МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧОРНОМОРСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ПЕТРА МОГИЛИ

Румянков Дмитро Ігорович

УДК 004.021:004.056.55

Створення модифікованого блокового методу шифрування на базі операції XOR для корпоративного мессенджера

122 – Комп’ютерні науки

Автореферат
магістерської наукової роботи на здобуття освітньої кваліфікації
«Магістр комп’ютерних наук»

Миколаїв – 2019

Магістерська наукова робота є рукопис.

Робота виконана в Чорноморському національному університеті імені Петра Могили Міністерства освіти і науки України на кафедрі інтелектуальних інформаційних систем.

Науковий керівник: кандидат технічних наук, доцент
І. М. Журавська,
Чорноморський національний університет ім. Петра Могили,
кафедра комп'ютерної інженерії

Рецензент: професор, доктор технічних наук
М. П. Мусієнко,
Чорноморський національний університет ім. Петра Могили,
кафедра комп'ютерної інженерії

Захист відбудеться 23 лютого 2019 р. о $9^{\underline{30}}$ год. на засіданні екзаменаційної комісії (ауд. 2-403) у Чорноморському національному університеті імені Петра Могили за адресою: 54003, м. Миколаїв, вул. 68-ми Десантників, 10.

З магістерською науковою роботою можна ознайомитися в бібліотеці Чорноморського національного університету імені Петра Могили за адресою: 54003, м. Миколаїв, вул. 68-ми Десантників, 10.

Автореферат представлений «___» лютого 2019 р.

Секретар
екзаменаційної комісії,
канд. пед. наук, доцент Н. М. Болюбаш

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. З кожним роком комп'ютерна інформація відіграє все більш важливу роль у житті людини, і все більшої актуальності набувають проблеми захисту такої інформації. Вимогою сьогодення є постійне спілкування між співробітниками будь-якої корпорації при вирішенні виробничих завдань. Таке спілкування найчастіше є найбільш ефективним, коли використовуються комп’ютерні засоби зв’язку – як при спілкуванні двох осіб («вироджена мережа»), так і у локальній мережі в межах одного приміщення (будинку), а також між територіально віддаленими філіями одного підприємства, розташованими навіть у різних містах та країнах.

В каналах зв’язку корпоративній інформації загрожує безліч найрізноманітніших небезпек, починаючи від суто технічних недоліків і закінчуючи протизаконними діями зловмисників. Захист від кожного типу небезпеки передбачає індивідуальний підхід до рішення проблем. Втім, є й універсальні підходи, які здатні забезпечити цілісність та конфіденційність даних від різних загроз:

– фізичні (перешкода, пристрої захисту від місць витоку інформації);

– законодавчі (складання законодавчих актів суто пов’язаних з кіберзлочинністю);

– управління доступом (надання чи обмеження прав доступу до інформації користувачам);

– криптографічне закриття (перетворення інформації до незрозумілого вигляду).

З-поміж усіх груп необхідно виділити криптографічне закриття. Шифрування інформації на сьогодення є найбільш ефективним способом захисту інформації. Для перетворення (шифрування) зазвичай використовується деякий алгоритм чи пристрій, що має реалізацію заданого алгоритму, при чому вони можуть бути відомі широкому колу осіб. Наприклад, це геш-функції MD2 чи MD5, що використовуються в стандартах захисту електронної пошти.

Загальна модель управління процесом шифрування здійснюється за допомогою періодичної зміни ключа шифрування, який забезпечує кожного разу оригінальне представлення інформації при використанні одного й того ж алгоритму або пристрою.

Втім, накопичений досвід використання загальновживаних алгоритмів шифрування підвищує кваліфікацію зловмисників, які полюють на корпоративну інформацію з метою або порушення її конфіденційності, або цілісності, або доступності. Тому актуальним є створення нових або модифікація існуючих алгоритмів шифрування з метою підвищення криптостійкості таких алгоритмів, але з обов'язковою умовою збереження їх швидкодії.

