Міністерство освіти і науки України
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»

ЗАТВЕРДЖУЮ
Проректор з наукової роботи
_____ В. В. Павліков
(підпис) (ініціали та прізвище)
«31» 08 2020 р.
Відділ аспірантури і докторантури

РОБОЧА ПРОГРАМА ВИБІРКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Теорія і методи сучасної криптології
(назва навчальної дисципліни)

Галузь знань: 12 "Інформаційні технології"
(шифр і найменування галузі знань)

Спеціальність: 125 "Кібербезпека"
(код та найменування спеціальності)

Освітньо-наукова програма: "Кібербезпека"
(найменування освітньої програми)

Рівень вищої освіти: третій (освітньо-науковий)

Форма навчання: денна

Харків 2020 рік

РОБОЧА ПРОГРАМА
ВИБІРКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Теорія і методи сучасної криптології
(назва дисципліни)

для здобувачів за спеціальністю 125 "Кібербезпека"

освітньо-наукової програми "Кібербезпека"

«26» 08 2020 р., – 11 с.

Розробник: доцент, к.т.н., доцент _____ _____ Пєвнєв В. Я..
(посада, науковий ступінь та вчене звання) (підпис) (прізвище та ініціали)

Гарант ОНП доцент, к.т.н., доцент _____ Колісник М.О.
(посада, науковий ступінь та вчене звання) (підпис) (прізвище та ініціали)

Протокол №1 від «27» серпня 2020 р. засідання кафедри № 503

Завідувач кафедри д.т.н., професор _____ Харченко В. С.
(науковий ступінь та вчене звання) (підпис) (прізвище та ініціали)

ПОГОДЖЕНО:

Завідувач відділу
аспірантури і докторантури В. Б. Селевко

Голова наукового товариства
студентів, аспірантів,
докторантів і молодих вчених Т. П. Старовойт

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, спеціальність, освітня програма, рівень вищої освіти</td><td>Характеристика навчальної дисципліни</td></tr>
<tr><td>Денна форма навчання</td></tr>
<tr><td>Кількість кредитів – 5</td><td rowspan="15">Галузь знань
12 "Інформаційні технології"
(шифр та найменування)

Спеціальність
125 "Кібербезпека"
(код та найменування)

Освітньо-наукова програма
"Кібербезпека"
(найменування)

Рівень вищої освіти:
третій (освітньо-науковий)</td><td>Вибіркова</td></tr>
<tr><td>Кількість модулів – 1</td><td>Навчальний рік</td></tr>
<tr><td>Кількість змістовних модулів – 2</td><td>2020/ 2021</td></tr>
<tr><td>Індивідуальне завдання - немає
(назва)</td><td>Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин
денна – 68/150</td><td>4-й</td></tr>
<tr><td>Лекції [1)]</td></tr>
<tr><td rowspan="6">Кількість тижневих годин для денної форми навчання:
аудиторних – 4
самостійної роботи аспіранта – 4,8</td><td>34 годин</td></tr>
<tr><td>Практичні, семінарські[1)]</td></tr>
<tr><td>0 годин</td></tr>
<tr><td>Лабораторні [1)]</td></tr>
<tr><td>34 годин</td></tr>
<tr><td>Самостійна робота</td></tr>
<tr><td>82 годин</td></tr>
<tr><td>Вид контролю</td></tr>
<tr><td>іспит</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної роботи становить: для денної форми навчання –*68/82*;

[1)] Аудиторне навантаження може бути зменшене або збільшене на одну годину в залежності від розкладу занять.

2. Мета та завдання навчальної дисципліни

Мета вивчення: – полягає в оволодінні науковими методами обґрунтування, вибору та аналізу криптографічних алгоритмів і протоколів.

Завдання: . Завдання: здійснювати порівняльний аналіз криптографічних алгоритмів та оцінку їх криптографічної стійкості; здійснювати розрахунок та вибір конкретних параметрів криптографічних алгоритмів і протоколів; використовувати спеціалізоване програмне забезпечення та розробляти на базі мов програмування високого рівня програмне забезпечення для вирішення задач криптозахисту даних.

