

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

“ЗАТВЕРДЖУЮ”

Проректор
з науково-педагогічної роботи

М.О. Азаренков

_____ 2020 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 програми підготовки докторів філософії
вид дисципліни	вибіркова
факультет	комп'ютерних наук

2020 / 2021 навчальний рік

Програму рекомендовано до затвердження Вченою радою факультету комп'ютерних наук
« 31 » серпня 2020 року, протокол № 12

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

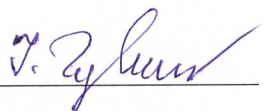
Програму схвалено на засіданні кафедри безпеки інформаційних систем і технологій
Протокол від « 31 » серпня 2020 року № 1

Завідувач кафедри безпеки інформаційних систем і технологій

 Сергій РАССОМАХІН

Програму погоджено з гарантом освітньо-наукової програми 125 «Кібербезпека»

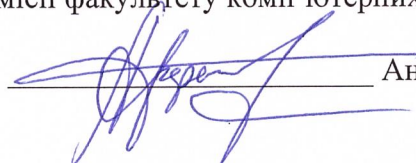
Гарант освітньо-професійної програми
«Кібербезпека»

 Іван ГОРБЕНКО

Програму погоджено методичною комісією факультету комп'ютерних наук

Протокол від « 31 » серпня 2020 року № 1

Голова методичної комісії факультету комп'ютерних наук

 Анатолій БЕРДНІКОВ

ВСТУП

Програма навчальної дисципліни «Математичні методи синтезу та аналізу криптографічних 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

1.1. 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.

1.2. 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.

1.3. Кількість кредитів – 6.

1.4. 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 асиметричних криптографічних примітивів КЗІ в кібербезпеці;
- основні математичні методи та системи аналізу та порівняння криптографічних примітивів 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 дотримуватися автори наукових публікацій;

ВМІТИ:

- обґрунтовувати та вибирати критерії та показники оцінки механізмів КЗІ;
- обґрунтовувати вибір та застосовувати методики аналізу та порівняння існуючих та перспективних 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 постквантові асиметричні та симетричні криптопримітиви. Критерії та показники оцінки безпечності та техніко – економічних і техніко – експлуатаційних характеристик криптопримітивів. Безумовні, умовні, та прагматичні критерії і методики оцінки та порівняння криптопримітивів. Приклади застосування методик для аналізу та порівняння стандартизованих асиметричних криптопримітивів.

Розділ 2. Стан, основні положення теорії та практики синтезу та аналізу асиметричних криптопримітивів.

Класифікація асиметричних криптопримітивів, національні та міжнародні вимоги до них. Основні математичні методи синтезу асиметричних примітивів електронного підпису(ЕП). асиметричного шифрування (АСШ) та протоколів інкапсуляції ключів(ПКК) та їх оцінка. Синтез, аналіз, оцінка та порівняння перспективних асиметричних криптоперетворень ЕП на основі алгебраїчних решіток та мультіваріативних перетворень. Синтез, аналіз та порівняння перспективних асиметричних криптоперетворень АСШ та ПКК на основі алгебраїчних решіток. Особливості синтезу, аналізу, оцінки та порівняння асиметричних криптоперетворень АСШ та ПКК на основі математичних кодів та ізогеній еліптичних кривих. Приклади застосування методик для аналізу, оцінки та порівняння асиметричних криптопримітивів типу ЕП, АСШ та ПКК.

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

Класифікація та характеристика асиметричних криптопримітивів ЕП, АСШ та ПКК на основі симетричних криптоперетворень. Основні методи синтезу асиметричних криптопримітивів ЕП, АСШ та ПКК 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 асиметричних криптоперетворень ЕП на основі симетричних криптоперетворень. Синтез, аналіз, оцінка та порівняння перспективних асиметричних криптоперетворень ЕП на основі одноразових ключів. Приклади застосування методик для аналізу, оцінки та порівняння асиметричних криптопримітивів типу ЕП, АСШ та ПКК 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 криптопримітивів типу ЕП, АСШ та ПКК. Методи та системи доведення безпеки асиметричних криптопримітивів типу ЕП, АСШ та ПКК. Методи криптоаналізу на класичних та квантових атаках. Моделі безпеки ЕП, АСШ та ПКК та умови і можливості їх реалізації.