Метою магістерської наукової роботи є розробка модифікованого блочного методу шифрування повідомлень між співробітниками віддалених філій корпорації та створення програмного додатку (мессенджера), який реалізує зазначений метод.

Об'єкт досліджень – процес передачі повідомлень з забезпеченням конфіденційності інформації, що передається відкритими каналами зв'язку через Інтернет.

Предмет досліджень – блочні методи шифрування повідомлень.

Методи дослідження. У процесі модифікації існуючого методу шифрування використовується математичний апарат теорії інформації, систем числення, методів дискретної математики.

Участь у наукових програмах:

– у Міжнародній програмі ЄС Erasmus+ "Internet of Things: Emerging Curriculum for Industry and Human Applications" (Erasmus+ ALIOT, reference number 573818-EPP-1-2016-1-UK–EPPKA2-CBHE–JP, 2016–2019 рр.) під керівництвом д-ра техн. наук, професора Ю. П. Кондратенко;

– у науково-дослідній роботі Чорноморського національного університету ім. Петра Могили «Розроблення бездротових енергонезалежних інформаційно-вимірювальних мереж критичного застосування військово-цивільного призначення» (№ держ. реєстрації 0117U000447, 2017–2018 рр.) під керівництвом д-ра техн. наук, професора М. П. Мусієнко.

Практичне значення отриманих результатів полягає у використанні запропонованого ПЗ із методом шифрування даних для забезпечення конфіденційності на підприємстві ТОВ «Схід-Захід-Енерго» при передачі інформації між віддаленими підрозділами з використанням відкритих каналів мережі Інтернет.

Апробація результатів магістерської наукової роботи. Матеріали роботи пройшли апробацію на двох Міжнародних конференціях (м. Бухарест, м. Вінниця), чотирьох Всеукраїнських конференціях (м. Кривий Ріг, м. Миколаїв).

Публікації. За результатами роботи опубліковано 9 наукових праць, з яких одна проіндексована в наукометричній базі Scopus, 2 опубліковані у наукових фахових журналах України, отриманий 1 патент України на корисну модель, надруковано 5 тез доповідей.

Структура магістерської наукової роботи. Магістерська наукова робота складається із вступу, 5 розділів, висновків, 4 додатків. Загальний обсяг роботи складає 128 сторінок, 37 рисунків, 2 таблиці та 47 посилань на літературні джерела.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі подано загальну характеристику досліджуваної теми, обґрунтовано актуальність магістерської наукової роботи, сформульовано мету, завдання досліджень, відзначено наукову новизну та практичну цінність отриманих результатів, подано інформацію про апробацію, структуру та обсяг роботи.

У першому розділі висвітлена проблема інформаційної безпеки, яка стала дуже важливим аспектом сучасних систем зв'язку. Необхідність використання мережі Інтернет як середовища зв'язку між територіально віддаленими користувачами комп'ютерних систем створює ризик для користувачів стати жертвами крадіжки надісланих чи отриманих повідомлень в мережі. У цьому випадку шифрування повідомлень стає невід'ємною частиною концепції безпечного зв'язку. Виконано аналіз інформаційних правопорушень, а також розглянуто існуючі типи методів шифрування і основні характеристики корпоративної мережі для підприємства.

У другому розділі проаналізовано алгоритми шифрування корпоративних мессенджерів Skype, Viber та Telegram, проведено дослідження криптостійкості методів шифрування на базі операції XOR, визначені кількісні показники стійкості до злому алгоритму з використанням функції XOR.

У третьому розділі здійснено розробку алгоритму шифрування модифікованою операцією XOR, а також було впроваджено геш-функції до модифікованого методу шифрування повідомлення. Модифікація методу шифрування полягає у застосуванні підмішування ключа до кожного блоку геш-функції шифрування для їх зціплення. Також модифіковано процес змішування даних блоків й застосування жорсткого зчеплення складових блоків випадковими величинами симетричного ключа із відповідними рангами. Більш докладніше роботу алгоритму можна побачити на відповідній блок-схемі.

