МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЧЕРНІГІВСЬКА ПОЛІТЕХНІКА»
Кафедра кібербезпеки та математичного моделювання

ОСНОВИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

МЕТОДИЧНІ ВКАЗІВКИ
до виконання курсової роботи
для здобувачів
першого (бакалаврського) рівня вищої освіти
освітньо-професійної програми «Кібербезпека»
спеціальності 125 Кібербезпека та захист інформації

Обговорено і рекомендовано
на засіданні кафедри
Кібербезпеки та математичного
моделювання
Протокол №2
від 13 лютого 2024 р.

Чернігів 2024

Основи криптографічного захисту інформації. Методичні вказівки до виконання курсової роботи для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. – Чернігів: НУ «Чернігівська політехніка», 2024 – 40 с.

Укладачі: СИНЕНКО МАРИНА АНАТОЛІЇВНА, доцент кафедри кібербезпеки та математичного моделювання, кандидат фізико-математичних наук, доцент;
ТКАЧ ЮЛІЯ МИКОЛАЇВНА, завідувач кафедри кібербезпеки та математичного моделювання, доктор педагогічних наук, професор;
ШЕЛЕСТ МИХАЙЛО ЄВГЕНОВИЧ, професор кафедри кібербезпеки та математичного моделювання, доктор технічних наук, професор;
СЕМЕНДЯЙ СЕРГІЙ МАТВІЙОВИЧ, старший викладач кафедри кібербезпеки та математичного моделювання

Відповідальний за випуск – ТКАЧ ЮЛІЯ МИКОЛАЇВНА,
завідувач кафедри кібербезпеки та математичного моделювання, доктор педагогічних наук, професор

Рецензент – ПЕТРЕНКО ТАРАС АНАТОЛІЙОВИЧ,
доцент кафедри кібербезпеки та математичного моделювання, кандидат технічних наук

ЗМІСТ

ВСТУП

Задача захисту інформації у комп'ютерних системах насьогодні є досить актуальною у наслідок широкого розповсюдження таких систем, розширення локальних та глобальних комп'ютерних мереж, впровадження у різні сфери діяльності електронного документообігу та інше. Ці та багато інших задач захисту інформації покликана розв'язувати криптографія. Виконання та захист курсової роботи є завершальним етапом вивчення дисципліни «Основи криптографічного захисту інформації», метою якої є встановлення відповідності рівня та обсягу знань, умінь, інших компетентностей вимогам стандартів вищої освіти та ОПП спеціальності 125 - Кібербезпека.

Курсова робота - це самостійне, навчально-наукове дослідження ЗВО, у процесі написання якого під керівництвом викладачів кафедри ЗВО опановують методи проведення наукового дослідження, формують навички аналізу та самостійного узагальнення, здатність застосувати одержані знання для вирішення конкретних завдань.

Курсова робота виконується на основі знань, отриманих у процесі навчання і придбаних під час науково-дослідної роботи.

Мета курсової роботи – систематизація, актуалізація, закріплення та поглиблення знань ЗВО і їх вміння вирішувати теоретичні та практичні задачі пов'язані з криптографічним захистом інформації

Основні задачі КР:

– оцінка рівня теоретичних знань і практичних вмінь ЗВО спеціальності 125 - Кібербезпека з дисципліни «Основи криптографічного захисту інформації» та використання їх під час розв'язання конкретних задач;

– демонстрація вміння ЗВО стисло, логічно, аргументовано викладати матеріал;

– розвиток та поглиблення навичок проведення самостійної роботи, оволодіння методиками наукових досліджень і експериментування;

У процесі виконання курсової роботи студенти розвивають широту мислення, одержують навички дослідницької роботи, демонструють рівень своєї професійної підготовки.

1. ОРГАНІЗАЦІЯ ТА ОСНОВНІ ЕТАПИ НАПИСАННЯ КУРСОВОЇ РОБОТИ

1.1 Вимоги до курсової роботи

Курсова робота передбачає:

– систематизацію, закріплення, розширення теоретичних і практичних знань з дисципліни «Основи криптографічного захисту інформації» та застосування їх при вирішенні конкретних завдань;

– вміння виявляти проблеми наукового і практичного змісту та пропонувати шляхи їх вирішення; розвиток навичок самостійної роботи й оволодіння методами дослідження;

– розвиток навичок пошуку та систематизації інформації, її оброблення із застосуванням комп'ютерних інформаційних систем, аналітичних методів її оброблення, моделювання та прогнозування;

– розвиток умінь та навичок у проведенні самостійної аналітичної роботи, а також оволодіння методами її виконання;

– вміння захищати свою роботу.

Основними етапами виконання ВКР є:

– ознайомлення ЗВО з основними вимогами до виконання КР;

– вибір теми роботи, узгодження з керівником, складання завдання до виконання курсової роботи;

– обробка літературних джерел, збір та вивчення теоретичних і практичних матеріалів з обраної теми, складання бібліографії, аналіз та узагальнення зібраного матеріалу;

– викладення проаналізованого та систематизованого матеріалу;

– формулювання висновків;

– підготовка графічної частини роботи: рисунків, таблиць (у разі необхідності);

– представлення курсової роботи керівнику для підготовки відгуку;

– написання доповіді й підготовка ілюстративного матеріалу (презентації для виступу);

– захист курсової роботи.

Курсова робота повинна містити:

– обґрунтування актуальності обраної теми;

– визначені предмет та об'єкт дослідження;

– встановлена мета дослідження та завдання із виконання наукових досліджень, які забезпечують досягнення визначених цілей;

– короткий науково-аналітичний огляд інформаційних джерел про виникнення і сучасний стан досліджуваної проблеми;

– подання ключової інформації у зручній для сприйняття формі (таблиці, діаграми, ілюстрації тощо);

1.2 Вибір теми роботи

Тема курсової роботи обирається ЗВО з орієнтовного переліку, запропонованого кафедрою кібербезпеки та математичного моделювання. Студент

може запропонувати свою тему відповідно до власних наукових інтересів, яка в разі згоди кафедри може бути включена до переліку.

Тематика курсової роботи стосується розв'язання за допомогою криптографічних методів наступних задач захисту інформації:

- автентифікація користувачів;
- автентифікація даних;
- захист даних, що зберігається на електронних носіях інформації;
- захист даних, які передаються відкритими каналами зв'язку;

Автентифікація користувачів. Завдання цього класу передбачає реалізацію одного з криптографічних протоколів одно- або багатосторонньої автентифікації. У курсовій роботі необхідно проаналізувати ряд протоколів автентифікації, визначити переваги і недоліки заданого протоколу порівняно з відомими аналогами, а також визначити задачі, у яких доцільно використовувати розроблюваний засіб. Основна увага в курсових роботах такого типу приділяється реалізації криптографічного протоколу та організації віддаленого обміну даних між користувачами відповідно до цього криптографічного протоколу.

Автентифікація даних передбачає реалізацію криптографічних методів перевірки цілісності та автентичності даних, які базуються на методах формування електронних цифрових підписів та гешуванні даних. Завдання такого типу потребують аналізу відомих методів формування електронних цифрових підписів або методів гешування, визначення переваг і недоліків цих методів, а також визначення задач, де їх доцільно використовувати. Основна увага має приділятися реалізації алгоритмів формування цифрових підписів або геш-значень даних, організації віддаленого обміну даними між користувачами відповідно вибраного криптографічного протоколу.

Захист даних, що зберігаються на електронних носіях інформації передбачає реалізацію одного з методів блокового шифрування. Даний клас завдань потребує аналізу ряду методів блокового шифрування, визначення переваг і недоліків заданого методу шифрування порівняно з відомими аналогами, а також визначення задач, де їх доцільно використовувати. Основна увага в таких курсових роботах приділяється реалізації процедури розгортання ключів, раундового криптоперетворення та організації обміну даними між засобом, що розробляється, та пристроєм, що зберігає інформацію.

Захист даних, що передаються каналами зв'язку передбачає реалізацію одного з методів потокового шифрування даних. Для виконання роботи цієї тематики необхідно проаналізувати основні характеристики та протоколи обміну даними в заданих каналах зв'язку, проаналізувати методи захисту каналів зв'язку та обґрунтувати вибір методу, який буде реалізовуватись при виконанні курсової роботи. Основна увага курсового проекту даної тематики повинна приділятися розробці засобів, що реалізують методи криптографічного захисту інформації.

Теми курсових робіт наведено у додатку А даних методичних вказівок.

1.3 Захист курсової роботи

Процедура захисту передбачає:

- наявність КР;
- доповідь ЗВО про зміст та сутність роботи;
- запитання до автора роботи;
- відповіді ЗВО на запитання членів екзаменаційної комісії та осіб, присутніх на захисті;
- оголошення відгуку наукового керівника;
- заключне слово студента;
- оголошення рішення комісії про оцінку роботи.

