Головчак В.З, Шимоняк А. І. – гр. КТм-51

Тернопільський національний технічний університет ім. І. Пулюя

ДОСЛІДЖЕННЯ ПРИСТРОЇВ КОНФІДЕНЦІЙНОГО ЗВ’ЯЗКУ ДЛЯ ПЕРЕТВОРЕННЯ МОВНИХ СИГНАЛІВ НА БАЗІ ТЕЛЕФОННИХ МЕРЕЖ

Науковий керівник к.т.н. доц. Курко А.М.

АВТОРЕФЕРАТ

Магістерської роботи

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми.

У сучасних умовах інформація відіграє вирішальну роль як у процесі економічного розвитку, так і в ході конкурентної боротьби на національному і міжнародному ринках. Протиборство розгорнулося за перевагу в тих областях, які визначають напрямки науково-технічного процесу. Це обумовлено тим, що отримання скільки-небудь достовірної інформації про об'єкти зацікавленості законним шляхом стає неможливим через створення і підтримку визначеної системи захисту цінної інформації від несанкціонованого, тобто протиправного, доступу з боку зловмисників.

Аналіз різних способів одержання інформації про конкурентів дозволив встановити, що підслуховування телефонних переговорів у ряді випадків може бути одним з ефективних способів несанкціонованого доступу до конфіденційної інформації. Це пояснюється тим, що в даний час обмін інформацією по телефону є дуже розповсюдженим і практично у всіх випадках, коли абонентам не потрібно письмового документа і є можливість скористатися телефонним зв'язком, вони нею користаються. Найефективнішим способом захисту телефонних повідомлень від несанкціонованого доступу є криптографічне перетворення. При цьому змінити його так, щоб відновлення вихідного повідомлення санкціонованим абонентом здійснювалося дуже просто, а відновлення повідомлення

зловмисником було б неможливим чи вимагало б істотних тимчасових чи матеріальних витрат, що робило б сам процес відновлення неефективним.

Саме такими властивостями і володіють криптографічні перетворювачі, задачею яких є забезпечення математичними методами захисту переданих конфіденційних телефонних повідомлень. Навіть у випадку їхнього перехоплення зловмисниками й обробки будь-якими способами з використанням самих швидкодіючих супер-ЕОМ і останніх досягнень науки та техніки зміст самих повідомлень повинен бути розкритий тільки на протязі заданого часу, наприклад, протягом декількох десятків років.

Мета і задачі дослідження. Метою написання дипломного проекту було дослідити пристрої конфіденційного зв’язку для перетворення мовних сигналів на базі телефонних мереж.

Наукова новизна і практичне значення одержаних результатів. Результати дослідження можуть бути використані в проектуванні систем криптозахисту.

Особистий внесок. Розроблений пристрій криптозахисту базується на використанні алгоритму шифрування DES, який дозволяє здійснювати обмін інформації при використанні з пристроями інших фірм з аналогічним алгоритмом шифрування.

ОСНОВНИЙ ЗМІСТ

У вступі описано важливість захисту інформації у сучасних умовах. Висвітлено актуальність даного дослідження і його основні переваги.

Перший розділ. Проведено аналіз відомих технічних рішень з питань захисту інформації, переданої по каналах електрозв'язку, від несанкціонованого доступу, а також аналіз основних шляхів витоку інформації. Приведено методи скремблювання і шифрування.

Другий розділ. Розглянуто алгоритм шифрування DES — алгоритм засекречування даних розроблений для шифрування і дешифрування блоків даних, які складаються з 64 біт, при впливі на них ключа, також 64 біти.

Дешифрування здійснюється за допомогою того ж самого ключа, який використовується для шифрування, але з адресацією біт, видозміненою так, щоб дешифрування було б оберненим процесу шифрування.

