ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«УЖГОРОДСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ»
ФІЗИЧНИЙ ФАКУЛЬТЕТ
Кафедра твердотільної електроніки та інформаційної безпеки

«ЗАТВЕРДЖУЮ»
Декан фізичного факультету
_____/Лазур В.Ю./
«28» 04 2022 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ТЕХНОЛОГІЯ ОРГАНІЗАЦІЇ ІНФРАСТРУКТУРИ ВІДКРИТИХ КЛЮЧІВ

Рівень вищої освіти	**другий (магістерський) рівень**
Галузь знань	**12 Інформаційні технології**
Спеціальність	**125 Кібербезпека**
Предметна спеціальність (Спеціалізація) *(за наявності)*	
Освітня програма	**Безпека інформаційних і комунікаційних систем.**
Статус дисципліни	**основна**
Мова навчання	**українська**

Ужгород 2022

Робоча програма навчальної дисципліни «**Технологія організації інфраструктури відкритих ключів**» для здобувачів вищої освіти галузі знань **12 Інформаційні технології** спеціальності **125 Кібербезпека** освітньої програми **Безпека інформаційних і комунікаційних систем.**

Розробники: Петрушко І.А., к. ф.-м. н., доцент кафедри ТЕІБ

Робочу програму розглянуто та затверджено на засіданні кафедри
твердотільної електроніки та інформаційної безпеки

протокол № 7 від «28» 04 2022р.

Завідувач кафедри _____ Різак В.М.

Схвалено науково-методичною комісією фізичного факультету

протокол № 10 від «29» 04 2022р.

Голова науково-методичної комісії _____ Карбованець М. І.

1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

<table>
<tr><td rowspan="2">Найменування показників</td><td colspan="2">Розподіл годин за навчальним планом</td></tr>
<tr><td>Денна форма навчання</td><td>Заочна форма навчання</td></tr>
<tr><td>Кількість кредитів ЄКТС – 3</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td>Загальна кількість годин – 90</td><td>1-й</td><td></td></tr>
<tr><td>Кількість модулів – 2</td><td colspan="2">Семестр:</td></tr>
<tr><td rowspan="6">Тижневих годин
для денної форми навчання:

аудиторних – 4

самостійної роботи студента – 4</td><td>1-й</td><td></td></tr>
<tr><td colspan="2">Лекції:</td></tr>
<tr><td>18</td><td></td></tr>
<tr><td colspan="2">Практичні (семінарські):</td></tr>
<tr><td></td><td></td></tr>
<tr><td colspan="2">Лабораторні:</td></tr>
<tr><td>Вид підсумкового контролю: залік</td><td>18</td><td></td></tr>
<tr><td rowspan="2">Форма підсумкового контролю: усна</td><td colspan="2">Самостійна робота:</td></tr>
<tr><td>54</td><td></td></tr>
</table>

2. МЕТА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Метою навчальної дисципліни **«Технологія організації інфраструктури відкритих ключів» є** закладання термінологічного фундаменту, навчання студентів основам сертифікації відкритих ключів, сучасним принципам побудови та застосування інфраструктури відкритих ключів, нормативному регулюванню та стандартизації ІВК.

З авданнями даного курсу є формування у студентів певних знань та вмінь з теорії та практики технології організації інфраструктури відкритих ключів.

Місце дисципліни в структурі освітньої програми: навчальна дисципліна **«Технологія організації інфраструктури відкритих ключів»** є обов'язковим компонентом циклу професійної підготовки освітньої програми підготовки магістрів спеціальності «**Безпека інформаційних і комунікаційних систем**».

Відповідно до освітньої програми, вивчення дисципліни сприяє формуванню у здобувачів вищої освіти таких компетентностей:

Інтегральна: здатність розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.

Загальні компетентності:

1. Здатність застосовувати знання у практичних ситуаціях (КЗ-1).
2. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності) (КЗ-5).

