Міністерство освіти і науки України
Харківський національний університет імені В.Н.Каразіна
Кафедра безпеки інформаційних систем і технологій

“ЗАТВЕРДЖУЮ”
В.о. декана факультету комп’ютерних наук
_____ Євгенія КОЛОВАНОВА
“_30_” ____червня____ 2023 р.

Робоча програма навчальної дисципліни

Математичні методи синтезу та аналізу криптографічних примітивів

Рівень вищої освіти	третій (освітньо-науковий) рівень
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека
Освітня програма	освітньо-наукова програма підготовки докторів філософії
Вид дисципліни	вибіркова
Факультет	комп'ютерних наук

2023/2024 навчальний рік

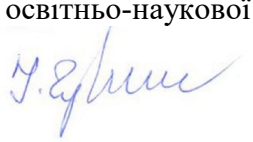
Програму рекомендовано до затвердження Вченою радою факультету комп'ютерних наук "29" червня 2023 року, протокол №14

РОЗРОБНИКИ ПРОГРАМИ: доктор технічних наук, професор, професор кафедри безпеки інформаційних систем і технологій ГОРБЕНКО Іван Дмитрович

Програму обговорено і схвалено на засіданні кафедри безпеки інформаційних систем і технологій "08" червня 2023 року, протокол № 12
В.о.завідувача кафедри безпеки інформаційних систем і технологій


Ігор СВАТОВСЬКИЙ

Програму погоджено з гарантом освітньо-наукової програми 125 "Кібербезпека"
Гарант освітньо-наукової програми "Кібербезпека"


Іван ГОРБЕНКО

Програму погоджено методичною комісією факультету комп'ютерних наук "21" червня 2023 року, протокол №12
Голова методичної комісії факультету комп'ютерних наук


Лариса ВАСИЛЬЄВА

ВСТУП

Програма навчальної дисципліни» «Математичні методи синтезу та аналізу криптогра- фічних примітивів» складена відповідно до освітньо - наукової програми підготовки фахівця третього (докторів філософії) рівня вищої освіти за спеціальністю 125 – «Кібербезпека» (ВБ 1.2).

1.Опис навчальної дисципліни

- Мета викладання навчальної дисципліни

Метою викладання навчальної дисципліни є навчання аспірантів щодо математичних методів аналізу існуючих криптографічних примітивів та математичних методів синтезу та аналізу перспективних криптографічних примітивів, в тому числі для застосування в перехідний та постквантовий періоди для надання користувачам послуг з криптографічного захисту інформації (КЗІ) в інформаційно – комунікаційних системах та інформаційних технологіях. Результатом навчання повинна бути забезпечена підготовленість аспірантів до проведенні наукових досліджень щодо комплексного аналізу існуючих та перспективних криптографічних примітивів для постквантового періоду по критеріям криптографічної стійкості, техніко – економічним і техніко – експлуатаційним критеріям..

В процесі вивчення дисципліни аспіранти мають можливість використовувати отримані компетенції, знання і вміння при проведенні наукових досліджень в криптології для оцінки та порівняння асиметричних та симетричних криптопримітивів, удосконалювати та розробляти стандартизовані криптографічні примітиви для перехідного та постквантового періодів, застосовувати асиметричні та симетричні криптопримітиви для надання користувачам послуг цілісності, справжності, доступності, неспростовності тощо, а також розробляти застосовувати математичні та програмні моделі існуючих та перспективних механізмів КЗІ. Мати компетенції та вміння щодо підготовки за результатами досліджень доповідей, звітів та наукових публікацій, використовувати їх при розробці кваліфікаційної роботи доктора філософії.

- Основні завдання вивчення дисципліни

Основними завданнями вивчення дисципліни є формування у аспірантів певних знань та вмінь в криптології з: вибору теми дослідження, формулювання назви роботи, визначення об'єкту та предмету дослідження, визначення мети і задач, вибору методів дослідження, роботи з літературою, формулювання висновків, обробки і представлення результатів дослідження, етичного кодексу автора наукових публікацій та доповідей, у тому числі формувати несприйняття академічного шахрайства, включаючи плагіат та самоплагіат.

- Кількість кредитів – 6.

- Загальна кількість годин – 180.

