Харківський національний університет імені В.Н. Каразіна
Факультет комп'ютерних наук
Кафедра безпеки інформаційних систем і технологій

Ухвалено
Вченою радою
факультету комп'ютерних наук
Протокол № 12 від 3 квітня 2020
Голова Вченої ради _____

Назва курсу	Математичні методи синтезу та аналізу криптографічних примітивів
Викладач (-і)	професор кафедри БІСТ Горбенко І.Д.
Профайл викладача (-ів)	http://www-csd.univer.kharkov.ua/about-us/sub-faculty/kafedra-bezpeki-informatsijnih-sistem-i/personalnij-sklad/
Контактний тел.	Кафедра: (057) 705-10-83
E-mail:	i.d.gorbenko@karazin.ua
Сторінка курсу в системі дистанційного навчання	
Консультації	*Очні консультації*: розклад в університеті (на кафедрі). *Он лайн консультації*: через e-mail.

1. Коротка анотація до курсу

Курс спрямований на ознайомлення аспірантів з основами математичних методів синтезу та аналізу криптографічних примітивів», а саме: як обґрунтовувати, вибирати та застосовувати при криптографічному захисті інформації(КЗІ) математичні методи синтезу та аналізу криптографічних примітивів від класичних, квантових та атак сторонніми каналами, результатом якого повинна бути підготовленість проводити інформаційний пошук з обраної теми, організовувати, планувати та проводити наукові дослідження, в тому числі засобом програмного моделювання, аналізувати і оформлювати їх результати, доповідати та опубліковувати результати, що отримані в процесі проведених наукових досліджень.

2. Мета та цілі курсу

Метою викладання навчальної дисципліни є навчання аспірантів існуючим та перспективним математичним методам синтезу та аналізу криптографічних примітивів з подальшою можливістю їх стандартизації чи перевіркою існуючих стандартів на відповідність вимогам та можливості подальшого застосування для захисту інформації в інформаційних та кібернетичних системах, навчання аспірантів сучасним методам синтезу та аналізу асиметричних та симетричних криптоперетворень та протоколів, включаючи протоколи інкапсуляції ключів(ПІК), основним положенням підготовки та здійснення наукових публікацій , в тому числі на іноземній мові.

Основні цілі курсу – формування у аспірантів певних знань та вмінь з:

- вибору теми дослідження щодо методів синтезу та аналізу криптопримітивів, в тому числі у постквантовий період ;
- формулювання назви роботи та вимог щодо методів синтезу та аналізу криптопримітивів для
- кіберзахисту, в тому числі для застосування у постквантовий період;
- визначення об'єкта і предмета дослідження щодо методів синтезу та аналізу криптопримітивів КЗІ при кіберзахисті ;
- визначення мети і задач досліджень щодо методів синтезу та аналізу криптопримітивів;
- обгрунтуванню вимог до рівнів кіберзахисту при застосуванні асиметричних та симетричних криптопримітивів та криптопротоколів, в тому числі у постквантовий період;
- роботи з джерелами інформації щодо алгоритмів та засобів КЗІ ;
- синтезу та аналізу криптоперетворень та криптопротоколів асиметричного, симетричного та змішаного типу, в тому числі у постквантовий період;
- формулювання висновків, пропозицій та рекомендацій, а також консультування за спеціальністю;
- обробки і представлення результатів дослідження, в отому числі електронним чином;
- етичного кодексу автора наукових публікацій, у тому числі сформувати неприйняття академічного шахрайства, включаючи плагіат

3. Формат курсу – очний.

4. Результати навчання

За результатами вивчення дисципліни аспіранти повинні

ЗНАТИ:

– криптографічні перетворення (криптографічні алгоритми, криптографічні протоколи та засоби КЗІ) для надання користувачам послуг з безпеки інформації та кібербезпеки, в тому числі при застосуванні в постквантовий період;

– науково – технічні основи методів синтезу та аналізу криптографічних примітивів, їх оцінки, аналізу та порівняння;

– сутність та можливості застосування методів синтезу та аналізу асиметричних та симетричних криптографічних примітивів КЗІ в кібербезпеці;

– основні методи синтезу, аналізу та порівняння криптографічних примітивів по безумовних, умовних та прагматичних критеріях;

– вимоги до системи національної та міжнародної стандартизації у галузі КЗІ, в тому числі у постквантовий перід;

– принципи та сутність визначення об’єкта і предмета, мети і задач дослідження, вибору методів дослідження;

– етичні принципи, яких мають додержуватися автори наукових публікацій;

ВМІТИ:

– обґрунтовувати та вибирати критерії та показники оцінки криптографічних примітивів при їх синтезі та аналізі, в тому числі для застосування у постквантовий період;

– обґрунтовувати вибір та застосовувати методики синтезу, аналізу та порівняння існуючих та перспективних криптопримітивів КЗІ в кібербезпеці, в тому числі для застосування у постквантовий період;

– 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, в тому числі кібербезпеці;

– проводити наукові та практичні дослідження існуючих та перспективних алгоритмів та протоколів КЗІ з використанням систем умовних, безумовних та прагматичних критеріях;

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

5. Обсяг курсу

Вид заняття	Загальна кількість годин
Лекції	16
Семінарські заняття / практичні / лабораторні	14
Самостійна робота	150
Разом:	180

6. Ознаки курсу:

Рік викладання	Семестр	Спеціальність	Курс (рік навчання)	Нормативний / вибірковий
2020	4	125 Кібербезпека	2	Вибірковий

7. Пререквізити

Попередньо прослухані курси: Математичні методи в кібербезпеці та Методологія і організація наукових досліджень (підготовка магістрів за спеціальністю 125 (або іншою з галузі знань 12 – інформаційні технології)).