Доповідь ЗВО повинна бути державною мовою (в окремих випадках, якщо цього вимагає специфіка теми дослідження, дозволяється також доповідати однією з іноземних мов). Доповідь ЗВО повинен підготувати заздалегідь у формі виступу, в якому доцільно висвітлити такі важливі питання:

- обґрунтування актуальності теми дослідження;
- мета, завдання, об'єкту, предмету дослідження;
- що вдалося дослідити, встановити, виявити, довести? Якими методами це досягнуто;
- елементи новизни в практичних рекомендаціях, практичну значимість;
- з якими труднощами довелося зіткнутися в процесі дослідження, які положення не знайшли підтвердження;
- основні результати роботи.

Доповідь ЗВО на захисті КР повинна тривати не більше 10 хвилин. Захист КР повинен супроводжуватись демонстрацією електронної презентації, яка є ілюстрацією доповіді під час захисту.

2. ВИМОГИ ДО СТРУКТУРНИХ ЕЛЕМЕНТІВ КУРСОВОЇ РОБОТИ

2.1 Структура курсової роботи

Зміст курсової роботи визначається її темою. Курсову роботу подають у вигляді рукопису, мова написання роботи – українська (за виключенням робіт іноземних студентів). Дозволяється деякі технічні терміни виконувати іноземною мовою.

Курсова робота повинна містити наступні структурні елементи:

– титульний аркуш;
– реферат;
– зміст;
– перелік умовних позначень (при необхідності);
– вступ, основна частина (розділи роботи);
– висновки;
– перелік посилань;
– додатки (при необхідності);

При написанні курсової роботи студент повинен обов'язково посилатися на авторів і джерела, з яких запозичав матеріали або окремі результати.

Титульний аркуш оформлюється виключно згідно наведеного зразка. Зразок оформлення наведено у додатку Б.

Реферат наводиться для швидкого знайомства з курсовою роботою, має бути стислим і відображати основну інформацію про роботу в такій послідовності: обсяг, об'єкт та предмет дослідження, мета та методи дослідження, результати та новизна, перелік ключових слів. Реферат розміщується на окремій сторінці. Обсягом реферату – біля 500 знаків.

2.2 Зміст

Зміст курсової роботи повинен послідовно містити назви всіх структурних елементів роботи (окрім титульного аркуша, завдання, та самого змісту) і посилання на номери сторінок, на яких починається даний структурний елемент. Зміст розташовується безпосередньо після реферату з нової сторінки. На початку по центру розміщується слово "ЗМІСТ" (без лапок).

2.3 Перелік умовних позначень

Перелік умовних позначень є необов'язковим елементом роботи. Він складається у випадку, коли робота містить маловідомі скорочення, абревіатури, символи, специфічні терміни.

Перелік друкується двома колонками, в яких ліворуч за абеткою наводять позначення чи терміни, праворуч - їх детальне розшифрування (тлумачення). Якщо в роботі певний термін, скорочення чи позначення повторюється менше трьох разів, його у перелік не включають, а його розшифрування наводять у тексті при першому згадуванні.

2.4 Вступ

У вступі коротко висвітлюють оцінку сучасного стану проблеми, її значущість, підстави і вихідні дані для розроблення теми, обґрунтування необхідності проведення дослідження.

Вступ повинен містити такі елементи (у такому ж порядку):

– *Актуальність теми.* Шляхом критичного аналізу та порівняння з відомими розв'язаннями проблеми обґрунтовується актуальність і доцільність роботи. Загалом актуальність повинна:

1. показати місце даної роботи у загальній проблемі;

2. визначити, що саме у загальній проблемі є нерозв'язаним та, відповідно, на спробу розв'язання чого спрямована робота.

– *Мета роботи, основні задачі (зміст роботи)*. Формулюють мету роботи і завдання, які необхідно вирішити для досягнення поставленої мети.

– *Об'єкт дослідження* - це процес або явище, що породжує проблемну ситуацію й обране для вивчення.

– *Предмет дослідження* міститься в межах об'єкта. Об'єкт і предмет дослідження як категорії наукового процесу співвідносяться між собою як загальне і часткове. В об'єкті виділяється та його частина, яка є предметом дослідження. Саме на нього спрямована основна увага ЗВО, оскільки предмет дослідження визначає тему курсової роботи.

– *Методи дослідження*. Наводяться використані методи дослідження для досягнення поставленої в роботі мети.

– *Практичне значення отриманих результатів*. У роботі прикладне значення – відомості про практичне застосування отриманих результатів або рекомендації щодо їх використання.

2.5 Основна частина курсової роботи

Основна частина роботи складається з послідовних розділів, підрозділів, пунктів та підпунктів. Кожний розділ починається з нової сторінки. У кінці кожного розділу формулюють висновки із стислим викладенням наведених у розділі наукових і практичних результатів.

Основна частина, як правило, містить:

– огляд літературних та інших інформаційних джерел за темою і вибір напрямків досліджень;

– обґрунтування і вибір теоретичних та експериментальних методів дослідження для вирішення поставлених задач;

– розроблення методики дослідження;

– аналіз основних науково-технічних результатів з точки зору вірогідності, практичної цінності і їх узагальнення;

– висновки до кожного розділу і загальні висновки до роботи.

Перший розділ містить теоретичне обґрунтування досліджуваних явищ та процесів в галузі криптографії. У цій частині КР викладається теоретична база, необхідна для вирішення визначеної проблеми, дається огляд джерел, нових розробок, опублікованих статистичних даних із посиланням на відповідні джерела.

На основі вивчення науково-технічної літератури розкриваються думки різних учених щодо розв'язання проблеми, обґрунтовуються погляди автора стосовно шляхів її вирішення.

Структурно складається з 2-4 підрозділів, містить теоретичний виклад важливих аспектів проблеми, критичний огляд джерел інформації, аналіз предмету дослідження.

Загалом, перший розділ повинен послідовно вирішувати такі задачі:

– розкриття сутності досліджуваного явища та його особливостей серед інших подібних явищ, при потребі - аналіз історії розвитку явища, його нормативно-правової бази;

– аналіз наукових та практичних підходів до аналізу обраного об'єкту дослідження;

– аналіз існуючої термінології у сфері дослідження, створення понятійно-категоріального апарату, на який автор спиратиметься у подальшій роботі;

– виявлення тих методів та інструментів, які можуть бути використані при дослідженні предмету роботи.

Обсяг першого розділу - у межах 25-30% від загального обсягу КР. Бажано закінчити цей розділ коротким резюме стосовно необхідності проведення досліджень у даній галузі.

Другий розділ має поєднувати набуті теоретичні знання та вміння використовувати обрані методи і певний методичний інструментарій на конкретних прикладах.

Зміст і структура даного розділу визначається темою і направлена на виявлення напрямів вдосконалення досліджуваної проблеми. Розділ має бути максимально насиченим фактичною інформацією (таблиці, графіки, діаграми, схеми), що відображають відповідні результати діяльності бази дослідження за останні 3-5 років. Аналітична частина завершується стислими висновками, в яких формулюють основні результати аналізу.

Обсяг другого розділу — у межах 35-40 % від загального обсягу КР.

У наступних розділах з вичерпною повнотою викладаються результати власних досліджень автора з висвітленням того нового, що він вносить у розробку проблеми (задачі).

Ця частина роботи повинна бути спрямована на розробку і обґрунтування пропозицій щодо предмету дослідження. Він повинен містити обґрунтовані практичні пропозиції студента, спрямовані на досягнення мети, поставленої у вступі.

2.6 Висновки

Висновки та пропозиції є стислим викладенням підсумків КР. У першому пункті висновків коротко оцінюють стан питання. Далі у висновках розкривають способи та результати розв'язання кожного із поставлених у вступі завдань. Наприкінці формулюють висновки та рекомендації щодо наукового та практичного використання здобутих результатів. Початок висновків доцільно починати із фрази "Проведено аналіз (далі "досліджено", "показано", "простежено", "виявлено", "окреслено", "виокремлено", "визначено", "обґрунтовано", "встановлено" "доцільно до впровадження" тощо).

Результати виконання кожного визначеного у вступі роботи завдання повинні бути відображені щонайменше в одному окремому пункті (смисловому блоці) висновків. Обсяг висновків і пропозицій не повинен перевищувати 2 сторінок.

2.7 Перелік посилань

Список посилань розміщується, починаючи з нової сторінки, і містить у собі тільки ті монографії, підручники, навчальні посібники, наукові статті тощо, що були використані під час виконання роботи та на які є посилання. Забороняється включати до переліку джерела, які не були реально використані у роботі.

Назви праць в списку використаних джерел зазначаються на мові оригіналу за бібліографічними правилами. Загальна кількість джерел повинна становити 10 -15 позицій.

Бібліографічний опис літературних (інформаційних) джерел складається за стандартоми ДСТУ ГОСТ 7.1:2006 «Система стандартів з інформації, бібліотечної та видавничої справи. Бібліографічний запис. Бібліографічний опис. Загальні вимоги та правила складання»; ДСТУ 3582:2013 «Інформація та документація. Бібліографічний опис. Скорочення слів і словосполучень українською мовою. Загальні вимоги та правила (ISO 4:1984, NEQ; ISO 832:1994, NEQ)»; ДСТУ ГОСТ 7.80:2007 «Бібліографічний запис. Заголовок. Загальні вимоги та правила складання»; ДСТУ 8302:2015 «Інформація та документація. Бібліографічне посилання. Загальні вимоги та правила складання».