Програмні компетентності. Дисципліна має допомогти сформувати у аспірантів такі компетентності:

- здатність до абстрактного мислення, аналізу та синтезу;
- здатність до пошуку, оброблення та аналізу інформації з різних джерел;
- здатність працювати в міжнародному контексті;
- здатність розробляти проекти та управляти ними;
- здатність застосовувати сучасні інформаційні технології, бази даних та інші електронні ресурси, спеціалізоване програмне забезпечення у науковій та навчальній діяльності;
- здатність здійснювати науково-педагогічну діяльність у вищій освіті;
- здатність виявляти, ставити та вирішувати проблеми дослідницького характеру в сфері кібербезпеки;
- здатність ініціювати, розробляти і реалізовувати комплексні інноваційні проекти в кібербезпеці та дотичні до неї міждисциплінарні проекти, лідерство під час їх реалізації;
- здатність дотримуватись етики досліджень, а також правил академічної доброчесності в наукових дослідженнях та науково-педагогічній діяльності;
- системний науковий світогляд та загальнокультурний кругозір.

Програмні результати навчання. В результаті вивчення дисципліни аспіранти мають досягти такі програмні результати навчання:

- мати передові концептуальні та методологічні знання з кібербезпеки і на межі предметних галузей, а також дослідницькі навички, достатні для проведення наукових і прикладних досліджень на рівні останніх світових досягнень з відповідного напряму, отримання нових знань та/або здійснення інновацій;
- формулювати і перевіряти гіпотези; використовувати для обґрунтування висновків належні докази, зокрема, результати теоретичного аналізу, експериментальних досліджень (опитувань, спостережень та інше) і математичного та/або комп'ютерного моделювання, наявні літературні дані;
- розробляти та досліджувати концептуальні, математичні і комп'ютерні моделі процесів і систем, ефективно використовувати їх для отримання нових знань та/або створення інноваційних продуктів у кібербезпеці та дотичних міждисциплінарних напрямах;
- планувати і виконувати експериментальні та/або теоретичні дослідження з

кібербезпеки та дотичних міждисциплінарних напрямів з використанням сучасних інструментів, критично аналізувати результати власних досліджень і результати інших дослідників у контексті усього комплексу сучасних знань щодо досліджуваної проблеми;

– вивчати, узагальнювати та впроваджувати в навчальний процес інновації кібербезпеки.

Міждисциплінарні зв'язки. Дисципліна є вибірковою компонентою освітньо-наукової програми «Кібербезпека» і базується на знаннях, отриманих під час вивчення дисциплін: «ІТ в практиці наукових досліджень», «Теорія і методи зеленої ІТ-інженерії», «Наукові англомовні комунікації», «Теорія і технології критичного комп'ютингу», що є обов'язковими компонентами.

Матеріал, засвоєний під час вивчення цієї дисципліни, є базою для підготовки дисертаційної роботи.

3. Програма навчальної дисципліни

Модуль 1.

Змістовний модуль 1.

Тема 1. Малоресурсна криптографія

Місце малоресурсної криптографії в забезпеченні інформаційної безпеки. Основні визначення. Етапи розвітку криптографічних систем. Класифікація малоресурсних криптографічних систем. Загальна схема малоресурсних криптографічних систем.

Тема 2. Використання малоресурсної криптографії

Основні класи симетричних криптосистем. Криптокселератори шифрування. Алгоритми шифрування AES-NI, Present и Clcfia. Шифр Trivium. Шифр «Кипарис».

Модуль 2.

Змістовний модуль 2.

Тема 3. Криптоаналіз симетричних шифрів

Метод грубої сили. Парадокс днів народження. Диференціальний криптоаналіз. Лінійний криптоаналіз. Метод відпалу. Словникова атака.

Тема 4. Криптоаналіз асиметричних шифрів.

Методи визначення простоти чисел. Методи факторизації великих чисел. Методи цілочислового логарифмування. Алгоритм Полларда. Алгоритм Ленстра. Алгоритм факторизації на основі рішення нерівності. Алгоритм дискретного логарифмування COS Алгоритм решета числового поля. Криптоаналіз систем на еліптичних кривих

Модуль 3.

Змістовний модуль 3.

