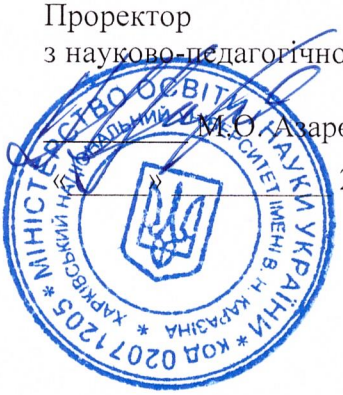
Міністерство освіти і науки України

Харківський національний університет імені В.Н. Каразіна

Кафедра безпеки інформаційних систем і технологій

“ЗАТВЕРДЖУЮ”

Проректор
з науково-педагогічної роботи



_____ М.О. Азарєнков

«____» _____ 2020 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Математичні методи в кібербезпеці

рівень вищої освіти	третій (освітньо-науковий) рівень
галузь знань	12 Інформаційні технології
спеціальність	125 Кібербезпека
освітня програма	освітньо-наукова програми підготовки докторов філософії
вид дисципліни	обов’язкова
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 в кібербезпеці» складена відповідно до освітньо-наукової програми підготовки фахівця третього (докторів філософії) рівня вищої освіти за спеціальністю 125 – «Кібербезпека» (ОК 5).

1. Опис навчальної дисципліни

1.1. Мета викладання навчальної дисципліни

Метою викладання навчальної дисципліни є навчання аспірантів існуючим та перспективним постквантовим математичним методам та стандартизованим алгоритмам криптографічного захисту інформації в кібербезпеці, результатом якого повинна бути підготовленість аспірантів до проведенні наукових досліджень зі створення, оцінки та порівняння механізмів КЗІ для забезпечення кібербезпеки.

Аспіранти мають можливість використовувати отримані компетенції, знання і вміння при проведенні наукових досліджень в криптології, для оцінки та порівняння механізмів КЗІ в кібербезпеці, розробляти та застосовувати математичні та програмні моделі існуючих та перспективних механізмів КЗІ, а також практично при підготовці наукових публікацій та звітів за результатами досліджень, які передують розробці кваліфікаційної роботи доктора філософії.

1.2. Основні завдання вивчення дисципліни

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

1.3. Кількість кредитів – 6.

1.4. Загальна кількість годин – 180.

1.5. Характеристика навчальної дисципліни	
Нормативна / за вибором	
Денна форма навчання	Заочна (дистанційна) форма навчання
Рік підготовки	
2-й	2-й
Семестр	
3-й	3-й
Лекції	
16 год	
Практичні, семінарські заняття	
14 год	
Лабораторні заняття	
Самостійна робота	
150 год	
Індивідуальні завдання	

1.6. Заплановані результати навчання

МАТИ КОМПЕТЕНЦІЇ:

Загальні

– **ЗК 4.** Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

Фахові компетентності

– **ФК 1**. Здатність використати сучасні досягнення науки і передових технологій;

– **ФК 2**. Здатність користуватися нормативною та законодавчою базою в сфері інтелектуальної власності;

– **ФК 6.** Професійне володіння комп'ютером та інформаційними технологіями.

За результатами вивчення дисципліни аспіранти повинні

ЗНАТИ:

- криптографічні механізми та послуги в кібербезпеці;
- науково – технічні основи оцінки та аналізу математичних методів КЗІ;
- сутність та аналіз математичних методів КЗІ в кібербезпеці;
- основні математичні методи та системи аналізу криптографічної стійкості механізмів КЗІ;
- вимоги до системи національної стандартизації у галузі КЗІ;
- принципи 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 методів КЗІ;
- обґрунтовувати вибір та застосовувати методики аналізу існуючих 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 кібербезпеки;
- демонструвати уміння представляти результати досліджень на державній та одній з іноземних мов.

