36)
9 – Академічна мобільність	
Національна кредитна мобільність	Участь студентів в програмах академічної мобільності, можливість укладення угод подвійне дипломування
Міжнародна кредитна мобільність	Можливість укладення угод про міжнародну академічну мобільність, про подвійне дипломування, про тривалі міжнародні проекти
Навчання іноземних здобувачів вищої освіти	Для іноземних громадян навчання здійснюється українською або англійською мовами

2. ПЕРЕЛІК КОМПОНЕНТ ОСВІТНЬОЇ ПРОГРАМИ

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
1. НОРМАТИВНІ освітні компоненти			
I.1. Цикл загальної підготовки			
ЗО 1	Інтелектуальна власність та патентознавство	3	Залік
ЗО 2	Основи інженерії та технології сталого розвитку	2	Залік
ЗО 3	Практикум іншомовного професійного спілкування	3	Залік
ЗО 4	Інноваційний менеджмент	3	Залік
ЗО 5	Математичне моделювання систем і процесів	4	Екзамен
I.2. Цикл професійної підготовки			
ПО 1	Ширококутні сигнали в системах ТЗІ	5	Екзамен
ПО 2	Курсова робота з ширококутних сигналів в системах ТЗІ	1	Залік
ПО 3	Радіомоніторинг і радіопротидія на об'єктах інформаційної діяльності	4	Екзамен
ПО 4	Системи захисту мовної інформації	3,5	Залік
ПО 5	Структурно-параметрична оптимізація пристроїв ТЗІ	4	Залік
Дослідницький (науковий) компонент			
ПО 6	Наукова робота за темою магістерської дисертації		
ПО 6.1	Основи наукових досліджень	2	Залік
ПО 6.2	Науково-дослідна робота за темою магістерської дисертації	2	Залік
ПО 7	Науково-дослідна практика	14	Залік
ПО 8	Робота над магістерською дисертацією	16	Захист дипломної роботи
2. ВИБІРКОВІ освітні компоненти			
II.1. Цикл професійної підготовки (Вибіркові освітні компоненти з факультетського/кафедрального Каталогів)			
ПВ 1	Освітня компонента 1 Ф-Каталогу	4	Залік
ПВ 2	Освітня компонента 2 Ф-Каталогу	4,5	Екзамен
ПВ 3	Освітня компонента 3 Ф-Каталогу	4	Залік
ПВ 4	Освітня компонента 4 Ф-Каталогу	4	Екзамен
ПВ 5	Освітня компонента 5 Ф-Каталогу	7	Екзамен
Загальний обсяг обов'язкових компонент:		66,5	
Загальний обсяг вибіркових компонент:		23,5	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		90	

3. СТРУКТУРНО-ЛОГІЧНА СХЕМА ОСВІТНЬОЇ ПРОГРАМИ



4. ФОРМА ВИПУСКНОЇ АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Випускна атестація здобувачів вищої освіти за освітньою програмою спеціальності 125 Кібербезпека проводиться у формі захисту кваліфікаційної магістерської роботи та завершується видачею документа встановленого зразка про присудження йому ступеня магістра з кібербезпеки за освітньою програмою “Системи технічного захисту інформації”.

Випускна атестація здійснюється відкрито і публічно.

5. МАТРИЦЯ ВІДПОВІДНОСТІ ПРОГРАМНИХ КОМПЕТЕНТНОСТЕЙ КОМПОНЕНТАМ ОСВІТНЬОЇ ПРОГРАМИ

	ЗО 1	ЗО 2	ЗО 3	ЗО 4	ЗО 5	ПО 1	ПО 2	ПО 3	ПО 4	ПО 5	ПО 6	ПО 7	ПО 8
ЗК1					+					+	+		
ЗК2											+	+	+
ЗК3													+
ЗК4		+									+		+
ЗК5			+										
ЗК6												+	+
ЗК7											+	+	+
ЗК8											+		+
ЗК9			+										
ЗК10					+					+	+		
ЗК11					+						+		
ЗК12					+						+		
ЗК13			+										
ЗК14					+						+	+	+
ФК 1	+			+									
ФК 2	+												
ФК 3								+	+				
ФК 4					+	+	+	+	+				
ФК 5								+	+				
ФК 6			+										
ФК 7			+										
ФК 8		+	+										
ФК 9								+					
ФК 10								+	+				
ФК 11					+					+			

**6. МАТРИЦЯ ЗАБЕЗПЕЧЕННЯ ПРОГРАМНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ
ВІДПОВІДНИМИ КОМПОНЕНТАМИ ОСВІТНЬОЇ ПРОГРАМИ**

	ЗО 1	ЗО 2	ЗО 3	ЗО 4	ЗО 5	ПО 1	ПО 2	ПО 3	ПО 4	ПО 5	ПО 6	ПО 7	ПО 8
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 14		+	+										
ПРН 15											+	+	
ПРН 16			+										
ПРН 17	+	+											
ПРН 18					+						+	+	+
ПРН 19					+	+	+	+	+				