Тема 5. Особливості використання криптографії в хмарних технологіях

Теоретичні основи побудови криптосистем в розподілених системах. Порівняльний аналіз систем шифрування, якими користуються в хмарних технологіях. Аналіз загроз. Генерація ключів. Системи шифрування. Електронний підпис.

Тема 6. Криптосистеми для хмарних технологій

Встановлення захищеного каналу. Встановлення доступу до інформації. Сегментування віртуальних машин. Методика шифрування. Гомоморфне шифрування.

4. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин				
	Денна форма				
	Усього	У тому числі			
		л	п	лаб.	с. р.
Модуль 1					
Змістовний модуль 1					
Тема 1. Теорія малоресурсної криптографії	26	6		6	14
Тема 2. Використання малоресурсної криптографії	20	4		4	12
Разом за змістовим модулем 1	46	10		10	26
Разом за модулем 1	46	10		10	26
Модуль 2					
Змістовний модуль 2					
Тема 3. Криптоаналіз симетричних шифрів	27	6		5	16
Модульний контроль	1			1	
Тема 3. Криптоаналіз асиметричних шифрів.	28	6		6	16
Разом за змістовим модулем 2	56	12		12	32
Разом за модулем 2	56	12		12	32
Модуль 3					
Змістовний модуль 3					
Тема 5. Особливості використання криптографії в хмарних технологіях	24	6		6	12
Тема 6. Криптосистеми для хмарних технологій	23	6		5	12
Модульний контроль	1			1	
Разом за змістовим модулем 3	48	12		12	24
Разом за модулем 3	48	12		12	24
Усього годин за семестр	150	34		34	82

5. Теми семінарських занять

№ з/п	Назва теми	Кількість годин
1	*Не передбачено*	
	Разом	

6. Теми практичних занять

№ з/п	Назва теми	Кількість годин
1	*Не передбачено*	
	Разом	

7. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Підходи до малоресурсної криптографії	2
2	Побудова малоресурсних шифрів	2
3	Блокові малоресурсні шифри	2
4	Використання шифрів Present і Clefia.	2
5	Використання шифрів Trivium і «Кипарис»	2
6	Використання диференціального криптоаналізу	2
7	Використання лінійного криптоаналізу	2
8	Використання методу відпалу.	2
9	Використання методів визначення простоти чисел.	2
10	Використання методів факторизації великих чисел.	2
11	Алгоритм дискретного логарифмування COS.	2
12	Аналіз загроз.	2
13	Генерація ключів.	2
14	Сегментування віртуальних машин.	2
15	Методика шифрування.	2
16	Гомоморфне шифрування.	2
17	Захист розподільних обчислень	2
	Разом	34

8. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Тема 1. Малоресурсна криптографія	14
2	Тема 2. Використання малоресурсної криптографії	12
3	Тема 3. Криптоаналіз симетричних шифрів	16
4	Тема 3. Криптоаналіз асиметричних шифрів.	16
5	Тема 5. Особливості використання криптографії в хмарних технологіях	12
6	Тема 6. Криптосистеми для хмарних технологій	12
	Разом	**82**

9. Індивідуальні завдання

Не передбачено

10. Методи навчання

Проведення аудиторних лекцій, лабораторних занять, консультацій, а також самостійна робота аспірантів за матеріалами, опублікованими кафедрою.

11. Методи контролю

Проведення поточного контролю, письмового модульного контролю, підсумковий контроль у вигляді іспиту.

12. Критерії оцінювання та розподіл балів, які отримують аспіранти

12.1. Розподіл балів, які отримують аспіранти (кількісні критерії оцінювання)

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Змістовний модуль 1			
Робота на лекціях	0…1	8	0…8
Виконання лабораторних робіт	0...3	8	0...24
Модульний контроль	0…18	1	0…18
Змістовний модуль 2			
Робота на лекціях	0…1	9	0…9

Виконання лабораторних робіт	0...3	9	0...27
Модульний контроль	0…14	1	0…14
Усього за семестр			**0…100**

Семестровий контроль у вигляді іспиту проводиться у разі відмови аспіранта від балів підсумкового модульного контролю й за наявності допуску до іспиту. Під час складання семестрового іспиту аспірант має можливість отримати максимум 100 балів.