2. Тематичний план навчальної дисципліни

Розділ 1. Криптографічні методи та послуги в кібербезпеці

Класифікація та вимоги до математичних методів криптографічного захисту інформації (КЗІ). Комплексні системи КЗІ та їх моделі. Моделі безпеки на основі КЗІ. Класичні та постквантові механізми КЗІ. Сутність та властивості асиметричних та симетричних механізмів КЗІ. Аналіз стану стандартизації та застосування національних та міжнародних асиметричних та симетричних алгоритмів КЗІ

Розділ 2. Наукові основи оцінки та аналізу математичних механізмів КЗІ.

Критерії та показники оцінки безпечності механізмів КЗІ. Математичні основи оцінки та порівняння механізмів КЗІ. Безумовні та умовні критерії та методики оцінки механізмів КЗІ. Прагматичні критерії та методики їх застосування. Приклади застосування методик для аналізу існуючих стандартизованих алгоритмів КЗІ в кібербезпеці.

Розділ 3. Сутність та аналіз математичних методів КЗІ в кібербезпеці.

Класифікація, вимоги та властивості класичних методів КЗІ. Класифікація, вимоги та властивості постквантових механізмів КЗІ. Порівняльний аналіз існуючих та перспективних механі-

змів КЗІ. Приклади оцінки та аналізу існуючих та перспективних стандартизованих алгоритмів КЗІ в кібербезпеці.

Розділ 4. Основні математичні методи криптографічного аналізу стійкості методів КЗІ.

Класифікація, призначення та можливості механізмів та методів КЗІ. Методи криптоаналізу існуючих стандартизованих алгоритмів КЗІ. Класифікація, вимоги та моделі безпеки щодо механізмів КЗІ для постквантового періоду. Математичні основи методик оцінки та порівняння перспективних проектів та стандартів КЗІ для постквантового періоду. Приклади порівняння проектів та стандартів КЗІ для постквантового періоду

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. Криптографічні методи та послуги в кібербезпеці												
Разом за розділом 1	36	4	2			30						
Розділ 2. Наукові основи оцінки та аналізу математичних механізмів КЗІ.												
Разом за розділом 2	46	4	4			38						
Розділ 3. Сутність та аналіз математичних методів КЗІ в кібербезпеці.												
Разом за розділом 3	48	4	4			40						
Розділ 4. Основні математичні методи криптографічного аналізу стійкості методів КЗІ												
	50	4	4			42						
Усього годин	**180**	**16**	**14**			**150**						

