Міністерство освіти і науки України
Вінницький національний технічний університет

Методичні вказівки до виконання курсового проекту

з дисципліни "Основи побудови мікропроцесорних систем"

Для студентів денної та заочної форм навчання
напряму підготовки 6.170101 – Безпека інформаційних та комунікаційних систем та спеціальності 125 – Кібербезпека

Вінниця 2018

Методичною радою Вінницького національного технічного університету Міністерства освіти і науки України (протокол № 8 від 19.04.2018 р.) надано гриф "Електронні методичні вказівки" та рекомендовано до використання в навчальному процесі.

Укладачі:
Володимир Андрійович Лужецький
Юрій Володимирович Баришев
Валентина Аполінаріївна Каплун

Рецензенти:
к. т. н., доцент Л. В. Крупельницький
к. т. н., доцент Ю. В. Булига

Затверджено на засіданні кафедри захисту інформації 22 червня 2016 року, протокол №19.

Методичні вказівки до виконання курсового проекту з дисципліни "Основи побудови мікропроцесорних систем"/Укладачі В. А. Лужецький, Ю. В. Баришев, В. А. Каплун. – Вінниця: ВНТУ, 2018. – 45 с.

Містять рекомендації та стислі теоретичні відомості щодо тематики та етапів виконання курсового проекту з дисципліни "Основи побудови мікропроцесорних систем" для студентів напряму підготовки 6.170101 – "Безпека інформаційних і комунікаційних систем" та спеціальності 125 – "Кібербезпека". Запропонована структура курсового проекту, визначено основні напрями та зміст курсового проектування. Наведено графік виконання курсового проекту відповідно до етапів. Наведено правила оформлення пояснювальної записки та графічної частини курсового проекту.

Навчальне самостійне електронне мережне видання
Методичні вказівки до виконання курсового проекту
з дисципліни "Основи побудови мікропроцесорних систем"

Укладачі:
Лужецький Володимир Андрійович
Баришев Юрій Володимирович
Каплун Валентина Аполінаріївна

Електронний ресурс PDF.
Підписано до видання 25.07.2018 р. Зам. № Р2018-011
Видавець та виготовлювач - Вінницький національний технічний університет,
Інформаційний редакційно-видавничий центр.
ВНТУ, ГНК, к.114, Хмельницьке шосе, 95, м. Вінниця, 21021,
тел. (0432) 65-18-06.
press.vntu.edu.ua;
Email: irvc.vntu@gmail.com.
Свідоцтво суб'єкта видавничої справи
серія ДК № 3516 від 01.07.2009 р.

ЗМІСТ

1 ОСНОВНІ ВИМОГИ ДО КУРСОВОГО ПРОЕКТУ

1.1 Мета та задачі курсового проектування

Курсовий проект – навчальний проект з дисципліни, який містить елементи ескізного і технічного проектів та робочої документації.

Внаслідок виконання курсового проекту з дисципліни "Основи побудови мікропроцесорних систем" студент повинен закріпити знання структури мікропроцесорних систем, основних підходів до їх проектування, принципів їх функціонування; здобути навички з розробки мікропроцесорних систем, розробки та програмування мікроконтролерів і програмованих логічних інтегральних схем, програмування обміну даними відповідно до протоколів, що використовуються сучасними мікропроцесорними системами, розв’язання задач з галузі кібербезпеки засобами мікропроцесорної техніки.

Під час виконання курсового проекту студенти повинні використати знання, отримані ними під час вивчення дисциплін "Технологія програмування", "Інформаційні технології", "Операційні системи", "Теорія інформації та кодування" "Електроніка", "Прикладна криптологія", "Інформаційно-комунікаційні системи", "Архітектура комп’ютерних систем".

Під час виконання курсового проекту студенти повинні вміти:

- правильно обґрунтовувати вибір способу розв’язання поставленого завдання;
- аналізувати методи захисту інформації та робити їх декомпозицію на структурні складові;
- розробляти структуру мікропроцесорних систем та пристроїв для захисту інформації;
- розробляти алгоритми розв’язання задач за допомогою мікропроцесорів;
- програмувати алгоритми для їх реалізації за допомогою мікропроцесорних пристроїв;
- тестувати коректність функціонування мікропроцесорних систем і

пристроїв.

1.2 Тематика курсового проектування

Зміст курсового проекту повинен відповідати навчальній програмі та робочому плану дисципліни "Основи побудови мікропроцесорних систем" і повинен відображати суть обраної студентом теми. Зміст курсового проекту визначається завданням, яке видається на першому тижні семестру викладачем кожному студенту.

Тематика курсового проекту стосується розв’язання за допомогою мікропроцесорних пристроїв та систем задач з галузі кібербезпеки:

- автентифікації користувачів;
- автентифікації даних;
- захисту даних, що зберігаються на електронних носіях інформації;
- захисту даних, що передаються каналами зв’язку;
- обмеження несанкціонованого доступу до приміщень.

Автентифікація користувачів передбачає реалізацію одного з криптографічних протоколів одно- або багатосторонньої автентифікації. Завдання цього класу потребують аналізу низки протоколів автентифікації, визначення переваг і недоліків заданого протоколу порівняно з відомими аналогами, а також визначення задач, в яких доцільно використовувати пристрій, що розробляється. Основна увага в курсових проектах 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 гешування даних. Завдання такого типу потребують аналізу студентом відомих методів формування електронних цифрових підписів або методів гешування, визначення переваг і недоліків цих методів порівняно з відомими аналогами, а також визначення

задач, в яких доцільно використовувати пристрій, що розробляється. При цьому основна увага має приділятися генеруванню відкритого та закритого ключів для електронних цифрових підписів, реалізації алгоритмів формування цифрових підписів або геш-значень даних, забезпеченню можливості діалогу мікропроцесорної системи, що розробляється, з іншими пристроями (в переважній більшості випадків – з комп'ютером) за допомогою відомих інтерфейсів.

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

Захист даних, що передаються каналами зв'язку передбачає реалізацію одного з методів потокового шифрування або скремблювання даних, що передаються в цифровому або аналоговому вигляді відповідно. Також курсові проекти цього напряму можуть передбачати захист цілісності даних за допомогою використання кодів, які забезпечують самосинхронізацію обміну, виявлення та виправлення помилок, ущільнення тощо. Для розв'язання завдань цієї тематики студенту 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 в ході курсового проектування. Основна увага курсового проекту даної тематики повинна приділятися розробці інтерфейсу, за допомогою якого мікропроцесорна система вбудовуватиметься в канал зв'язку, а також реалізації методів захисту інформації.

Обмеження несанкціонованого доступу до приміщень передбачає реалізацію одного з методів контролю доступу до периметру, що

контролюється, в якому відбувається зберігання носіїв інформації та засобів її обробки. Завдання цього типу потребують аналізу студентом методів контролю доступу та основних складових засобів, за допомогою яких ці методи реалізуються, аналізу сучасного стану розвитку виробництва даних складових та обґрунтування їх вибору для реалізації завдання курсового проекту. Основна увага курсових проектів цього напряму приділяється реалізації обміну даними між різними структурними складовими мікропроцесорної системи (пристрою), аналізу цих даних, виявленню небезпеки й індикації її появи.

Індивідуальне завдання для курсових проектів визначається викладачем із загального переліку завдань на курсовий проект. Типові завдання наведені у додатку А даних методичних вказівок. Пропозиції студентів щодо вибору теми курсового проекту поза межами запропонованого переліку заохочуються і враховуються при оцінюванні результатів курсового проектування. Однак такі теми потребують обов'язкового попереднього узгодження з викладачем та присвоєння темі унікального номера варіанта завдання, який в подальшому буде використовуватись студентом при оформленні графічної частини та пояснювальної записки до курсового проекту.

1.3 Етапи курсового проектування

Процес проектування мікропроцесорної системи (пристрою) умовно розбивається на такі етапи:

а) аналіз відомих розв'язків задачі;

б) аналіз та обґрунтування вибору засобів, які будуть використовуватись для досягнення мети проектування;

в) розробка структури мікропроцесорної системи (пристрою);

г) розробка алгоритму роботи системи (пристрою);

д) розробка програмного забезпечення, що реалізує розроблені алгоритми або розробка моделі мікропроцесорної системи (пристрою);

е) тестування мікропроцесорної системи (пристрою).

Аналіз відомих розв'язків задачі. На даному етапі розглядаються відомі

засоби (з посиланням на джерела та наведенням їх технічних характеристик) для розв’язання задачі. Так для спеціалізованих процесорів, які реалізовуватимуть криптографічні алгоритми, мають розглядатися особливості алгоритму, який реалізовуватиметься. Для пристроїв, що передбачатимуть реалізацію охоронної сигналізації – типи датчиків. Завершити аналіз бажано порівнянням характеристик рішень та навести огляд мікропроцесорних систем (пристроїв), що ці рішення реалізують.