Білет для іспиту складається з одного теоретичного та одного практичного запитань, максимальна кількість за кожне із запитань, складає 50 балів.

12.2. Якісні критерії оцінювання

Необхідний обсяг знань для одержання позитивної оцінки:

- загальні аспекти проблематики в галузі інформаційної безпеки (сучасний стан задач та проблем, загрози та види вірусних атак на інформаційні та комунікаційні системи, вимоги до їх захищеності), а також тенденції і перспективи створення механізмів захисту інформації за допомогою систем криптографічного захисту;
- характеристику методів і засобів криптографічного перетворення інформації, а також основних методів крипто аналізу;
- принципи побудови симетричних (блочних і потокових) та асиметричних малоресурсних криптографічних алгоритмів та протоколів, що використовуються для забезпечення конфіденційності та автентичності і цілісності повідомлень, а також показники ефективності криптографічних систем;
- методи забезпечення автентичності користувачів комп'ютерної мережі та при використанні хмарних технологій;
- характеристику методів реалізації основних функцій системи управління ключовими структурами.

Необхідний обсяг вмінь для одержання позитивної оцінки.

Аспірант повинен вміти:

- виконувати криптографічні перетворення у відповідності зі схемами алгоритмів симетричного і несиметричного шифрування, а також проводити порівняльний аналіз крипостійкості симетричних та несиметричних криптографічних систем;
- розраховувати параметри асиметричних алгоритмів цифрового підпису, протоколів автентифікації користувачів та схем формування ключів;
- здійснювати оцінку криптографічної стійкості криптографічних алгоритмів при використанні квантових комп'ютерів.

12.3 Критерії оцінювання роботи аспіранта протягом семестру

Задовільно (60-74). Показати знання та уміння, виконати 90% лабораторних завдань. Знати базові поняття, що стосуються криптографічного захисту інформації в малоресурсних системах та хмарних технологій.

Добре (75-89). Твердо знати теоретичний матеріал, опанувати матеріали всіх лекцій і виконати не менше 90% лабораторних завдань. Показати вміння виконувати всі лабораторні завдання в обумовлений викладачем строк з обґрунтуванням рішень та заходів, які наведено у методичних посібниках з лабораторних занять.

Відмінно (90-100). Повно знати основний та додатковий матеріал. Знати усі теми. Орієнтуватися у підручниках та посібниках.

Шкала оцінювання: бальна і традиційна

Сума балів	Оцінка за традиційною шкалою	
	Іспит, диференційований залік	Залік
90 – 100	Відмінно	Зараховано
75 – 89	Добре	
60 – 74	Задовільно	
0 – 59	Незадовільно	Не зараховано

13. Методичне забезпечення

1. Тексти лекцій.
2. Презентації лекцій
3. Керівництво до лабораторних занять
4. Електронний ресурс

14. Рекомендована література

Базова

1. Горбенко І. Д., Горбенко Ю. І. Побудування та аналіз систем, протоколів та засобів криптографічного захисту інформації. . Монографія. Харків. Форт. 2015 , 902с.

2. Горбенко Ю. І., Горбенко І. Д. Інфраструктури відкритих ключів . Системи ЕЦП. Теорія та практика. Монографія. Харків. Форт. 2010 , 593с.

3. Потій О. В., Лєншин А. В., Сорока Л. С., Єсін В. І. і ін. Інфраструктура відкритих ключів: технології, архітектура, побудова та впровадження. Дніпропетровськ: Академія митної служби України, 2011. 202с.

4. Горбенко І. Д., Горбенко Ю. І. Прикладна криптологія. Підручник. Харків. Форт. 2013р. 878с.

Допоміжна

1. Serious Cryptography: A Practical Introduction to Modern Encryption / Jean-Philippe Aumasson - No Starch Press - 312p., 2017.
2. Applied Cryptography: Protocols, Algorithms and Source Code in C / Bruce Schneier - John Wiley & Sons - 784p., 2015.
3. Practical Cryptography / Niels Ferguson, Bruce Schneier - Wiley - 432p. - 2003.

15. Інформаційні ресурси

1. http://www.kernel.org
2. http://fedoraproject.org
3. http://www.ubuntu.com
4. http://www.csn.khai.edu