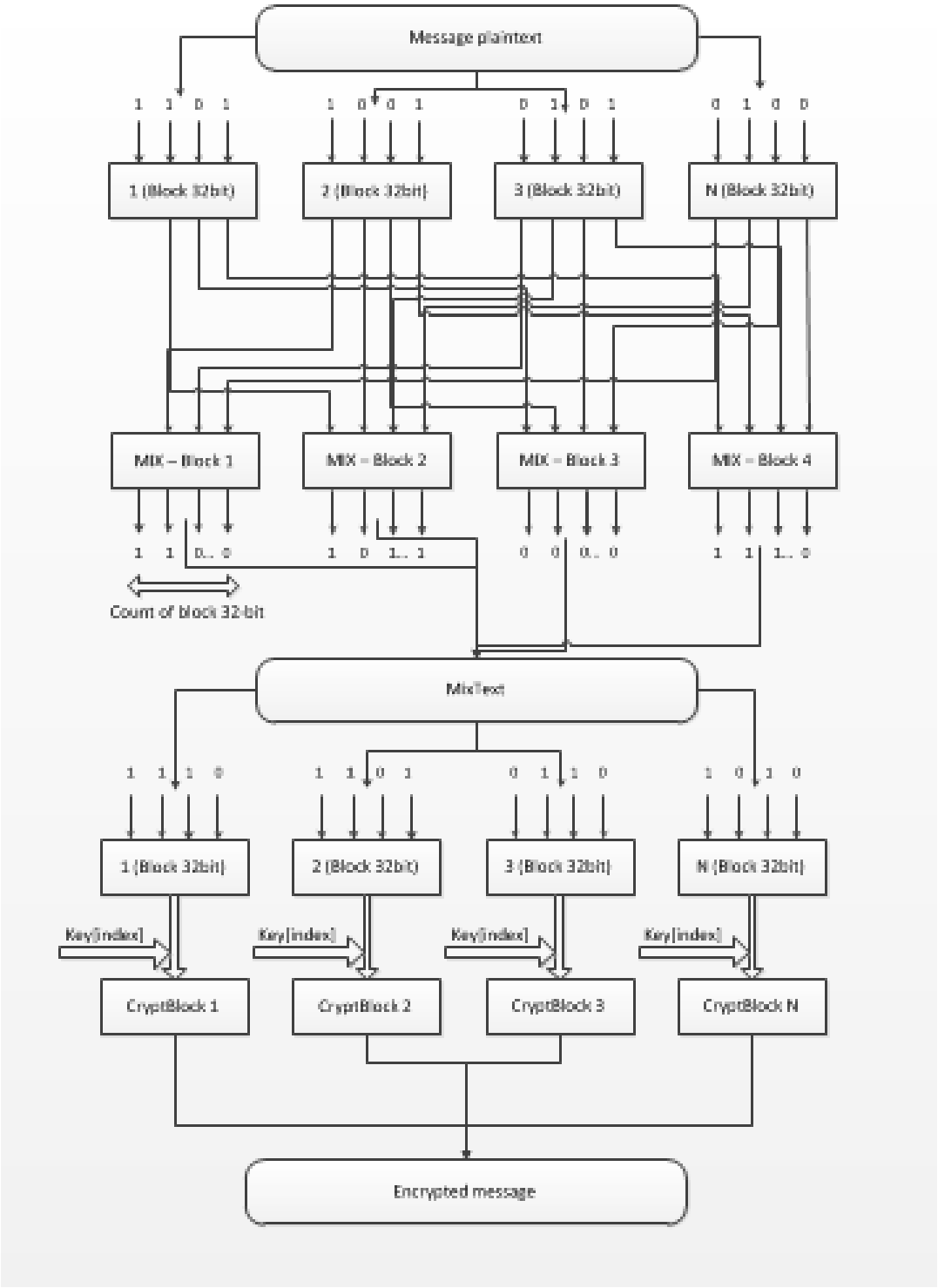

Рис. 1. Узагальнена блок-схема роботи алгоритму шифрування

Запропоновано нові методи утворення раундів без використання складних математичних обчислень множення, обрахунку кореня та зведення числа в ступінь, а лише на основі операції XOR, яка виконує домішування до загальної послідовності окремих значень, що вводять залежність для розшифрування та не збільшують час виконання методу.

