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

ЗАТВЕРДЖЕНО
на засіданні кафедри
кібербезпеки та
інформаційних технологій
Протокол № 2 від 31.08.2023 р.

ПОГОДЖЕНО
Проректор з навчально-методичної роботи
_____ Каріна НЕМАШКАЛО

ОСНОВИ КРИПТОГРАФІЧНОГО ЗАХИСТУ

робоча програма навчальної дисципліни (РПНД)

Галузь знань	***12 Інформаційні технології***
Спеціальність	***125 Кібербезпека та захист інформації***
Освітній рівень	***перший (бакалаврський)***
Освітня програма	***Кібербезпека***
Статус дисципліни	***обов'язкова***
Мова викладання, навчання та оцінювання	***українська***

Розробники:
д.т.н., проф. _____ Андрій ЧУГАЙ

к.т.н., доц. _____ Олена ШАПОВАЛОВА

Завідувач кафедри
кібербезпеки та
інформаційних технологій _____ Ольга СТАРКОВА

Гарант програми _____ Вячеслав ЛИМАРЕНКО

Харків
2023

ВСТУП

Слід відзначити, що на сьогоднішній день питання безпеки, зокрема в кіберпросторі є вкрай важливими. В умовах ведення бізнесу, навчання, спілкування в онлайн режимі це стосується абсолютно всіх: об'єктів стратегічного значення, комерційних підприємств, середньопересічнних громадян, а одним з ключових моментів організації безпечного зв'язку і передачі даних є використання арсеналу криптографічних методів та інструментів.

В РПНД наведено розгорнутий план лекцій навчальної дисципліни "Основи криптографічного захисту" за модулями та темами, перелік лабораторних занять. Революційні зміни останнього десятиліття, що відбулися в Інтернет-ресурсах, зумовили до об'єднання інформаційних та комп'ютерних мереж в єдиний інформаційний та кібернетичний простір, що спонукало до створення інформаційно- корпоративних мереж на основі Інтернет-технологій, які істотно розширили спектр електронних послуг суспільства в цілому та людині окремо. Як наслідок, суттєво трансформувалися і загрози такому інформаційному ресурсу, як Інтернет-ресурс (ІР). Загрози безпеці ІР набули ознак гібридності. Прояви ознак гібридності унаслідок одночасного впливу загроз інформаційній безпеці, кібернетичній безпеці (КБ) та безпеці інформації (БІ) на ІР призвели до виникнення явища синергізму, негативні прояви якого потребують кардинального перегляду концепцій побудови діючих систем безпеки.

Розповсюдження Інтернет-технологій також, безперечно, вимагає добре поставленого захисту інформації, яка циркулює в кіберпросторі. Тому вивчення основних механізмів забезпечення безпеки, захисту програмного забезпечення на всьому циклі його існування приділяється багато уваги.

Мета – дати здобувачам знання і навички для вивчення і засвоєння подальших дисциплін, пов'язаних з захистом інформації та її обробкою, у значній мірі визначає рівень загальнонаукової підготовки спеціалістів і становить основу для вивчення принципів, методів, алгоритмів та обчислювальних технологій обробки інформації з обмеженим доступом.

Завданнями навчальної дисципліни є:

- отримання практичних навичок застосування криптографії для захисту та збереження інформації;
- отримання знань щодо застосування новітніх способів захисту інформаційного контенту при розгортанні та функціонуванні застосунків;
- ознайомлення з можливостями забезпечення надійного захисту в умовах постквантового періоду.

Об'єктом вивчення дисципліни є криптографічні методи захисту інформації та інструменти його організації.

Предметом навчальної дисципліни є технічні та програмні засоби та математичний апарат для реалізації криптографічних методів захисту інформації.