Фахові компетентності:

1. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.(КФ6)
2. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації (КФ8).

3. ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ

Відповідно до освітньої програми **«Безпека інформаційних і комунікаційних систем»**, вивчення навчальної дисципліни **«Технологія організації інфраструктури відкритих ключів»** повинно забезпечити досягнення здобувачами вищої освіти таких програмних результатів навчання (ПРН):

Програмні результати навчання	Шифр ПРН
Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.	ПРН 3
Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.	ПРН5
Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.	ПРН 6
Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.	ПРН 9
Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.	ПРН 13
Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.	ПРН 23

Очікувані результати навчання, які повинні бути досягнуті здобувачами освіти після опанування навчальної дисципліни **«Технологія організації інфраструктури відкритих ключів»**:

Очікувані результати навчання з дисципліни	Шифр ПРН
Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.	ПРН 3
Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.	ПРН 5
Обґрунтовано аналізувати та оцінювати захищеність КСЗІ, КТЗІ, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.	ПРН 6
Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.	ПРН 9
Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання	ПРН 13

в інформаційних системах, на об’єктах інформаційної діяльності та критичної інфраструктури.	
Обґрунтовувати вибір програмного забезпечення під час автоматизованої обробки інформації з обмеженим доступом, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань.	ПРН 23

4. ЗАСОБИ ДІАГНОСТИКИ ТА КРИТЕРІЇ ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Засоби оцінювання та методи демонстрування результатів навчання

Засобами оцінювання та методами демонстрування результатів навчання з навчальної дисципліни **«Технологія організації інфраструктури відкритих ключів»** є:

- залік;
- виконання завдань лабораторних робіт;
- стандартизовані тести;
- фронтальне та/або письмове опитування

Форми контролю та критерії оцінювання результатів навчання

Модульний контроль з навчальної дисципліни **«Технологія організації інфраструктури відкритих ключів»** складається з поточного контролю та модульного контрольного оцінювання результатів навчання.

Форми поточного контролю:

- фронтальне стандартизоване усне та/або письмове опитування за основними питаннями теми заняття;
- захист результатів лабораторної роботи;
- тестування;
- перевірка якості виконання завдань для самостійної роботи, зокрема за конспектами матеріалів.

Форма модульного контрольного оцінювання: письмова модульна контрольна робота та/або тестування.

Форма підсумкового семестрового контролю: залік.

До заліку допускаються студенти, які відпрацювали пропущені заняття і виконали модульні контрольні роботи та завдання для самостійної роботи. Контроль самостійної роботи здійснюється шляхом перевірки виконаних завдань на лабораторних та індивідуальних заняттях, під час захисту лабораторних робіт, тестування при поточному оцінюванні, презентації результатів виконаних завдань та досліджень.

Розподіл балів, які отримують здобувачі вищої освіти (модуль 1)

Поточний контроль успішності					**Модульна контрольна робота**	**Сума**
Поточне оцінювання та самостійна робота						
Т1	Т2	Т3	Т4	Т5	60	**100**
5	5	10	5	15		

Т1, Т2 ... – теми

Розподіл балів, які отримують здобувачі вищої освіти (модуль 2)

Поточний контроль успішності					Модульна контрольна робота	Сума
Поточне оцінювання та самостійна робота						
Т1	Т2	Т3	Т4	Т5	60	**100**
5	10	15	5	5		

Т1, Т2 ... – теми

Оцінювання окремих видів навчальної роботи з дисципліни «Автоматизація обробки інформації з обмеженим доступом»

Вид діяльності здобувача вищої освіти	**Модуль 1**		**Модуль 2**	
	Кількість	Максимальна кількість балів (сумарна)	Кількість	Максимальна кількість балів (сумарна)
Лабораторні заняття (допуск, виконання та захист)	3	15	5	25
Комп'ютерне тестування при тематичному оцінюванні	2	25	1	15
Модульна контрольна робота	1	60	1	60
Разом		**100**		**100**

Критерії оцінювання модульної контрольної роботи

Модульна контрольна робота проводиться у письмовій формі шляхом відповідей на питання навчального модуля та вирішення тестових завдань. Кожна правильна відповідь оцінюється певною кількістю балів. Максимальна кількість балів за кожний модуль становить 100 балів.