Таблиця 1. Середній час тестів для криптографічних перетворень

Вид тестування	**Результати**
Швидкість виконання шифрування (с)	0,253 с (500 байтів)
Швидкість виконання дешифрування (с)	0,259 с (500 байтів)
Частотність (%)	12 % (500 байтів)
Актуальність переданої інформації	1 година
Криптостійкість	5 днів

Як показують наведені в табл. 1 результати, запропонований метод швидко виконує операції шифрування та дешифрування інформації. За рахунок розбиття на блоки буде отримана унікальність значень байтів для кожного блоку на основі циклічних повторів використання операції XOR до кожного байту відповідного блоку. Це дозволяє отримати послідовності байтів, які містять у собі «білий шум» разом з чистою інформацією.

Завдяки модифікації шифрування на основі простих обчислювальних операцій перестановок, зміщенням та використання бінарної операції XOR, отримані високі показники криптостійкості системи до злому та збалансованість між виконанням шифрування/дешифрування інформації. Запропоновані підходи щодо вирішення питання оптимізації затрат обчислювальних ресурсів на основі операції XOR з реалізацією всередині блокового стандарту шифрування спрощеної раундової функції, при простій технічній реалізації та невисокій вартості виробництва, дозволяють зекономити ресурси, якими володіє електронне обладнання БПЛА. Результати проведених досліджень визначають ефективність використання для досягнення закодованими даними та надання їй відповідної криптостійкості та практичну значимість запропонованих методів належної швидкості обміну.

Здійснено реалізацію мессенджеру, як програмного додатку між двома віддаленими комп'ютерами та застосовано метод шифрування в апаратній реалізації БПЛА.

Частиною програми є інтерфейс користувача. Для забезпечення динамічного додавання друзів чи співрозмовників до списку «контактів», використовується візуальний елемент фреймворку Qt – Qlabel. Але є одне зауваження, стосовно даного елементу: він не має в собі обробника подій, чи як в називають в мові Java – «слухача». Для того, щоб забезпечити взаємодію візуального елементу з користувачем, необхідно реалізувати свій інтерфейс, який містить клас подій.

Після реалізації усіх основних модулів програми отримана наступна архітектура програми чи так звана ієрархія класів (рис. 2).