4. Теми семінарських (практичних, лабораторних) занять

№з/п	***Назва теми***	***Кількість годин***
1	Сутність та властивості асиметричних та симетричних механізмів КЗІ. Аналіз стану стандартизації та застосування національних та міжнародних асиметричних та симетричних алгоритмів КЗІ	2
2	Безумовні та умовні критерії та методики оцінки механізмів КЗІ. Прагматичні критерії та методики їх застосування.	2
3	Приклади застосування методик для аналізу існуючих стандартизованих алгоритмів КЗІ в кібербезпеці	2
4	Порівняльний аналіз існуючих та перспективних механізмів КЗІ.	2
5	Приклади оцінки та аналізу існуючих та перспективних стандартизованих алгоритмів КЗІ в кібербезпеці	2
6	Математичні основи методик оцінки та порівняння перспективних проектів та стандартів КЗІ для постквантового періоду.	2
7	Приклади порівняння проектів та стандартів КЗІ для постквантового періоду	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 постквантових математичних методів криптографічного захисту інв. кібербезпеці. Сутність та властивості асиметричних та симетричних механізмів КЗІ. Переклад та оформлення основних даних перекладу, їх представлення на семінарі.	30
2	Критерії та показники оцінки безпечності механізмів КЗІ. Математичні основи оцінки та порівняння механізмів КЗІ. Безумовні та умовні критерії та методики оцінки механізмів КЗІ. Виконання індивідуального завдання.	18
3	. Прагматичні критерії та методики їх застосування. Приклади застосування методик для аналізу існуючих стандартизованих алгоритмів КЗІ в кібербезпеці. Підготовка доповіді на семінарі з презентацією.	20
4	Класифікація, вимоги та оцінка властивостей класичних методів КЗІ. Класифікація, вимоги, оцінка та порівняння властивості класичних та постквантових механізмів КЗІ. Підготовка доповіді на семінарі згідно індивідуального завдання..	20
5	Порівняльний аналіз існуючих та перспективних механізмів КЗІ. Приклади оцінки та аналізу існуючих та перспективних стандартизованих алгоритмів КЗІ в кібербезпеці. Підготовка доповіді на НТК згідно індивідуального завдання..	20
6	Методи криптоаналізу існуючих стандартизованих алгоритмів КЗІ. Класифікація, вимоги та моделі безпеки щодо механізмів КЗІ для постквантового періоду. Підготовка доповіді на НТК згідно індивідуального завдання..	20
7	Математичні основи методик оцінки та порівняння перспективних проектів та стандартів КЗІ для постквантового періоду. Приклади порівняння проектів та стандартів КЗІ для постквантового періоду. Підготовка доповіді на НТК чи науково – практичної статі.	42
	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 оформлення звіту і його захисту. 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	6
ПЗ 2	7
ПЗ 3	10
ПЗ 4	13
ПЗ 5	10
ПЗ 6	10
ПЗ 7	14
Піідготовка та прийняття доповіді на НТК	10
Підготовка та отримання позитивної рецензії на статю	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	25	25	30		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.	$[N_{max} - \left\lfloor \frac{N_{max}}{7} \right\rfloor, N_{max} - 1]$

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.	$[N_{max} - 2 \times \left\lfloor \frac{N_{max}}{7} \right\rfloor, N_{max} - \left\lfloor \frac{N_{max}}{7} \right\rfloor]$
Індивідуальне завдання з практичного заняття виконане. Звіт оформлений з помилками і недоліками. При захисті звіту були виявлені суттєві помилки у знанні теоретичного матеріалу.	$max - 3 \times \left\lfloor \frac{N_{max}}{7} \right\rfloor, N_{max} - 4 \times \left\lfloor \frac{N_{max}}{7} \right\rfloor]$
Показано недосконале знання навчального матеріалу, допущені суттєві помилки, які носять принциповий характер. Звіт оформлений з помилками і суттєвими недоліками.	$[1, N_{max} - 4 \times \left\lfloor \frac{N_{max}}{7} \right\rfloor]$
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/ 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.

3. 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.

4. 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.

5. 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.

6. 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.

7. 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.

8. 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.

9. 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 // Радиотехника. – Х. : Харьковский национальный университет радиоэлектроники, 2018. – Выпуск 193 – С. 5–16.

10. 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. : Харьковский национальный университет радиоэлектроники, 2018. – Выпуск 195 – С. 5–16.

11. 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. : Харьковский национальный университет радиоэлектроники, 2018. – Выпуск 195 – С. 17–26.

12. 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. : Харківский національний університет радіоелектроніки, 2020. – Вип. 202. С. 5-28.

13. 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. : Харківский національний університет радіоелектроніки, 2020. – Вип. 202. С. 57–63.

14. 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.

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

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. Положення про систему запобігання та виявлення академічного плагіату у наукових та навчальних працях працівників і здобувачів вищої освіти Харківського національного університету імені В. Н. Каразіна. URL: http://www.univer.kharkov.ua/docs/antiplagiat_nakaz_polozhennya.pdf.

4. Академічна чесність як основа сталого розвитку університету / Міжнарод. благод. Фонд “Міжнарод. фонд. дослідж. освіт. політики”; за заг. ред. Т. В. Фінікова, А. Є. Артюхова – К.; Таксон, 2016. – 234 с.

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.

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, Tancrède 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

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. : Харківский національний університет радіоелектроніки, 2020. – Вип. 202. С. 72–78.

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

11.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.

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/.