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

Кафедра комп'ютерних систем, мереж і кібербезпеки (№ 503)

ЗАТВЕРДЖУЮ

Гарант ОНП «Кібербезпека»

_____ М.О. Колісник
(підпис) (ініціали та прізвище)

«31» 08 2020 р.

СИЛАБУС 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)

Освітня програма: Кібербезпека
(найменування освітньої програми)

Форма навчання: денна

Рівень вищої освіти: третій (освітньо-науковий)

Харків 2020 рік

Силабус Теорія і методи сучасної криптології
(назва дисципліни)

для аспірантів за спеціальністю 125 «Кібербезпека»
(код та найменування спеціальності)

освітньою програмою «Кібербезпека»
(найменування програми)

«26» 08 2020 р., – 8 с.

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

Силабус розглянуто на засіданні кафедри
комп'ютерних систем, мереж і кібербезпеки
(назва кафедри)

Протокол № 1 від «27» 08 2020 р.

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

1. Опис навчальної дисципліни

Галузь знань – 12 «Інформаційні технології»
Спеціальність – 125 Кібербезпека
Освітня програма – Кібербезпека
Рівень вищої освіти – третій (освітньо-науковий)
Форма навчання – денна
Семестр, в якому викладається дисципліна – 3-й
Дисципліна *вибіркова*
Загальна кількість годин за навчальним планом - 150 годин/ 5 кредитів ЄКТС.
Види занять – *лекції, практичні*
Вид контролю - іспит

2. Мета та завдання навчальної дисципліни

Мета: володіння науковими методами обґрунтування, вибору та аналізу криптографічних алгоритмів і протоколів.

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

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

Очікувані 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 кібербезпеки 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, здійснювати пошук та критичний аналіз інформації, концептуалізацію та реалізацію наукових проектів з кібербезпеки.

Пререквізити: матеріал дисципліни базується на знаннях, отриманих під час вивчення дисциплін "Обробка та аналіз результатів наукових досліджень з використанням ІТ".

Постреквізити: матеріал дисципліни є підґрунтям щодо написання дисертаційної роботи.

3. Програма навчальної дисципліни

Модуль 1.

Змістовний модуль 1. Малоресурсна криптографія

Тема 1. Теорія малоресурсної криптографії. 26 год.

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

Підходи до малоресурсної криптографії. Побудова малоресурсних шифрів. Блокові малоресурсні шифри.

Тема 2. Використання малоресурсної криптографії. 21 год.

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

Використання шифрів Present і Clcfia. Використання шифрів Trivium і «Кипарис»

Модульний контроль

Модуль 2.

Змістовний модуль 2. Методи криптоаналізу

Тема 3. Криптоаналіз симетричних шифрів. 28 год.

Метод грубої сили. Парадокс днів народження. Диференціальний криптоаналіз. Лінійний криптоаналіз. Метод відпалу. Словникова атака.
Використання диференціального криптоаналізу. Використання лінійного криптоаналізу. Використання методу відпалу.

Тема 4. Криптоаналіз асиметричних шифрів. 28 год.

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
Використання методів визначення простоти чисел. Використання методів факторизації великих чисел. Алгоритм дискретного логарифмування COS

Модуль 3.

Змістовний модуль 3. Криптографія в хмарних технологіях

Тема 5. Особливості використання криптографії в хмарних технологіях для наукових досліджень 26 год.

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

Тема 6. Криптосистеми для хмарних технологій. 21 год.

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

4. Індивідуальні завдання

Не має.

5. Методи навчання

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

6. Методи контролю

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

7. Критерії оцінювання та розподіл балів, які отримують аспіранти

7.1. 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	5	0…5
Виконання і захист лабораторних (практичних) робіт	0...3	5	0...15
Модульний контроль	0…15	1	0…15
Змістовний модуль 2			
Робота на лекціях	0…1	6	0…6
Виконання і захист лабораторних (практичних) робіт	0...3	6	0...18
Змістовний модуль 3			
Робота на лекціях	0…1	5	0…5
Виконання і захист лабораторних (практичних) робіт	0...3	5	0...15
Модульний контроль	0…15	1	0…15
Стаття, тези	0…6	1	0…6
Усього за семестр			**0…100**

Семестровий контроль (іспит) проводиться у разі відмови аспіранта від балів поточного тестування й за наявності допуску до іспиту. Під час складання семестрового іспиту аспірант має можливість отримати максимум 100 балів.

Білет для іспиту складається з двох теоретичних питання (0…30 балів за кожне питання) та одно практичне завдання (0…40 балів).

7.2. Якісні критерії оцінювання

Необхідний обсяг знань для одержання позитивної оцінки.

Аспірант повинен знати:

- 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.

7.3 Критерії оцінювання роботи аспіранта протягом семестру

Задовільно (60-74). Досягти очікуваних результатів навчання. Відпрацювати та захистити всі лабораторні роботи. Вміти самостійно давати характеристику існуючим криптосистемам, проводити їх аналіз, встановлювати і настроювати операційної системи у мереженому режиму. Вміти складати технічну документацію на комп'ютерну мережу.

Добре (75 - 89). Крім базових вимог на оцінку «задовільно», показати вміння виконувати та захищати всі лабораторні роботи в обумовлений викладачем строк з обґрунтуванням рішень та заходів, які запропоновано у роботах. Вміти пояснювати складні способи криптоаналізу систем шифрування, забезпечити налаштування систем захисту при використанні хмарним технологій.

Відмінно (90 - 100). Повно знати основній та додатковий матеріал. Знати усі теми. Орієнтуватися у підручниках та посібниках. Досконально знать усі технології, які використовуються при забезпеченні конфіденціальної інформаційних потоків в мережи,. Безпомилково виконувати та захищати всі лабораторні роботи в обумовлений викладачем строк з докладним обґрунтуванням рішень та заходів, які запропоновано у роботах. Під час вивчення курсу представити наукову роботу, згідно з темами, які вивчаються

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

8. Методичне забезпечення

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

9. 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.

10. Інформаційні ресурси

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