Методики оцінки та порівняння існуючих та перспективних ЕП, АСШ та ПКК та приклади їх оцінки та порівняння по сукупності безумовних, умовних та прагматичних критеріїв. Приклади оцінки та порівняння складності криптоаналізу симетричних та асиметричних криптопримітивів з використанням квантових методів Гровера, Шора тощо. Стан, умови та можливості здійснення квантового криптоаналізу. Оцінка та порівняння стійкості існуючих та перспективних 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	
<i>Розділ 1. Науково – методичні основи аналізу та порівняння криптопримітивів</i>													
Разом за розділом 1	34	2	2			30							
<i>Розділ 2. Стан, основні положення теорії та практики синтезу та аналізу асиметричних криптопримітивів</i>													
Разом за розділом 2	58	6	6			46							
<i>Розділ 3. Стан, основні положення теорії та практики синтезу та аналізу асиметричних криптопримітивів на основі симетричних криптоперетворень</i>													
Разом за розділом 3	46	4	2			40							
<i>Розділ 4. Основні математичні методи криптографічного аналізу стійкості методів КЗІ</i>													
	42	4	4			34							
Усього годин	180	16	14			150							

4. Теми семінарських (практичних, лабораторних) занять

<i>№з/н</i>	<i>Назва теми</i>	<i>Кількість годин</i>
1	Критерії та показники оцінки безпечності та техніко – економічних і техніко – експлуатаційних характеристик криптопримітивів. Безумовні, умовні, та прагматичні критерії і методики оцінки та порівняння криптопримітивів. Приклади застосування методик для аналізу та порівняння стандартизованих асиметричних криптопримітивів.	2
2	Синтез, аналіз, оцінка та порівняння перспективних асиметричних криптоперетворень ЕП на основі алгебраїчних решіток та мультівариативних перетворень. Приклади застосування методик для аналізу, оцінки та порівняння асиметричних криптопримітивів типу ЕП.	2
3	. Синтез, аналіз та порівняння перспективних асиметричних криптоперетворень АСШ та ППК на основі алгебраїчних решіток. Особливості синтезу, аналізу, оцінки та порівняння асиметричних криптоперетворень АСШ та ППК на основі математичних кодів та ізогеній еліптичних кривих.	2
4	Приклади застосування методик для аналізу, оцінки та порівняння асиметричних криптопримітивів типу АСШ та ППК. Розробка рекомендацій щодо умов застосування АСШ та ППК.	2
5	Синтез, аналіз та оцінка перспективних симетричних криптоперетворень гешування, блокового та потокового шифрування. Синтез, аналіз, оцінка та порівняння перспективних асиметричних криптоперетворень ЕП на основі симетричних криптоперетворень.	2
6	Приклади оцінки та порівняння складності криптоаналізу симетричних 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

<i>№з/п</i>	Види, зміст самостійної роботи	<i>Кількість годин</i>
1	Пошук та вивчення джерел інформації щодо вимог до класичних та постквантових криптопримітивів ЕП, АСШ, ППК. Порядок розробки моделей порушника, загроз та безпеки. Критерії та показники оцінки безпечності та техніко – економічних і техніко – експлуатаційних характеристик криптопримітивів. Безумовні, умовні, та прагматичні критерії і методики оцінки та порівняння криптопримітивів. Переклад та оформлення основних даних перекладу, їх представлення на семінарі.	30
2	Класифікація, аналіз, оцінка та порівняння перспективних асиметричних криптоперетворень ЕП на основі алгебраїчних решіток.. Підготовка пропозицій, розробка програмного забезпечення та аналіз, оцінка та порівняння асиметричних криптопримітивів типу ЕП. Виконання індивідуального завдання.	16
3	Класифікація, аналіз, оцінка та порівняння перспективних асиметричних криптоперетворень АСШ та ППК на основі алгебраїчних решіток.. Підготовка пропозицій, розробка програмного забезпечення та аналіз, оцінка та порівняння асиметричних криптопримітивів типу АСШ та ППК. Виконання індивідуального завдання.	14
4	Виконання індивідуального завдання щодо застосування методик для аналізу, оцінки та порівняння асиметричних криптопримітивів типу ЕП, АСШ та ППК. Розробка рекомендацій щодо умов застосування АСШ та ППК.	16
5	Обґрунтування та розробка вимог до постквантових стандартів симетричних криптоперетворень. Аналіз та оцінка перспективних симетричних криптоперетворень гешування, блокового та потокового шифрування. Виконання індивідуального завдання щодо оцінки стійкості БСШ.	20
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 доповіді на НТК згідно індивідуального завдання чи підготовка та подача статті для рецензування.	34
Разом:		150

