МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ

ЗАТВЕРДЖЕНО
на засіданні кафедри кібербезпеки та інформаційних технологій
Протокол № 18 від 26.08.2025 р.

ПОГОДЖЕНО
Проректор з навчально-методичної роботи
_____ Карина НЕМАШКАЛО

СУЧАСНІ МЕТОДИ ДЕЦЕНТРАЛІЗОВАНОГО РОЗПОДІЛУ ТА КРИПТОГРАФІЧНОГО ЗАХИСТУ ДАНИХ

робоча програма навчальної дисципліни (РПНД)

Галузь знань	**F Інформаційні технології**
Спеціальність	**F5 Кібербезпека та захист інформації**
Освітній рівень	**другий (магістерський)**
Освітня програма	**Кібербезпека**
Статус дисципліни	**обов'язкова**
Мова викладання, навчання та оцінювання	**українська**

Розробник д.т.н., с.н.с. Андрій ЧУГАЙ

Завідувач кафедри кібербезпеки та інформаційних технологій Ольга СТАРКОВА

Гарант програми *підписано КЕП* Ганна СОЛОДОВНИК

Харків
2025

ВСТУП

Дисципліна «Сучасні методи децентралізованого розподілу та криптографічного захисту даних» належить до фундаментальних курсів підготовки фахівців у сфері інформаційної безпеки, розподілених обчислювальних систем та кібербезпеки. Сучасне інформаційне суспільство характеризується активним розвитком цифрових технологій, широким використанням хмарних і розподілених платформ, блокчейн-систем, а також високою динамікою потоків даних у різних сферах діяльності - від фінансів і медицини до державного управління та науки.

Разом із розширенням використання інформаційних систем зростає і кількість інформаційних загроз, спрямованих на порушення конфіденційності, цілісності та доступності даних. Це визначає потребу у високоефективних математично обґрунтованих методах захисту інформації, здатних забезпечити надійність, прозорість та довіру до електронних транзакцій і розподілених процесів.

Дисципліна фокусується на комплексному вивченні сучасних методів децентралізованого розподілу даних, таких як блокчейн, розподілені реєстри та протоколи консенсусу, а також на криптографічних механізмах захисту інформації, включно з симетричними та асиметричними алгоритмами, цифровими підписами, хеш-функціями, протоколами автентифікації та доказами з нульовим розголошенням (ZKP).

Вивчення дисципліни забезпечує здобувачам:

- розуміння математичних основ сучасних криптографічних та розподілених алгоритмів;
- практичні навички побудови і моделювання протоколів захисту даних у децентралізованих системах;
- здатність оцінювати стійкість алгоритмів до атак та обчислювальну складність задач;
- розвиток аналітичного і критичного мислення у контексті побудови безпечних інформаційних систем.

Актуальність дисципліни обумовлена:

1. Зростанням обсягів і складності обробки даних у розподілених і хмарних середовищах.
2. Поширенням блокчейн-технологій і потребою у надійних методах забезпечення цілісності та аутентифікації даних.
3. Потребою у підготовці фахівців, здатних застосовувати сучасні математичні та криптографічні методи для забезпечення безпеки інформаційних систем.

Мета дисципліни: формування у здобувачів системи знань і практичних навичок щодо побудови, аналізу та оцінки ефективності криптографічних і децентралізованих рішень для захисту інформації.

Завдання дисципліни:

- засвоєння базових понять та принципів криптографії, криптоаналізу та децентралізованих протоколів;
- оволодіння математичними методами, що лежать в основі сучасних алгоритмів шифрування і розподілених систем;

- розвиток вмінь моделювати процеси захисту даних у комп'ютерних та розподілених системах;
- формування здатності оцінювати ризики та обчислювальну складність алгоритмів у сфері інформаційної безпеки.

Предмет вивчення: методи, моделі та алгоритми, що забезпечують криптографічний захист і безпечний децентралізований розподіл даних.

Об'єкт вивчення: сучасні криптографічні та децентралізовані системи захисту інформації, що базуються на математичних теоріях і використовуються у практичних інформаційних технологіях.

Результати навчання та компетентності, які формує навчальна дисципліна визначено в табл. 1.

Таблиця 1

Результати навчання та компетентності, які формує навчальна дисципліна

Результати навчання	**Компетентності, якими повинен оволодіти здобувач вищої освіти**
РН 5	КЗ3, КФ6
РН 6	КФ 3
РН 9	КЗ 1, КЗ 2, КЗ 3
РН 14	КЗ 1, КЗ 3, КЗ 4, КФ6
РН 15	КЗ 4
РН 20	КЗ 4
РН 21	КЗ 1, КЗ 2, КЗ 4
РН 24	КФ 4, КФ 7
РН 25	КФ 1, КФ 9

де РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізикоматематичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.

РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.

РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.

РН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.

РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.

РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для

дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.

РН24. Аналізувати, розробляти і супроводжувати інфраструктуру та стек застосунків у безперервному потоці змін Agile DevSecOps.

РН25. Досліджувати, обґрунтовувати вибір та застосовувати платформи та інструменти, що використовуються для реалізації підходу DevSecOps.

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

КЗ 2. Здатність проводити дослідження на відповідному рівні.

КЗ 3. Здатність до абстрактного мислення, аналізу та синтезу.

КЗ 4. Здатність оцінювати та забезпечувати якість виконуваних робіт.

КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.

КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.

КФ4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.

КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

КФ7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.

КФ9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Зміст навчальної дисципліни

Змістовий модуль 1. Основи децентралізованих систем

Тема 1. Основи децентралізованих систем.

1.1.Поняття та архітектура децентралізованих систем.

Визначення децентралізованих систем, їх відмінності від централізованих і розподілених моделей. Огляд архітектурних принципів побудови — вузлова структура, механізми комунікації між учасниками, обмін та узгодження даних у мережі.

1.2.Характеристики та властивості децентралізації.

Розгляд ключових властивостей: відмовостійкість, масштабованість, ефективне використання ресурсів, а також самовідновлення мережі. Аналіз факторів, що впливають на продуктивність і стабільність роботи систем без центрального керування.

1.3.Практичні приклади та виклики децентралізованих систем.

Аналіз застосувань децентралізованих технологій у фінансовій сфері (блокчейн), соціальних мережах і системах обміну файлами. Обговорення проблем безпеки, управління, контролю доступу, синхронізації та узгодження стану між вузлами.

Тема 2. Дослідження особливостей розгортання піринговых мереж та протоколу BitTorrent.

2.1.Архітектура та принципи функціонування піринговых мереж.

Розгляд основ побудови P2P-мереж, способів взаємодії вузлів без централізованого сервера, механізмів розподілу даних і ролі кожного вузла у спільній системі. Аналіз особливостей сегментації файлів і одночасного завантаження з кількох джерел.

2.2. Протокол BitTorrent та його механізми роботи.

Дослідження структури протоколу BitTorrent, принципів пошуку та підключення до трекерів, розподілу навантаження між учасниками, стратегій обміну фрагментами файлів і управління пропускною здатністю. Вивчення алгоритмів, що забезпечують ефективність і швидкість передачі даних.

2.3.Надійність, масштабування та безпека піринговых систем.

Аналіз стійкості BitTorrent-мереж до збоїв, методів відновлення даних і контролю цілісності файлів. Розгляд практичних аспектів розгортання, масштабування та загроз безпеці включно з поширенням шкідливого контенту й атаками на вузли мережі.

Тема 3. Криптографія у децентралізованих системах.

3.1.Основи криптографічного захисту в децентралізованих мережах.

Розгляд основних принципів забезпечення конфіденційності, цілісності та автентичності даних у мережах без централізованого контролю. Аналіз ролі криптографії у забезпеченні довіри між вузлами та запобіганні несанкціонованому доступу.

3.2. Криптографічні методи та засоби захисту.

Ознайомлення з симетричними та асиметричними алгоритмами шифрування, цифровими підписами, хеш-функціями та протоколами управління ключами. Розгляд їх застосування у забезпеченні безпечної взаємодії між учасниками P2P-середовища.

3.3.Практичні аспекти використання криптографії в децентралізованих системах.

Приклади застосування криптографії для захисту інформації, запобігання підробкам, забезпечення перевірки автентичності даних та формування довіри у розподілених середовищах. Аналіз викликів, пов’язаних із розповсюдженням ключів і збереженням стійкості до атак.

Змістовий модуль 2. Теоретичні засади функціонування блокчейн-технологій

Тема 4. Протоколи консенсусу у технології блокчейн.

4.1.Поняття консенсусу та його роль у блокчейн-системах.

Визначення консенсусу як механізму узгодження стану розподіленого реєстру між вузлами. Розгляд задач, які вирішують протоколи консенсусу: підтвердження транзакцій, запобігання подвійним витратам, забезпечення синхронізації та цілісності блокчейну.

4.2. Основні алгоритми консенсусу: Proof of Work і Proof of Stake.

