УДК 004.432; 621.391

УКПП

№ держрегистрації

Інв. №

Міністерство освіти і науки України

Запорізький національний технічний університет

69063, м. Запоріжжя, вул. Жуковського, 64; тел./факс (061)224-42-36

ЗАТВЕРДЖУЮ
Проректор з НР та МД ЗНТУ
д-р техн. наук, проф.
_____ В.В. Наумик
„__” _____ 2018р.
М.П.

ЗВІТ
ПРО НАУКОВО-ДОСЛІДНУ РОБОТУ
ДОСЛІДЖЕННЯ І РОЗРОБКА КРИПТОГРАФІЧНИХ ТА ТЕХНІЧНИХ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ

(остаточний)

Шифр НДР 04515

Завідувач кафедрою, керівник НДР
д-р техн. наук, професор Л.М. Карпуков

Нормоконтроль А.В. Коротун

2018

СПИСОК АВТОРІВ

Керівник НДР д-р техн. наук, проф. , зав. каф.	Л.М. Карпуков (вступ, 3.2, 3.3, висновки)
доцент, канд. техн. наук	С.І. Лізунов (1.2,1.3,3.3,3.4)
доцент, канд. техн. наук	В.О. Воскобойник (1.1,3.6)
доцент, канд. фіз.-мат. наук	Г.Л. Козіна (2.1,2.2,2.3)
доцент, канд. техн. наук	Г.В. Неласа (2.1,2.4,3.5)
доцент, канд. фіз.-мат. наук	С.М. Романенко (3.2)
доцент, канд. техн. наук	О.В. Щекотихін (3.1)
старший викладач	С.В. Куцак (1.3,1.4,3.5,3.6)
старший викладач	Р.Ю. Корольков (1.5,3.6)
старший викладач	Г.І. Нікуліщев (1.1,2.1)

РЕФЕРАТ

Звіт: 91 стор., 1 рис., 77 джерел.

КІБЕРЗАГРОЗИ, ПРИХОВАНИЙ МАЙНІНГ, ЕЛЕКТРОННИЙ ЦИФРОВИЙ ПІДПИС, ГРУПОВИЙ ПІДПИС, СЛІПИЙ ПІДПИС, КЛЕПТОГРАФІЧНА АТАКА, ЗАПЕРЕЧУВАНЕ ШИФРУВАННЯ, КВАНТОВА КРИПТОГРАФІЯ, ГРАФІЧНИЙ ПРОЦЕСОР, CUDA, ВОЛОКОННО-ОПТИЧНІ ЛІНІЇ ЗВ'ЯЗКУ, НЕЛІНІЙНА ЛОКАЦІЯ, КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ

Мета роботи – дослідження та розробка нових криптографічних та технічних методів захисту інформації.

Об'єкт дослідження – інформаційні та комунікаційні системи і мережі, системи передачі інформації.

В результаті НДР досліджено захищеність інформації в мережах, запропоновано методи захисту від прихованого підключення до інформаційних мереж, запропоновано підхід до формування схем сліпого підпису, досліджено клептографічні атаки та запропоновано засобі захисту від них, модифіковано алгоритм заперечуваного шифрування, створено модель протоколу квантової криптографії на платформі CUDA, запропоновано новий спосіб захисту інформації у волоконно-оптичних лініях зв'язку від несанкціонованого доступу.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ ТА ПОЗНАЧЕНЬ

АС	Автоматизована система
БПЛА	Безпілотний літальний апарат
ВАХ	Вольт-амперна характеристика
ВОЛЗ	Волоконно-оптичні лінії зв’язку
ДФ	Дестабілізуючій фактор
ЕЦП	Електронний цифровий підпис
ЗП	Закладний пристрій
ІТС	Інформаційно-телекомунікаційна система
КРК	Квантове розподілення ключів
КСЗІ	Комплексна система захисту інформації
МОМ	Метал-Оксид-Метал
НЗІ	Несанкціоноване знімання інформації
НКУ	Наземний комплекс управління
ОІД	Об’єкт інформаційної діяльності
РІС	Розподілена інформаційна система
РП	Радіозакладний пристрій
СУІБ	Система управління інформаційною безпекою
AES	Advanced Encryption Standard (Новий стандарт шифрування
IoT	Internet of Things (Інтернет речей)
NFC	Near Field Communication (Близький безконтактний зв’язок)
OSI	Open systems interconnection (Взаємодія відкритих систем)
PCA	Principal Component Analysis (Метод головних компонент)
SETUP	Secretly Embedded Trapdoor with Universal Protection (Секретно вбудована лазівка з універсальним захистом)

ВСТУП

В даний час розвиток інформаційних технологій, їх поширення в усі сфери життєдіяльності людини та суспільства стали нормою подальшої еволюції цивілізації.

Стрімкий розвиток інформаційних технологій обумовлює появу нових загроз національній та міжнародній безпеці. Зростає кількість та потужність кібератак, мотивованих інтересами окремих держав, груп та осіб. З цього випливає актуальність розробки, вибору і правильного використання методів, засобів і заходів ефективної протидії ним.