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 2	КЗ 1, КЗ2 , КЗ 4, КЗ 5
РН 3	КЗ 1, КЗ2 , КЗ 4, КЗ 5
РН 4	КЗ 1, КЗ2 , КЗ 4, КЗ 5
РН 10	КЗ 1, КФ 2, КФ 11
РН 14	КФ 2, КФ 3, КФ 5, КФ 8, КФ 10, КФ 11
РН 15	КФ2, КФ3, КФ11
РН 18	КЗ 1, КФ2, КФ3, КФ5, КФ11
РН 19	КЗ 1, КФ 2, КФ 5, КФ 8, КФ 11
РН 23	КФ 5, КФ 6, КФ 8, КФ 11
РН 24	КЗ 1, КФ 4, КФ 5, КФ 9, КФ 11
РН 31	КФ 2, КФ 6, КФ 10
РН 32	КЗ 1, КФ 4, КФ 5, КФ 8, КФ 11
РН 40	КФ 10
РН 47	КФ 2, КФ 3, КФ 5, КФ 10
РН 48	КФ 5, КФ 6, КФ 8, КФ 10, КФ 11

де КЗ 1 здатність застосовувати знання у практичних ситуаціях;

КЗ 2 знання та розуміння предметної області та розуміння професії;

КЗ 4 вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням;

КЗ 5 здатність до пошуку, оброблення та аналізу інформації;

КФ 2 здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки;

КФ 3 здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах;

КФ 5 здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки;

КФ 6 здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження;

КФ 8 здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку;

КФ 9 здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою;

КФ 10 здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності;

КФ 11 здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки;

РН 2 організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;

РН 3 використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;

РН 4 аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;

РН10 виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем;

РН 14 вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень;

РН 15 використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій;

РН 18 використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів;

РН 19 застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;

РН 23 реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;

РН 24 – вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових);

РН 31 застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем;

РН 32 вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки;

РН 40 інтерпретувати результати проведення спеціальних вимірювань з

використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації;

РН 47 вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації;

РН 48 виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ЗМІСТ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ЗМІСТОВИЙ МОДУЛЬ 1. МЕХАНІЗМИ ЗАХИСТУ НА ОСНОВІ СИМЕТРИЧНИХ ТА НЕСИМЕТРИЧНИХ АЛГОРИТМІВ

Тема 1. Теоретичні основи захисту інформації.

Основні визначення. Комплекс засобів захисту даних. Політики безпеки. Підходи до забезпечення захисту інформації АСОІ

Криптографічне перетворення інформації та криптографічний захист. Криптографічний аналіз.

Аутентифікація джерела. Основні завдання системи безпеки.

Симетричні криптосистеми. Нелінійні вузли замін симетричних криптоалгоритмів. Блокові та поточні алгоритми. Показники ефективності криптографічних булевих функцій (нелінійних вузлів замін).

Алгоритми double та triple DES. Advanced Encryption Standard (AES). Алгоритм RIJNDAEL. Алгоритм симетричного блочного перетворення "Калина-256".

Режими роботи блокових алгоритмів шифрування стандарт ISO/IEC 10116:1997. Режим електронної кодової книги (electronic code book mode).

Звичайний та вдосконалений режими зворотного зв'язку з шифртексту (ciphertext feed back mode). Режим зворотного зв'язку за виходом (output feed back mode).

Асиметричні схеми шифрування. NP - повні завдання. Факторизація числа, дискретний логарифм у групі точок елептичної кривої, декодування випадкового коду.

Асиметрична система RSA. Система обміну ключами Діффі-Хеллмана. Протокол забезпечення автентичності та конфіденційності.

Тема 2. Протоколи автентичності. Цифровий підпис .

Механізми забезпечення автентичності. Класифікація та способи організації цифрових підписів.

Цифровий підпис на RSA. Цифровий підпис: СТАНДАРТ DSA, DSS, ДСТУ

P-3410.

Методи хешування. Безключові та ключові хеш-функції. Односторонні (one - way hash function (OWHF)) і стійкі до колізій хеш-функції (СКХФ). Хеш-функція ДСТУ 7564 («Купіна- n »).