Наприклад, при виконанні теми курсового проекту "Мікропроцесорна система автентифікації користувачів за протоколом Фіата-Шаміра" на цьому етапі передбачається аналіз протоколів автентифікації користувачів, звертаючи особливу увагу на інші протоколи автентифікації з "нульовим знанням", зокрема на протоколи Шнорра (Schnorr) та Жилю-Куїзквотера (Guillou-Quisquater). Як приклади реалізації алгоритму необхідно навести зразки комутаційного обладнання комп’ютерних мереж та "електронних ключів" для автентифікації користувачів.

Аналіз та обґрунтування вибору засобів, які будуть використовуватись для досягнення мети проектування. Даний етап присвячений визначенню конкретних мікропроцесорів та/або мікроконтролерів, які обираються для проектування системи (пристрою), обсягу та типу пам’яті, периферійних пристроїв, які пов’язані з мікропроцесорами, інтерфейсів тощо. Для цього виконується огляд відомих засобів та обґрунтовується вибір одного з них. Якщо при проектування необхідно розробити новий мікропроцесор, то обґрунтовується недостатність відомих засобів для досягнення мети та визначаються переваги, якими повинен володіти новий мікропроцесор порівняно з відомими.

Зокрема, при виконанні теми курсового проекту "Мікропроцесорна система автентифікації користувачів за протоколом Фіата-Шаміра" на цьому етапі доцільно обрати шлях реалізації мікропроцесорної системи на основі процесорів власної архітектури, оскільки протокол Фіата-Шаміра передбачає багатократне повторення операцій множення за модулем простого числа, яка неприродною для сучасних архітектур мікроконтролерів. Таким чином, задля

досягнення високих показників швидкодії та низьких показників енергоспоживання необхідно розробляти процесор спеціалізованої архітектури та реалізовувати його за допомогою програмованих логічних інтегральних схем.

Розробка структури мікропроцесорної системи (пристрою). Розробляється загальна структура системи (пристрою), розглядаються зв'язки між структурними компонентами, визначається низка задач, які розв'язуватимуться кожним структурним компонентом. Після розробки загальної схеми, деталізується реалізація кожного структурного компоненту, алгоритму його роботи, задач, які він розв'язуватиме. Визначаються порти мікропроцесора (мікроконтролера), які будуть задіяні при проектуванні мікропроцесорної системи (пристрою) для взаємодії із зовнішнім середовищем. За необхідністю визначаються сигнали, які керуватимуть роботою системи (пристрою), що розробляється. За результатами даного етапу розробляється схема електрична структурна.

Так для реалізації протоколу Фіата-Шаміра до складу узагальненої структури системи необхідно включити два пристрої: на стороні А та на стороні В, оскільки згідно з протоколом ці сторони відіграють різні ролі під час обміну інформацією. Основними складовими цих пристроїв є такі:

- інтерфейс UART – для обміну даними між сторонами А та В;

- блок модульної арифметики, який забезпечує реалізацію специфічних для протоколу обчислень;

- блоки підтримки протоколів специфічні для кожної зі сторін;

- блок формування запитів на стороні В;

- блок формування відповідей на ці запити на стороні А;

- блок перевірки відповідей на стороні В.

Розробка алгоритму роботи системи (пристрою). Спочатку визначаються основні етапи роботи розробки, які в подальшому деталізуються до рівня виконання операцій в межах кожного структурного блоку. За результатами даного етапу розробляється схема роботи системи.

У мікропроцесорній системі автентифікації користувачів за протоколом

Фіата-Шаміра необхідно передбачити такі основі процедури:

- процедуру реалізації модульної арифметики;
- процедуру формування ключів;
- алгоритм формування запитів сторони В;
- алгоритм генерування відповідей стороною А;
- процедуру перевірки коректності відповідей стороною В.

На основі даного етапу реалізується програмне забезпечення для керування мікропроцесором (мікроконтролером). Якщо була визначена необхідність у розробці нового мікропроцесора, то реалізується не лише програма роботи, але й описуються основні семантичні одиниці при описі мікропроцесора та розробляється його програмна модель.

Розробка програмного забезпечення, що реалізує розроблені алгоритми. Даний етап відбувається для розробок, які передбачають використання мікропроцесорів (мікроконтролерів) відомої архітектури. Він передбачає розробку та відлагодження програм, написаних мовою асемблера для обраної моделі мікропроцесора (мікроконтролера).

Оскільки для мікропроцесорної системи автентифікації користувачів на основі протоколу Фіата-Шаміра доцільніше розробляти систему на основі спеціалізованого процесора, тому цей етап не реалізується в курсовому проекті такої тематики.

Розробка моделі мікропроцесорної системи (пристрою). У випадку використання спеціалізованих мікропроцесорів відбувається опис структури та алгоритмів роботи цього мікропроцесора однією з мов опису апаратури, наприклад, VHDL.

Так для мікропроцесорної системи автентифікації користувачів за протоколом Фіата-Шаміра на цьому етапі реалізуються основні семантичні елементи (сутності та архітектури), що описують структуру та алгоритми роботи відповідних елементів системи в середовищі ModelSim.

Тестування мікропроцесорної системи (пристрою). На даному етапі обирається середовище комп’ютерного моделювання для спроектованої мікропроцесорної системи (пристрою), симулюється її робота. Для

демонстрації правильності розв’язання задач, які ставляться перед мікропроцесорною системою (пристроєм), передбачається використання низки експериментів, покликаних перевірити роботу системи (пристрою) при отриманні ним коректних вхідних даних. Додатково буде оцінено експерименти, покликані перевірити коректність роботи пристрою у випадку, коли на його входи подаються некоректні дані.

При тестуванні системи автентифікації користувачів за протоколом Фіата-Шаміра доцільно передбачити такі види тестування:

- створення ключів для автентифікації;
- генерування рівномірно розподілених запитів сторони В;
- перевірка коректності повідомлення від сторони А;
- перевірка коректності спотвореного повідомлення від сторони А.

Для проведення тестування необхідно буде розробити додаткові сутності, що пов’язують пристрої сторони А та В, а також моделюють зовнішнє середовище, зокрема, спотворення, які вносяться у повідомлення сторони А.

2 ВИМОГИ ДО СТРУКТУРИ ТА ОФОРМЛЕННЯ КУРСОВОГО ПРОЕКТУ

2.1 Загальна структура пояснювальної записки

Кожен етап курсового проектування обов'язково має знайти своє відображення у пояснювальній записці. Пояснювальна записка повинна відповідати індивідуальному завданню, а її оформлення – ГОСТ 2.105-95, які слід враховувати на момент виконання розробки з врахуванням всіх офіційних змін, введених в дію.

Пояснювальна записка до курсового проекту повинна мати таку структуру:

1 ***Інформаційно-змістовна частина,*** яка містить:

- титульний аркуш;
- індивідуальне завдання;
- анотацію;
- зміст.

2 ***Основна частина***, яка складається з:

- вступу;
- аналізу джерел інформації;
- розробки структури системи (пристрою);
- розробки програмного забезпечення або комп'ютерної моделі системи (пристрою) та тестування коректності її роботи;
- висновків;
- переліку використаних джерел.

3 ***Додатки***, які складаються з технічного завдання, лістингу програмного забезпечення, а також, за необхідності, рисунків, таблиць, розрахунків, результатів тестування тощо, які з певних причин не увійшли до складу основної частини пояснювальної записки, однак нерозривно з нею пов'язані і дозволяють детальніше висвітлювати певні етапи проектування.

Крім пояснювальної записки курсовий проект включає ***графічну***

частину, яка містить результати курсового проектування, оформлені у вигляді схем. Наприкінці подається відомість курсового проекту, яка описує перелік документів, розроблених під час курсового проектування.

2.2 Інформаційно-змістовна частина пояснювальної записки

Титульний аркуш є першою сторінкою курсового проекту, на якій не проставляється номер. На титульному аркуші позначаються повні назви вищого навчального закладу, факультету, кафедри, назва виду документа, тема, розробник, керівник, члени комісії, рік написання. Крім того титульний аркуш містить рамку спеціального типу.

Приклад оформлення титульного аркушу наводиться у додатку Б.

В ***індивідуальному завданні*** подається конкретний зміст кожного курсового проекту, етапи його виконання, вихідні дані розробки, які визначаються керівником. Воно розглядається і затверджується на засіданні кафедри, про свідчить відповідний підпис завідувача кафедри. Індивідуальне завдання в перелік змісту не вноситься і має бути другою сторінкою після титульного аркуша.

Приклад індивідуального завдання до курсового проекту наведено в додатку Д.

Керівник проекту пропонує зміст пояснювальної записки, як правило, в розроблених методичних вказівках, або в навчальних цілях зміст може висвітлюватись в індивідуальному завданні.

На підставі індивідуального завдання розробляється технічне завдання, яке подається першим з додатків. Приклад оформлення технічного завдання наведено у додатку Ж.