1.5. Характеристика навчальної дисципліни	
Нормативна / <u>за вибором</u>	
Денна форма навчання	Заочна (дистанційна) форма навчання
Рік підготовки	
2-й	2-й
Семестр	

4-й	4-й
Лекції	
16 год	

Практичні, семінарські заняття	
14 год	
Лабораторні заняття	
Самостійна робота	
150 год	
Індивідуальні завдання	
30	

1.6. Заплановані результати навчання

МАТИ КОМПЕТЕНЦІЇ:

Загальні

- **ЗК 5.** Вміння виявляти, ставити та вирішувати проблеми.

Фахові компетентності

- **ФК 1**. Здатність використати сучасні досягнення науки і передових технологій;
- **ФК 6**. Професійне володіння комп'ютером та інформаційними технологіями;
- **ФК 7.** Здатність виконувати роботи з проектування складних комплексів засобів захисту та управління безпекою інформаційних і телекомунікаційних систем відповідно до сфери їх застосування;
- **ФК 8.** Здатність здійснювати та детально обґрунтовувати вибір структури, принципів організації, комплексів засобів і технологій забезпечення безпеки інформаційних і телекомунікаційних систем;
- **ФК 9.** Здатність здійснювати аналіз та синтез криптографічних примітивів.

За результатами вивчення дисципліни аспіранти повинні

ЗНАТИ:

- криптографічні механізми (методи, стандартизовані протоколи, алгоритми та засоби) надання користувачам послуг з безпеки інформації та кібербезпеки;
- науково – технічні основи оцінки, аналізу та порівняння асиметричних та симетричних криптографічних примітивів КЗІ;
- сутність та можливості застосування математичних методів синтезу та аналізу асимет- ричних криптографічних примітивів КЗІ в кібербезпеці;
- основні математичні методи та системи аналізу та порівняння криптографічних приміти- вів по безумовним, умовним та прагматичним критеріям;
- вимоги до системи національної стандартизації у галузі КЗІ;
- принципи та сутність визначення об'єкта і предмета дослідження, мети і задач, вибору методів дослідження;
- етичні принципи, яких мають додержуватися автори наукових публікацій;

ВМІТИ:

- обґрунтовувати та вибирати критерії та показники оцінки механізмів КЗІ;
- обґрунтовувати вибір та застосовувати методики аналізу та порівняння існуючих та пер- спективних стандартизованих механізмів КЗІ в кібербезпеці;

- демонструвати уміння проводити пошук інформації з різних джерел, її обробку та аналіз із залученням сучасних інформаційних технологій;
- планувати, здійснювати та оформляти власне наукове дослідження, присвячене суттєвій проблемі сучасної науки у галузі безпеки інформації;
- проводити наукові та практичні дослідження існуючих та перспективних механізмів КЗІ з використанням систем умовних, безумовних та прагматичних критеріях;

- демонструвати уміння представляти результати досліджень на державній та одній з іноземних мов.

2. Тематичний план навчальної дисципліни

Розділ 1. Науково – методичні основи аналізу та порівняння криптопримітивів. Класифікація та вимоги до існуючих та перспективних криптопримітивів. . Класичні та по-
стквантові асиметричні та симетричні криптопримітиви. Критерії та показники оцінки без- печності та техніко – економічних і техніко – експлуатаційних характеристик криптоприміти- вів. Безумовні, умовні, та прагматичні критерії і методики оцінки та порівняння криптопримі- тивів. Приклади застосування методик для аналізу та порівняння стандартизованих асиметрич- них криптопримітивів.

Розділ 2. Стан, основні положення теорії та практики синтезу та аналізу асиметричних кри- птопримітивів.

Класифікація асиметричних криптопримітивів, національні та міжнародні вимоги до них. Основні математичні методи синтезу асиметричних примітивів електронного підпису(ЕП). аси- метричного шифрування (АСШ) та протоколів інкапсуляції ключів(ПІК) та їх оцінка. Синтез, аналіз, оцінка та порівняння перспективних асиметричних криптоперетворень ЕП на основі алгебраїчних решіток та мультиваріативних перетворень. Синтез, аналіз та порівняння перспе- ктивних асиметричних криптоперетворень АСШ та ПІК на основі алгебраїчних решіток. Особ- ливості синтезу , аналізу, оцінки та порівняння асиметричних криптоперетворень АСШ та ПІК на основі математичних кодів та ізогеній еліптичних кривих. Приклади застосування мето- дик для аналізу, оцінки та порівняння асиметричних криптопримітивів типу ЕП, АСШ та ПІК.

Розділ 3. Стан, основні положення теорії та практики синтезу та аналізу асиметричних кри- птопримітивів на основі симетричних криптоперетворень.