6. Індивідуальні завдання

/Не передбачено/

7. Методи контролю

Контроль засвоєння аспірантами навчального матеріалу на лекційному занятті 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}
<i>Практичні(семінарські) заняття</i>	
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
<i>Всього за семестр</i>	
	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 розділах 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 діяльності 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 семінарі) виконане самостійно в повному обсязі. Звіт оформлений акуратно відповідно до вимог методичних вказівок. При захисті звіту показано розуміння суті і змісту проведених досліджень	N_{max}
Індивідуальне завдання з практичного заняття (виступ на семінарі) виконане самостійно в повному обсязі. Звіт оформлений достатньо акуратно відповідно до вимог методичних вказівок. При захисті звіту були виявлені незначні помилки у знанні теоретичного матеріалу.	$[N_{max} - \lfloor \frac{N_{max}}{7} \rfloor, N_{max} - 1]$
Індивідуальне завдання з практичного заняття (виступ на семінарі) 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.	$[N_{max} - 2 \times \lfloor \frac{N_{max}}{7} \rfloor, N_{max} - \lfloor \frac{N_{max}}{7} \rfloor]$
Індивідуальне завдання з практичного заняття виконане. Звіт оформлений з помилками і недоліками. При захисті звіту були виявлені суттєві помилки у знанні теоретичного матеріалу.	$max - 3 \times \lfloor \frac{N_{max}}{7} \rfloor, N_{max} - 4 \times \lfloor \frac{N_{max}}{7} \rfloor]$
Показано недосконале знання навчального матеріалу, допущені суттєві помилки, які носять принциповий характер. Звіт оформлений з помилками і суттєвими недоліками.	$[1, N_{max} - 4 \times \lfloor \frac{N_{max}}{7} \rfloor]$
Доповідь на НТК прийнято та успішно зроблено	N_{max}
Доповідь на НТК прийнято	$N_{max} - 4$
Стаття опублікована	N_{max}
На статтю отримано позитивну рецензію	$N_{max} - 5$

* N_{max} – максимальна кількість балів для відповідного заняття відповідно до таблиці 7.1.

9. Рекомендована література

9.1 Основна література

1. Горбенко Ю. І. Методи побудування та аналізу криптографічних систем: монографія. / Ю. І. Горбенко. Х. Під заг. Ред.. Горбенко І.Д.: Форт, 2015. – 959 с.
2. 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>
3. 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>
4. 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 крип-

тографія та механізми її реалізації / І. Д. Горбенко, О. О. Кузнецов, О. В. Потій, Ю. І. Горбенко, Р. С. Ганзя, В. А. Пономар // Радіотехніка. – 2014. – Вип. 184. – С. 32-52.

5. 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 5TH – 7TH LEVELS OF STABILITY. PRODUCT FORM. Telecommunications and Radio Engineering, vol. 78. <https://doi.org/10.1615/TelecomRadEng.v78.i7.30>

6. Аналіз сутності та моделі протоколу інкапсуляції ключів у кільці поліномів над скінченим полем />Горбенко< І. Д., Качко О. Г., >Пономар< В. А., М. В., Акользіна О. С., >Кулібаба В. А.< // Прикладна радіоелектроніка, 2018, Том 17, № 3, 4.

7. Порівняння кандидатів електронного підпису на постквантовий стандарт NIST PQC на базі MQ-перетворень та функцій гешування />Горбенко Ю. І., Кудряшов І. С., Науменко Д. С., < Онопрієнко В. В. // Прикладна радіоелектроніка, 2018, Том 17, № 3, 4.

8. Модель безпеки постквантових протоколів інкапсуляції ключів />Єсіна< М. В. // Прикладна радіоелектроніка, 2018, Том 17, № 3, 4.

9. Математична структура потокового шифру Струмок / О.О. >Кузнецов<, І.Д. >Горбенко<, Ю.І.>Горбенко<, А.М. Олексійчук, В.А. >Тимченко< // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2018. Вип. 193. С. 17 – 27.