Схеми на модулярних перетвореннях. Схема алгоритма хешування MASH-1. Хеш-функція CBC - MAC ISO / IEC 6796.

Спеціалізовані хеш-функції. Secure Hash Algorithm. Хеш-функції із сімейства RIPEMD.

Механізми аутентифікації: на основі використання програмно-апаратних засобів; у стеку TCP/ IP. Система аутентифікації серверу KERBEROS.

Аутентифікація за допомогою сертифікатів. Проходження IP-пакету даних (транспортний та тунельний режими).

Тема 3. Протоколи суворої автентифікації

Алгоритми та протоколи двофакторної аутентифікації (2 FA).

Метод суворої автентифікації PASSWINDOWS: обмеження програмної реалізації алгоритму. Алгоритм моніторингу 2FA PASSWINDOWS.

Рівні достовірності автентифікації: вимоги та обмеження. Загрози у разі двофакторної аутентифікації

Багатофакторна аутентифікація. Технологія RSA SecurID.

Двуфакторна аутентифікація в LINUX. Налаштування Google authenticator для кожного користувача.

Налаштування SSH. Забезпечення безпеки SSH.

Тема 4. Протоколи цілісності SSL, TLS.

Протоколи цілісності SSL, TLS. Синергетична модель загроз синтезу на CCISI на CFS.

Структура, функції та версії протоколу SSL. Використання протоколу SSL. Структура, функції та версії протоколу TLS. Використання протоколу TLS.

Атаки на SSL/TLS: "CHOSEN PLAINTEXT" (WEI DAI). "PADDING ORACLE" (SERGE VAUDENAY), POODLE. Атаки на протокол HANDSHAKE.

Record Layer у TLS 1.3: шифрування AEAD. Шифрування із CHACHA20. Аутентифіковане шифрування. Метод шифрування за допомогою поля Галуа: AES-GSM. Принцип та алгоритм роботи.

Поєднання можливостей потокового шифру CHACHA20 та POLY1305. Проект I2P (Invisible Internet Project). Мережі I2P. Тунелювання.

Новий транспортний протокол NTCP2. Зміни у ROUTERINFO. Генерація ключів передачі даних під час встановлення з'єднання.

Поля Галуа. Структура кінцевих полів та їх властивості. Поля Галуа на кільцях багаточленів. Основні властивості полів Галуа.

Тема 5. Система PGP.

Поняття системи PGP та її функції. Послуги PGP: аутентифікація, конфіденційність, цифровий підпис, сумісність.

Вимоги до ключів в системі PGP. Ідентифікатори ключів. Створення повідомлень в PGP.

Забезпечення довіри в PGP. Сертифікати PGP. Операції визначення ступеня довіри.

Тема 6. Основи технології PKI

Алгоритми поширення ключів. Компоненти та послуги інфраструктури відкритих ключів. Засвідчувані центри та їхні функції. Реєстр та архів сертифікатів. Сервіси. Архітектура і топологія PKI. Взаємодія компонентів PKI. Стандарти і специфікації PKI.

Програмно-технічний комплекс «Центр сертифікації ключів» і його компоненти.

Класифікація ключів. Ієрархія ключів і крипто період.

Життєвий цикл управління ключами. Моделі управління ключами. Варіанти використання центру передачі ключів.

Модель процесу сертифікації.

Узгодження ключів Діффі-Хеллмана. Механізми управління ключами на основі використання несиметричних методів.

ЗМІСТОВИЙ МОДУЛЬ 2. МЕХАНІЗМИ ЗАХИСТУ В УМОВАХ ПОСТКВАНТОВОГО ПЕРІОДУ

Тема 7. Основи постквантової криптографії.

Комбіновані криптосистеми.. Специфіка протоколів SSL\ TLS в постквантовий період.

Протоколи SET та HTTPS в постквантовому періоді.