Класифікація та характеристика асиметричних криптопримітивів ЕП, АСШ та ПІК на осно- ві симетричних криптоперетворень. Основні методи синтезу асиметричних криптопримітивів ЕП, АСШ та ПІК на основі симетричних криптоперетворень та їх попередня оцінка та умови реалізації. Синтез, аналіз та оцінка перспективних симетричних криптоперетворень гешування, блокового та потокового шифрування. Синтез, аналіз, оцінка та порівняння перспективних аси- метричних криптоперетворень ЕП на основі симетричних криптоперетворень. Синтез, аналіз, оцінка та порівняння перспективних асиметричних криптоперетворень ЕП на основі одноразо- вих ключів. Приклади застосування методик для аналізу, оцінки та порівняння асиметричних криптопримітивів типу ЕП, АСШ та ПІК на основі симетричних криптопримітивів.

Розділ 4. Методи та системи криптографічного аналізу та умови і можливості забезпечення безпеки від них.

Класифікація та можливості і умови успішного криптоаналізу асиметричних криптопримі- тивів типу ЕП, АСШ та ПІК. Методи та системи доведення безпеки асиметричних криптопри- мітивів типу ЕП, АСШ та ПІК. Методи криптоаналізу на

класичних та квантових атак. Моделі безпеки ЕП, АСШ та ПІК та умови і можливості їх реалізації.

Методики оцінки та порівняння існуючих та перспективних ЕП, АСШ та ПІК та приклади їх оцінки та порівняння по сукупності безумовних, умовних та прагматичних критеріїв. Прик- лади оцінки та порівняння складності криптоаналізу симетричних та асиметричних криптопри- мітивів з використанням квантових методів Гровера, Шора тощо. Стан, умови та можливості здійснення квантового криптоаналізу . Оцінка та порівняння стійкості існуючих та перспектив- них ЕП та АСШ проти класичного та квантового криптоаналізу та здійснення атак.

3. Структура навчальної дисципліни

Назви розділів	Кількість годин											
	денна форма						заочна форма					
	усього	у тому числі					усього	у тому числі				
		л	п	лаб.	інд.	с. р.		л	п	лаб.	інд.	с. р.
1	2	3	4	5	6	7	8	9	10	11	12	13
Розділ 1. Науково – методичні основи аналізу та порівняння криптопримітивів												
Разом за розділом 1	34	2	2			30						
Розділ 2. Стан, основні положення теорії та практики синтезу та аналізу асиметричних крипто- примітивів												
Разом за розділом 2	58	6	6			46						
Розділ 3. Стан, основні положення теорії та практики синтезу та аналізу асиметричних крипто- примітивів на основі симетричних криптоперетворень												
Разом за розділом 3	46	4	2			40						
Розділ 4. Основні математичні методи криптографічного аналізу стійкості методів КЗІ												
	42	4	4			34						
Усього годин	**180**	**16**	**14**			**150**						

4. Теми семінарських (практичних, лабораторних) занять

№з/п	***Назва теми***	***Кількість годин***
1	Критерії та показники оцінки безпечності та техніко – економічних і техніко – експлуатаційних характеристик криптопримітивів. Безу- мовні, умовні, та прагматичні критерії і методики оцінки та порів- няння криптопримітивів. Приклади застосування методик для аналі- зу та порівняння стандартизованих асиметричних криптопримітивів.	2
2	Синтез, аналіз, оцінка та порівняння перспективних асиметричних криптоперетворень ЕП на основі алгебраїчних решіток та мультива- ріативних перетворень. Приклади застосування методик для аналізу, оцінки та порівняння асиметричних криптопримітивів типу ЕП. .	2
3	. Синтез, аналіз та порівняння перспективних асиметричних крип- топеретворень АСШ та ПІК на основі алгебраїчних решіток. Особ- ливості синтезу , аналізу, оцінки та порівняння асиметричних кри- птоперетворень АСШ та ПІК	2

	на основі математичних кодів та ізоге- ній еліптичних кривих.	
4	Приклади застосування методик для аналізу, оцінки та порівняння асиметричних криптопримітивів типу АСШ та ПІК. Розробка реко- мендацій щодо умов застосування АСШ та ПІК.	2
5	Синтез, аналіз та оцінка перспективних симетричних криптопере- творень гешування, блокового та потокового шифрування. Синтез, аналіз, оцінка та порівняння перспективних асиметричних крипто- перетворень ЕП на основі симетричних криптоперетворень.	2
6	Приклади оцінки та порівняння складності криптоаналізу симетри- чних та асиметричних криптопримітивів з використанням квантових методів Гровера, Шора тощо.	2