Критерії оцінювання підсумкового семестрового контролю

Підсумковий семестровий контроль з дисципліни **«Технологія організації інфраструктури відкритих ключів»** здійснюється у формі заліку, що проводиться в усній формі шляхом співбесіди. Результати заліку оцінюються за двобальною шкалою: „зараховано", „незараховано". Підсумкова оцінка визначається наступними критеріями:

Оцінка "зараховано" - якщо студент достатньо чітко і грамотно відповідає на питання в межах матеріалу, викладеного у рамках лекційних занять, може показати та обгрунтувати взаємозв'язок різних частин матеріалу, пройденого у межах матеріалу навчальної дисципліни; демонструє здатність до мислення, при відповіді на питання розмірковує, спираючись на отримані у рамках курсу знання, не допускає істотних неточностей у відповіді, правильно вибудовує логіку вирішення типових завдань;

Оцінка "незараховано" - якщо студент викладає основні питання недостатньо чітко або допускає істотні помилки при їх викладі, не може пояснити зв'язків у рамках викладеного матеріалу, не знає значної частини програмного матеріалу, не може дати точних визначень понять, пройдених у рамках курсу, дає розпливчасті формулювання і не володіє в належній мірі термінологією, плутається при відповіді на додаткові питання, не володіє прийомами вирішення типових завдань.

За бажанням студента результуюча підсумкова оцінка може бути визначена як інтегрована оцінка засвоєння всіх тем дисципліни і кількісно дорівнює середньому арифметичному балів, отриманих за кожний модуль.

Переведення результатів, отриманих за 100-бальною шкалою оцінювання в національну 4-х бальну та шкалу за системою ECTS здійснюється за наступною схемою:

Оцінка за шкалою балів	Залік	ECTS	
		Оцінка	Характеристика
90-100	зараховано	A	відмінно
82-89		B	добре
74-81		C	добре
64-73		D	задовільно
60-64		E	задовільно
35-59	незараховано	FX	незадовільно з можливістю перескладання
1-34		F	незадовільно з обов'язковим повторним навчанням

Студент, який отримав за результатами підсумкового контролю оцінку «незараховано» або «незадовільно з обов'язковим повторним навчанням» (1-34 балів, F), зобов'язаний пройти повторний курс вивчення дисципліни (під час додаткового семестру) і скласти залік або екзамен.

Результати підсумкового контролю знань вносяться до відомості обліку успішності.

5. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

5.1. Зміст навчальної дисципліни

Модуль 1. ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ ІНФРАСТРУКТУРИ ВІДКРИТИХ КЛЮЧІВ (ІВК)

Тема 1. Основи сертифікації відкритих ключів.
Вступ до інфраструктури відкритих ключів (ІВК) та системи електронних цифрових підписів ЕЦП. Електронні довірчі послуги. Класифікація та формати сертифікатів відкритих ключів.

Тема 2. Життєві цикли особистих ключів та сертифікатів відкритих ключів
Формати особистих ключів. Обслуговування сертифікатів відкритих ключів

Тема 3. Моделі та механізми електронних довірчих послуг. Електронні довірчі послуги на основі ЕЦП
Вимоги до архітектури ІВК (ЕЦП), побудова та аналіз шляхів сертифікації. Валідація (перевірка) шляхів сертифікації при наданні електронних довірчих послуг.

Тема 4. Нормативне регулювання та стандартизація інфраструктури відкритих ключів.
Стандартизація у галузі ІВК та надання електронних довірчих послуг. Класифікація протоколів ІВК, особливості, застосування та аналіз.