Вивчення принципів роботи, переваг і недоліків PoW та PoS. Порівняння їх впливу на безпеку мережі, швидкість обробки транзакцій, масштабованість і енергоспоживання. Аналіз еволюції від класичних до гібридних та енергозберігаючих моделей.

4.3. Сучасні підходи до консенсусу та їх ефективність.

Ознайомлення з новими протоколами — Delegated Proof of Stake (DPoS), Practical Byzantine Fault Tolerance (PBFT) та іншими. Аналіз їхніх механізмів роботи, стійкості до атак, рівня децентралізації та практичного застосування у сучасних блокчейн-платформах.

Тема 5. Технологічні деталі функціонування блокчейн.

5.1.Структура блокчейну та принцип формування блоків.

Розглядається будова блоку, структура заголовка, зв’язок блоків через хеш-функції та роль криптографічного хешування у забезпеченні незмінності даних. Пояснюється формування ланцюга транзакцій і процес їхнього включення у блок.

5.2.Роль вузлів і механізми перевірки транзакцій.

Аналізуються типи вузлів у мережі (повні, легкі, майнери, валідатори), процеси перевірки та підтвердження транзакцій, формування нових блоків і розповсюдження інформації між учасниками мережі. Розкривається принцип розподіленого зберігання даних та забезпечення відмовостійкості системи.

5.3. Безпека та захист у блокчейн-мережах.

Вивчаються методи запобігання підробці даних, атакам типу “double spending” і спробам компрометації мережі. Розглядаються механізми контролю доступу без централізованого управління, а також способи підвищення надійності та стійкості блокчейну до зловмисних дій.

Тема 6. Застосування технології блокчейн.

6.1. Блокчейн у різних сферах діяльності.

Ознайомлення з практичними кейсами застосування технології: фінанси, управління ланцюгами постачання, охорона здоров’я, державне управління та

смарт-контракти. Розгляд конкретних прикладів реалізації та функціональних можливостей блокчейну.

6.2. Переваги та обмеження блокчейн-технологій.

Аналіз ефективності використання блокчейну для забезпечення прозорості, відстежуваності та безпеки даних. Вивчення сильних сторін технології і ситуацій, коли її застосування може бути обмеженим або неефективним.

6.3. Ризики та виклики впровадження.

Оцінка потенційних загроз і проблем при інтеграції блокчейну у бізнес-процеси, включно з технічними, організаційними та регуляторними аспектами. Розгляд способів мінімізації ризиків та забезпечення стійкості децентралізованих систем.

Перелік лабораторних занять за навчальною дисципліною наведено в табл. 2.

Таблиця 2

Перелік лабораторних робіт

Назва теми та / або завдання	Зміст
Тема 1, 2. Лабораторна робота 1. Дослідження особливостей розгортання піринговых мереж та протоколу BitTorrent	У роботі здобувачі досліджують архітектуру піринговых (P2P) мереж та принципи роботи протоколу BitTorrent. Вони ознайомлюються з процесом сегментації файлів на шматки, організацією обміну даними між вузлами, роллю трекерів та механізмами балансування навантаження. Під час роботи здобувачі створюють локальні експерименти з розгортанням кількох вузлів мережі, спостерігають процес обміну файлами, вивчають ефективність передачі даних і вплив кількості вузлів на швидкість та стабільність роботи мережі. Також аналізується стійкість мережі до відмов окремих вузлів та методи забезпечення цілісності даних.
Тема 1,2. Лабораторна робота 2. Mesh мережі	У цій роботі здобувачі знайомляться з архітектурою mesh-мереж та особливостями маршрутизації в таких системах. Вони досліджують принципи побудови вузлів, алгоритми динамічного формування маршрутів, стратегії розподілу навантаження та стійкості до відмов вузлів. Здобувачі моделюють невелику mesh-мережу, аналізують передачу даних між вузлами та вплив топології мережі на швидкість і надійність обміну інформацією. Додатково розглядаються питання забезпечення безпеки і контролю доступу у mesh-мережах.