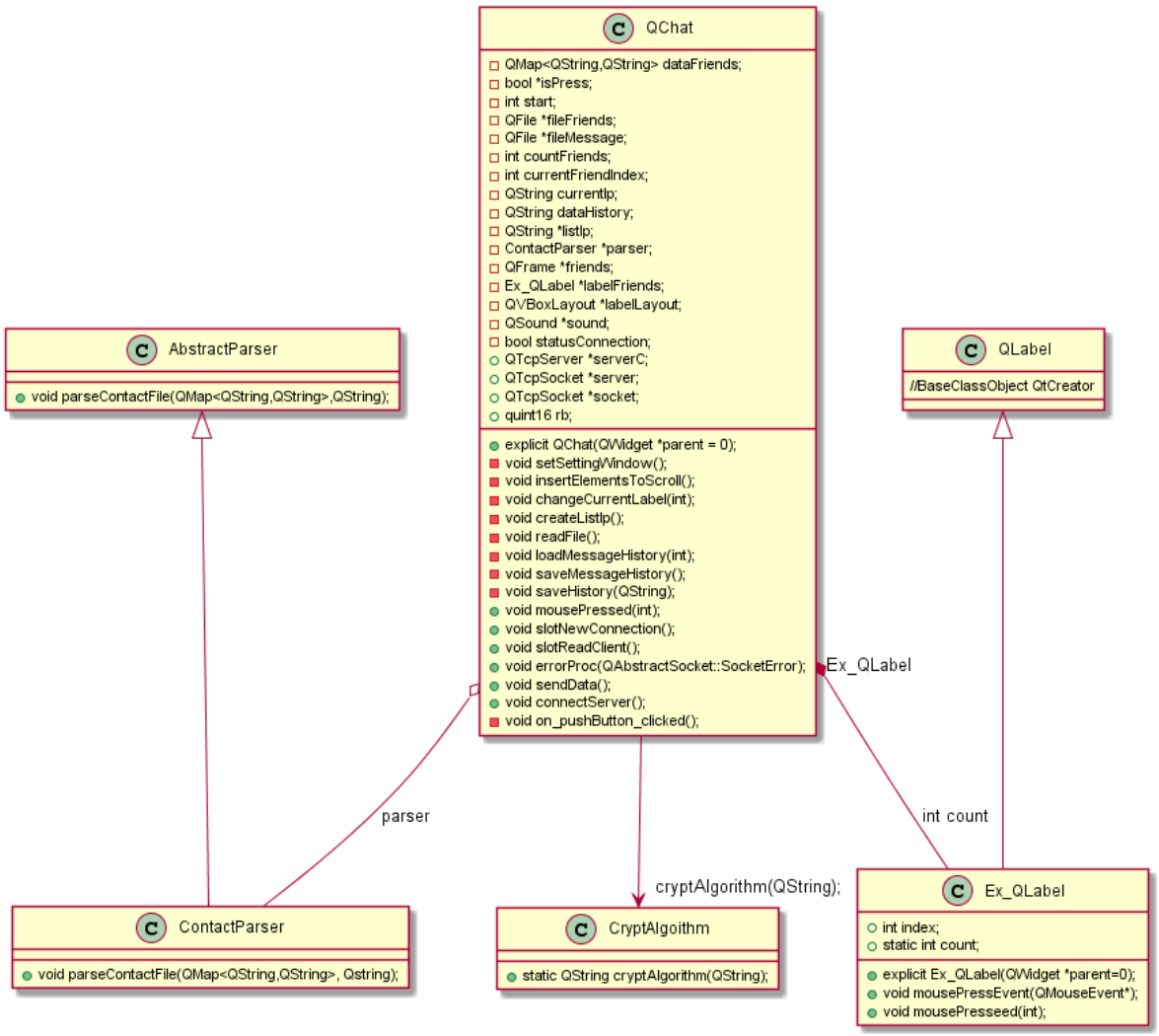

Рис. 2. Ієрархія класів програми QChat

У четвертому розділі розроблено заходи щодо охорони праці та безпеки у надзвичайних ситуаціях, а саме: виконано аналіз нормативно-технічних вимог до робочих місць робочого приміщення працівників ІТ сфери, аналіз організації та обладнання робочого місця, виконано розрахунок освітлення і здійснено інструктаж з поведінки працівників під час ураження електричним струмом.

У п’ятому розділі подана методична частина налаштування основних сервісів для серверу під управлінням операційної системи CentOS 7. Розроблено дві практичних роботи з дисципліни «Комп’ютерні мережі», наведена рекомендована література та хід робот.

ВИСНОВКИ

Під час виконання роботи було проаналізовано застосування криптосистем в повсякденному житті користувача Інтернет-мережі, а також організацію алгоритмів та механізмів шифрування даних в таких відомих програмах як Tor, Skype, Viber, WhatsApp та Telegram.

В даній роботі було розглянуто стійкості алгоритмів, які застосовують міжнародні відомі корпорації в своїх програмних продуктах, турбуючись про конфіденційність передачі даних від одного ПК до іншого в світовій мережі.