Ці стандарти застосовується при складанні будь-яких звітів про наукові дослідження, включаючи курсові, дипломні та дисертаційні роботи.

Список використаних джерел розміщують у алфавітному порядку прізвищ авторів або в порядку посилання в тексті у хронологічному порядку.

Приклади оформлення бібліографічного опису у списках літератури при написанні випускної кваліфікаційної роботи:

Книги

Один автор

1. Тарнавський Ю.А. Технології захисту інформації: підручник для студ. спеціальності 122 «Комп'ютерні науки», спеціалізацій «Інформаційні технології моніторингу довкілля», «Геометричне моделювання в інформаційних системах» / Юрій Адамович Тарнавський. – Київ: КПІ ім. Ігоря Сікорського, 2018. – 162 с.

2. Корченко А. Г. Построение систем защити информации на нечетких множествах. Теория и практические решения / Александр Григорьевич Корченко. – К: МК-Пресс, 2006. – 320 с.

Два автори

3. Грайворонський М. В. Безпека інформаційно-комунікаційних систем / М.В. Грайворонський, О. М. Новіков. – К.: Видавнича група BHV, 2009. – 608с.

Три автори

4. Мехед Д. Б. Спеціальні глави математики: навч.посіб. для студ. спец. 125 "Кібербезпека" / Д. Б. Мехед, Ю. М. Ткач, В. М. Базилевич. – Ніжин: ФОП Лукяненко В.В. ТПК "Орхідея", 2018. – 124 с.

5. Даник Ю.Г. Основи кібербезпеки та кібероборони: підручник / П.П. Воробієнко, В.М. Чернега. – О.: ОНАЗ ім. О.С. Попова, 2018. − 228 с.

Чотири автори

6. Гур'єв В.І., Інформаційна безпека держави / В. І. Гур'єв, Д. Б. Мехед, Ю. М. Ткач, І. В. Фірсова. – Ніжин: ФОП Лукяненко В.В. ТПК "Орхідея", 2018. – 166 с.

П'ять і більше авторів

7. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби / В. Л. Бурячок, С.В. Толюпа, В.В. Семко [та ін.]; за ред. В.Л. Бурячка. – К. : ДУТ - КНУ, 2016. – 178 с.

Матеріали конференцій, семінарів

8. Аналіз загроз інформаційної безпеки в WI-FI мережах / Ю.М. Ткач, Д.Б. Мехед, В.М. Базилевич, Т.А. Петренко // Актуальні питання забезпечення кібербезпеки та захисту інформації: тези доповідей учасників II Міжнародної науково-практичної конференції (Закарпатська область, Міжгірський район, село Вернє Студене, туристичний комплекс «Едельвейс», 24-27 лютого 2016 року), К., 2016, С. 151–155.

Наукові статті

9. Петренко Т.А. Інформаційна безпека в сучасних умовах / Т.А. Петренко // Вісник Чернігівського державного інституту права, соціальних технологій та праці. – 2009. – №2. – С. 98–102.

10. Лахно В.А. Моделювання роботи адаптивної системи розпізнавання кібератак в умовах неоднорідних потоків запитів в модулях e-business / В.А. Лахно, Т.А Петренко і М.В. Пирог // Безпека інформації - 2016. - т. 22, № 2, с. 135–142.

Електронні ресурси

11. Інформаційна безпека [Електронний ресурс] / Wikipedia. – 2019. – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Інформаційна_безпека.

12. НД ТЗІ "Засоби активного захисту мовної інформації з акустичними та віброакустичними джерелами випромінювання. Класифікація та загальні технічні вимоги" [Електронний ресурс] // Державна служба спеціального зв'язку. - Київ. – 2000. – Режим доступу до ресурсу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=101924&cat_id=89734&ctime=1344501363205.

Патенти та авторські свідоцтва

13. Виявлення сканування портів на основі нечіткої логіки : Комп'ютерна програма / А.О. Корченко, Є.В. Іванченко, А.О. Охріменко та інші - К. : НАУ. - Свідоцтво про реєстрацію авторського права на твір №41897 від 23.01.2012.

14. Патент № 43779 України, МПК. Система передачі криптографічних ключів / Корченко О.Г., Паціра Є.В., Гнатюк С.О., Кінзерявий В.М.; заявник та патентовласник Національний авіаційний університет. - № u200904239; заявл. 29.04.2009; опубл. 25.08.2009, Бюл. №16. - 8 с.

Словники

15. Бабак В.П. Інформаційна безпека та сучасні мережеві технології : Англо-українсько-російський словник термінів / В.П. Бабак, О.Г. Корченко. - Київ: НАУ, 2003. - 670 с.

Закони та нормативні документи

16. Про електронні довірчі послуги[Текст]: Закон України 2155-VIII від 5 жовтня 2017р. / Верховна Рада України // Відомості Верховної Ради України. – 2017 р., № 45, стор. 5, Ст. 400.

Дисертації

17. Фуаре Е. В. Методологія захисту інформації на основі факторіального кодування даних : дис. докт. техн. наук : 05.13.21 / Фуаре Еміль Віталійович – НАУ. - Київ, 2019. – 477 с.

Автореферати дисертацій

18. Петренко Т. А. Методи та моделі експертних систем розпізнавання кібератак на основі кластеризації реалізацій ознак : автореф. дис. на здобуття наук. ступеня канд. техн. наук : спец. 05.13.21 "Системи захисту інформації" / Петренко Т. А. НАУ. - Київ, 2019. – 22 с.

Іншомовні видання

19. Lakhno V.A. Development of adaptive expert system of information security using a procedure of clustering the attributes of anomalies and cyber attacks / V. Lakhno, Y. Tkach, T. Petrenko, S. Zaitsev and V. Bazylevych, Eastern-European Journal of Enterprise Technologies, no. 6/9 (84), pp. 32–44, 2016.

20. Gnatyuk S.O. Prospects of quantum technologies implementation in security of e-banking systems in Ukraine / S. Gnatyuk, V. Kinzeryavyy, S. Prystayko, E. Didych // Science-based Technologies. - 2010. - №3. - P. 89-92.

У процесі написання роботи ЗВО повинен давати посилання на джерела, матеріали або окремі результати, які він наводить у роботі, або на яких ідеях і висновках розробляється проблема. Посилання в тексті подаються у квадратних дужках, де проставляється номер, під яким джерело значиться в переліку посилань, наприклад [1-3].

При посиланнях на розділи, підрозділи, пункти, підпункти, ілюстрації, таблиці, формули, рівняння, додатки зазначають їх номери. При посиланнях слід писати: “... у розділі 4 ...”, “... дивись 2.1 ...”, “... за 3.3.4 ...”, “... відповідно до 2.3.4.1 ...”, “... на рис. 1.3 ...” або “... на рисунку 1.3 ...”, “... у таблиці 3.2 ...”, “... (див. 3.2) ...”, “... за формулою (3.1) ...”, “... у рівняннях (1.23) - (1.25) ...”, “... у додатку Б ...”

2.10 Додатки

Додатки є необов'язковим елементом КР. Обсяг додатків не обмежується.

Додатки слід позначати послідовно великими літерами української абетки, за винятком літер Г, Ґ, Є, З, І, Ї, Й, О, Ч, Ь, наприклад, «Додаток Б». Кожний додаток розміщується з нової сторінки.

У додатках розміщують матеріал, який є необхідним для повноти роботи, але через великий обсяг чи способи подання не може бути розміщений в основній частині. Додатки можуть вміщати в себе 2 типи інформаційних матеріалів:

- громіздкі рисунки чи таблиці, які містять результати проведених досліджень, розмір яких не дозволяє включити їх в основний текст роботи.

- текстові або графічні інформаційні матеріали, таблиці, які доповнюють зміст роботи. Це можуть бути витяги із нормативних актів і документів, актів, угод і т.п., фотографії, карти, проміжні математичні докази та розрахунки, ілюстрації, методики та опис комп'ютерних програм, опис нового обладнання та приладів, що використовувались під час проведення експериментів, протоколи випробувань, звіти, окремі інструкції/положення/правила , тексти розроблених програм тощо. Таблиці та рисунки додатків нумеруються послідовно у кожному додатку окремо при ньому першою є літера позначення додатку, наприклад: Таблиця Б.2. друга таблиця «Додатку Б».

Обсяг додатків не обмежується, але повинен визначатись реальними потребами роботи. Якщо розміщений у додатках матеріал не є авторським, обов'язково потрібно вказувати посилання на джерело.