8. Технічне та програмне забезпечення /обладнання

Для виконання практичних робіт студентам при синтезі та аналізі криптопримітивів знадобиться програмне забезпечення: сучасні мови програмування, програмні моделі та бібліотеки КЗІ, програмні пакети реалізації постквантової та існуючої криптографії, програмні моделі застосування методик оцінки та порівняння систем КЗ в тому числі основи системи комп’ютерної алгебри «Магма».

9. Політики курсу

Політика академічної доброчесності.

10. Схема курсу

Тиж. / акад. год.	**Тема, план, короткі тези**	**Форма діяльності (заняття)* / Формат****	**Матеріали**	**Завдання, год**
Тиж. 1 / 2 год.	Розділ 1. Л.1. Вступ. 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	Лекція / (*аудиторна*)	Презентація лекції, та електронна лекція. Засоби КЗІ.	Ознайомитись з літературою, переглянути презентацію, доопрацювати лекцію згідно завдання, 4 год
Тиж. 2 / 2 год	Розділ 1. СЗ 1.Сутність та властивості асиметричних та симетричних криптоперетворень. Класичні та постквантові асиметричні та симетричні криптопримітиви. Критерії та показники оцінки безпечності та техніко – економічних і техніко – експлуатаційних характеристик криптопримітивів	Семінарське заняття / *аудиторне*	Перелік джерел до СЗ, Індивідуальне завдання до СЗ . Копії алгоритмів національних та міжнародних стандартів електронного підпису	Виконати завдання до СЗ (виступ та захист доповіді на семінарі), 26 год
Тиж. 3 / 2 год	Розділ 2. Л.2 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(ПІК) та їх оцінка.	Лекція / *аудиторна*	Презентація лекції та електронна лекція. Копії та презентація національних стандартів. Індивідуальні завдання до самостійної роботи	Ознайомитись з літературою, переглянути презентацію, доорацювати лекцію згідно завдання, 6 год
Тиж. 4 / 2 год	Розділ 2. Л.3. Синтез, аналіз, оцінка та порівняння перспективних асиметричних криптоперетворень ЕП на основі алгебраїчних решіток та мультиваріативних перетворень	Лекція / *аудиторна*	Презентація лекції, та електронна лекція. Індивідуальні завдання до самостійної роботи	Ознайомитись з літературою, переглянути презентацію, доопрацювати лекцію згідно завдання, 4 год
Тиж. 5 / 2 год	Розділ 2. Л.4. Синтез, аналіз та порівняння перспективних асиметричних	Лекція / *аудиторна*	Презентація лекції та електронна	Ознайомитись з літературою, доопрацювати

	криптоперетворень АСШ та ПІК на основі алгебраїчних решіток. Приклади застосування методик для аналізу, оцінки та порівняння асиметричних криптопримітивів типу АСШ та ПІК..		лекція. Індивідуальні завдання. Методика аналізу КЗІ.	лекцію згідно завдання, ознайомитись з застосуванням методики 6 год
Тиж. 6 / 2 год	Розділ 2. ПЗ.2 . Синтез, аналіз, оцінка та порівняння перспективних асиметричних криптоперетворень ЕП на основі алгебраїчних решіток та мультиваріативних перетворень.	Практичне заняття / *аудиторне*	Перелік джерел до ПЗ, Індивідуальне завдання та. виступ на семінарі.	Виконати завдання та його захист на ПЗ, 10 год
Тиж. 7 / 2 год	Розділ 2. ПЗ.3 Синтез, аналіз та порівняння перспективних асиметричних криптоперетворень АСШ та ПІК на основі алгебраїчних решіток. Особливості синтезу криптоперетворень АСШ та ПІК на основі кодів та ізогеній	Практичне заняття / *аудиторне*	Перелік джерел до ПЗ, Індивідуальне завдання до ПЗ.	Виконати завдання до ПЗ та його захист, 10 год
Тиж. 8 / 2 год	Розділ 2. СЗ.4 Приклади застосування методик для аналізу, оцінки та порівняння асиметричних криптопримітивів типу ЕП, АСШ та ПІК.	Семінарське заняття / *аудиторне*	Перелік джерел до СЗ, Індивідуальне завдання до СЗ. Методика аналізу	Виконати завдання до СЗ (виступ та захист доповіді на семінарі), 10 год
Тиж. 9 / 2 год	Розділ 3. Л.5. Класифікація та характеристика асиметричних криптопримітивів ЕП, АСШ та ПІК на основі симетричних крипто перетворень. Основні методи синтезу асиметричних криптопримітивів ЕП, АСШ та ПІК на основі симетричних криптоперетворень та їх попередня оцінка та умови реалізації..	Лекція / *аудиторна*	Презентація лекції та електронна лекція. Індивідуальні завдання до самостійної роботи..	Ознайомитись з літературою, доопрацювати лекцію та виконати індивідуальне завдання, 6год
Тиж.10 / 2 год	Розділ 3. Л.6. . 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 та одноразових ключів	Лекція / *аудиторна*	Презентація лекції та електронна лекція. Копії та презентація національних стандартів. Індивідуальні завдання до самостійної роботи	Ознайомитись з літературою, переглянути презентацію, доопрацювати лекцію та виконати індивідуальне завдання, 6 год