7	Оцінка та порівняння стійкості існуючих та перспективних ЕП та АСШ проти класичного та квантового криптоаналізу та здійснення атак.	2

5. Завдання для самостійної роботи

№з/п	Види, зміст самостійної роботи	***Кількість годин***
1	Пошук та вивчення джерел інформації щодо вимог до класичних та по- стквантових криптопримітивів ЕП, АСШ, ПІК . Порядок розробки мо- делей порушника, загроз та безпеки. Критерії та показники оцінки без- печності та техніко – економічних і техніко – експлуатаційних характе- ристик криптопримітивів. Безумовні, умовні, та прагматичні критерії і методики оцінки та порівняння криптопримітивів. Переклад та оформ- лення основних даних перекладу, їх представлення на семінарі.	30
2	Класифікація, аналіз, оцінка та порівняння перспективних асиметри- чних криптоперетворень ЕП на основі алгебраїчних решіток.. Підготов- ка пропозицій, розробка програмного забезпечення та аналіз, оцінка та порівняння асиметричних криптопримітивів типу ЕП . Виконання індивідуального завдання.	16
3	Класифікація, аналіз, оцінка та порівняння перспективних асиметрич- них криптоперетворень АСШ та ПІК на основі алгебраїчних решіток.. Підготовка пропозицій, розробка програмного забезпечення та аналіз, оцінка та порівняння асиметричних криптопримітивів типу АСШ та ПІК. Виконання індивідуального завдання.	14
4	Виконання індивідуального завдання щодо застосування методик для аналізу, оцінки та порівняння асиметричних криптопримітивів типу ЕП, АСШ та ПІК. Розробка рекомендацій щодо умов застосування АСШ та ПІК.	16
5	Обгрунтування та розробка вимог до постквантових стандартів симет- ричних криптоперетворень. Аналіз та оцінка перспективних	20

	симетрич- них криптоперетворень гешування, блокового та потокового шифруван- ня. Виконання індивідуального завдання щодо оцінкт стійкості БСШ.	
6	Основні методи криптоаналізу існуючих стандартизованих алгоритмів блокового та потокового шифрування. Класифікація, вимоги та моделі безпеки щодо механізмів КЗІ для пост квантового періоду. Підготовка доповіді на семінар згідно індивідуального завдання.	20
7	Приклади оцінки та порівняння складності криптоаналізу симетричних та асиметричних криптопримітивів з використанням квантових методів Гровера, Шора тощо. Стан, умови та можливості здійснення квантового криптоаналізу на класичних та квантових комп'ютерах. Підготовка до- повіді на НТК згідно індивідуального завдання чи підготовка та подача статі для рецензування.	34
	Разом:	**150**

6. Індивідуальні завдання */Не передбачено/*

7. Методи контролю

Контроль засвоєння аспірантами навчального матеріалу на лекційному зайнятті здійснюється шляхом концентрації уваги аспірантів постановкою питань за раніше вивченим матеріалом, пов'язаним з тематикою лекції.

На семінарських та практичних заняттях контроль засвоєння аспірантами навчального матеріалу здійснюється шляхом оцінки якості виконання індивідуальних завдань. Рівень знань, продемонстрований аспірантами при оформленні і захисті звітів з практичних занять оцінюється окремо для кожного практичного заняття (ПЗ) та семінарського заняття кількістю балів відповідно до наведеної нижче таблиці.

Максимальна кількість балів за результатами контролю поточної успішності складає 100
балів.

Таблиця 7.1 – Розподіл балів, які отримують аспіранти за результатами контролю поточної успішності

Вид заняття / контрольний захід	**Оцінка** N_{max}
Практичні(семінарські) заняття	
ПЗ 1	10
ПЗ 2	11
ПЗ 3	10
ПЗ 4	9
ПЗ 5	10
ПЗ 6	10
ПЗ 7	10
Підготовка та прийняття доповіді на НТК	10
Підготовка та отримання позитивної рецензії на статтю	20
Всього за семестр	100

Згідно рішення кафедри безпеки інформаційних систем і технологій до екзамену не допускаються аспіранти, що не захистили звіти з практичних занять.

Підсумковий контроль здійснюється за результатами поточного контролю шляхом підсумовування оцінок, отриманих за практичні заняття, виступи на семінарах та за виступом на НТК і підготовлені статі .