На додатки повинні бути посилання у тексті роботи: «користуючись даними таблиці, наведеної у додатку Б, визначимо …»

3 ВИМОГИ ДО ОФОРМЛЕННЯ РОБОТИ

3.1 Загальні вимоги до оформлення текстової частини

Загальний обсяг КР повинен бути у межах 20-30 сторінок формату А4. Допускається відхилення в межах ± 10 %. Курсова робота оформлюються відповідно до вимог ДСТУ 3008:2015 "Звіти у сфері науки і техніки. Структура та правила оформлення".

До загального обсягу роботи не входять сторінки, які повністю зайняті рисунком чи таблицею, «ДОДАТКИ» та «ПЕРЕЛІК ПОСИЛАНЬ», але сторінки всіх зазначених елементів роботи нумеруються на загальних засадах.

Сторінки текстової частини нумеруються арабськими числами. Номер сторінки проставляється у правому верхньому куті аркуша. Титульний аркуш включається до загальної нумерації сторінок, але номер на ньому не проставляється. Не ставиться номер сторінки також на таких структурних елементах, як «ЗАВДАННЯ», «РЕФЕРАТ», «ЗМІСТ».

Текстова частина виконується на одному боці аркушів білого паперу формату А4 (297х210 мм). Текст набирається на комп'ютері у будь-якому текстовому редакторі з використанням шрифту Times New Roman розміром 14 пунктів, міжрядковий інтервал - 1,5 (полуторний). З боків аркуша залишають поля: ліве - 25 мм, верхнє та нижнє - 20 мм, праве 10 мм. Абзацний відступ повинен бути однаковим впродовж всього тексту і дорівнювати 1,25 см.

Текст основної частини, в якій викладається суть дослідження, розділяється на розділи у відповідності до завдання.

Розділи завжди починаються з нової сторінки і повинні мати порядковий номер арабськими цифрами (1, 2, і т.д.) та назву. Заголовки розділів слід розміщувати посередині рядка і писати (друкувати) великими літерами без крапки в кінці. Після назви розділу обов’язково вставляється пустий рядок або встановлюється після-абзацний відступ 24 пт.

Розділи роботи можуть бути поділені на підрозділи. Вони нумеруються за розділами (наприклад, 2.1, 2.2 і т.д.) Написання назви підрозділів необхідно починати з абзацного відступу і писати (друкувати) малими літерами крім першої великої без крапки в кінці. Перед та після назви підрозділу обов’язково вставляється пустий рядок або встановлюється перед- та після-абзацний відступ 24пт.

Не допускається розміщувати назву розділу чи підрозділу в нижній частині сторінки, якщо після неї розміщено не більше одного рядка тексту.

Основний текст має бути чітким і не допускати різних тлумачень.

Стиль письмової наукової роботи - безособовий монолог. Бажано використовувати безособові конструкції речень (наприклад, «проведено вимірювання», «розроблено комплексний підхід», «застосовано метод»).

Культуру наукової мови визначають точність, ясність і стислість викладення думки. Варто уникати зайвої деталізації, повторів, тавтології.

Формули та рівняння набираються в редакторі MS Equation та розміщують безпосередньо після тексту, в якому вони згадуються, посередині з нового рядка посередині. Номер формули ставиться на її рівні в круглих дужках у крайньому

правому положенні у рядку і складається з номера розділу та порядкового номера формули, відокремленого крапкою

Наприклад, друга формула третього розділу:

$$\boldsymbol{L_i = R_{i-1}\,;\quad R_i = L_{i-1} \oplus F(R_{i-1}, K_i);} \qquad \boldsymbol{(3.2)}$$

Пояснення значень символів та числових коефіцієнтів, що входять до формули, слід наводити безпосередньо під формулою, з нового рядка у тій послідовності, в якій вони наведенні у формулі. У формулах та рівняннях латинські букви друкуються курсивом, крім математичних функцій.

До використаних формул надаються посилання на джерела, а до використаних числових значень - пояснення щодо їх походження.

Цифровий матеріал обумовлюється, як правило, у вигляді таблиці, яка розташовується після тексту, в якому вона згадується вперше, або на наступній сторінці. Таблиці зазвичай використовуються для представлення масиву числових та інших однотипних даних. Горизонтальні вертикальні лінії, які розмежовують рядки таблиці, а також лінії зліва, справа та знизу, що обмежовують таблицю, можна не проводити, якщо їх відсутність не ускладнює користування таблицею. Таблиці обов'язково нумерують та надають назву (наприклад: «Таблиця 2.1. Етапи розбиття простору ознак кібератаки на кластери - перша таблиця другого розділу). Номер та назва розміщуються зверху (над таблицею). Після назви з нового рядка розміщується сама таблиця, яка не може відриватись від назви та номеру (розміщуватись на іншій сторінці). (Додаток Ж)

Переліки, скорочення, виноски та примітки в тексті подають по-різному залежно від будови і значення. Розрізняють внутрішньо абзацні переліки та переліки з елементами-абзацами.

Внутрішньо абзацні переліки нумерують, літерують або виділяють графічно за допомогою тих чи інших символів. Перед переліком ставлять двокрапку, елементи переліку відділяють один від одного крапкою з комою і починають з малої літери, перед кожною позицією переліку доцільно ставити відповідний графічний знак або арабську цифру з дужкою - це так званий перший рівень підпорядкованості. Для інших рівнів підпорядкованості потрібно використовувати якийсь інший графічний знак або малі літери української абетки, після яких також ставлять дужку.

Скорочення слів і словосполучень дозволено робити тільки однотипні, загальновживані, відповідно до чинних стандартів з бібліотечної та видавничої справи. Розрізняють загальноприйняті скорочення, зрозумілі без додаткових пояснень, і умовні, тобто такі, які застосовують лише у спеціальній літературі.

Загальноприйняті скорочення: див. - дивися; рис. - рисунок; табл. - таблиця; р. - рік; рр. - роки; в. - вік; вв. - віки; ст. - століття; і т. д. - і так далі; і т. п. - і тому подібне; та ін. - та інше; ун-т - університет; тис. - тисяча; напр. - наприклад.

Усі умовні скорочення варто розшифровувати у тексті. Перший раз слово або словосполучення пишуть повністю, а в дужках наводять скорочення, наприклад, аналіз та оцінка ризиків (АОР); інформаційна безпека (ІБ); інформаційний ресурс (ІР).

Скорочення мають бути уніфіковані. Неприпустимо скорочувати те саме слово по-різному або писати в одному місці повністю, а в другому - скорочено.

Виноски використовують для пояснення фрагментів тексту або як коментар до якого-небудь слова.

Виноски поділяють на звичайні і кінцеві. Звичайну виноску розташовують внизу сторінки, кінцеву - в кінці розділу або документа. Звичайні виноски позначають переважно цифрами (арабськими), зірочками (*) чи іншими знаками, а кінцеві виноски позначають цифрами.

Примітки - це додаткові пояснення чи зауваження до тексту. Їх розташовують безпосередньо після тексту, таблиці, ілюстрації, яких вони стосуються. Текст примітки відокремлюють від основного тексту порожнім рядком і набирають шрифтом, меншим від основного. Слово «Примітка» друкують з великої літери з абзацного відступу, не підкреслюють, після нього ставлять крапку і з великої літери у тому ж рядку подають текст примітки, наприклад:

Примітка. Утім варто зазначити, що вибір матеріалу...

Виділення в тексті застосовують для того, щоб підкреслити головні положення, зробити логічний наголос на окремих словах або реченнях тощо. Найчастіше виділяють текст світлим курсивом або розрядкою. Не рекомендується занадто велика кількість виділень, оскільки текст стає строкатим.

3.2 Вимоги до оформлення графічної частини

Графічну частину КР складають ілюстрації або презентації. До ілюстрацій відносяться схеми, графіки, діаграми, графічне зображення алгоритмів, фотознімки тощо. Кількість ілюстрацій, не обмежується.

Під час виготовлення графічної частини використовують комп'ютерну графіку.

Демонстраційні аркуші виконуються у вигляді слайдів. Ілюстрацію, розміщують безпосередньо після тексту, де вона згадується вперше, або на наступній сторінці.

У текст роботи можуть включатись рисунки, які ілюструють окремі її положення або унаочнюють певні дані (наприклад, це можуть бути діаграми, графіки, схеми тощо). Ілюстрації слід розмішувати так, щоб їх, можна було розглядати без повороту аркуша з текстом. Якщо таке розміщення неможливе, ілюстрації розміщують так, щоб для їх розгляду треба було б повернути аркуш за годинниковою стрілкою на 90°.

Усі ілюстрації називаються рисунками, їх обов'язково нумерують за розділами та надають назву (наприклад: Рисунок 1.1. Зміна ентропії системи залежно від довжини переданих мережних пакетів). Підпис не може відриватись від самого рисунку (розміщуватись на іншій сторінці). Номер та назва розміщуються внизу. (Додаток К)

Вимоги щодо оформлення рисунків та підписів: абзацний відступ відсутній; вирівнювання — по центру; шрифт — звичайний; крапка в кінці назви рисунку не ставиться.