10. 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.

11. 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>.

12. Lily Chen Report on Post-Quantum 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.

13. 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>.

14. 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.

15. 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. Yesina // Telecommunications and Radio Engineering, 2019. – Volume 78, Issue 7 – P. 579-594. DOI: 10.1615/TelecomRadEng.v78.i7.30.

16. 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.

17. Gorbenko I. D. General statements and analysis of the end-to-end encryption algorithm NRTU Prime IT Ukraine / I. D. Gorbenko, O. G. Kachko, M. V. Yesina // Радиотехника. – Х. : Харьковський національний університет радіоелектроніки, 2018. – Випуск 193 – С. 5–16.

18. 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 // Радиотехника. – Х. : Харьковський національний університет радіоелектроніки, 2018. – Випуск 195 – С. 5–16.

19. 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 // Радиотехника. – Х. : Харьковський національний університет радіоелектроніки, 2018. – Випуск 195 – С. 17–26.

20. 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. : Харківський національний університет радіоелектроніки, 2020. – Вип. 202. С. 5-28.

21. 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. Остряньська // Радіотехніка. – Х. : Харківський національний університет радіоелектроніки, 2020. – Вип. 202. С. 57–63.

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

23. Falcon. [Електронний ресурс]. – Режим доступу: <https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions>.

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

9.2 Допоміжна література

1. 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).

2. 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).

3. ISCI'2019: Information Security in Critical Infrastructures. Collective monograph. Edited 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>

4. A. Kuznetsov, Y. Gorbenko, I. Kolovanova, S. Smirnov, I. Perevozova, and T. Kuznetsova, “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%2F978-3-030-43070-2_27

5. Мчедлов-Петросян Н. О. Этический аспект научных публикаций в условиях информационного взрыва // Вісник НАН України, 2014, № 8. – С. 77-87.
6. Михельсон Т. Н., Успенская Н. В. Как писать по-английски научные статьи, рефераты и рецензии. – Санкт-Петербург : «Специальная литература», 1995. – 101 с.
7. 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.
8. Сутність та особливості реалізації методу Гровера на класичному комп'ютері для симетричного криптоаналізу / Ю.І. >Горбенко<, Є.Ю. Каптьол // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2018. – Вип. 195. – С. 89 – 100.
9. Математична модель сигналів з ортогональним частотним розподілом і мультиплексуванням(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
10. Можливості застосування механізмів повністю гомоморфного шифрування в системах електронного голосування / І.Д. >Горбенко<, О.Г. Качко, Ю.І. >Горбенко<, М.В. >Єсіна<, С.О. Кандій, Є.В. Острианська, А.С. >Д'яченко< // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 200. С. 98 – 113

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

1. 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.
2. Vadim Lyubashevsky CRYSTALS-Dilithium / Vadim Lyubashevsky, Léo Ducas, Eike Kiltz, Tancrede Lepoint, Peter Schwabe, Gregor Seiler, Damien Stehlé // Submission to the NIST Post-Quantum Cryptography Standardization, 2017. – Режим доступу: <https://pq-crystals.org/dilithium>.
3. Falcon. [Електронний ресурс]. – Режим доступу: <https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions>.
4. Thomas Pornin New Efficient, Constant-Time Implementations of Falcon
5. ДСТУ 7564:2014 Інформаційні технології. Криптографічний захист інформації. Функція гешування. – Режим доступу: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66229.
6. ДСТУ 7624:2014 Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. – Режим доступу: <https://www.twirpx.com/file/2878521/>.
7. 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.
8. 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.
9. Горбенко Ю. І. Моделі загроз щодо асиметричних криптоперетворень перспективного електронного підпису / Ю.І. Горбенко, М.В. Єсіна, В.В. Онопрієнко, Г.А. Малєєва // Радіотехніка. – Х. : Харківський національний університет радіоелектроніки, 2020. – Вип. 202. С.

10. 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. : Харківський національний університет радіоелектроніки, 2020. – Вип. 202. С. 28-36.

11. Yesina Maryna, Gorbenko Yuriy (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.

12. J. Ding Rainbow / J. Ding, M. Chen, A. Petzoldt et al.//, 2019. [Електронний ресурс]. – Режим доступу: <https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-2/submissions/Rainbow-Round2.zip>.

13. 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/>.