Максимальна кількість балів за результатами вивчення дисципліні складає 100 балів.

8. Схема нарахування балів

Бали за поточний контроль знань по розділам протягом семестру				Курсова робота	Разом сума балів у семестрі	Іспит	Загальна сума балів
Розділ 1	Розділ 2	Розділ 3	Розділ 4				
20	30	25	25		100		100

Шкала оцінювання

Сума балів за всі види навчальної діяльно-сті протягом семестру	Оцінка
	для чотирьох шкали оцінювання
90 – 100	відмінно
70 –-89	добре
50 – 69	задовільно
<50	не задовільно

Критерії оцінювання

Критерії оцінювання знань студентів за виконання практичних занять

Визначення	Кількість балів*
Індивідуальне завдання з практичного заняття(виступ на семі- нарі) виконане самостійно в повному обсязі. Звіт оформлений акуратно відповідно до вимог методичних вказівок. При захис- ті звіту показано розуміння суті і змісту проведених дослі- джень	$Nmax$
Індивідуальне завдання з практичного заняття (виступ на семі- нарі) виконане самостійно в повному обсязі. Звіт оформлений достатньо акуратно відповідно до вимог методичних вказівок. При захисті звіту були виявлені незначні помилки у знанні тео- ретичного матеріалу.	$[N_{max} - \lfloor N_{max} / 7 \rfloor, N_{max} - 1]$
Індивідуальне завдання з практичного заняття (виступ на семі- нарі)виконане в повному обсязі. Звіт оформлений достатньо акуратно, в оформленні звіту є незначні недоліки. При захисті звіту були виявлені незначні помилки у знанні теоретичного матеріалу.	$[N_{max} - 2 \times \lfloor N_{max} / 7 \rfloor, N_{max} - \lfloor N_{max} / 7 \rfloor]$
Індивідуальне завдання з практичного заняття виконане. Звіт оформлений з помилками і недоліками. При захисті звіту були виявлені суттєві помилки у знанні теоретичного матеріалу.	$N_{max} - 3 \times \lfloor N_{max} / 7 \rfloor, N_{max} - 4 \times \lfloor N_{max} / 7 \rfloor]$
Показано недосконале знання навчального матеріалу, допущені суттєві помилки, які носять принциповий характер. Звіт офор- млений з помилками і суттєвими недоліками.	$[1, N_{max} - 4 \times \lfloor N_{max} / 7 \rfloor]$
Доповідь на НТК прийнято та успішно зроблено	$Nmax$
Доповідь на НТК прийнято	$N_{max} - 4$

Стаття опублікована	*Nmax*
На статтю отримано позитивну рецензію	*Nmax* – 5

* *Nmax*

– максимальна кількість балів для відповідного заняття відповідно до таблиці 7.1.