На всі ілюстрації та таблиці необхідні посилання в текстовій частині. При цьому можна застосувати скорочення - рис. 1.1, табл. 4.2. У випадку використання ілюстрації, створеної іншим автором, необхідно надати посилання на джерело.

Якщо під час виконання роботи була розроблена комп'ютерна програма, то в КР необхідно привести блок-схему алгоритму, текст програми, надрукований на принтері, тестовий розрахунок, мову програмування, методику користування програмою. Аркуші з текстом програми розміщують або в основній частині, або в якомусь додатку, якщо програма громіздка.

4. КРИТЕРІЇ ОЦІНЮВАННЯ КУРСОВОЇ РОБОТИ

Оцінювання здійснюється за модульно-рейтинговою системою. Максимальний рейтинг кожного ЗВО складається з оцінювання в балах за всіма критеріями, виставляється під час захисту і переводиться в оцінку за Європейською системою трансферу оцінок ECTS:

90–100 балів — A — "відмінно"
82–89 балів — B — "дуже добре"
75–81 бали — C — "добре"
67–74 бали — D — "достатньо"
60–66 бали — E — "задовільно"
Менше 60 балів — FX — "незадовільно"/

Таблиця 4.1.

Критерії оцінювання результатів виконання та захисту ВКР

№	Критерії	Макс. кіл.балів	Зміст критеріїв оцінювання	Оцінка в Балах
1.	Актуальність теми, її відповідність сучасним вимогам	10	- відповідає повністю - відповідає неповністю - відповідає недостатньо - відповідність відсутня	10 7 3 0/3
2.	Повнота, науковий рівень обґрунтування розробок та запропонованих рішень	30	- повно та обґрунтовано - недостатньо - неповно і недостатньо - відповідь відсутня/незадовільна	30 14 10 0/5
3.	Відповідність ВКР нормативним актам України, державним стандартам; якість оформлених матеріалів	10	- достатньо повна, висока якість - недостатньо повна, прийнятна якість - недостатньо повна, низька якість - не відповідає, низька якість	10 7 5 0/3
4.	Змістовність доповіді та відповідей на запитання членів екзаменаційної комісії під час Захисту	40	- повні, послідовні, логічні - недостатньо повні, послідовні, логічні - непослідовно та нелогічно побудована доповідь, недостатньо повні відповіді на запитання - відповідь на запитання відсутня або незадовільна	40 32 24 0/7

	Разом:	**100**		

ІНФОРМАЦІЙНІ ДЖЕРЕЛА

1. Бібліографічний запис. Бібліографічний опис. Загальні вимоги та правила складання: ДСТУ ГОСТ 7.1:2006. Чинний від 07.01.2007. - К. : Держспоживстандарт України, 2007. - 47 с.
2. ДСТУ 3008:2015 "Звіти у сфері науки і техніки. Структура та правила оформлення".
3. ДСТУ 3582:2013 «Інформація та документація. Бібліографічний опис. Скорочення слів і словосполучень українською мовою. Загальні вимоги та правила»
4. ДСТУ ГОСТ 7.1:2006 «Система стандартів з інформації, бібліотечної та видавничої справи. Бібліографічний запис. Бібліографічний опис. Загальні вимоги та правила складання»;
5. Методичні рекомендації щодо виконання та оформлення випускних кваліфікаційних робіт (проектів) здобувачів вищої освіти освітніх ступенів «бакалавр» і «магістр» Чернігівського національного технологічного університету. – ЧНТУ: Чернігів, 2016. - 15 с.
6. Оформлення наукових джерел відповідно до вимог Вищої атестаційної комісії України [Електронний ресурс] // Вища атестаційна комісія України. – 2019. – Режим доступу до ресурсу: https://vak.in.ua.
7. Стандарт вищої освіти України: перший (бакалаврський) рівень вищої освіти, галузь знань 12 - інформаційні технології, спеціальність 125- Кібербезпека. - Наказ Міністерства освіти і науки України №1074 від 04.10.2018.
8. Ткач Ю. М. Мультимедійні презентації як засіб підвищення ефективності навчального процесу. Навчально-методичний посібник / Ю. М. Ткач, Т. А. Петренко. – Чернігів: ЧДІПСТіП, 2010. – 58 с.

Додаток А. Перелік тем курсових робіт.

Тема: **Статистичні властивості мови та критерії відкритого тексту. Їх використання в криптоаналізі та дешифруванні.**

Замовник: кафедра кібербезпеки та математичного моделювання Національного університету «Чернігівська Політехніка».

Мета: вивчення статистичних властивостей різних видів інформації, що підлягають закриттю (моделі даних, можливі критерії відкритого тексту тощо).

Завдання:

- дослідити частотні характеристик мови (української та англійської);
- побудувати модель відкритого тексту та критерій на відкритий текст;
- дослідити статистичні особливості тестових та нетекстових повідомлень;
- вивчити шляхи застосування моделей мови у дослідженнях криптографічних алгоритмів заміни та перестановки.

2

Тема: **Розробка програмного лабораторного модуля «Вивчення найпростіших алгоритмів шифрування”**.

Замовник: кафедра кібербезпеки та математичного моделювання Національного університету «Чернігівська Політехніка».

Мета: вивчення основних моноалфавітних та поліалфавітних алгоритмів шифрування та на основі отриманих знань створити універсальний програмний комплекс шифрування та дешифрування з навчальними елементами.

Завдання:

- вивчити моноалфавітні та поліалфавітні алгоритми шифрування;
- розробити довідкову систему з алгоритмів шифрування;
- запропонувати можливі способи вивчення найпростіших алгоритмів шифрування за допомоги розробленого програмного комплексу;
- підготувати відповідні проекти лабораторних робіт.

3

Тема: **Проведення порівняльного аналізу ефективності сучасних програмних, програмно-апаратних та апаратних засобів криптографічного захисту.**

Замовник: кафедра кібербезпеки та математичного моделювання Національного університету «Чернігівська Політехніка».

Мета: вивчення основних типів засобів забезпечення криптографічного захисту та розробити практичні рекомендації щодо вимог до криптосистеми та її розгортання на об’єкті господарювання.

Завдання:

- сформувати систему показників ефективності та основні вимоги до криптосистеми;

- провести порівняльний аналіз ефективності сучасних програмних, програмно-апаратних та апаратних засобів криптографічного захисту у відповідності з обраними критеріями;
- сформувати практичні рекомендації до вибору засобів криптографічного захисту на обраному об’єкті господарювання;
- запропонувати схему криптографічного захисту на обраному об’єкті господарювання.

4

Тема: **Методи криптографічного захисту інформації в клієнт-серверній архітектурі.**

Замовник: кафедра кібербезпеки та математичного моделювання Національного університету «Чернігівська Політехніка».

Мета: дослідження особливостей застосування криптографічних методів захисту інформації в клієнт-серверній архітектурі.

Завдання:
- вивчити особливості технології «клієнт-сервер»;
- проаналізувати актуальні атаки на безпеку в клієнт-серверних застосуваннях, їх ефективність та способи захисту;
- запропонувати варіант схеми криптозахисту інформації в клієнт-серверній архітектурі.

5

Тема: **Використання криптографічних інтерфейсів для забезпечення безпеки зберігання та передачі інформації.**

Замовник: кафедра кібербезпеки та математичного моделювання Національного університету «Чернігівська Політехніка».

Мета: закріпити теоретичні знання про криптографічні засоби захисту інформації та практичні навички роботи з криптографічними інтерфейсами.

Завдання:
- ;
- .

6

Тема: **Застосування алгоритмів шифрування та електронного цифрового підпису в автоматизованій системі електронного документообігу.**

Замовник: кафедра кібербезпеки та математичного моделювання Національного університету «Чернігівська Політехніка».

Мета: дослідження особливостей застосування криптографічного захисту в автоматизованій системі електронного документообігу.

Завдання:
- аналіз видів шифрування для створення електронного цифрового підпису (ЕЦП);

– аналіз вимог до ЕЦП;
– застосування кваліфікованих електронних підписів;
– аналіз методів криптографічного захисту електронної пошти та баз даних.

7

Тема: **Проектування підсистеми криптографічного захисту інформації підприємства.**

Замовник: кафедра кібербезпеки та математичного моделювання Національного університету «Чернігівська Політехніка».

Мета: розробка проекту підсистеми криптографічного захисту інформації підприємства.

Завдання:
– провести аналіз установи щодо необхідності захисту інформації;
– вивчити нормативні правові акти, що регулюють створення та застосування криптографічних засобів;
– вивчити криптографічні засоби, обрані для побудови підсистеми криптографічного захисту інформації;
– розробити проект підсистеми криптографічного захисту;
– підготувати перелік організаційно-розпорядчі документи, необхідних для функціонування підсистеми криптографічного захисту інформації.

8

Тема: **Застосування булевих функцій у криптографії.**

Замовник: кафедра кібербезпеки та математичного моделювання Національного університету «Чернігівська Політехніка».

Мета: дослідження властивостей булевих функцій як структурних елементів блочних і поточних шифрів та відомих криптографічних ґеш-функцій.