Тема 5. Класифікація протоколів ІВК, особливості, застосування та аналіз.
Основні існуючі та перспективні положення політик сертифікації

Модуль 2. ПРАКТИЧНІ АСПЕКТИ ІНФРАСТРУКТУРИ ВІДКРИТИХ КЛЮЧІВ

Тема 1. ІВК для організації захисту бездротових мереж.

Протоколи, які використовуються для організації ІВК в бездротових мережах, типи шифрування. Особливості налаштування ІВК для бездротових мереж

Тема 2. ІВК для організації захисту інтернету речей (IoT) на прикладі розумного будинку.
Можливості ІВК для зниження безпекових ризиків в системі IoT.

Тема 3. Сховища центрів сертифікації.
ІВК в протоколові HTTPS. Використання хешів для виявлення прослуховування.

Тема 4. ІВК в безпеці e-mail – комунікацій.
Протоколи, які використовуються для організації ІВК в e-mail-комунікаціях, типи шифрування. Особливості налаштування ІВК для e-mail-комунікацій.

Тема 5. ІВК в організації захисту хмарних сервісів в IoT
Налаштування безпечної веб-комунікації на веб-сервері в мережі постачальників хмарних сервісів.

5.2. Структура навчальної дисципліни

Денна форма навчання

Назви змістових модулів і тем	Кількість годин					
	Форма навчання: денна					
	Усього	у тому числі				
		лекції	практичні (семінарські)	лабораторні	індивідуальна робота	самостійна робота
Модуль 1						
Тема 1. Основи сертифікації відкритих ключів	7	2				5
Тема 2. Життєві цикли особистих ключів та сертифікатів відкритих ключів	8	2		1		5
Тема 3. Моделі та механізми електронних довірчих послуг. Електронні довірчі послуги на основі ЕЦП	9	2		2		5
Тема 4. Нормативне регулювання та стандартизація інфраструктури відкритих ключів.	7	2				5
Тема 5. Класифікація протоколів ІВК, особливості, застосування та аналіз.	12	2		2		8
Модульна контрольна робота	2	2				
Разом за модуль	45	12		5		28
Модуль 2						
Тема 1. ІВК для організації захисту бездротових мереж. Можливості ІВК для зниження безпекових ризиків в системі IoT	9	1		2		6
Тема 2. ІВК для організації захисту інтернету речей (IoT) на прикладі розумного будинку. Можливості ІВК для зниження безпекових ризиків в системі IoT.	8	1		2		5

Тема 3. Сховища центрів сертифікації. ІВК в протоколові HTTPS. Використання хешів для виявлення прослуховування.	8	1		2		5
Тема 4. ІВК в безпеці e-mail – комунікацій. Протоколи, які використовуються для організації ІВК в e-mail-комунікаціях, типи шифрування. Особливості налаштування ІВК для e-mail-комунікацій.	9	1		3		5
Тема 5. ІВК в організації захисту хмарних сервісів в IoT	9			4		5
Модульна контрольна робота	2	2				
Разом за модуль	45	6		13		26
Разом за семестр	**90**	**18**		**18**		**54**

5.3. Теми лабораторних занять

№ з/п	Назва теми	Кількість Годин	
		Денна	Заочна
1	ІВК для підвищення рівнябезпеки бездротових мереж	3	
2	ІВК для а організації захисту інтернету речей (IoT)	3	
3	Сховища центрів сертифікації	4	
4	ІВК в безпеці e-mail – комунікацій	4	
5	Налаштування безпечної веб-комунікації на веб-сервері(ІВК в організації захисту хмарних сервісів в IoT)	4	
	Разом	**18**	