9. Рекомендована література

9.1. Основна література

- Горбенко Ю. І. Методи побудування та аналізу криптографічних систем: монографія. / Ю. І. Горбенко. Х. Під заг. Ред.. Горбенко І.Д.: Форт, 2015. – 959 с.
- Gorbenko, I.D., Kachko, O.G., Yesina, M.V., 2018. ANALYSIS OF ASYMMETRIC NTRU PRIME IIT UKRAINE ENCRYPTION ALGORITHM WITH REGARDS TO KNOWN ATTACKS.Telecommunications and Radio Engineering,vol.77. https://doi.org/10.1615/TelecomRadEng.v77.i9.50
- Gorbenko, Y.I., Melnik, T.V., Gorbenko, I.D., 2018. ANALYSIS OF POTENTIAL POST-QUANTUM SCHEMES OF HASH-BASED DIGITAL SIGNATUR. Telecommunications and Radio Engineering, vol. 77. https://doi.org/10.1615/TelecomRadEng.v77.i7.40
- Gorbenko, I., Kuznetsov, A., Gorbenko, Y., Vdovenko, S., Tymchenko, V., Lutsenko, M., 2019b. STUDIES ON STATISTICAL ANALYSIS AND PERFORMANCE EVALUATION FOR SOME STREAM CIPHERS. International Journal of Computing 18, 82–88. https://www.computingonline.net/computing/article/view/12772/
- Горбенко І. Д. Постквантова криптографія та механізми її реалізації / І. Д. Горбенко, О. О. Кузнєцов, О. В. Потій, Ю. І. Горбенко, Р. С. Ганзя, В. А. Пономар // Радіотехніка. – 2014. – Вип. 184. – С. 32-52.
- Gorbenko, I.D., Kachko, O.G., Gorbenko, Y.I., Stelnik, I.V., Kandy, S.O., Yesina, M.V., 2019b. METHODS OF BUILDING GENERAL PARAMETERS AND KEYS FOR NTRU PRIME UKRAINE OF 5^{TH} – 7^{TH} LEVELS OF STABILITY. PRODUCT FORM. Telecommunications and Radio Engineering, vol. 78. https://doi.org/10.1615/TelecomRadEng.v78.i7.30
- Аналіз сутності та моделі протоколу інкапсуляції ключів у кільці поліномів над скін- ченим полем/*Горбенко І. Д., Качко О. Г., Пономар В. А., М. В., Акользіна О. С., Кулібаба В. А.//Прикладна радіоелектроніка, 2018, Том 17, No 3, 4.*
- Порівняння кандидатів електронного підпису на постквантовий стандарт NIST PQC на базі MQ-перетворень та функцій ґешування /*Горбенко Ю. І., Кудряшов І. С., Науменко Д. С., Онопрієнко В. В. //Прикладна радіоелектроніка, 2018, Том 17, No 3, 4.*
- Модель безпеки постквантових протоколів інкапсуляції ключів/*Єсіна М. В.//Прикладна радіоелектроніка, 2018, Том 17, No 3, 4.*
- Математична структура потокового шифру Струмок / О.О. Кузнецов, І.Д. Горбенко, Ю.І.Горбенко, А.М. Олексійчук, В.А. Тимченко // Радіотехніка : Всеукр. міжвід. на- ук.-техн. зб. 2018. Вип. 193. С. 17 – 27.

- Методи побудування загальних параметрів та ключів для NTRU PRIME UKRAINE 5 – 7 рівнів стійкості. Product form / І.Д. Горбенко, О.Г. Качко, Ю.І. Горбенко, І.В. Стельнік, С.О. Кандій, М.В. Єсіна // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2018. – Вип. 195. – С. 5 – 16.
- Neal Koblitz and Alfred J. Menezes A Riddle wrapped in an Enigma. Department of Mathematics, Box 353.350, University of Washington, Seattle, WA 98195 U.S.A. – Режим доступу: https://eprint.iacr.org/2015/1018.pdf.
- Lily Chen Report on Post-Quatum Cryptography. NISTIR 8105 (DRAFT) / Lili Chen, Stephen Jordan, Yi-Kai-Liu, Dustin Moody, Rene Peralta, Ray Perlner, Daniel Smith-Tone // – Режим доступу:http://csrc.nist.gov/publications/drafts/nistir-8105/nistir_8105_draft.pdf.
- Gorjan Alagic NISTIR 8309 Status Report on the Second Round of the NIST Post- Quantum Cryptography Standardization Process / Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, John Kelsey, Yi-Kai Liu, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, Daniel Smith-Tone //. – Режим доступу: https://doi.org/10.6028/NIST.IR.8309 HYPERLINK "https://doi.org/10.6028/NIST.IR.8309".
- Gorbenko I. D. Calculation of general parameters for NTRU Prime Ukraine of 6-7 levels of stability / I. D. Gorbenko, A. N. Alekseychuk, O. G. Kachko, M. V. Yesina, I. V. Stelnik, S. O. Kandy,V. A. Bobukh, V. A. Ponomar // Telecommunications and Radio Engineering, 2019. – Volume 78, Issue 4 – P. 327-340. DOI: 10.1615/TelecomRadEng.v78.i4.40.
- Gorbenko I.D. Methods of building general parameters and keys for NTRU Prime Ukraine of 5^{th}–7^{th} levels of stability. Product form / I.D. Gorbenko, O.G. Kachko, Yu.I. Gorbenko, I.V. Stelnik, S.O. Kandyi, M.V. Yesina // Telecommunications and Radio Engineering, 2019. – Volume 78, Issue 7
– P. 579-594. DOI: 10.1615/TelecomRadEng.v78.i7.30.
- Gorbenko I. D. Analysis of asymmetric NTRU Prime IIT Ukraine encryption algorithm with regards to known attacks / I. D. Gorbenko, O. G. Kachko, M. V. Yesina // Telecommunications and Radio Engineering, 2018. – Volume 77, Issue 9 – P. 799-816. DOI: 10.1615/TelecomRadEng.v77.i9.50.
- Gorbenko I. D. General statements and analysis of the end-to-end encryption algorithm NRTU Prime IIT Ukraine / I. D. Gorbenko, O. G. Kachko, M. V. Yesina // Радіотехніка. – Х. : ХНУРЕ, 2018. – Вип. 193 – С. 5–16.
- Gorbenko I.D. Methods of building general parameters and keys for NTRU Prime Ukraine of 5th–7th levels of stability. Product form / I.D. Gorbenko, O.G. Kachko, Yu.I. Gorbenko, I.V. Stelnik, S.O. Kandyi, M.V. Esina // Радіотехніка. – Х. : ХНУРЕ, 2018. – Вип. 195 – С. 5–16.
- Gorbenko I.D. Calculation of general parameters for NTRU Prime Ukraine of 6-7 levels of stability / I.D. Gorbenko, A.N. Alekseychuk, O.H. Kachko, M.V. Yesina, V.A. Bobukh, S.O. Kandyi,
V.A. Ponomar // Радіотехніка. – Х. :ХНУРЕ, 2018. – Вип. 195 – С. 17–26.
- Горбенко І. Д. Методи обчислення системних параметрів для електронного підпису «Crystals-Dilithium» 128, 256, 384 та 512 біт рівнів безпеки / І.Д. Горбенко, А.М. Олексійчук, О.Г. Качко, Ю.І. Горбенко, М.В. Єсіна, С.О. Кандій // Радіотехніка. – Х. : ХНУРЕ, 2020. – Вип. 202. С. 5-28.