Завдання:
– вивчити основні криптографічні властивості булевих функцій (кореляційна та алгебраїчна імунність, нелінійність, лавинні характеристики тощо);
– дослідити застосування булевих функцій у сучасних шифрах та ґеш-функціях;
– провести огляд існуючих програмних засобів дослідження булевих функцій.

9

Тема: **Аналіз методів та механізмів автентифікації в криптосистемах.**

Замовник: кафедра кібербезпеки та математичного моделювання Національного університету «Чернігівська Політехніка».

Мета: дослідження сучасних систем і засобів автентифікації та їх застосування в системах криптографічного захисту інформації.

Завдання:
– описати область застосування механізму автентифікації та її важливість для захисту інформації;

– провести класифікацію сучасних систем і засобів автентифікації;
– дослідити сутність і вимоги до протоколів автентифікації;
– дослідити моделі протоколів автентифікації та оцінити їх вразливість.

10

***Тема*: Дослідження властивостей автентифікації користувачів за допомогою алгоритму RC6.**

Замовник: кафедра кібербезпеки та математичного моделювання Національного університету «Чернігівська Політехніка».

Мета: вивчення сучасних протоколів автентифікації абонента та виконати програмну реалізацію одного з них.

Завдання:
– дослідити алгоритм автентифікації за алгоритмом RC6;
– розробити їх програмну реалізацію;
– створити зручний інтерфейс користувача програми.

11

***Тема:* Засоби автентифікації користувачів за протоколами Шнорра та Окамото.**

Замовник: кафедра кібербезпеки та математичного моделювання Національного університету «Чернігівська Політехніка».

Мета: вивчення сучасних протоколи автентифікації абонента та виконати програмну реалізацію одного з них.

Завдання:
– вивчити та провести порівняльний аналіз автентифікації за протоколами Шнорра та Окамото;
– розробити їх програмну реалізацію;
– створити зручний інтерфейс користувача програми.

12

***Тема:* Засоби для автентифікації даних за допомогою алгоритму SHA-3.**

Замовник: кафедра кібербезпеки та математичного моделювання Національного університету «Чернігівська Політехніка».

Мета: вивчення сучасних алгоритмів автентифікації та виконати програмну реалізацію одного з них.

Завдання:
– дослідити алгоритм автентифікації за алгоритмом SHA-3;
– розробити їх програмну реалізацію;
– створити зручний інтерфейс користувача програми.

13

Тема: **Розробка системи автентифікації співробітників компанії на основі криптографічних методів.**

Замовник: кафедра кібербезпеки та математичного моделювання Національного університету «Чернігівська Політехніка».

Мета: дослідження особливості організації автентифікації на основі криптографічних методів та запропонувати систему багатофакторної автентифікації співробітників компанії.

Завдання:

- проаналізувати застосування методів та механізмів автентифікації;
- провести порівняльний аналіз методів та протоколів автентифікації;
- запропонувати систему багатофакторної автентифікації співробітників компанії, у тому числі з використанням криптографічних методів.

14

Тема: **Побудова доказово простих чисел та реалізація програмного пакету тестів перевірки на простоту.**

Замовник: кафедра кібербезпеки та математичного моделювання Національного університету «Чернігівська Політехніка».

Мета: вивчення основних принципів створення класу великих чисел і роботи з ним, практичного застосування ймовірнісних та детерміністичних тестів на простоту, уміння розраховувати необхідну кількість ітерацій тесту для досягнення заданої імовірності помилки.

Завдання:

- дослідити основні принципи створення класу великих чисел і роботи з ним;
- дослідити способи отримання простих чисел та теоретико-числові принципи, на яких засновані тести на простоту;
- вивчити відмінність ймовірнісних і детерміністичних тестів на простоту.
- провести оцінку надійності тестів на простоту та їх швидкодії;
- реалізувати пакет тестів для побудови доказово простих чисел.

15

Тема: **Оцінка якості генераторів псевдовипадкових послідовностей.**

Замовник: кафедра кібербезпеки та математичного моделювання Національного університету «Чернігівська Політехніка».

Мета: дослідження якості генераторів псевдовипадкових послідовностей, що базуються на теоретико-числових проблемах.

Завдання:

- дослідити властивості генераторів псевдовипадкових послідовностей Dual EC DRBG та Мікалі-Шнорра;
- запропонувати систему критеріїв якості детермінованих генераторів випадкових чисел;
- розробити програмну реалізацію генераторів Dual EC DRBG та Мікалі-Шнорра;

– розробити програму оцінки якості генератора за допомоги зображень.

16

Тема: **Оцінка ефективності криптографічних генераторів, заснованих на алгоритмах Фібоначчі та BBS.**

Замовник: кафедра кібербезпеки та математичного моделювання Національного університету «Чернігівська Політехніка».

Мета: дослідження якості генераторів псевдовипадкових послідовностей, заснованих на алгоритмах Фібоначчі та BBS.

Завдання:

– дослідити властивості генераторів псевдовипадкових послідовностей, заснованих на алгоритмах Фібоначчі та BBS;
– розробити програмну реалізацію Фібоначчі та BBS;
– запропонувати метод оцінки якості генератора.

17

Тема: **Застосування криптографічних методів захисту інформації на різних рівнях моделі OSI.**

Замовник: кафедра кібербезпеки та математичного моделювання Національного університету «Чернігівська Політехніка».

Мета: дослідження застосування криптографічних засобів захисту на різних рівнях моделі OSI та запропонувати комплект засобів криптозахисту для обраної інформаційної системи.

Завдання:

– проаналізувати рівні моделі OSI, взаємозв’язки між ними та можливості їх криптографічного захисту;
- запропонувати комплект засобів криптозахисту для обраної інформаційної системи.

18

Тема: **Дослідження властивостей поточних шифраторів на основі регістрів зсуву з зворотнім зв’язком».**

Замовник: кафедра кібербезпеки та математичного моделювання Національного університету «Чернігівська Політехніка».

Мета: дослідження особливості застосування регістрів зсуву у криптографічному захисті.

Завдання:

– вивчити особливості побудови поточних шифраторів та генераторів псевдовипадкових чисел, побудованих за допомогою регістрів зсуву з зворотнім лінійним або нелінійним зворотнім зв’язком;

– дослідити статистичні властивості послідовностей, які генеруються регістрами зсуву з зворотнім зв’язком;
– запропонувати схему поточного шифратора на основі комбінації регістрів зсуву та оцінити його якість.

19

Тема: **Розробка програмного лабораторного модуля «Шифрування-дешифрування інформації потоковим шифром RC5”.**

Замовник: кафедра кібербезпеки та математичного моделювання Національного університету «Чернігівська Політехніка».

Мета: вивчення сучасних потокових шифрів та виконання програмної реалізації одного з них.

Завдання:
– вивчити та дослідити блоковий криптоалгоритм RC5;
– розробити програмну реалізацію криптоалгоритма RC5;
– створити зручний інтерфейс користувача програми.

20

Тема: **Розробка програмного лабораторного модуля «Шифрування-дешифрування інформації блоковим криптоалгоритмом AES”.**

Замовник: кафедра кібербезпеки та математичного моделювання Національного університету «Чернігівська Політехніка».

Мета: вивчення сучасних блокових шифрів та виконання програмної реалізації одного з них.

Завдання:
– вивчити та дослідити блоковий криптоалгоритм AES;
– розробити програмну реалізацію криптоалгоритма AES;
– створити зручний інтерфейс користувача програми.

21

Тема: **Розробка програмного лабораторного модуля «Шифрування-дешифрування інформації блоковим криптоалгоритмом ДСТУ 7624:2014 («Калина»)”.**

Замовник: кафедра кібербезпеки та математичного моделювання Національного університету «Чернігівська Політехніка».

Мета: вивчення сучасних блокових шифрів та виконання програмної реалізації одного з них.

Завдання:
– вивчити та дослідити блоковий криптоалгоритм «Калина»;
– провести порівняльний аналіз алгоритмів «Калина» та AES;
– розробити програмну реалізацію криптоалгоритма «Калина»;
– створити зручний інтерфейс користувача програми.

22

Тема: **Розробка програмного лабораторного модуля «Шифрування-дешифрування інформації асиметричним криптоалгоритмом RSA”.**

Замовник: Кафедра кібербезпеки та математичного моделювання Національного університету «Чернігівська Політехніка».

Мета: забезпечення студентів кафедри програмним комплексом та методичними матеріалами, що дозволяють досліджувати стійкість криптоситеми RSA.

Завдання:

- вивчити такі види атак на криптосистему RSA як:
  - безключове читання RSA,
  - атака на підпис RSA у схемі з нотаріусом,
  - атака на підпис RSA за обраним шифртекстом;
- розробити програмний лабораторний модуль «Експериментальне дослідження стійкості криптосистеми RSA»;
- підготувати проекти лабораторних робіт, які можуть бути виконані з використанням розробленого програмного комплексу.