Тема 3. Лабораторна робота 3. Створення та верифікація дерева Merkle	У цій роботі здобувачі створюють дерево Merkle на основі набору даних і вивчають процес побудови хеш-дерева для забезпечення цілісності інформації. Здобувачі виконують операції хешування окремих блоків даних, формують вузли дерева та перевіряють правильність обчислення кореневого хешу. Досліджуються механізми верифікації окремих транзакцій або блоків без необхідності перевірки всього дерева, що демонструє ефективність Merkle-дерев у децентралізованих системах, зокрема у блокчейн-технологіях.
Тема 4, 5. Лабораторна робота 4. Створення прототипу блокчейн	Ця робота присвячена практичному створенню простого прототипу блокчейн-системи. Здобувачі реалізують структуру блоків, механізм хешування, зв'язування блоків у ланцюг та алгоритми додавання нових блоків. Досліджуються принципи перевірки транзакцій, управління станом мережі та стійкість блокчейну до підробки даних. Здобувачі проводять експерименти зі зміною даних у блоках і спостерігають, як порушується цілісність ланцюга. Робота дозволяє на практиці зрозуміти основні механізми функціонування блокчейну та роль криптографії у забезпеченні безпеки.
Тема 6. Лабораторна робота 5. Методи забезпечення конфіденційності у децентралізованих системах	У цій роботі здобувачі досліджують різні методи забезпечення конфіденційності у децентралізованих мережах. Розглядаються симетричні і асиметричні алгоритми шифрування, цифрові підписи, хеш-функції та протоколи управління ключами. Здобувачі виконують практичні завдання з шифрування і дешифрування повідомлень, перевірки цифрового підпису, а також моделюють процес обміну конфіденційними даними між вузлами P2P-мережі. Додатково аналізуються питання захисту від атак та несанкціонованого доступу, забезпечення анонімності і стійкості до перехоплення даних.

Перелік самостійної роботи за навчальною дисципліною наведено в табл.3

Таблиця 3

Перелік самостійної роботи

Тема	Зміст роботи
Тема 1. Основи децентралізованих систем	1. Дослідження відмінностей між централізованими, децентралізованими та розподіленими системами. 2.Аналіз стійкості та відмовостійкості різних типів мереж. 3. Вивчення реальних прикладів децентралізованих платформ (P2P-системи, соціальні мережі, хмарні сервіси).

Тема 2. Дослідження особливостей розгортання піринговых мереж та протоколу BitTorrent.	1. Моделювання піринговой мережі для обміну файлами та аналіз ефективності передачі даних. 2. Дослідження впливу кількості вузлів на швидкість і стабільність мережі. 3. Аналіз стійкості мережі до відмов окремих вузлів та способів забезпечення цілісності переданих файлів.
Тема 3. Криптографія у децентралізованих системах	1. Практичне використання симетричних і асиметричних алгоритмів для захисту P2P-зв'язку. 2. Створення цифрових підписів і перевірка їх коректності. 3. Вивчення хеш-функцій та їх застосування для перевірки цілісності даних у децентралізованих системах.
Тема 4. Протоколи консенсусу у технології блокчейн.	1. Порівняння протоколів Proof of Work і Proof of Stake, аналіз їх переваг і обмежень. 2. Дослідження механізмів узгодження стану розподіленого реєстру та запобігання подвійним витратам. 3. Моделювання роботи простого протоколу консенсусу на прикладі невеликої мережі вузлів.
Тема 5. Технологічні деталі функціонування блокчейн	1. Вивчення структури блоків, хешування та формування ланцюга транзакцій. 2. Аналіз процесу перевірки та підтвердження транзакцій у розподіленій мережі. 3. Дослідження способів забезпечення цілісності блокчейну та захисту від підробки даних.
Тема 6. Застосування технології блокчейн	1. Аналіз практичних кейсів використання блокчейн у фінансах, управлінні ланцюгами постачання, смарт-контрактах та державному управлінні. 2. Визначення переваг і обмежень застосування блокчейну для різних сфер. 3. Розробка невеликого концептуального проекту на основі блокчейн для вирішення конкретної практичної задачі.

Кількість годин лекційних та лабораторних занять та годин самостійної роботи наведено в робочому плані (технологічній карті) з навчальної дисципліни.

МЕТОДИ НАВЧАННЯ

У процесі викладання навчальної дисципліни для набуття визначених результатів навчання, активізації освітнього процесу передбачено застосування таких методів навчання, як:

Словесні (Теми 1-6).

Наочні (демонстрація (Тема 1-6)).
Лабораторні роботи (Теми 1-6)).

ФОРМИ ТА МЕТОДИ ОЦІНЮВАННЯ

Університет використовує 100 бальну накопичувальну систему оцінювання результатів навчання здобувачів вищої освіти.

Поточний контроль здійснюється під час проведення лекційних, лабораторних занять і має на меті перевірку рівня підготовленості здобувача вищої освіти до виконання конкретної роботи і оцінюється сумою набраних балів: для дисциплін з формою семестрового контролю залік: максимальна сума – 100 балів; мінімальна сума – 60 балів.

Підсумковий контроль включає семестровий контроль та атестацію здобувача вищої освіти.

Семестровий контроль проводиться у формі диференційованого заліку.