• Горбенко І. Д. Генерація загальносистемних параметрів для криптосистеми Falcon для 256, 384, 512 біт безпеки /І.Д. Горбенко, С.О. Кандій, М. В. Єсіна, Є. В. Острянська // Радіотехніка. – Х. :ХНУРЕ, 2020. – Вип. 202. С. 57–63.

• Vadim Lyubashevsky CRYSTALS-Dilithium / Vadim Lyubashevsky, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Peter Schwabe, Gregor Seiler, Damien Stehlé //. Submission to the NIST Post-Quantum Cryptography Standardization, 2017. – Режим доступу: https://pq- crystals.org/dilithium HYPERLINK "https://pq-crystals.org/dilithium".

• Falcon. [Електронний ресурс]. – Режим доступу: https://csrc.nist.gov/projects/post- quantum-cryptography/round-1-submissions HYPERLINK "https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions".

• Генерація загальносистемних параметрів для криптосистеми Falcon для 256, 384, 512 біт безпеки /І.Д. Горбенко, С.О. Кандій, М.В. Єсіна, Є.В. Острянська // Радіотехніка : Все- укр. міжвід. наук.-техн. зб. 2020. Вип. 202. С. 57 – 63.

9.2. Допоміжна література

• Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлення. ДСТУ 3008-2015. – Чинний від 2017-07-01. – К. : ДП «УкрНДНЦ», 2016. – 26 с. –(Національний стандарт України).

• Інформація та документація. Бібліографічне посилання. Загальні положення та правила складання. ДСТУ 8302:2015. – Чинний від 2016-07-01. – К. : ДП «УкрНДНЦ», 2016. – 16 с. – (Національний стандарт України).

• ISCI'2019: Information Security in Critical Infrastructures. Collective monograph. Ed- ited by Ivan D. Gorbenko and Alexandr A. Kuznetsov. ASC Academic Publishing, USA, 2019, 445 p. ISBN:978-0-9989826-8-7 (Hardback), ISBN: 978-0-9989826-9-4 (Ebook).
https://www.amazon.com/dp/B08NGZ77CM

• A. Kuznetsov, Y. Gorbenko, I. Kolovanova, S. Smirnov, I. Perevozova, and T. Kuz- netsova, "Output Feedback Encryption Mode: Periodic Features of Output Blocks Sequence," in *Data- Centric Business and Applications*, vol. 48, T. Radivilova, D. Ageyev, and N. Kryvinska, Eds. Cham: Springer International Publishing, 2021, pp. 621–648.

https://link.springer.com/chapter/10.1007%2F978-3-030-43070- HYPERLINK "https://link.springer.com/chapter/10.1007%2F978-3-030-43070-2_27"2_27

• Мчедлов-Петросян Н.О. Етичний аспект наукових публікацій в умовах інформаційного вибуху // Вісник НАН України, 2014, № 8. С.77-87.