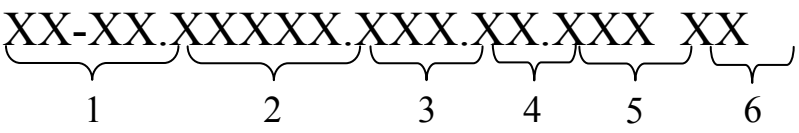
Анотація призначена для ознайомлення з текстовим документом курсового проекту. Вона повинна коротко характеризувати мету проекту, засоби, використані для досягнення поставленої задачі, коротку інформацію про досягнуті результати. Розмір анотації повинен становити приблизно третину сторінки.

Анотацію розміщують безпосередньо за аркушем з індивідуальним завданням, починаючи з нової сторінки (третьої), нумерація якої не позначається. Заголовок (слово АНОТАЦІЯ) розміщується по центру сторінки, після нього пропускається один рядок. Анотація подається двома мовами – українською та однією з міжнародних мов (зазвичай англійською).

Зміст розташовують безпосередньо після анотації, починаючи з нової сторінки. До змісту включають: вступ; послідовно перелічені назви всіх розділів, підрозділів, пунктів і підпунктів (якщо вони мають заголовки) пояснювальної записки; висновки; перелік використаних джерел; назви додатків і номери сторінок, з яких починається викладення відповідного матеріалу. До змісту не вносяться титульний аркуш, індивідуальне завдання на курсовий проект та анотація.

Перша сторінка змісту оформляється на аркуші з рамкою, яка має великий штамп, в якому зазначається назва документу, умовне позначення (див далі), розробник, нормоконтролер тощо, решта сторінок – на аркуші з рамкою іншої форми, яка містить лише умовне позначення (додаток В). Номер сторінки на першій сторінці змісту проставляється у відповідній графі рамки. Сам зміст за нумерацією пояснювальної записки є, як правило, четвертою сторінкою.

Для курсових проектів доцільною є предметна система умовних позначень, яка має таку структуру:



де 1 (XX-XX) – числовий шифр кафедри, прийнятий у ВНТУ (для кафедри захисту інформації – 08-20);

2 (XXXXX) – умовне скорочення для дисципліни (ОПМПС);

3 (XXX) – перша цифра 0 позначає, що це проект (1 – якщо робота), друга і третя цифри означають рік, наприклад, 17 – 2017 рік);

4 (XX) – варіант завдання (наприклад, 01, 02, ..., 99);

5 (XXX) – перша цифра – номер групи (1, 2 тощо), наступні дві цифри

позначають таке:

- номер студента за списком у журналі академічної групи – для пояснювальної записки, технічного завдання, відомості курсового проекту;
- порядковий номер – для схем та переліків елементів (наприклад, 001, 002 тощо).

6 (ХХ) – код документа (наприклад ПЗ – для пояснювальної записки, ТЗ – для технічного завдання, Е1 – для схеми електричної структурної, А8 – для схеми роботи системи та схеми ресурсів системи).

Таким чином, пояснювальна записка до курсового проекту, виконаного у 2017 році студентом першої групи, якому в переліку академічної групи відповідає порядковий номер 25, на тему, що має порядковий номер 3 в загальному переліку тем курсових проектів, повинен використовувати умовне позначення 08-20.ОПМПС.017.03.125 ПЗ. При цьому для даного випадку структура мікропроцесорної системи (пристрою) виконана як схема електрична структурна повинна позначатися 08-20.ОПМПС.017.03.001 Е1, а схема роботи системи відповідно – 08-20.ОПМПС.017.03.002 А8.

Нумерація у змісті починається зі вступу (відповідно до нумерації у пояснювальній записці). Нумерація сторінок по всій пояснювальній записці, включаючи додатки, повинна бути наскрізною.

Назви заголовків змісту повинні однозначно відповідати назвам заголовків пояснювальної записки за текстом. Формування змісту у текстовому документі бажано здійснювати автоматично, використовуючи засоби обраного текстового редактора. Назви усіх розділів, підрозділів, пунктів, підпунктів повинні використовувати вирівнювання до лівого краю аркуша.

2.3 Зміст та оформлення основної частини

У ***вступі*** заголовок "ВСТУП" розташовують посередині з нової пронумерованої сторінки на аркуші з рамкою.

Вступ повинен стисло висвітлювати такі питання:

- стан розвитку проблеми в даній галузі;
- галузь використання та призначення даної розробки;
- актуальність;
- мету та задачі проектування.

У вступі і далі за текстом не дозволяється використовувати скорочені слова, терміни, крім загальноприйнятих. Якщо ж в тексті є необхідність використовувати певні загальноприйняті скорочення (абревіатури), то при введенні їх вперше в дужках слід вказати скорочення. І лише після цього дане скорочення можна використовувати по тексту. Наприклад, мікропроцесор (МП). У назвах розділів, підрозділів, пунктів і підпунктів використовувати скорочення не рекомендується.

При викладенні актуальності основну увагу необхідно приділити конкретній розробці, уникаючи узагальненої характеристики переваг мікропроцесорних систем (пристроїв).

Мета курсового проектування формулюється таким чином, щоб вказувати на конкретну характеристику, яка покращується під час проектування. Приклад оформлення та подання вступу наведено у додатку Г.

Обсяг вступу не повинен перевищувати 2 сторінки.

Розділ ***аналізу предметної області*** передбачає огляд алгоритмів та пристроїв, що використовуються у курсовому проекті, а також відомих аналогів. На основі даного огляду відзначаються недоліки аналогів та обґрунтовується вибір засобів, необхідних для досягнення мети курсового проектування. Посилання на джерела інформації, використаної в тексті пояснювальної записки загалом і в даному підрозділі зокрема є обов'язковими.

Рекомендований обсяг розділу – 5-7 сторінок.

Розділ, присвячений ***розробці структури системи (пристрою)*** , повинен містити опис основних блоків, їх взаємозв'язків та подальший детальний опис їх структури, що детальніше описано у підрозділі 1.3 цих методичних вказівок. Він повинен відображати суть прийнятих рішень щодо структури мікропроцесорної системи та її основних структурних блоків. При цьому

рекомендується використовувати рівень деталізації на рівні схем електричних структурних.

Рекомендований обсяг розділу – 7-9 сторінок.

Розділ, присвячений ***розробці алгоритмів роботи системи (пристрою)***, передбачає представлення узагальненого алгоритму роботи мікропроцесорної системи та її основних структурних блоків. Крім того, даний розділ повинен містити опис обраних студентом засобів для комп'ютерного моделювання, визначення способів проведення тестування і результати цього тестування.

Рекомендований обсяг розділу – 8-10 сторінок.

Висновки оформлюють з нової пронумерованої сторінки, починаючи зі слова "ВИСНОВКИ" посередині рядку великими літерами, після чого пропускається один рядок.

У висновках наводяться основні результати роботи над курсовим проектом. Коротко по основних розділах описуються етапи реалізації задачі курсового проекту. Визначається тип установ та підприємств для яких доцільне впровадження розробки.

На основі отриманих в ході курсового проектування результатів надаються обґрунтовані висновки щодо переваг та недоліків розробленої мікропроцесорної системи (пристрою). Обов'язково слід зазначити перспективи удосконалення розробленої системи (пристрою).

Перелік використаних джерел оформлюють з нової пронумерованої сторінки, починаючи із заголовку "ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ" посередині рядка великими літерами, після чого пропускається один рядок.

Перелік повинен містити використані джерела інформації, які було використано в процесі виконання проекту, і на які повинні бути обов'язкові посилання в тексті пояснювальної записки. Джерела інформації (книги, статті, патенти, журнали, інтернет-сторінки) в загальний список записується в порядку посилання на них в тексті пояснювальної записки. Посилання на літературу наводять в квадратних дужках в місця використання інформації з даного джерела, вказуючи порядковий номер за списком. Наприклад, посилання на певну статтю, яка подається третьою в переліку використаних джерел,

оформлюється таким чином: "У статті [3] наводиться класифікація систем охоронної сигналізації. Відповідно до даної класифікації охоронні сигналізації поділяються на ..." або "Системи охоронної сигналізації поділяються на такі класи [3]: ...".

Якщо виникає необхідність послатися на декілька джерел їх записують в порядку зростання номерів. При цьому, якщо в послідовності номерів джерел поспіль зустрічається більше двох номерів, то з даної частини переліку вказується лише перше та останнє джерело, а між ними ставлять дефіс. В інших випадках між номерами джерел ставиться кома. Наприклад, посилання на джерела, які мають в переліку номера 1, 4, 5, 6, 8 повинно оформлюватись таким чином: [1, 4-6, 8].

Кожне джерело повинно бути вказано разом з видавництвом, роком видання, кількістю сторінок. Джерела інформації в перелік записують мовою оригіналу. У переліку кожне джерело записують з абзацу, нумерують арабськими цифрами, починаючи з одиниці. Правильне оформлення певного джерела інформації можна переглянути у переліку літературних джерел у будь-якому навчальному посібнику. Якщо у списку використаних джерел є посилання на електронні ресурси, слід наводити режим доступу до даного ресурсу. Наприклад, для електронних журналів вказується уніфікований локатор ресурсів (URL).