Також було проведено дослідження ефективності інструментів хакерів, що застосовуються в здобутті інформації, яку користувачі пересилають один одному. А саме було введено в програму алгоритм швидкого шифрування XOR й проведено аналіз на стійкість до злому криптосистеми на базі зазначеного методу шифрування.

За результатами досліджень був запропонований новий модифікований блочний метод шифрування з використанням операції XOR та введено ряд вдосконалень. Розроблений метод був покладений в основу створення корпоративного мессенджера з шифруванням повідомлень, який забезпечує захищене спілкування засобами чату між співробітниками територіально розосереджених філій одної корпорації.

Практична цінність роботи підтверджена Актом впровадженням у поточну діяльність ТОВ «Схід-Захід-Енерго» (м. Миколаїв), яка має розгалужену систему складів на території області, а також філію ТОВ «Київ-Електрик» (м. Київ).

Чат-програма, яку було створено, реалізує основні функції передачі та шифрування самих повідомлень, виконує ряд відповідних й мабуть основних задач, які були поставлені, але на даний момент знаходиться на етапі «альфа-версії». В подальших ітераціях релізів, функціонал може досить сильно розширитись від введення нових алгоритмів генерування ключів шифрування на період існування зв’язку між двома користувачами. Тим самим є перспектива збільшити надійність захисту інформації, що передається відкритими каналами зв’язку.

Також метод шифрування даних було запропоновано для використання в малогабаритних авіаційних системах керуванням БПЛА, що мають обмежені обчислювальні можливості. Застосування мікроконтроллерів в БПЛА дозволяє інтегрувати модуль шифрування й дешифрування даних, утворивши захищений канал для обміну даними.

Простота технічної реалізації та одночасне покращення криптостійкості системи внаслідок використання запропонованого методу з перемішуванням, розбиттям на блоки байтів й утворенням зв'язку між ними всередині кожного з блоків, визначають ефективність застосування модифікованого методу блокового шифрування в системах як з великими обчислювальними можливостями, так і з обмеженими, у т. ч. для захисту даних, що передаються з/до БПЛА.

Матеріали роботи були представлені у фіналі Всеукраїнського конкурсу студентських наукових робіт із напряму «Інформатика, обчислювальна техніка та автоматизація» (Вінницький нац. техн. ун-т), на якому були відзначені Дипломом 1-го ступеня (наказ МОНУ від 20.07.2016 № 859).

Розроблене у магістерській науковій роботі ПЗ на основі зазначеного методу шифрування отримало перше місце в рамках регіонального етапу конкурсної програми «Кращий студент України 2016» (м. Миколаїв) та було представлене на другому, національному етапі, який проходив у м. Суми.

Результати роботи обговорені на:

– двох міжнародних наукових конференціях «Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications IDAACS'2017» (Бухарест, Румунія), «Методи та засоби кодування, захисту й ущільнення інформації» (м. Вінниця);

– трьох всеукраїнських наукових конференціях: «Комп'ютерні інтелектуальні системи та мережі» (м. Кривий Ріг), «Могилянські читання» (м. Миколаїв), «Інтелектуальні інформаційні системи» (м. Миколаїв);

– тренінгу «Інформаційні системи і технології у сталому розвитку сучасного світу» в межах Міжнародної конференції «Ольвійський форум» (м. Миколаїв).

За результатами роботи надруковано 9 публікацій, з них 2 статті – у фахових журналах за спеціальністю, 1 патент України на корисну модель, 5 тез доповідей, одна з яких проіндексована у науковометричній базі Scopus.

У спеціальному розділі охорони праці та цивільного захисту було проаналізовано НТВ до робочих місць щодо офісного приміщення. Розглянуто небезпеки здоров'ю людини, що працює за комп'ютером. Виконано розрахунок осітлення в офісному приміщенні ТОВ "Схід-Захід-Енерго" та в результаті визначено, що приміщення відповідає усім вимогам для роботи за комп'ютером.