Підсумкова оцінка за навчальною дисципліною визначається: для дисциплін з формою семестрового контролю залік – сумуванням всіх балів, отриманих під час поточного контролю.

Під час викладання навчальної дисципліни використовуються наступні контрольні заходи: Поточний контроль: лабораторні роботи (90 балів), письмова контрольна робота (10 балів). Семестровий контроль: Залік.

Більш детальну інформацію щодо системи оцінювання наведено в робочому плані (технологічній карті) з навчальної дисципліни.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Кравченко П. Блокчейн і децентралізовані системи : навч. посібник для студ. закладів вищ. освіти : в 3 частинах. Ч. 1 / П. Кравченко, Б. Скрябін, О. Дубініна. – Харків : ПРОМАРТ, 2019. – 452 с.
2. Кравченко П. Блокчейн і децентралізовані системи: навч. посібник для студ. закладів вищ. освіти: в 3 частинах. Ч. 2 / П. Кравченко, Б. Скрябін, О. Курбатов, О. Дубініна. - Харків, 2019. – 412 с.
3. Kravchenko, P. Blockchain and decentralized systems : in three volumes. V.3 / P. Kravchenko, B. Skriabin, O. Kurbatov, O. Dubinina. – Kharkiv : 2020. 298 p.
4. Кібербезпека : сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсеєв, О.Г. Король. – Львів: «Новий Світ- 2000», 2020 . – 678 с.
5. Євсеєв, С. П. Лабораторний практикум з основ криптографічного захисту [Електронний ресурс] : навч. посіб. / С. П. Євсеєв, О. В. Мілов, О. Г. Король ; Харківський національний економічний університет ім. С. Кузнеця. - Електрон. текстові дан. (12,3 МБ). - Харків : ХНЕУ ім. С. Кузнеця, 2020. - 221 с. http://www.repository.hneu.edu.ua/handle/123456789/24508

6. Математичні моделі і методи прийняття рішень. Лабораторний практикум для здобувачів вищої освіти спеціальностей 122 “Комп’ютерні науки”, 126 “Інформаційні системи та технології” другого (магістерського) рівня / Н. Д. Сізова, О. О. Шаповалова. - Харків: ХНУБА, 2021. - 144 с. http://repository.hneu.edu.ua/handle/123456789/31956

Додаткова

7. Жураковський, Б. Ю. Комп’ютерні мережі. Частина 1. Навчальний посібник [Електронний ресурс]: навч. посіб. / Б. Ю. Жураковський, І.О. Зенів; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 8,6 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2020. – 336 с. Режим доступа : https://ela.kpi.ua/handle/123456789/36615

8. Жураковський, Б. Ю. Комп’ютерні мережі. Частина 2. Навчальний посібник [Електронний ресурс] : навчальний посібник / Б. Ю. Жураковський, І. О. Зенів ; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 4,73 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2020. – 372 с. – Режим доступа : https://ela.kpi.ua/handle/123456789/36641

9. Юрчишин, В. Я. Хмарні та Грід-технології: конспект лекцій [Електронний ресурс] : навчальний посібник для студентів спеціальності 121 «Інженерія програмного забезпечення» (освітня програма «Програмне забезпечення комп’ютерних та інформаційно-пошукових систем») / В. Я. Юрчишин ; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 5,93 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2019. – 263 с. – Режим доступу: https://ela.kpi.ua/handle/123456789/2996.

10. Сучасні інформаційні технології та системи [Електронний ресурс] : монографія / Н. Г. Аксак, Л. Е. Гризун, О. В. Щербаков [та ін.] ; за заг. ред. Пономаренка В. С. — Електрон. текстові дан. (22,9 МБ). — Харків: ХНЕУ ім. С. Кузнеця, 2022. — 270 с. http://repository.hneu.edu.ua/handle/123456789/29233

11. Yevseiev S. Evaluation of Cryptographic Strength and Energy Intensity of Design of Modified Crypto-Code Structure of McEliece with Modified Elliptic Codes / S. Yevseiev, O. Korol, O. Veselska, S. Pohasii, V. Khvostenko // Міжнар. наук.-практ. конф. «Інформаційна безпека та інформаційні технології», Харків – Одеса, 13-19 вер. 2021 р. : матер. конф. – Харків : ХНЕУ ім. С. К узнеця. http://repository.hneu.edu.ua/handle/123456789/26827

Інформаційні ресурси

12. Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця за дисципліною " Сучасні методи децентралізованого розподілу та криптографічного захисту даних" https://pns.hneu.edu.ua/course/view.php?id=10226