Приклад оформлення переліку використаних джерел різного характеру:

Посилання на книги:

1. Цирульник С. М. Проектування мікропроцесорних систем / С. М. Цирульник, Г. Л. Лисенко. – Вінниця: ВНТУ, 2010. – 201 с.

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

3. Мікропроцесорна техніка: Підручник / [Ю. І. Якименко та ін.]; за ред. Т. О. Терещенко. – 2-ге вид., перероб. і доповн. – К.: ІВЦ "Політехніка"; "Кондор", 2004. – 440 с.

Посилання на статті в журналах:

4. Рудницький В. М. Модель уніфікованого пристрою криптографічного перетворення інформації / В. М. Рудницький, В. Г. Бабенко // Системи обробки інформації. – №3. – 2009. – С. 91-95.

5. Лужецький В. А. Апаратні засоби для реалізації багатоканального керованого хешування. / В. А. Лужецький, Ю. В. Баришев. // Системи обробки інформації. – №3. – 2011. – С. 130-133.

Посилання на матеріали та тези конференцій:

6. V.A. Luzhetskyi Methods of Generic Attacks Infeasibility Increasing for Hash Functions / Volodymyr Luzhetskyi, Yurii Baryshev // The 7th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS'2013), September 12-14, 2013 Berlin, Germany. – P. 661-664

7. Баришев Ю. В. Структури спеціалізованих процесорів для гешування, стійкого до загальних атак / Баришев Ю. В., Зозуля А. О. // Тези доповідей Четвертої Міжнародної науково-практичної конференції «Інформаційні технології та комп'ютерна інженерія» м. Вінниця, 28-30 травня 2014 року. – Вінниця: ВНТУ, 2014. – С 216-219.

8. Баришев Ю. В. Структури спеціалізованих мікропроцесорів для передавання даних в лініях з великим рівнем завад. / Баришев Ю. В., Репетій В. М. // Тези доповідей Четвертої Міжнародної науково-практичної конференції «Інформаційні технології та комп'ютерна інженерія» м. Вінниця, 28-30 травня 2014 року. – Вінниця: ВНТУ, 2014. – С 222-223.

Посилання на стандарти:

9. Захист інформації. Технічний захист інформації. Основні положення : ДСТУ 3396.0-96. – К.: Держспоживстандарт України, 1996. – 5 с.

Посилання на патенти:

10. Патент України на корисну модель № 94039 МПК G 09 C 1/00. Спосіб паралельного ключового гешування даних теоретично доведеної стійкості /

Лужецький В. А., Баришев Ю. В.; .заявник та патентовласник Вінницький національний технічний університет. – № u201405191; заявл. 16.05.2014; опубл. 27.10.2014, Бюл. № 20.

11. Патент України на корисну модель № 53615 МПК H 04 L 9/06. Спосіб шифрування даних на основі трьох несумісних груп операцій / Лужецький В. А., Дмитришин О. В., Баришев Ю. В.; .заявник та патентовласник Вінницький національний технічний університет. – № u201004697; заявл. 20.04.2010; опубл. 11.10.2010, Бюл. № 19.

12. Патент України на корисну модель № 55211 МПК H 04 L 9/06. Конвеєрний криптографічний обчислювач. / Корченко О. Г., Паціра Є. В., Панасюк А. Л., Гнатюк С. О., Кінзерявий В. М.; заявник та патентовласник Національний авіаційний університет. – № u201006041; заявл. 19.05.10; опубл. 10.12.10, Бюл. №23.

Посилання на web-сторінки:

13. Van der Spiegel J. VHDL Tutorial / Jan Van der Spiegel [Електроний ресурс]. – Режим доступу: http://www.seas.upenn.edu/~ese171/vhdl/ vhdl_primer.html (дата звернення 22.08.2016) – Назва з екрану.

14. Лабораторія імені професора Канєвського. [Електроний ресурс]. Режим доступу: http://kanyevsky.kpi.ua/VHDLlabukraine/VHDLlabukraine.html/ (дата звернення 22.08.2016) – Назва з екрану

2.4 Оформлення додатків

Першим аркушем додатків для курсових проектів має бути технічне завдання, в якому вказуються: найменування та галузь застосування розробки; основа для розробки; мета і призначення; джерела розробки; технічні вимоги (показники призначення, показники надійності, вимоги безпеки тощо); стадії та етапи розробки; порядок контролю та приймання. Технічне завдання повинно бути додатком А до пояснювальної записки. Приклад оформлення технічного завдання наведений у додатку Ж.

Крім технічного завдання, додатки містять матеріал, який:

- є необхідним для повноти викладення результатів і розуміння пояснювальної записки, але їх включення до основної частини може змінити впорядковане й логічне уявлення про курсовий проект;
- не може бути послідовно розміщений в основній частині звіту через великий обсяг (додаткові ілюстрації, схеми або таблиці, лістинг програми, інструкції, методики, опис комп'ютерних програм, розроблених або використаних у процесі курсового проектування тощо).

Додатки необхідно починати з нової сторінки, вказуючи зверху посередині рядка слово "Додаток" і через пропуск – його позначення. Додатки позначають послідовно великими українськими літерами, за винятком літер Ґ, Є, З, І, Ї, Й, О, Ч, Ь. Якщо додатків більше ніж літер, то продовжують позначати арабськими цифрами. Дозволяється позначати додатки латинськими літерами, за винятком літер *I* і *O*.

Кожен додаток повинен мати тематичний (змістовний) заголовок, який записують посередині рядка, наприклад, "Додаток Б. Лістинг програми".

У тексті пояснювальної записки необхідно обов'язково посилатись на додатки у відповідних місцях з метою звернення уваги читача на те, що результати виконання певного етапу курсового проектування не обмежуються лише наведеними в пояснювальній записці. Крім того, допускається посилання на певні частини додатків. Наприклад посилання на певні таблиці та рисунки оформлюються таким чином: "(у табл. В.3)", "... технічні характеристики обраних датчиків наведено у табл. В.3", "... на рис. Г.1 наведено вигляд вхідних вихідних сигналів блоку піднесення до степеня за модулем простого числа після обробки першого блоку даних".

Сторінки додатків нумеруються, продовжуючи загальну нумерацію у пояснювальній записці. Всі додатки включають до змісту, вказуючи номер, заголовок і сторінки, з яких вони починаються.

2.5 Оформлення графічної частини

Графічна частина розміщується після додатків. Для відділення графічної частини від пояснювальної записки використовується аркуш формату А4 на якому по центру великими літерами пишуть "ГРАФІЧНА ЧАСТИНА", після якого подають розроблені схеми.

У графічній частині курсового проекту повинні подаватись схеми, які призначені для використання під час реалізації прототипу мікропроцесорної системи (пристрою). Схеми, наведені в графічній частині мають шифр, який визначається відповідно до загальних правил для курсового проекту (див. підрозділ 2.2), де як код документа використовується позначення виду та типу схем відповідно ГОСТ 2.701-84.

Для відображення основних результатів, пов’язаних зі структурою мікропроцесорних систем, пристроїв, спеціалізованих процесорів необхідно використовувати схеми електричні, які оформлюються відповідно до ДСТУ ГОСТ 2.702:2013, ГОСТ 2.708-81, ГОСТ 2.721-74 (з урахуванням внесених змін, зокрема редакції 2000 року). З урахуванням мети курсового проектування рекомендується оформляти результати у вигляді схем структурних, також допускається оформлення у вигляді схем функціональних та схем об’єднаних (лише за умови, що вони об’єднують елементи схем структурних або функціональних з елементами схем іншого типу, наприклад з елементами схеми з’єднань або схеми загальної).

Для відображення основних результатів, пов’язаних з алгоритмами роботи та програмами для мікропроцесорних систем, пристроїв, спеціалізованих процесорів необхідно використовувати схеми алгоритмів, програм, систем. Дані схеми оформлюються відповідно до ГОСТ 19.701-90 (з урахуванням внесених змін, зокрема редакції 2008 року). Згідно з метою курсового проектування рекомендується оформлювати результати у вигляді схеми роботи системи або схеми програми. У випадку використання декількох мікропроцесорів (мікроконтролерів) в системі допускається використання схем взаємодії програм для відображення особливостей організації спільної обробки

даних цими мікропроцесорами та особливостей передавання керування між різними мікропроцесорами (у випадку наявності).