Закон Мура. Алгоритм Шора. Квантові біти.

Квантові об’єкти та переплутані стани. Квантове прискорення обчислень.

Квантовий комп'ютер D-WAVE. Квантове перетворення Фур'є. Алгоритм Гровера.

Квантовий розподіл ключів. Поляризація фотонів. Інші протоколи розподілу ключів. Атаки на квантові протоколи.

Квантові гроші С. Візнера.

Протокол Субхашу Кака. Засоби пом’якшення наслідків постквантового прориву.

Тема 8. Пост квантові алгоритми на основі крипто-кодових конструкцій Мак-Еліса і Нідеррайтера. Гібридні системи захисту на збиткових кодах.

Вимоги до крипто алгоритмів пост квантового періоду. Криптографічні типи (за рейтингом конкурса NIST). Показники оцінювання якості.

Кандидати на новий пост квантовий стандарт несиметричної криптографії. Класифікація крипто-кодових конструкцій

Атака Сидельникова на крипто-кодові конструкції. Крипто-кодова конструкція Нідеррайтера на ЕС.

Алгоритм рівноважного кодування. Методи модифікації завадостійких кодів

Модифіковані крипто-кодові конструкції на МЕС. Результати дослідження властивостей крипто-кодових конструкцій.

Неповноцінна криптографія, способи завдання шкоди. Вибір оптимального способу нанесення шкоди.

Способи побудови гібридних крипто-кодових конструкцій. Протокол обміну на основі ГККК Мак-Елісу.

Результати досліджень ГККК на збиткових кодах.

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

Таблиця 2

Перелік лабораторних занять / завдань

Назва теми та / або завдання	Зміст
Тема 1. Лабораторна робота 1	Дослідження властивостей режимів роботи блокових шифрів
Тема 2. Лабораторна робота 2	Дослідження протоколів автентичності та конфіденційності за допомогою RSA
Тема 3. Лабораторна робота 3	Дослідження протоколів цифрового підпису
Тема 4. Лабораторна робота 4	Дослідження протоколів системи PGP
Тема 5-6. Лабораторна робота 5	Методика NIST. Оцінки статистичних властивостей криптографічних алгоритмів
Тема 7-8. Лабораторна робота 6	Робота з кубітами. Емуляція вимірювань

Перелік самостійної роботи за навчальною дисципліною наведено в табл.3

Таблиця 3

Перелік самостійної роботи

Назва теми та / або завдання	Зміст
Тема 1 - 8	Вивчення лекційного матеріалу та більш детальне ознайомлення з ресурсами, посилання на які надано на лекції
Тема 1 - 8	Підготовка до лабораторних занять
Тема 1 - 8	Підготовка до екзамену

Кількість годин лекційних, 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 (лекція (Тема 1, 2, 3, 4, 5, 6), проблемна лекція (Тема 7, 8,));

наочні (демонстрація (Тема 1–8));

практичні (лабораторні роботи (Тема 1–8)).

ФОРМИ ТА МЕТОДИ ОЦІНЮВАННЯ

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

Поточний контроль здійснюється під час проведення лекційних та 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 екзамен (іспит): максимальна сума – 60 балів; мінімальна сума, що дозволяє здобувачу вищої освіти складати екзамен (іспит) – 35 балів.

Підсумковий контроль включає семестровий контроль та атестацію здобувача вищої освіти.

Семестровий контроль проводиться у формах семестрового екзамену (іспиту). Складання семестрового екзамену (іспиту) здійснюється під час екзаменаційної сесії.

Максимальна сума балів, яку може отримати здобувач вищої освіти під час екзамену (іспиту) – 40 балів. Мінімальна сума, за якою екзамен (іспит) вважається складеним – 25 балів.

Підсумкова оцінка за навчальною дисципліною визначається для дисциплін з формою семестрового контролю екзамен (іспит) – сумуванням балів за поточний та підсумковий контроль.