• NIST PQC: Кодові криптосистеми / О.О. Кузнецов, Ю.І.Горбенко, М.С.Луценко, Д.І. Прокопович-Ткаченко, М.В. Пастухов // Радіотехніка : Всеукр. міжвід. наук.- техн. зб. – 2018. – Вип. 195. – С. 32 – 40.

• Сутність та особливості реалізації методу Гровера на класичному комп'ютері для симет-ричного криптоаналізу / Ю.І. Горбенко, Є.Ю. Каптьол // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2018. – Вип. 195. – С. 89 – 100.

• Математична модель сигналів з ортогональним частотним розподілом і мультип- лексуванням(OFDM) / І.Д. Горбенко, О.А. Замула, В.Л. Морозов, С.В Родіонов // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2019. Вип. 47198. С. 32 – 44

- Можливості застосування механізмів повністю гомоморфного шифрування в сис- темах електронного голосування / І.Д. Горбенко, О.Г. Качко, Ю.І. Горбенко, М.В. Єсіна, С.О. Кандій, Є.В. Острянська, А.С. Д'яченко // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 200. С. 98 – 113

9.3. Посилання на інформаційні ресурси в Інтернеті, відео-лекції, інше методичне забезпечення

- ETSI GR QSC 001 V.1.1.1 (2016-07). Quantum-Safe Cryptography (QSC); Quantum- safe algorithmic framework.– Режим доступу: https://www.etsi.org/deliver/etsi_gr/QSC/001_099/001/01.01.01_60/gr_QSC001v010101p.pdf.
- Vadim Lyubashevsky CRYSTALS-Dilithium / Vadim Lyubashevsky, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Peter Schwabe, Gregor Seiler, Damien Stehlé //. Submission to the NIST Post-Quantum Cryptography Standardization, 2017. – Режим доступу: https://pq- crystals.org/dilithium.
- Falcon. [Електронний ресурс]. – Режим доступу: https://csrc.nist.gov/projects/post- quantum-cryptography/round-1-submissions.
- Thomas Pornin New Efficient, Constant-Time Implementations of Falcon
- ДСТУ 7564:2014 Інформаційні технології. Криптографічний захист інформації. Функція гешування. – Режим доступу: http://online.budstandart.com/ua/catalog/doc- page.html?id_doc=66229.
- ДСТУ 7624:2014 Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. – Режим доступу: https://www.twirpx.com/file/2878521/.
- ДСТУ 8845:2019 Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного потокового перетворення. – Режим доступу: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=82494.
- ДСТУ 8961:2019 Інформаційні технології. Криптографічний захист інформації. Алгоритми асиметричного шифрування та інкапсуляції ключів. – Режим доступу: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=88056.
- Горбенко Ю. І. Моделі загроз щодо асиметричних криптоперетворень перспекти- вного електронного підпису / Ю.І. Горбенко, М.В. Єсіна, В.В. Онопрієнко, Г.А. Малєєва // Радіотехніка. – Х. : ХНУРЕ, 2020. – Вип. 202. С.72–78.
- Горбенко Ю. І. Основні положення щодо моделі безпеки для асиметричних криптоперетворень типу ЕП з урахуванням вимог та загроз постквантового періоду/ Ю.І. Горбенко, О.В. Потій, В.В. Онопрієнко, М.В. Єсіна, Г.А.Малєєва // Радіотехніка. – Х. : ХНУРЕ, 2020. – Вип. 202. С. 28-36.
- Yesina Maryna, Gorbenko Yurij (supervisor). Methods of cryptographic primitives comparative analysis // Inżynier XXI wieku ("Engineer of XXI Century" – the VI Inter University Conference of Students, PhD Students and Young Scientists: University of Bielsko-Biala, Poland, December 02, 2016). – Bielsko-Biała: Wydawnictwo Naukowe Akademii Techniczno-Humanistycznej w Bielsku-Białej, 2016. – P. 451–462. – ISBN 978-83-65182-51-7. – Chapter in monograph.
- J. Ding Rainbow / J. Ding, M. Chen, A. Petzoldt et al.//, 2019. [Електронний ресурс]. – Режимдоступу: https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum- Cryptography/documents/round-2/submissions/Rainbow-Round2.zip.

• Gorbenko I. Examining a possibility to use and the benefits of post-quantum algorithms dependent on the conditions of their application / Gorbenko I., Ponomar V. // Eastern-European Journal of Enterprise Technologies. – 2017. – Vol. 2 NO 9 (86). – P.21–32. – Режим доступу: http://journals.uran.ua/.