Відповідно до тематики курсового проектування рекомендується розробляти не менше чотирьох схем: дві електричні та дві схеми алгоритмів, програм, систем. Наприклад, для курсового проекту, що реалізує мікропроцесорну систему для реалізації протоколу автентифікації Фіата-Шаміра графічна частина може складатися з таких схем:

- Узагальнена структура мікропроцесорної системи. Схема електрична структурна – для відображення основних структурних блоків мікропроцесорної системи, їх з'єднань один з одним та передбачених інтерфейсів для взаємодії із зовнішніми пристроями;

- Узагальнена структура мікропроцесорної системи. Схема роботи системи – для відображення основних процесів, які виникають під час роботи системи, особливостей взаємодії її структурних блоків один з одним та із зовнішніми пристроями;

- Блок формування відповідей на запити сторони А. Схема електрична структурна – для відображення структурних елементів, необхідних для формування відповідей на запити сторони В, та з'єднань цих елементів;

- Блок формування відповідей на запити сторони А. Схема програми – для відображення процесів, які відбуваються під час роботи даного блоку, обміні даними та взаємодії між структурними елементами цього блоку та структурними елементами інших блоків системи;

- Блок перевірки відповідей на стороні Б. Схема електрична структурна – для відображення структурних елементів даного блоку системи та їх з'єднань;

- Блок перевірки відповідей на стороні Б. Схема програми – для відображення процесів, які відбуваються під час роботи даного блоку, обміні даними та взаємодії між структурними елементами цього блоку та структурними елементами інших блоків системи;

- Блок модульної арифметики. Схема електрична структурна – для відображення елементів та їх зв'язків, необхідних для реалізації арифметичних операцій за модулем простого числа, передбачених протоколом Фіата-Шаміра;

- Блок модульної арифметики. Схема роботи системи – для відображення послідовності дій, що забезпечують виконання арифметичних операцій за модулем простого числа, передбачених протоколом Фіата-Шаміра у відповідному блоці.

2.6 Загальні правила оформлення

Пояснювальна записка відноситься до текстових документів, які містять інформацію, подану в основному технічною мовою та графічну інформацію у вигляді ілюстрацій. Пояснювальна записка виконується згідно вимог міждержавного стандарту ГОСТ 2.105-95. Текст пояснювальної записки повинен бути набраний на комп'ютері та роздрукований на стандартних аркушах паперу формату А4 (210×297 мм) з однієї сторони.

Рамки. Кожен аркуш пояснювальної записки до курсового проекту (крім анотації та індивідуального завдання) повинен мати стандартну рамку робочого поля і основний напис. Титульний аркуш повинен мати рамку, наведену у додатку Б, перша сторінка розділу ЗМІСТ повинна бути оформлена на аркуші з рамкою, наведеною у додатку В, наступна та всі інші сторінки повинні бути оформлені на аркушах з рамкою, наведеною у додатку Г. У кожну рамку (окрім рамки титульного аркуша) обов'язково повинні бути вписані номер сторінки та шифровий код проекту. Для формування рамок при виконанні пояснювальної записки у текстовому редакторі Microsoft Office Word рекомендується користуватись можливостями оформлення колонтитулів.

Шрифт і відступи. Текст пояснювальної записки повинен бути набраний у будь-якому текстовому редакторі (наприклад, Microsoft Office Word) шрифтом гарнітури Times New Roman кеглем 14. Текст записки слід друкувати через півтора інтервали. Текст розміщують таким чином, щоб відстань від рамки до робочого поля становила: зліва і справа – не менше 5 мм; зверху і знизу – не менше 10 мм. Наявність рамок у додатках не є обов'язковою.

Нумерація сторінок. Сторінки повинні бути пронумеровані, починаючи з четвертої (перша сторінка розділу ЗМІСТ). Сторінки 1-3 (які містять

титульний аркуш, індивідуальне завдання, анотація) не нумеруються. Сторінки пояснювальної записки слід нумерувати арабськими цифрами, додержуючись наскрізної нумерації впродовж усього тексту. Номер сторінки проставляють у відповідному місці рамки. Нумерація додатків продовжує основну нумерацію.

Оформлення розділів і підрозділів. Структурними елементами основної частини ПЗ є розділи, підрозділи, пункти, підпункти, переліки.

Розділ – головна ступінь поділу тексту, позначена номером і має заголовок. *Підрозділ* – частина розділу, позначена номером і має заголовок. *Пункт* – частина розділу чи підрозділу, позначена номером і може мати заголовок. *Підпункт* – частина пункту, позначена номером і може мати заголовок. Заголовки структурних елементів необхідно нумерувати тільки арабськими числами.

Кожен розділ рекомендується починати з нової сторінки. Заголовки усіх основних розділів (заголовки першого рівня) записуються з абзацу великими літерами з вирівнюванням по ширині. Заголовки розділів, що містять анотацію, зміст, список використаних джерел виконують також великими літерами, однак вирівнювання відбувається посередині рядка. Після заголовків розділів пропускають один рядок.

Заголовки усіх підрозділів, пунктів та підпунктів записують з абзацу. Перед заголовками підрозділів і після них пропускають один рядок. Назви розділів і підрозділів не повинні мати крапки в кінці.

В кінці назви пунктів та підпунктів ставиться крапка і потім з нового речення починається викладення їх змісту, тобто виділяти їх заголовки відступами не потрібно. Заголовки розділів і підрозділів, пунктів і підпунктів не повинні містити знаків переносу на новий рядок.

Основні розділи нумерують порядковими номерами в межах всього документа (1, 2, і т.д.). Підрозділи нумерують в межах кожного розділу, пункти – в межах підрозділу і т.д. за формою: 1.1, 1.2 – для розділів; 1.2.1, 1.2.2 – для пунктів; 1.2.2.1, 1.2.2.2 – для підпунктів. Цифри, які вказують номер, не повинні виступати за абзац. Після номера крапку не ставлять, а пропускають один знак. Допускається розміщувати текст між заголовками розділу і підрозділу.

Переліки. В тексті документа може наводитись перелік, який рекомендується нумерувати малими літерами української абетки з дужкою або дефіс перед текстом. Для подальшої деталізації використовують арабські цифри з дужкою. Наприклад,

а) тут пишеться текст першого пункту з переліку та його продовження;

б) тут пишеться текст другого пункту з переліку і подальша його деталізація:

1) текст переліку подальшої деталізації переліку вищого рівня та його продовження;

2) . . . ;

в) останній пункт переліку.

Оформлення таблиць. Таблицю розміщують симетрично до тексту після першого посилання на даній сторінці або на наступній, якщо на даній вона не уміщується і таким чином, щоб зручно було її розглядати без повороту або з поворотом на кут 90°. Таблиці у тексті пояснювальної записки набираються шрифтом розміром 10-12. Таблиці у тексті пояснювальної записки набираються основним шрифтом, в деяких випадках розмір шрифту може бути зменшений до 10-12. Підписи таблиць розташовуються над таблицею із зазначенням її номеру і назви, вирівнявши за лівою межею. Наприклад,

Таблиця 2.1 – Характеристики давачів

Характеристика	Аргус-2	Аргус-3	Волна-5	Тюльпан-3
Максимальна дальність дії, м	2-16	2-7,5	2-16	1,5-17
Ширина зони чутливості при максимальній дальності, м	7	4	6	12
Висота зони чутливості при максимальній дальності, м	5	3	8	7
Кут огляду у горизонтальній плошині, гр.	100	110	-	100
Кут огляду у вертикальній плошині, гр.	75	75	-	60
Площа контролю, $м^2$	90	25	90	90
Об’єм контролю, $м^3$	200	40	-	250

На всі таблиці мають бути посилання за формою “ ... в табл. 2.1 або в дужках за текстом (табл. 2.1). Посилання на раніше наведену таблицю дають зі

скороченим словом "дивись" (див. табл. 2.1) за ходом чи в кінці речення.

При перенесенні частин таблиці на інші сторінки, повторюють або продовжують найменування граф. Допускається виконувати нумерацію граф на початку таблиці і при перенесенні частин таблиці на наступні сторінки повторювати тільки нумерацію граф. У всіх випадках найменування (при його наявності) таблиці розміщують тільки над першою частиною, а над іншими частинами зліва пишуть "Продовження таблиці 2.1" без крапки в кінці, наприклад,

Продовження таблиці 2.1

Характеристика	Аргус-2	Аргус-3	Волна-5	Тюльпан-3
Діапазон швидкостей переміщення, що фіксуються м/с	від 0,3 до 3	від 0,3 до 3	від 0,3 до 3	від 0,3 до 3
Напруга живлення, В	10,2 - 15	10,2 - 15	10 - 72	10,2 - 24
Струм, мА	16	30	70	30
Діапазон робочих температур, 0С	-30...+50	-10...+50	-30...+50	-30...+50
Габарити, мм	98x85x62	90x75x40	98x85x62	90x75x40
Маса, г	250	100	200	250

Оформлення рисунків. Рисунки розміщують в тексті або в додатках. В тексті рисунок розміщують симетрично до тексту після першого посилання на нього або на наступній сторінці, якщо на даній для нього не вистачає місця, без повороту. На всі рисунки мають бути посилання за формою: " ... на рис. 2.1", або в дужках по тексту (рис. 2.1). Посилання на раніше наведений рисунок дають зі скороченим словом "дивись" (див. рис. 2.1) за ходом чи в кінці речення.

Кожен рисунок повинен мати номер і підпис, розташовані під рисунком по центру. Нумерують рисунки в межах розділів, вказуючи номер розділу і порядковий номер рисунку в розділі, розділяючи їх крапкою. Дозволяється нумерувати рисунки в межах всього документа. Між номером та назвою рисунку ставлять тире. Крапку в кінці підпису не ставлять, знак переносу не використовують. Якщо найменування рисунка довге, то його продовжують у наступному рядку.