Тиж.11 / 2 год	Розділ 3. ПЗ 5.. Приклади застосування методик для аналізу, оцінки та порівняння асиметричних криптопримітивів типу ЕП, АСШ та ПІК на основі симетричних криптопримітивів.	Практичне заняття / *аудиторне*	Перелік джерел до ПЗ, Індивідуальне завдання та теми виступів на семінарі.	Виконати завдання до ПЗ та його захист, 28 год
Тиж. 12 / 2 год	Розділ 4. Л 7 Класифікація та можливості і умови успішного криптоаналізу асиметричних криптопримітивів типу ЕП, АСШ та ПІК. Методи та системи доведення безпеки асиметричних криптопримітивів типу ЕП, АСШ та ПІК. Методи криптоаналізу накласичних та квантових атак. Моделі безпеки ЕП, АСШ та ПІК та умови і можливості їх реалізаці	Лекція / *аудиторна*	Презентація лекції та електронна лекція. Індивідуальні завдання до самостійної роботи	Ознайомитись з літературою, доопрацювати лекцію згідно завдання, 4 год
Тиж. 13 / 2 год	Розділ 4. Л. 8. Методики оцінки та порівняння існуючих та перспективних ЕП, АСШ та ПІК 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	Лекція / *аудиторна*	Презентація лекції та електронна лекція. Індивідуальні завдання. Перелік джерел до ПЗ.	Ознайомитись з літературою, доопрацювати лекцію згідно завдання, 6 год
Тиж. 14 / 2 год	Розділ 4. СЗ.6. Методи криптоаналізу на класичних та квантових атак. Моделі безпеки ЕП, АСШ та ПІК та умови і можливості їх реалізації..	Семінарське заняття / *аудиторне*	Подання та захист проекта доповіді на семінарі	Підготувати доповідь та презентацію доповіді для виступу на НТК та її захист на семінарі, 16 год.
Тиж. 15. 2 год	Розділ 4. СЗ.7. 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.	Семінарське заняття / *аудиторне*	Подання та захист проекта статі на семінарі	Підготувати проект статі та її захист на семінарі, 16 год.

11. Система оцінювання та вимоги

Загальна система оцінювання курсу	Участь в роботі впродовж семестру – 100 балів. Розподіл балів, що присвоюються аспірантам з навчальної дисципліни «Математичні методи синтезу та аналізу криптографічних примітивів » є сумою балів за виконання всіх практичних завдань та підготовки звітних матеріалів.
Практичні заняття	Аспірант отримує максимальну кількість балів за індивідуальне завдання, якщо: завдання виконане повністю та без допомоги викладача; аспірант самостійно може узагальнити, систематизувати матеріал та вільно застосовує його у стандартних ситуаціях та у ситуаціях невизначеності.
Умови допуску до підсумкового контролю	Виконання та захист всіх індивідуальних практичних завдань та звітів, а також виступи на семінарах.

Розподіл балів, які отримують аспіранти за результатами контролю поточної успішності

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

Схема нарахування балів

Бали за поточний контроль знань по розділам протягом семестру				Разом сума балів у семестрі	Іспит	Загальна сума балів
Розділ 1	Розділ 2	Розділ 3	Розділ 4			
15	20	10	15	60	40	100

Критерії оцінювання

Критерії оцінювання знань студентів за виконання практичних занять

Визначення	Кількість балів*
Завдання з практичного заняття чи семінару виконане самостійно в повному обсязі. Звіт оформлений акуратно відповідно до вимог методичних вказівок. При захисті звіту показано розуміння суті і змісту проведених досліджень.	25

Завдання з практичного заняття чи семінару 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.	19-24
Завдання з практичного заняття чи семінару 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.	13-18
Завдання з практичного заняття чи семінару виконане. Звіт оформлений з помилками і недоліками. При захисті звіту були виявлені суттєві помилки у знанні теоретичного матеріалу.	7-12
Показано недосконале знання навчального матеріалу, допущені суттєві помилки, які носять принциповий характер. Звіт оформлений з помилками і суттєвими недоліками.	1-6

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

12. Рекомендована література

12.1 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 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.

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.

12.2 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.

13. 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/.