Під час викладання навчальної дисципліни використовуються наступні контрольні заходи:

Поточний контроль: Лабораторні роботи (50 балів), письмова контрольна робота (10 балів).

Семестровий контроль: Екзамен (40 балів).

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

Приклад екзаменаційного білета та критерії оцінювання для навчальної дисципліни.

Приклад екзаменаційного білета

Харківський національний економічний університет імені Семена Кузнеця
Перший (бакалаврський) рівень вищої освіти
Спеціальність 125 «Кібербезпека та захист інформації»
Освітньо-професійна програма «Кібербезпека»
Семестр V
Навчальна дисципліна "Основи криптографічного захисту"

ЕКЗАМЕНАЦІЙНИЙ БІЛЕТ № 1

1	Оберіть коректне продовження фрази з двох варіантів Безпека інформації – це… а. Стан інформації, яка зберігається, оброблюється, чи передається б. Сукупність цілеспрямованих дій та заходів
2	Оберіть одну або декілька правильних відповідей зі списку В якому алгоритмі шифрування застосовується функція Ейлера? а. RSA б. DES в. ГОСТ 28147-89 г. TripleDES
3	Оберіть одну або декілька правильних відповідей зі списку В якому розділі не застосовуються в криптографії еліптичні криві? а. Симетричне шифрування. б. Асиметричне шифрування. в. Електронні цифрові підписи. г. Симетричне та асиметричне шифрування.
4	Оберіть одну або декілька правильних відповідей зі списку Вимоги, що пред’являються до шифрів: а. Низька криптостійкість б. Простота процедур шифрування и разшифрування в. Чутливість до найменших помилок
5	Оберіть одну відповідь зі списку Чи справедливо твердження щодо відкритості алгоритмів шифрування/розшифрування для асиметричних систем? а. Так б. Ні в. Частково
6	Оберіть одне або кілька коректних продовжень фрази з наведених варіантів Геш-функція … а. призначена для збільшення якості підписаного документу б. приймає у якості аргументу повідомлення довільної довжини та повертає геш-значення фіксованої довжини в. Значення геш-функції не залежить від тексту та дозволяє відновити сам документ
7	Оберіть одну або декілька правильних відповідей зі списку Довжина ключа для симетричного блочного шифру DES складає … а. 256 б. 128 в. 56 г. 32

8	Оберіть одну або декілька правильних відповідей зі списку У функції центру управління ключовою системою не входить … а. Створення ключів. б. Створення сертифікатів. в. Створення алгоритмів електронних цифрових підписів. г. Управління ключами.
9	Оберіть одну або декілька правильних відповідей зі списку У якому з режимів шифрування з використанням блочних алгоритмів існує можливість розпаралелювання обчислень? а. ECB б. CBC в. CFB г. OFB
10	Оберіть коректне продовження фрази Запропонована у 1917 році система Вернама є: а. Безумовно-стійкою (теоретично-недешифруємою) б. Обчислювано-стійким (гарантованої стійкості) в. Імовірно-стійким (доказово-стійкі) г. Обчислювано-нестійким(часової стійкості)
11	Оберіть коректне продовження фрази Криптоаналіз методом «дня народження» - це а. Імовірнісний метод б. Аналітичний метод
12	Оберіть одну або декілька правильних відповідей зі списку Кількість циклів перетворення даних для симетричного блочного шифру DES складає а. 64 б. 16 в. 32
13	Оберіть одну або декілька правильних відповідей зі списку Реалізована загроза безпеці – це: а. Порушення стану захищеності інформації б. Атака на засоби обробки інформації в. Пошук та використання тієї чи іншої уразливості
14	Оберіть коректне продовження фрази Криптостійкість RSA заснована на … а. Складностях факторизації великих чисел б. Складностях знаходження дискретного логарифму
15	Оберіть коректне продовження фрази Методологія побудови асиметричних криптосистем побудована на застосуванні: а. Стійких сучасних криптоалгоритмів б. Односпрямованих функцій
16	Оберіть коректне продовження фрази Механізм забезпечення цілісності та автентичності повідомлення для симетричних систем а. Цифровий підпис б. Формування імітовставки
17	Оберіть коректне продовження фрази Можливість доказу факту підробки повідомлення у разі компрометації відправника зі сторони одержувача для асиметричних систем а. Існує б. Не існує