23

Тема: **Розробка програмного лабораторного модуля «Шифрування-дешифрування інформації асиметричним криптоалгоритмом Ель Гамаля”.**

Замовник: кафедра кібербезпеки та математичного моделювання Національного університету «Чернігівська Політехніка».

Мета: забезпечення студентів кафедри програмним комплексом та методичними матеріалами, що дозволяють вивчити асиметричний криптоалгоритм Ель Гамаля.

Завдання:

- вивчити та дослідити асиметричний криптоалгоритм Ель Гамаля;
- провести порівняльний аналіз алгоритмів Ель Гамаля та RSA;
- розробити програмну реалізацію шифрування-дешифрування інформації асиметричним криптоалгоритмом Ель Гамаля.

24

Тема: **Розробка програмного лабораторного модуля «Генерування та обмін сеансовими ключами за протоколом Діффі-Хеллмана”.**

Замовник: кафедра кібербезпеки та математичного моделювання Національного університету «Чернігівська Політехніка».

Мета: вивчення сучасних блокових шифрів та виконання програмної реалізації одного з них.

Завдання:

- дослідити задачу Діффі-Хеллмана та проблему дискретного логарифмування;

– розробити програмну реалізацію генерування та обміну сеансовими ключами за протоколом Діффі-Хеллмана;
– створити зручний інтерфейс користувача програми.

25

Тема: **Розробка схеми контролю цілісності програмних та інформаційних ресурсів на основі криптографічних перетворень.**

Замовник: кафедра кібербезпеки та математичного моделювання Національного університету «Чернігівська Політехніка».

Мета: дослідження застосування криптографічних методів для контролю цілісності та справжності програмних та інформаційних ресурсів.

Завдання:
– проаналізувати можливості контролю цілісності й справжності програмних та інформаційних ресурсів на основі криптографічних перетворень;
– побудувати систему захисту від загроз порушення цілісності та справжності програмних та інформаційних ресурсів.

26

Тема: **Порівняльний аналіз алгоритмів формування функцій ґешування**.

Мета: дослідження застосування криптографічних функцій ґешування для контролю цілісності інформаційних ресурсів.
- Проаналізувати вимоги до функцій ґешування;
- Проаналізувати сучасні алгоритми формування функцій ґешування;
- Провести порівняльний аналіз декількох підходів.

27

Тема: **Розробка протоколу спільного підписання контракту у разі наявності арбітра.**

Замовник: кафедра кібербезпеки та математичного моделювання Національного університету «Чернігівська Політехніка».

Мета: дослідження застосування криптографічних протоколів при електронному доументообігу.

Завдання:
– проаналізувати можливі проблеми при спільному підписанні контракту, які вимагають звернення до арбітра;
– розробити протокол спільного підписання контракту при наявності арбітра.

28

Тема: **Розробка протоколу групового підписання документу на основі стандартів ЕЦП.**

Замовник: кафедра кібербезпеки та математичного моделювання Національного університету «Чернігівська Політехніка».

Мета: дослідження застосування криптографічних протоколів при електронному доументообігу.

Завдання:

- проаналізувати проблеми, які можуть виникати при груповому підписання документу;
- розробити протокол групового підписання документу на основі стандартів ЕЦП.

29

Тема: **Розробка протоколу сліпого підписання документу на базі алгоритму Ель Гамаля та її програмна реалізація.**

Замовник: кафедра кібербезпеки та математичного моделювання Національного університету «Чернігівська Політехніка».

Мета: дослідження застосування криптографічних протоколів при електронному доументообігу.

Завдання:

- проаналізувати проблеми, які можуть виникати при сліпому підписані документу та шляхи їх подолання;
- розробити протокол сліпого підписання документу на основі стандартів ЕЦП.

Додаток Б - Титульний аркуш курсової роботи

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НУ «Чернігівська політехніка»
Навчально-науковий інститут електронних та інформаційних технологій
Кафедра кібербезпеки та математичного моделювання

КУРСОВА РОБОТА

30

_____

(тема роботи)

_____

_____

(шифр і назва спеціальності)

_____

(галузь знань)

Виконавець: студент групи _____

_____ _____

(підпис) *(ініціали, прізвище)*

Керівник: _____

(науковий ступінь, вчене звання, посада)

_____ _____

(підпис) *(ініціали, прізвище)*

Чернігів – 202__

Додаток В – Приклад написання реферату курсової роботи

РЕФЕРАТ

Курсова робота складається зі вступу, трьох розділів, висновку, списку використаних джерел, додатків, загальним обсягом робота складає 25 сторінок, має 4 рисунків, 2 таблиці, 6 сторінок додатків. Список використаних джерел має 12 найменувань.

Метою курової роботи є дослідження можливостей системи автентифікованого шифрування на базі *sponge*-функцій.

У роботі розглядається алгоритм автентифікованого шифрування на базі sponge-функції, який дозволяє одночасне виконання шифрування інформації та її автентифікацію. Алгоритми такого типу виявились в реалізації більш ефективними по швидкості, можуть вдало бути реалізовані на сучасних ПЛІС. Проведено аналіз стійкості обраного алгоритму до атаки типу "компроміс час-пам’ять" та деяких інших базових атак.

АВТЕНТИФІКОВАНЕ ШИФРУВАННЯ, SPONGE-ФУНКЦІЯ, СТІЙКІСТЬ КРИПТОАЛГОРИТМУ НА БАЗІ SPONGE-ФУНКЦІЇ.

Додаток Д – Приклад написання вступу курсової роботи

ВСТУП

Актуальність. Бурхливий розвиток інформаційних технологій, що розпочався наприкінці минулого сторіччя, та впровадження автоматизованих методів і засобів обробки інформації практично в усі сфери діяльності людей призвели до необхідності більш широкого використання криптографічних засобів захисту інформації, в першу чергу, для її передачі й зберегання. До криптографічних засобів захисту інформації з кожним роком, окрім стандартних вимог, стають більш жорсткіши вимоги щодо їх продуктивності, криптостійкості, універсальності.

Криза в галузі криптографії, що була пов'язана зі стійкістю хеш-функцій, найяскравіше проявилася в середині 2000-х років та змусила американський інститут стандартів і технологій (NIST) оголосити конкурс на створення нового стандарту хешування (англ. Secure Hash Standart, SHS).

У ході конкурсу поширились та широко обговорювались різні ідеї, пов'язані з дизайном як самих хеш-функцій, так і симетричних криптопримітивів загалом. Особливо цікавим явищем стало те, що у фіналі конкурсу з п'яти фіналістів двоє виявилися універсальними криптопримітивами, які можуть використовуватися не тільки для хешування, а й для виконання багатьох інших криптографічних операцій. Це може призвести на практиці до значного спрощення криптографічних протоколів, як уже існуючих, так і проектованих.

У 2012 році офіційним переможцем конкурсу став алгоритм *Keccak* (вимовляється як "Ketchak") та отримав ім'я хеш-функції *SHA-3*.

Автори алгоритму впровадили низку радикальних рішень, у тому числі вони вирішили не використовувати функцію стиснення у вигляді окремого будівельного блоку, а як стійке криптоперетворення запропонували сконструювати безключову псевдовипадкову перестановку *PRP* (Pseudo Random Permutation). Все це вони запакували у дуже просту конструкцію *Sponge* (від англ. "Губка"), яку автори вперше представили ще у 2007 році на конференції *ECRYPT Hash function* як альтернативу традиційному дизайну Меркла-Дамгора.

Sponge-функції відносяться до *LRX*-класу криптографічних перетворень і можуть ефективно реалізуватися на програмованих логічних інтегральних схемах, тому що в них задіяні тільки логічні операції (*L*), циклічні зсуви (*R*) та виключні або - *XOR* (*X*). Це дає їм переваги при створенні разноманітних криптоалгоритмів (поточного шифрування, генерації псевдовипадкових чисел, хешування, імітозахисту, тощо) та високопродуктивних засобів криптографічного захисту інформації.

З вищесказаного напрошується висновок, що дослідження та оцінювання нових рішень в сфері криптографії, у тому числі алгоритмів автентифікованого шифрування на базі *sponge*-функцій, завжди є актуальними у зв'язку з можливим їх застосуванням для задач безпеки сучасного кіберпростору.

Метою курсової роботи є дослідження високопродуктивного криптографічного алгоритму шифрування з одночасним імітозахистом на базі *sponge*-функції.

Для досягнення мети потребується розв'язати такі ***завдання***:

- провести аналіз сучасних підходів до побудови автентифікованих систем шифрування;
- дослідити основні схеми *sponge*-функцій та алгоритми шифрування і імітозахисту на їх основі, запропонувати алгоритм для реалізації;
- оцінити надійність обраного алгоритму, його стійкість до базових атак.

Об'єкт дослідження: процес захисту інформації автентифікованими системами шифрування.

Предмет дослідження: криптографічний алгоритм на базі *sponge*-функції.