У третьому приведено загальні принципи побудови пристроїв конфіденційного зв'язку. Розглянуто методи шифрування й основні поняття криптографії, а саме:

1) метод шифрування "перестановками";
2) метод використання гратів та циферблатів;
3) метода використання тексту будь-якої книги або книжкових шифрів;
4) методи використання механічних машин;
5) метод засекречування даних DES (Data Encryption Standard).

Оглянуто стандарт шифрування DES, наведено основні визначення.

У четвертому розділі було описано технічні вимоги до системи взаємодії з периферійними пристроями при обробці даних у системі DES. Наведено опис розроблення функціональної схеми системи взаємодії з периферійними пристроями. Проведено вибір елементної бази та розроблено електричну схему системи взаємодії з периферійними пристроями. Описано структурну схему OMEOM MCS51 та її основні функціональні вузли:

1) центральний процесорний пристрій;
2) постійний запам'ятовуючий пристрій пам'яті програми;
3) оперативний запам'ятовуючий пристрій пам'яті даних;
4) задаючий генератор;
5) програмовані паралельні порти;
6) послідовний порт;
7) таймери/лічильники;
8) розширювач шини для роботи з зовнішнім запам'ятовуючим пристроєм.

У п’ятому розділі розроблено і налагоджено алгоритмічне і програмне забезпечення системи взаємодії з периферійними пристроями. Наведені правила запису програми мовою ассемблер**.**

У шостому розділі приведено способи покращення організації конструктивної підготовки виробництва, проведено техніко-економічне обґрунтування розробки, розраховано техніко-економічні показники системи взаємодії периферійних пристроїв, оцінено економічну ефективність системи взаємодії периферійних пристроїв при обробці даних у форматі DES.

У сьомому розділі проаналізовано небезпеку і шкідливість при розробці криптосистеми. Розраховано освітленість робочого місця при розробці криптографічних систем. Вказано основні заходи підвищення стійкості роботи виробництва при дії електромагнітного поля або імпульсу на організм людини і заходи захисту. Розглянуто вражаючу дія електромагнітного випромінювання. Наведено методи захисту від впливу електромагнітного випромінювання. Оцінено стійкість промислового цеху до впливу ударної хвилі ядерного вибуху

У восьмому розділі проаналізовано забруднення виробничого та навколишнього середовища відходами виробництва, наведені вимоги до приміщень для експлуатації моніторів і ПЕОМ, а саме:

1) вимоги до моніторів (ВДТ) і ПЕОМ;
2) вимоги до шуму і вібрації;
3) вимоги до освітлення приміщень і робочих місць з моніторами і ПЕОМ.

Висновок. Використавши в даному дипломному проекті однокристальну мікро-ЕОМ, нам вдалося реалізувати в досить компактному пристрої винятково складний алгоритм, який вимагає для своєї реалізації десятки тисяч електронних елементів, об'єднаних у сотні регістрів і схем. Застосування малогабаритної цифрової пам'яті з великими термінами зберігання й обсягами збереженої інформації дозволяє постачати пристрій взапас великою кількістю ключів.

Розроблений пристрій криптозахисту базується на використанні алгоритму шифрування DES, який дозволяє здійснювати обмін інформації

при використанні з пристроями інших фірм з аналогічним алгоритмом шифрування.

СПСОК ОПУБЛІКОВАНИХ АВТОРОМ ПРАЦЬ ЗА ТЕМОЮ РОБОТИ

1. Микитишин А.Г. Головчак В.З. Шимоняк А.І. ДОСЛІДЖЕННЯ ПРИСТРОЇВ КОНФІДЕНЦІЙНОГО ЗВ’ЯЗКУ ДЛЯ ПЕРЕТВОРЕННЯ МОВНИХ СИГНАЛІВ НА БАЗІ ТЕЛЕФОННИХ МЕРЕЖ, // Збірник тез доповідей міжнародної науково-технічної конференції «Фундаментальні та прикладні проблеми сучасних технологій» – Тернопіль 2015