18	Оберіть коректне продовження фрази Обчислювано-стійкі криптосистеми – це а. Криптосистеми, що взагалі не можуть бути розкриті за допомогою криптоаналізу навіть за наявних необмежених обчислювано-часових можливостей криптоаналитика б. Для зламування таких криптосистем потрібні величезні обчислювано-часові можливості для проведенні криптоатаки, що заснована на повному переборі варіантів
19	Оберіть коректне продовження фрази Основи p и q для алгоритма повинні бути … а. Великими простими числами однакової довжини б. Взаємно простими числами різної довжини в. Будь-якими великими числами
20	Оберіть коректний варіант Порушення повноважень – це … а. Загроза проникнення б. Загроза впровадження в. Базові загрози

Затверджено на засіданні кафедри КІТ протокол № _____від «____»_20___р.

Екзаменатор д.т.н., проф. Чугай А.М.

Зав. кафедрою д.т.н., проф. Старкова О.В.

Критерії оцінювання

Підсумкові бали за екзамен складаються із суми балів за виконання всіх завдань, що округлені до цілого числа за правилами математики. Екзамен містить 20 рівноцінних питань. За кожну правильну відповідь – 2 бали.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Yevseiev S. Research of collision properties of the modified UMAC algorithm on crypto-code constructions / S. Yevseiev, A. Havrylova, O. Korol, O. Dmitriiev, O. Nesmiian, Y. Yufa, A. Hrebennikov // EUREKA: Physics and Engineering. – 2022. – № 1 (38). – P. 34-43. http://repository.hneu.edu.ua/handle/123456789/26814

2. Milov O. Creation of a methodology for building security systems for multimedia information resources in social networks / O. Milov, S. Milevskyi, V. Aleksiyev. // Przetwarzanie, transmisja i bezpieczenstwo informacji. – Bielsko-Biala : Wydawnictwo naukowe Akademii Techniczno-Humanistycznej w Bielsku-Bialej, 2020. - Vol. 12. http://repository.hneu.edu.ua/handle/123456789/24817

3. Остапов С. Е. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с. (Укр. мов.) http://repository.hneu.edu.ua/handle/123456789/22547

Додаткова

4. Havrylova A. Development of a pseudo-random substrate for the UMAC algorithm on crypto-code constructions / A. Havrylova, A. Tkachov, A. Shmatko // Information protection and information systems security : proc. of of VIII-th International Scientific and Technical Conferenc, Lviv, November 11-12, 2021. – Lviv : Polytechnic Publishing House 2021. – P. 49-50 http://repository.hneu.edu.ua/handle/123456789/26840

5. 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. Кузнеця, 2021. – С. 144-157. http://repository.hneu.edu.ua/handle/123456789/26827

6. Encrypt Pad https://evpo.net/encryptpad/#when-encryptpad

7. Tutorial SSH: Understanding Encryption, Ports and Connection https://www.hostinger.com/tutorials/ssh-tutorial-how-does-ssh-work

8. Social Engineering in Cybersecurity: A Domain Ontology and Knowledge Graph Application Examples (ISSN: 2523-3246) on 28 April. doi:10.1186/s42400-021-00094-6) https://arxiv.org/ftp/arxiv/papers/2106/2106.01157.pdf

9. What is the difference between SSL vs. TLS? Which Gives Your Website the Best Protection? https://www.websitepulse.com/blog/ssl-vs-tls-difference-and-best-protection

Інформаційні ресурси

12. Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця навчальної дисципліни “Основи криптографічного захисту” https://pns.hneu.edu.ua/course/view.php?id=8980