Розроблено інструктаж для роботи з персоналом для унеможливлення ураження електричним струмом. Розроблено правила поведінки під час виникнення подібної надзвичайної ситуації для кожного працівника, розроблено організаційно-технічні заходи (організаційні, технічні та експлуатаційні). Описано обов'язки керівників підприємств і працівників.

В методичному розділі було розроблено дві практичні роботи з дисципліни «Комп'ютерні мережі». Практичні роботи ознайомлюють із методами налаштування сервісів доступу, FTP та віртуальних хостів для серверів під управлінням операційної системи CentOS версії 7.0.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ МАГІСТЕРСЬКОЇ НАУКОВОЇ РОБОТИ

1. Zhuravska, I., Solobuto, L., Musiyenko, M., and Rumiankov, D. Reduce noise like solar interference in computer networks based on Power Line Communication. Proceedings of the 2017 IEEE 9th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS'2017) // Proceeding of the 8th IEEE International Conference. Bucharest, Romania, Sep. 21–23, 2017. P. 215–221.

2. Журавська, І. М. Створення модифікованого блокового методу шифрування на базі операції XOR для корпоративного мессенджера / І. М. Журавська, Д. І. Румянков // Наукові праці [Чорномор. держ. ун-ту ім. Петра Могили комплексу «Києво-Могилянська академія»]. Серія : Комп'ютерні технології : наук.-метод. журн. – 2015. – Т. 266, Вип. 254. – С. 97–104. – ISSN 1609-7742. – Режим доступу : URL : http://nbuv.gov.ua/UJRN/Npchduct_2015_266_254_17, http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/Npchduct_2015_266_254_17.pdf, http://kt.chdu.edu.ua/article/view/65398/60649 (дата звернення : 25.08.2016).

3. Журавська, І. М. Блоковий метод шифрування для рухомих об'єктів з обмеженими обчислювальними ресурсами / І. М. Журавська, М. П. Мусієнко, Д. І. Румянков // Інформаційні технології та комп'ютерна інженерія ; Вінницький нац. політехн. ун-т. 2016. Том 3, № 37. С. 28–32. ISSN 1999-9941. – Режим доступу : URL : http://itce.vntu.edu.ua/index.php/itce/article/view/523/394 (дата звернення: 21.02.2017).

4. Патент 130608 UA, МПК B64C 39/02 (2006.01) Малогабаритна безпілотна авіаційна система повітряного спостереження з наземної станції контролю та управління / Румянков Д. І., Мусієнко М. П., Журавська І. М., Олійник В. В. ; заявник Чорноморський національний університет ім. Петра Могили. № u 201808713 ; заявл. 14.08.2018 ; опубл. 10.12.2018, Бюл. № 23.

5. Румянков, Д. І., Організація шифрованого каналу звязку в корпоративній мережі // Інтелектуальні інформаційні системи : тези доп. Всеукр. наук.-практ.

конф., Миколаїв, 19–21 лютого 2019 р. / Чорном. нац. ун-т ім. Петра Могили. – Миколаїв : Вид-во ЧНУ ім. Петра Могили, 2019. –С. 16–17.

6. Журавська, І. М. Підвищення ефективності шифрування керуючого трафіку БПЛА засобами модифікованого блокового методу / І. М. Журавська, М. П. Мусієнко, Д. І. Румянков // Методи та засоби кодування, захисту й ущільнення інформації : тези доп. V-ї Міжнар. наук.-практ. конф., 19-21 квітня 2016 р., Вінниця. – Вінниця : Вид-во Вінниц. нац. техн. ун-ту, 2016. – С. 75–77.

7. Журавська І. М. Корпоративний мессенджер з шифруванням трафіку модифікованим блочним методом на базі операції XOR / І. М. Журавська, Д. І. Румянков // Комп'ютерні інтелектуальні системи та мережі (КІСМ-2016) : тези доп. IX-ї Всеукр. наук.-практ. WEB конф. студентів, аспірантів та молодих вчених, 22–24 березня 2016 р., Кривий Ріг. – Кр. Ріг : Вид-во ДВНЗ «Криворіз. нац. ун-т», 2016. – С. 135–137.