Між рисунком і текстом пропускають один рядок. Наприклад,

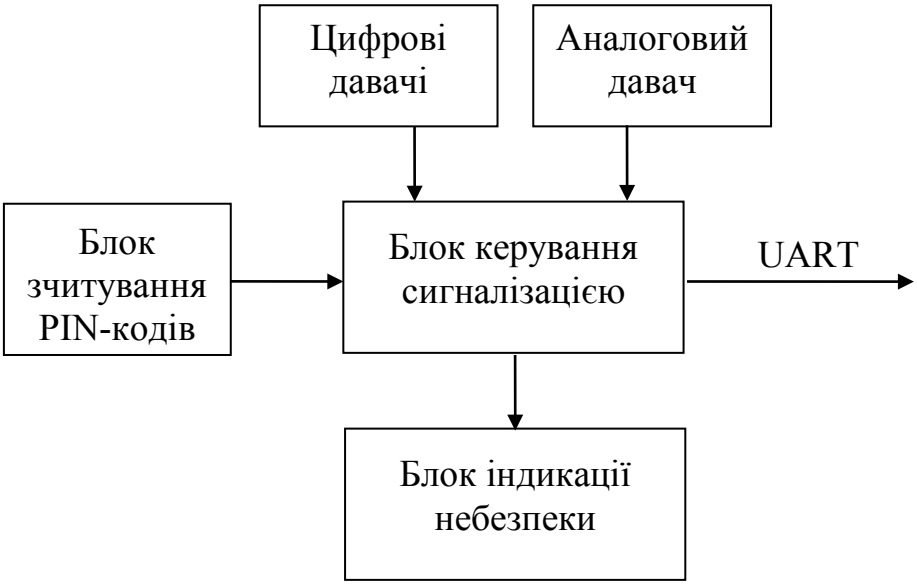


Рисунок 2.1 – Узагальнена схема охоронної сигналізації

Оформлення формул. Кожну формулу записують з нового рядка, симетрично до тексту, курсивом. Між формулою і текстом пропускають один рядок.

Умовні літерні позначення (символи) в формулі повинні відповідати установленим ДСТУ IEC 60027-1, ДСТУ IEC 60027-2. Їх пояснення наводять в тексті або зразу ж під формулою. Для цього після формули ставлять кому і записують пояснення до кожного символу з нового рядка в тій послідовності, в якій вони наведені у формулі, розділяючи крапкою з комою. Перший рядок повинен починатися з абзацу зі слова "де" і без будь-якого знака після нього.

Всі формули нумерують в межах розділу арабськими числами. Номер вказують в круглих дужках з правої сторони, в кінці рядка, на рівні закінчення формули. Номер формули складається з номера розділу і порядкового номера формули в розділі, розділених крапкою. Дозволяється виконувати нумерацію в межах всього документа.

2.7 Графік виконання курсового проекту і порядок його захисту

Рекомендується такий графік виконання курсового проекту, який враховує самостійну роботу студентів під час 10-го триместру бакалаврату (16 тижнів).

Зміст розділу	Термін виконання
Отримання завдання на курсовий проект, розробка і оформлення індивідуального завдання	1 тиждень
Аналіз підходів до проектування та обґрунтування вибору одного з них. Аналіз структури об’єкта захисту, оформлення індивідуального завдання	2 тиждень
Оформлення технічного завдання	3 тиждень
Розробка загальної структури пристрою та алгоритму його роботи. Розробка схеми роботи системи.	4-7 тижні
Розробка та деталізація структурних компонентів пристрою	8-10 тижні
Реалізація пристрою. Розробка схеми електричної.	11-12 тижні
Написання програми для мікроконтролера.	12-14 тижні
Здача курсового проекту на попередню перевірку: демонстрація чернетки пояснювальної записки	14 тиждень
Корегування і доповнення згідно зауважень керівника курсового проекту, врахування і виправлення пояснювальної записки	15 тиждень
Захист курсового проекту	16 тиждень

Готовність до захисту курсового проекту визначає керівник за результатами попередньої перевірки якості пояснювальної. Записка повинна бути здана керівнику на перевірку не менш, як за тиждень до визначеного терміну захисту проекту. Якщо курсовий проект виконаний в повному обсязі та у ньому відсутні принципові помилки, керівник допускає студента до захисту. В іншому випадку проект повертається студенту на доопрацювання. Після позитивного висновку про готовність курсового проекту студент повинен захистити його перед комісією у складі двох викладачів, які призначені кафедрою.

ПЕРЕЛІК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1. Лужецький В. А. Основи інформаційної безпеки / В. А. Лужецький, А. Д. Кожухівський, О. П. Войтович. – Вінниця: ВНТУ, 2013. – 267 с.

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

3. Цирульник С. М. Проектування мікропроцесорних систем / С. М. Цирульник, Г. Л. Лисенко. – Вінниця: ВНТУ, 2010. – 201 с.

4. Мікропроцесорна техніка: Підручник / [Ю. І. Якименко, Т. О. Терещенко, Є. І. Сокол та ін.]; за ред. Т. О. Терещенко. – 2-ге вид., перероб. і доповн. – К.: ІВЦ "Політехніка"; "Кондор", 2004. – 440 с.

5. Тимошенко, Л. П. Схемотехніка пристроїв технічного захисту інформацції [Текст] : навчальний посібник. Ч. 2 / Л. П. Тимошенко ; за ред. В. М. Карташова. – Харків : СМІТ, 2015. – 232 с.

6. Мікропроцесорна техніка: Підручник / [Ю. І. Якименко та ін.]; за ред. Т. О. Терещенко. – 2-ге вид., перероб. і доповн. – К.: ІВЦ "Політехніка"; "Кондор", 2004. – 440 с.

7. Van der Spiegel J. VHDL Tutorial / Jan Van der Spiegel [Електроний ресурс]. – Режим доступу: http://www.seas.upenn.edu/~ese171/vhdl/vhdl_primer.html (дата звернення 22.05.2016) – Назва з екрану.

8. Сергієнко А. М. Вивчення VHDL. Рукопис / Сергієнко А. М. – Режим доступу до ресурсу: – http://kanyevsky.kpi.ua/VHDLlabukraine/resourse/All/VHDL/VHDL_context.html (дата звернення 22.05.2016) – Назва з екрану.

9. Самофалов К. Г. Цифровые ЭВМ. Теория и применение. / К. Г. Самофалов, В. И. Корнейчук, В. П. Тарасенко. – К.: Выща школа, 1983. – 454 с.

10. Казимир В. В. Проектування комп'ютерних систем на основі мікросхем програмованої логіки : монографія / С. А. Іванець, Ю. О. Зубань, В. В. Казимир, В. В. Литвинов. – Суми : Сумський державний університет, 2013. – 313 с.

11. Мілих, В. І. Електротехніка, електроніка та мікропроцесорна техніка [Текст] : підручник / В. І. Мілих, О. О. Шавьолкін ; за ред. В.І. Мілих. – 2-ге вид. – К. : Каравела, 2008. – 688 с.

12. AVR Tutorials [Електроний ресурс]. Режим доступу: http://www.avr-tutorials.com/ (дата звернення 23.05.2016) – Назва з екрану.

13. Lilja D. Designing Digital Computer Systems with Verilog. / David J. Lilja, Sachin S. Sapatnekar. – New York: Cambridge University Press, 2004. – 160 p.

14. Поляков А. К. Языки VHDL и Verilog в проектировании цифровой аппаратуры. / А. К. Поялков. – М. : СОЛОН-Пресс, 2003. – 320 с.

15. Баранов В. Н. Применение микроконтроллеров AVR : схемы, алгоритмы, программы. / В. Н. Баранов. – М. : Издательский дом "Додэка-XXI", 2004. – 288 с.

16. Beginners Programming in AVR Assembler [Електроний ресурс]. Режим доступу: http://www.avr-asm-tutorial.net/avr_en/beginner/ (дата звернення 10.05.2016) – Назва з екрану.

17. Бродин В. Б. Системы на микроконтролерах и БИС программируемой логики / В. Б. Бродин, А. В. Калинин. – М.: Издательство Эком, 2002. – 400 с.

18. Бабич М. П. Комп’ютерна схемотехніка: Навчальний посібник / М. П. Бабич, І. А. Жуков. – К.: "МК-Прес", 2004. – 412 с.

19. Мельник А. Архітектура комп’ютера. Наукове видання / А. Мельник. – Луцьк: Волинська обласна друкарня, 2008. – 470 с.

20. Злобін Г. Г. Архітектура та апаратне забезпечення ППК: навчальний посібник для студентів вищих навчальних закладів / Г. Г. Злобін, Р. Є. Рикалюк – К. : Каравела, 2006. - 304 с.

21. Поточные шифры. / [А. В. Асосков и др.] – М. : КУДИЦ-ОБРАЗ, 2003. – 336 с.

22. Фергюсон Н. Практическая криптография : пер. с англ. / Н. Фергюсон, Б. Шнайер. - М. : Издательский дом "Вильямс", 2005. – 424 с.