Оцінка сучасного стану проблеми на основі вітчизняної та зарубіжної літератури. Після конференції *ECRYPT Hash function* значний внесок у розробку теорії автентичного шифрування внесли іноземні вчені М. Беллар, Ч. Нампремпре, В. Глігор, П. Донеску, [1]. Питаннями щодо *sponge*-функцій щільно займаються закордонні вчені Г. Бертоні, Дж. Даємен, М. Пітерс, М. Боровський, В. Марчук, [2-5].

Досліджень вітчизняних вчених з даного питання майже немає, за виключенням кількох праць фахівців з НУ «Чернігівська політехніка»: М. Шелест, Ю. Ткач, С. Семендяй, М. Синенко [6].

У працях зазначених авторів досить повно розглянута теоретична база побудови криптографічних систем, застосування конструкцій та схем *sponge*-функцій, у тому числі властивостей систем автентифікованого шифрування.

Виявилось, що додатково до класичного гешування, *sponge*-функція може використовуватися також для організації деревоподібного хешування, потокового шифрування, імітозахисту, генерації псевдовипадкових чисел, організації захищених з'єднань. Використання ітераційних конструкцій типу *sponge* є альтернативним підходом у побудові алгоритмів автентифікованого шифрування.

Sponge-функція *Bash-f* допускає ефективну реалізацію на мікросхемах ПЛІС. Є передумови створення на основі *Bash-f* високопродуктивних алгоритмів потокового шифрування та імітозахисту у стилі *PBC*. Важливо, що у цих алгоритмах замість *Bash-f* можна використовувати іншу більш надійну та ефективну *sponge*-функцію – структура алгоритмів не зміниться.

Основними параметрами, за якими оцінюють алгоритм шифрування, зазвичай, є його стійкість до атак, направлених на розшифрування шифртексту (відновлення ключа шифрування), та швидкодія процесу шифрування. У випадку з алгоритмом автентифікованого шифрування, додається ще оцінювання його стійкості щодо атак, направлений на порушення цілісності (підробка імітовставки). Як правило, оцінюють стійкість алгоритму як до відомих атак загального призначення, наприклад, *tradeoff*-атаки, так і до базових атак, що розробляються спеціально під певний алгоритм.

Питання оцінювання стійкості алгоритмів автентифікаційного шифрування ще не в повній мірі вивчено у працях дослідників, саме це і буде однією з цілей даної роботи.

Галузь застосування – підвищення загального рівня кібербезпеки об'єкту, шляхом застосування розглянутого типу алгоритмів автентичного шифрування на базі *sponge*-функцій у взаємодії із іншими методами захисту інформації.

Новизна. Вивчено стійкість алгоритму щодо різних видів *tradeoff*-атак. Незважаючи на те, що обчислювальна складність *tradeoff*-атак менше, ніж атаки "брутальної сили", необхідні для її успішного проведення об’ємів пам’яті та кількості префіксів є достатньо великими. Тому застосування на практиці такої атаки є малоймовірним.

Практична цінність полягає у тому, що отримана оцінка стійкості алгоритму автентифікованого шифрування на базі *sponge*-функції до ряду відомих атак підтверджують, що він є стійким.

Додаток Е – Приклад написання висновку до курсової роботи

ВИСНОВКИ

1. Проведений аналіз відомих конструкцій та схем, побудованих на базі *sponge*-функцій, виявив, що найбільш перспективними схемами є схеми SpongeWrap та DuplexWrap.
2. Сконструйовані алгоритми шифрування та імітозахисту (автентичного шифрування) на базі *sponge*-функції ***Bash-f***, які побудовані по схемі SpongeWrap / DuplexWrap.
3. Розроблені алгоритми представлені криптографічним автоматом. Обгрунтовані принципи побудови та роботи автомата. Показано, як використовувати автомат для організації захищених з'єднань.
4. Проведена оцінка стійкості розроблених алгоритмів автентичного шифрування до універсальної атаки «компроміс час-пам'ять» та до базових атак. Отримані оцінки показують, що розроблені алгоритми є стійкими.
5. Проведена порівняльна оцінка швидкодії показала переваги над аналогічними стандартними алгоритмами.

Додаток Ж – Приклад оформлення таблиці

Таблиця 1.3.

Порівняльна характеристика методів виявлення кібератак

№	Математичний апарат	Нечіткі кібератаки, можливість адаптації до помилок під час завдання на прийняття рішення в ході процедур машинного навчання	База даних	Кількість вхідних параметрів	Пошук вторгнень та нормальної поведінки, %	Пошук нових ознак
1	Ієрархічна самоорганізуюча карта	–	KDD– 99	41	Norm–96,4; DoS–96,2; U2R–37,1; R2L–43,1; Probe–94,3	–
2	Метод опорних векторів	–			Norm–99,8; DoS–97,5; U2R–86,6; R2L–81,3; Probe–92,8	–
3	Кластерні моделі на основі алгоритму DBSCAN	–			Norm–96,2; DoS–98,2; U2R–72,2; R2L–84; Probe–81,0	+
4	Гібридні нейроні мережі	+			Norm–96; DoS–98,8; U2R–72,8; R2L–33,45; Probe–86,2	+

5	Метод інтелектуальної технології машинного навчання та модель кластеризації реалізацій ознак для експертних систем	+		10–12	Norm–98,7; DoS–99,1; U2R–76,5; R2L–90; Probe–84,2	+

Додаток З – Приклад оформлення рисунків

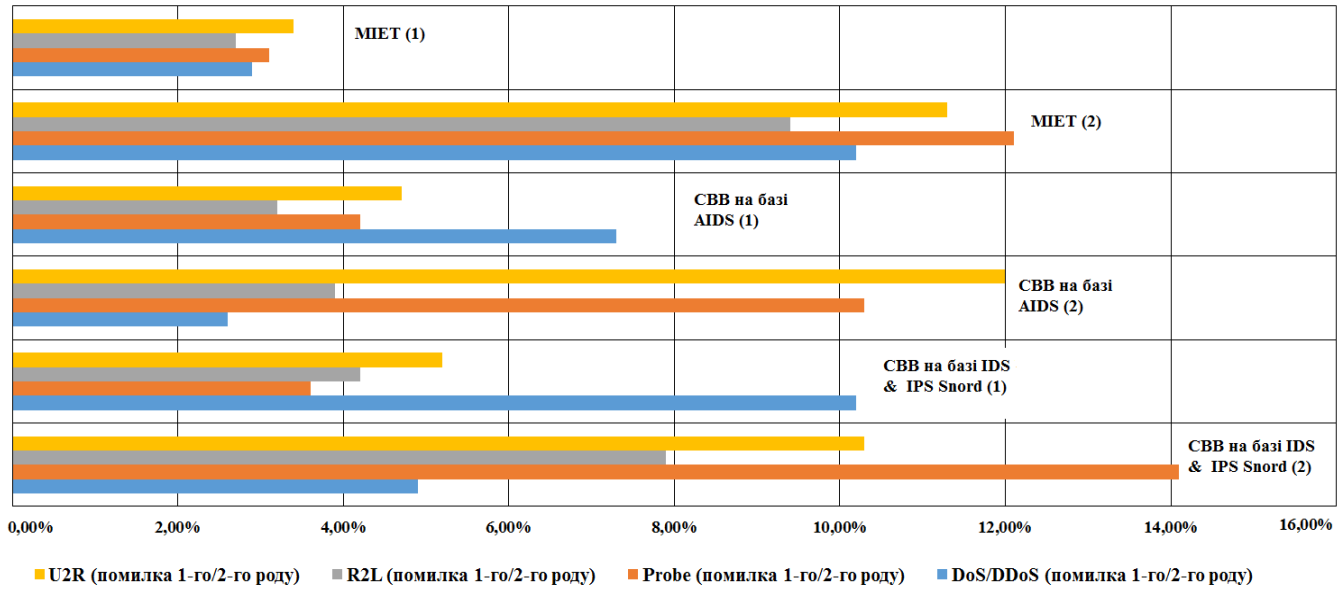

Рис. 1.1. Порівняння ймовірності виникнення помилок першого та другого роду при виявленні кібератак різними системами

Додаток К– Акт перевірки на плагіат КР інформаційним центром запобігання та виявлення плагіату

АКТ

За результатами перевірки курсової роботи здобувача вищої освіти _____ на тему:
(прізвище, ім'я, по батькові)

_____
(назва теми)

_____

встановлено:

- *значення коефіцієнта подібності 1* (КП1) _____%;
(використовується для вивчення мовної незалежності автора документів).

- *значення коефіцієнта подібності 2* (КП2) _____%;
(визначає частини документу, що містить фразу з 25 слів або більше знайдених в базах даних ЧНТУ, базі даних програми обміну базами даних, бази даних RefBooks або інтернет-ресурсів (за винятком бази даних правових актів).

- *значення коефіцієнта подібності DLA* (КП DLA) _____%.
(вказує відсоток аналізованого документа, який формується виключно з фраз 8 або більше слів, які знаходяться в Базі даних правових актів).

Звіт про технічну перевірку роботи (звіт подібності) додається.

Адміністратор ІЦЗВП _____ _____
(підпис) *(ініціали, прізвище)*