5.4. Самостійна робота

№ з/п	Назва теми	Кількість годин	
		денна	заочна
1.	Нормативно – правова база створення та застосування національної системи ЕЦП	3	
2.	Стандартизовані криптографічні протоколи ЕЦП: стійкість і складність	4	
3.	Створення запиту на виготовлення сертифікатів відкритих ключів	4	
4.	Генерування асиметричних пар відкритих ключів	4	
5.	Криптографічна живучість ІВК	4	
6.	Акредитовані центри сертифікації ключів	4	
7.	Списки відкликаних сертифікатів	4	
8.	Розгортання центрів сертифікації ключів (ЦСК)	4	
9.	Національна та міжнародна нормативно-правова база в частині ІВК	4	
10.	Базові архітектури ІВК	4	
11.	Сертифікація в системі ІВК	4	
12.	Стандартизація в системі ІВК	4	
13.	Шляхи вдосконалення ІВК	7	
	Разом	**54**	

6. ІНСТРУМЕНТИ, ОБЛАДНАННЯ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ВИКОРИСТАННЯ ЯКИХ ПЕРЕДБАЧАЄ НАВЧАЛЬНА ДИСЦИПЛІНА

Технічні засоби: технічні засоби навчання, зокрема мультимедійний проектор, маршрутизатори Cisco, комутатори Cisco 2965.
Обладнання: персональні комп'ютери з можливістю доступу в Інтернет.
Програмне забезпечення: хмарні підручники Cisco NetAcad, Packet Tracer, віртуальні машини.

7. РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

Основна література

1. Горбенко Ю.І., Горбенко І.Д. Інфраструктури відкритих ключів . Системи ЕЦП. Теорія та практика. Монографія. Харків. Форт. 2010 , 593с.
2. Інфраструктура відкритих ключів: технології, архітектура, побудова та впровадження / [О. В. Потій, А. В. Лєншин, Л. С. Сорока, В. І. Єсін і ін.]. –521 Дніпропетровськ: Академія митної служби України, 2011. – 202с.
3. 3.Потій О.В., Іщенко Ю.М., Лєншин А.В. Текст лекцій з дисципліни «Побудова та розгортання інфраструктури відкритих ключів», Харків, ХНУРЕ, 2009 р.
4. 4.Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Підручник. Харків. Форт. 2013р. , 878с.
5. 5.Горбатов В.С. Основы технологии PKI / В.С. Горбатов, О.Ю. Полянская. – М. : Горячая линия – Телеком, 2004. – 246с.

Допоміжна література

1. Потій О.В. Стандартизація та сертифікація в галузі захисту інформації. Стандарти управління ключами / О.В. Потій. – Х. : ХНУРЕ, 2002. – 80 с.
2. Потій О.В. Стандартизація та сертифікація в галузі захисту інформації. Стандарти механізмів безпеки/ О.В. Потій. – Х. : ХНУРЕ, 2001. – 80 с.
3. Есин В. И. Безопасность информационных систем и технологий / В. И. Есин, А. А. Кузнецов, Л. С. Сорока. – Х. : ООО «ЭДЭНА», 2010. – 656 с.
4. Єсін В. І. Безпека інформаційних систем і технологій: навчальний посібник [для студентів вищих навчальних закладів, які навчаються за напрямами підготовки «Безпека інформаційних і комунікаційних систем»] / В. І. Єсін, О. О. Кузнецов, Л. С. Сорока. – Х. : ХНУ імені В. Н. Каразіна, 2013. – 632 с.
5. Закон України «Про електронний цифровий підпис» від 22.05.2003 № 852-IX
6. Постанова Кабінету Міністрів України від 28.10.04. №1453 «Про затвердження Типового порядку здійснення електронного документообігу в органах виконавчої влади».

Інформаційні ресурси в мережі Інтернет

1. www.austinlinks.com

2. http://world.std.com/~franl/crypto.html

3. www.cryptonessie.org

4. www.cryptography.ru

5. www.osti.gov/eprints

6. Інформаційні ресурси Cisco NetAcad.