23. Введение в криптографию. / Под ред. В. В. Ященко. – М. : МЦНМО, 2000. – 288 с.

24. Рябко Б. Я. Криптографические методы защиты информации. Учебное пособие для вузов. / Б. Я. Рябко, А. Н. Фионов. – М.: Горячая линия-Телеком, 2005. – 229 с.

25. Смарт Н. Криптография / Н. Смарт. – М.: Техносфера, 2005. – 528 с.

26. Логачев О. А. Булевы функции в теории кодирования и криптологии. / О. А. Логачев, А. А., Сальников, В. В. Ященко. – М.: МЦНМО, 2004. – 470 с.

27. Щербаков Л. Ю. Прикладная криптография. Использование и синтез криптографических интерфейсов. / Л. Ю. Щербаков, А. В. Домашев. – М.: Издательско-торговый дом "Русская Редакция", 2003. – 416 с.

28. Василенко О. Н. Теоретико-числовые алгоритмы в криптографии / О. Н. Василенко. – М. : МЦНМО, 2003. – 328 с.

29. Петров А. А. Компьютерная безопасность. Криптографические методы защиты / А. А. Петров. – М.: ДМК, 2000. – 448 с.

30. Лужецький В. А. Апаратні засоби для реалізації багатоканального керованого хешування. / В. А. Лужецький, Ю. В. Баришев // Системи обробки інформації. – №3. – 2011. – С. 130-133.

31. Лужецький В. А. Криптографічні примітиви для реалізації керованого хешування / В. А. Лужецький, Ю. В. Баришев // Вісник ВПІ. – №1. – 2011. – С. 108-111.

32. Лужецький В. А. Підходи до побудови швидких алгоритмів хешування / В. А. Лужецький, Ю. В. Баришев // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – №. 2 (19), 2009 р. – С. 57-65.

33. Luzhetskyi V. A. Methods of Generic Attacks Infeasibility Increasing for Hash Functions / Volodymyr Luzhetskyi, Yurii Baryshev // The 7th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS’2013), September 12-14, 2013 Berlin, Germany. – P. 661-664

34. Баришев Ю. В. Структура спеціалізованого криптографічного процесора для керованого хешування / Баришев Ю. В. // Сучасні проблеми радіоелектроніки, телекомунікацій та приладобудування (СПРТП-2011):

матеріали V Міжнародної науково-технічної конференції, м. Вінниця, 19-21 травня 2011 р. – Вінниця: ВНТУ, 2011. – С. 169-170.

35. Баришев Ю. В. Структури спеціалізованих процесорів для гешування, стійкого до загальних атак / Баришев Ю. В., Зозуля А. О. // Тези доповідей Четвертої Міжнародної науково-практичної конференції «Інформаційні технології та комп'ютерна інженерія» м. Вінниця, 28-30 травня 2014 року. – Вінниця: ВНТУ, 2014. – С 216-219.

36. Баришев Ю. В. Структури спеціалізованих мікропроцесорів для передавання даних в лініях з великим рівнем завад. / Баришев Ю. В., Репетій В. М. // Тези доповідей Четвертої Міжнародної науково-практичної конференції «Інформаційні технології та комп'ютерна інженерія» м. Вінниця, 28-30 травня 2014 року. – Вінниця: ВНТУ, 2014. – С 222-223.

37. Рудницький В. М. Модель уніфікованого пристрою криптографічного перетворення інформації / В. М. Рудницький, В. Г. Бабенко // Системи обробки інформації. – №3. – 2009. – С. 91-95.

38. Патент України на корисну модель № 94039 МПК G 09 C 1/00. Спосіб паралельного ключового гешування даних теоретично доведеної стійкості / Лужецький В. А., Баришев Ю. В.; .заявник та патентовласник Вінницький національний технічний університет. – № u201405191; заявл. 16.05.2014; опубл. 27.10.2014, Бюл. № 20.

39. Патент України на корисну модель № 53615 МПК H 04 L 9/06. Спосіб шифрування даних на основі трьох несумісних груп операцій / Лужецький В. А., Дмитришин О. В., Баришев Ю. В.; .заявник та патентовласник Вінницький національний технічний університет. – № u201004697; заявл. 20.04.2010; опубл. 11.10.2010, Бюл. № 19.

40. Шауман А. М. Основы машинной арифметики / Шауман А. М. – Л. : Изд-во Ленингр. ун-та, 1979. – 312 с.

Додаток А. Тематика курсового проектування

1. Пристрій для шифрування даних за допомогою алгоритму Seal
2. Пристрій для шифрування даних за допомогою регістрів зсуву з нелінійним зворотнім зв’язком.
3. Пристрій для шифрування даних за допомогою алгоритму RC5
4. Пристрій для шифрування даних за допомогою алгоритму AES
5. Пристрій для шифрування даних за допомогою алгоритму ГОСТ
6. Пристрій для шифрування даних за допомогою алгоритму Threefish
7. Пристрій для шифрування даних за допомогою алгоритму RSA
8. Пристрій для шифрування даних за допомогою алгоритму ElGamal
9. Пристрій для створення електронного цифрового підпису DSA
10. Пристрій для створення електронного цифрового підпису ECDSA
11. Пристрій для створення електронного цифрового підпису ГОСТ
12. Пристрій для автентифікації даних за допомогою алгоритму SHA-3
13. Пристрій для автентифікації даних за допомогою алгоритму Skein
14. Пристрій для автентифікації даних за допомогою алгоритму BMW
15. Пристрій для автентифікації даних за допомогою алгоритму Blake
16. Засіб захищеного зберігання паролів
17. Апаратний електронний гаманець
18. Електронний ключ для багатофакторної автентифікації локальних користувачів комп’ютерних систем
19. Електронний ключ для багатофакторної автентифікації віддалених користувачів комп’ютерних систем
20. Мікропроцесорна система автентифікації даних за допомогою алгоритму N-геш.
21. Мікропроцесорна система автентифікації користувачів за протоколом Фейга-Фіата-Шаміра
22. Мікропроцесорна система автентифікації користувачів за протоколом Шнорра

23. Мікропроцесорна система генерування та обміну сеансовими ключами за протоколом Діффі-Хеллмана.

24. Мікропроцесорна система генерування та обміну сеансовими ключами за протоколом ECDH

25. Мікропроцесорна система генерування та обміну сеансовими ключами за протоколом "точка-точка".

26. Пристрій для передавання даних лінією із високим рівнем завад на основі кодування Хеммінга.

27. Пристрій для передавання даних лінією із високим рівнем завад на основі групових кодів

28. Пристрій для передавання даних лінією із високим рівнем завад на основі циклічних кодів

29. Пристрій для передавання даних лінією із високим рівнем завад на основі кодування Ріда-Соломона.

30. Охоронна сигналізація з UART інтерфейсом.

31. Охоронна сигналізація з SPI інтерфейсом.

32. Охоронна сигналізація з I2C інтерфейсом.

33. Охоронна сигналізація з USB інтерфейсом.

34. Охоронна сигналізація з системою оповіщення за допомогою SMS.

35. Інтелектуальний кодовий замок.

36. Система контролю доступу до приміщень.

37. Генератор маскуючого шумоподібного сигналу.

38. Пристрій захисту від перехоплення інформації з клавіатури комп’ютера.

39. Скремблер на основі частотної перестановки мови.

40. Скремблер на основі частотної інверсії.

41. Скремблер на основі часової перестановки сигналу.

42. Скремблер на основі алгоримту A5.

43. Скремблер на основі алгоримту Sober.

44. Скремблер на основі алгоримту SQ1-R.

45. Скремблер на основі алгоримту Sapphire II.

46. Скремблер на основі схеми Маурера.
47. Скремблер на основі генератора Геффе
48. Скремблер на основі алгоримту Gate.
49. Пристрій біометричної автентифікації користувача.
50. Система відеоспостереження з керуванням видимих зон.

Додаток Б. Приклад оформлення титульного аркуша

Міністерство освіти і науки України
Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації

КУРСОВИЙ ПРОЕКТ
з дисципліни "Основи побудови мікропроцесорних систем"
на тему: "Мікропроцесорна система автентифікації користувачів за протоколом Фіата-Шаміра"
08-20.ОПМПС.017.01.101 ПЗ

Студента (ки) 4 курсу 1БС-16б групи
напряму підготовки 125 – Кібербезпека
спеціальності _____
Іваненка Бориса Степановича
(прізвище та ініціали)
Керівник доц. каф. ЗІ, к. т. н.
Баришев Ю. В.
(посада, вчене звання, науковий ступінь, прізвище та ініціали)

Національна шкала _____
Кількість балів: _____ Оцінка: ECTS _____

Члени комісії:
_____ _____
(підпис) (прізвище та ініціали)
_____ _____
(підпис) (прізвище та ініціали)
_____ _____
(підпис) (прізвище та ініціали)

м Вінниця 2017 року

Інв. № | Підпис та | На зам. | Інв. № | Підпис та

ЗМІСТ

					08-20.ОПМПС.017.01.101 ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата				
Розроб.		Іваненко Б. С.			Мікропроцесорна система автентифікації користувачів за протоколом Фіата-Шаміра. Пояснювальна записка	Літ.	Арк.	Аркушів
Перевір.		Баришев Ю. В.					4	42
Реценз.						ВНТУ, гр. 1 БС-16б		
Н. Контр.		Баришев Ю. В.						
Затверд.		Лужецький В. А.						