8. Журавська І. М. Система автоматичного управління на основі Arduino з мікроконтролером ATMega для прийняття рішення щодо поправки курсу польоту БПЛА / І. М. Журавська, Д. І. Румянков // Могилянські читання–2016 : тези доп. XIX-ї Всеукр. наук.-метод. конф., м. Миколаїв, 14-18 листопада 2016 р. – Миколаїв : Вид-во Чорномор. нац. ун-ту ім. Петра Могили, 2016. – Том 5. – С. 24–26.

9. Журавська, І. М. Проектування системи керування безпілотним літальним пристроєм на основі мікроконтролерів ATMega на базі Arduino / І. М. Журавська, Д. І. Румянков // Інтелектуальні інформаційні системи : Всеукраїнська науково-практична конференція молодих вчених, аспірантів і студентів : програма та тези, м. Миколаїв, 15–17 лютого 2017 р. – Миколаїв : Вид-во ЧНУ ім. Петра Могили, 2017. – С. 126–128.

10. Румянков, Д. І. Програмно-апаратні рішення для встановлення зв'язку між мобільним та програмованим периферійним пристроями // Студентські наукові студії : молод. наук. журн. /ЧНУ ім. Петра Могили ; [відп. ред. Л. С. Мельничук]. – Миколаїв : Вид-во Чорномор. нац. ун-ту ім. Петра Могили, 2017. – С. 94–98. – ISSN 1609-8099.

АНОТАЦІЯ

Румянков Д. І. Створення модифікованого блокового методу шифрування на базі операції XOR для корпоративного мессенджера. – На правах рукопису.

Магістерська наукова робота на здобуття освітньої кваліфікації «Магістр комп'ютерних наук».

Чорноморський національний університет імені Петра Могили, Миколаїв, 2019.

У процесі модифікації методу шифрування використовується математичний апарат теорії інформації, систем числення, методів дискретної математики.

В процесі виконання магістерської наукової роботи було досліджено роботу соціальних мереж й мессенджерів та на основі результатів дослідження розроблено ПЗ корпоративного чату з шифрованим трафіком. Для забезпечення конфіденційності перемовин створений модифікований метод шифрування з використанням операції XOR. Зазначений мессенджер забезпечує спілкування співробітників віддалених філій корпорацій без використання проміжних сторонніх серверів, на яких існує загроза несанкціонованого зберігання та розшифрування перемовин.

Результати дипломної роботи можуть бути корисними при створенні корпоративної мережі бюджетного типу з обмеженими фінансовими ресурсами.

Робота складається з вступу, 3 розділів, висновків, розділу з охорони праці, методичної частини.

Магістерська наукова робота містить 108 с. (без додатків), 2 табл., 37 рис., 4 додатки, 47 джерел посилання.

Ключові слова: блочний метод шифрування, операція XOR, корпоративний мессенджер, корпоративна мережа.

ABSTRACT

Rumiankov D. I. Corporate Messenger with Traffic Encryption Modified Block Method Based on XOR Operation. – Manuscript.

In the process of updating the method of encryption the mathematical apparatus of information theory, numerical systems, discrete mathematical methods are used.

The development of logical functions suitable for cryptographic re-encoding of information according to the proposed approach is based on the provisions of the theory of logic, cryptography. In the process of doing the thesis work was investigated the work of social networks and messengers and based on the results of the study developed and created a modified method of encryption. Based on the created data encryption method, a messenger was developed that can be used for corporate purposes. means of chat of employees of remote corporations' affiliates without the use of intermediate servers, where there is a threat of preservation and decryption of negotiations.

The results of the thesis may be useful when creating a corporate network of budget type, with limited financial costs.

Research contains 108 p. (without appendices), 2 tables, 37 figures, 4 appendices, 47 references.

Keywords: block encryption method, XOR operating system, corporate messenger, corporate network.