ВСТУП

Віддалена обробка інформації сприяє збільшенню швидкості її обробки та передавання, а як наслідок покращенню прийнятих управлінських рішень. Така можливість забезпечується низкою технологій, зокрема криптографічними протоколами автентифікації користувачів, які дозволяють захистити конфіденційність та автентичність інформації, що обробляється віддалено. Водночас впровадження протоколів автентифікації ускладнюється низкою обставин. Основними з яких є недостатня швидкість реалізації алгоритмів автентифікації та низка атак на підсистеми автентифікації, зокрема перехоплення повторне надсилання автентифікаційних даних користувача. Використання спеціалізованих процесорів як основи для реалізації криптографічних перетворень дозволить усунути перший недолік, а використання протоколів "з нульовим знанням" – другий [1, 2]. Саме тому розробка пристрою, що реалізує протокол Фіата-Шаміра, стійкість якого не потребує передавання стороною, що автентифікується, її секрету іншій стороні [1, 3-5], є актуальною для галузі кібербезпеки зокрема та інформаційних технологій загалом.

Об’єктом курсового проектування є мікропроцесорні системи автентифікації користувачів. Предметом – мікропроцесорна система автентифікації за протоколом Фіата-Шаміра.

Метою даного курсового проекту є збільшення швидкодії інформаційних систем під час автентифікації користувачів.

Для досягнення мети необхідно розв’язати такі задачі:

- аналіз відомих протоколів автентифікації;
- огляд відомих пристроїв автентифікації;
- розробка структури мікропроцесорної системи автентифікації користувачів;
- розробка алгоритмів роботи блоків даної структури;
- реалізація та тестування коректності роботи мікропроцесорної системи.

Додаток Д. Приклад оформлення індивідуального завдання

Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії

ЗАТВЕРДЖУЮ

Зав. кафедри ЗІ, д. т. н., професор

_____В. А. Лужецький

ІНДИВІДУАЛЬНЕ ЗАВДАННЯ

на курсовий проект з дисципліни "Основи побудови мікропроцесорних систем"
студенту групи 1БС-16б Іваненку Борису Степановичу
Тема: "Мікропроцесорна система автентифікації користувачів за протоколом Фіата-Шаміра"

1. Проаналізувати відомі мікропроцесорні системи електронного цифрового підпису та алгоритми їх роботи.
2. Розробити структуру мікропроцесорної системи та деталізувати її елементи. Результати роботи оформити у вигляді схеми електричної структурної.
3. Розробити алгоритм роботи мікропроцесорної системи та її структурних елементів. Результати роботи оформити у вигляді схеми роботи системи.
4. Виконати перевірку коректності роботи системи за допомогою середовища моделювання.

Вихідні дані:
тип мікроконтролера – з жорсткою логікою;
середовище моделювання – ModelSim;
розрядність ключа – 256 бітів;
інтерфейс – UART;
швидкість обміну даними – 19 200 біт/с.

Дата видачі 04 вересня 2017 р.

Керівник _____ Ю. В. Баришев

Завдання отримав _____ Б. С. Іваненко

Додаток Ж. Приклад оформлення технічного завдання

Вінницький національний технічний університет
Факультет інформаційних технологій та комп’ютерної інженерії

ЗАТВЕРДЖУЮ
Керівник, к. т. н., доцент кафедри ЗІ
_____ Ю. В. Баришев
_____ 20__ р.

ТЕХНІЧНЕ ЗАВДАННЯ
на курсовий проект
з дисципліни "Основи побудови мікропроцесорних систем"
на тему: "Мікропроцесорна система автентифікації користувачів за протоколом Фіата-Шаміра"
08-20.ОПМПС.017.01.101 ТЗ

Вінниця 2017

1 Назва та галузь використання

Мікропроцесорна система автентифікації користувачів за протоколом Фіата-Шаміра призначена для захисту автентичності джерела даних, що зберігаються та передаються інформаційно-комунікаційними мережами.

2 Основа для розробки

Робоча навчальна програма та робочий план дисципліни "Основи побудови мікропроцесорних систем".

3 Мета та призначення розробки

Покращення швидкості автентифікації користувачів комп’ютерної системи шляхом розробки спеціалізованох мікропроцесорної системи, що реалізує протокол Фіата-Шаміра.

Мікропроцесорна система призначена для перевірки автентичності користувача комп’ютерної системи "з нульовим знанням" його секретної інформації.

4 Джерела розробки

1. Казимир В. В. Проектування комп'ютерних систем на основі мікросхем програмованої логіки : монографія / С. А. Іванець, Ю. О. Зубань, В. В. Казимир, В. В. Литвинов. – Суми : Сумський державний університет, 2013. – 313 с.

2. Fiat A. How to Prove Yourself: Practical Solutions to Identification and Signature Problems / Amos Fiat, Adi Shamir. – p. 9. – Режим доступу до джерела: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.13.8796&rep=rep1&type=pdf

3. Фергюсон Н. Практическая криптография : пер. с англ. / Н. Фергюсон, Б. Шнайер. - М. : Издательский дом "Вильямс", 2005. – 424 с.

5 Вимоги до системи

5.1 Параметри розроблюваної системи:

- протокол автентифікації – схема Фіата-Шаміра;
- кількість ітерації автентифікації – 10;
- довжина ключа – 256 бітів;
- тип мікроконтролера – з жорсткою логікою;
- тактова частота роботи системи – не менше 4 МГц;
- діапазон робочих температур – від +12 до +30 ^{0}C;
- швидкість обміну даними – 19 200 біт/с.

5.2. Вимоги до апаратного і програмного забезпечення, на якому повинна працювати система:

- інтерфейс – UART;

- формат кадру – 11 біт;
- середовище моделювання – ModelSim;
- мова розробки – VHDL.

5.3 Вимоги щодо тестування. Тестування повинно проводитись методом комп'ютерного моделювання з використанням програмного пакету ModelSim. Тестування повинно передбачати проведення таких експериментів:

- створення ключів для автентифікації;
- генерування рівномірно розподілених запитів сторони В довжиною 10 біт;
- перевірка коректності повідомлення від сторони А;
- перевірка коректності спотвореного повідомлення від сторони А.

5.4 Вимоги до техніки безпеки при роботі з системою повинні відповідати існуючим вимогам та стандартам з техніки безпеки при користуванні комп'ютерною технікою.

6 Вимоги до супровідної документації

6.1 Графічна і текстова документація повинна відповідати діючим стандартам України.

6.2 Пристрій повинен супроводжуватись:

- лістингом програми;
- результатами тестування роботи мікропроцесорної системи;
- схемою електричною структурною мікропроцесорної системи автентифікації користувачів за протоколом Фіата-Шаміра;
- схемою роботи системи автентифікації користувачів за протоколом Фіата-Шаміра;
- схемою електричною структурною блоку модульної арифметики;
- схемою роботи системи для блоку модульної арифметики.

7 Стадії та етапи розробки

Робота з теми виконується у 7 етапів.

Етап	Зміст	Початок	Закінчення	Результат
1	Аналіз протоколів автентифікації	15.09.17	22.09.17	Чорновий варіант розділу 1
2	Огляд відомих мікропроцесорних систем формування електронних цифрових підписів	23.09.17	29.09.17	Чорновий варіант розділу 1
3	Розробка структури мікропроцесорної системи	30.09.17	21.10.17	Схема електрична структурна, чорновий варіант розділу 2

Етап	Зміст	Початок	Закінчення	Результат
4	Розробка алгоритмів роботи мікропроцесорної системи	22.10.17	05.11.17	Схема роботи системи, чорновий варіант розділу 3
5	Розробка програми	06.11.17	20.11.17	Лістинг програми, чорновий варіант розділу 3
6	Тестування роботи мікропроцесорної системи	20.11.17	02.12.17	Результати тестування, чорновий варіант розділу 3
7	Оформлення пояснювальної записки	03.12.17	10.12.17	Пояснювальна записка

8 Порядок контролю та прийому.

До прийому і захисту курсового проекту подається:
- заключний звіт;
- лістинг програми;
- Мікропроцесорна система автентифікації користувачів за протоколом Фіата-Шаміра. Схема електрична структурна;
- Мікропроцесорна система автентифікації користувачів за протоколом Фіата-Шаміра. Схема роботи системи;
- Блок модульної арифметики. Схема електрична структурна;
- Блок модульної арифметики. Схема роботи системи.

Початок розробки 15. 09.2017.
Крайній термін виконання курсового проекту 10.12.2017.

Розробив студент групи 1БС-16б _____ Б. С. Іваненко