Проблеми стратегічного кіберзахисту в сучасних умовах України розглядається в роботах [1-3]. Авторами проведено аналіз національної стратегії кіберзахисту України, аналіз нормативно-правової бази кібербезпеки, виделено особливості розробки політики безпеки в державних установах. Наведено огляд ефективних заходів протидії кіберзагрозам [4].

Дослідження захищеності інформації в мережах розглядається в роботах [5-8]. Окрема увага приділена дослідженню захищеності закритих Wi-Fi мереж. Проведено тестування Wi-Fi мереж за допомогою відповідних програмних продуктів [7]. Проведено аналіз брандмауерів на захищеність [8].

Засоби прихованого підключення до мереж розглядаються в роботах [9-11]. Ці засоби можуть бути як суто апаратними, наприклад, закладні пристрої, так і програмними, тобто замаскованими в лігальні програмні продукти. Досліджено та проаналізовано застосування сучасних радіоелектронних закладних пристроїв. Авторами розглянуті способи прихованого майнінгу та захист від нього, а також приховане під’єднання до оптоволоконної лінії зв’язку.

Дослідження захищеності мовної інформації в інформаційних системах проведено в роботах [12-13]. Авторами класіфіковані фактори, що впливають

на захищеність мовної інформації в розподілених інформаційних системах. Проведено порівняльний аналіз методів оцінки захищеності мовної інформації.

В роботах [14-15] розглянуті методи розпізнавання зображень з використанням технологій штучних нейронних і капсульних мереж та специфікованоого алгоритму розпізнавання облич Eigenface.

Дослідження і розробка криптографічних методів захисту інформації розглядається в роботах [16-32].

Проведено огляд різних схем цифрового підпису [16-18], описано загальний підхід до формування схем сліпого підпису [19]. Сліпий підпис вирішує специфічну задачу підтвердження справжності документів без розкриття їхнього авторства і, завдяки цьому, може використовуватись , наприклад, в схемах електронного голосування.

Запропоновано криптографічний протокол групового підпису [20]. Протокол групового цифрового підпису забезпечує можливість формування цифрового підпису від імені деякого колегіального органу – групи підписантів, один з яких є лідером (керівником). Запропонований протокол групової цифрового підпису відрізняється від відомих раніше набором додаткових властивостей. На відміну від індивідуальної електронного цифрового підпису групова цифрова підпис містить три елементи, що істотно збільшує розмір підписи в порівнянні з випадком протоколів індивідуальної цифровий підписи, заснованих на складності завдання дискретного логарифмування.

Однак розмір груповий цифрового підпису (1344 біт) незначно перевищує розмір індивідуальної цифрового підпису в криптосистеме RSA (1024 біт) при заданому рівні стійкості.

Запропоновано протокол колективного цифрового підпису на основі EC-GDSA для використання в телемедицині [21]. Протокол реалізує забезпечення безпечної автентифікації загального медичного висновку при проведенні консиліуму лікарів.

Клептографічні атаки та захист від клептографічних атак на криптосистеми розглянуто в [22-23]. Клептографічна атака – це створення

"закладки", що впроваджується в криптосистему, що розробляється, яка може бути реалізована у вигляді апаратного пристрою (наприклад, смарт-карти) або програми (наприклад, Web-сервера або поштового клієнта). Авторами наведено вимоги щодо криптосистем з метою захищення від клептоатак.

Дослідження властивостей алгоритмів заперечуваного шифрування та модифікація відомого алгоритму заперечуваного шифрування Менга запропоновано в [24-25]. Метод заперечуваного шифрування має на меті не скільки приховати секретну інформацію, скільки заперечити сам факт її існування. Оскільки на етапі генерації ключів виникає проблема, яка пов’язана з розподілом ключів між абонентами, то її вирішення полягає у модифікації первісного алгоритму шляхом функціональної заміни задачі дискретного логарифмування на протокол «непомітної» передачі $OTn1$. Моделювання роботи модифікованого алгоритму заперечуваного шифрування Менга було виконано за допомогою 128-бітного ключа та продемонстровано його особливості, які забезпечують надійний захист інформації від атак на основі примусу.

На сьогоднішній день паралельні та квантові технології, такі як розподілені системи, квантові системи та комунікації, квантове шифрування, квантові алгоритми, квантові лінії зв’язку та ін. мають високий потенціал в системі захисту інформації. Саме тому квантові системи передачі інформації викликають інтерес у фахівців із захисту інформації.

Використання паралельних та квантових обчислень при реалізації криптографічних алгоритмів розглядається в [26-32]. Проведено розпаралелювання та порівняльний аналіз методів дискретного логарифмування на графічному процесорі, порівняльний аналіз протоколів квантового розподілення ключів. Розроблено паралельні моделі протоколів квантової криптографії під технологію GPGPU та модель квантового алгоритма Шора факторизации натуральных чисел. Моделювання протоколів квантової криптографії проведено на платформі CUDA.

В даний час все більше конфіденційної інформації передається саме волоконно-оптичними мережами зв’язку. З точки зору надійності та захищеності волоконно-оптичні лінії посідають провідне місце серед безпечних мереж передачі інформації. Але, при певних умовах, за яких зловмисник має безпосередній доступ до волоконно-оптичної лінії, перехоплення інформації та її трактування стає цілком можливим. Тому, виникає актуальна задача створення більш надійного способу передачі інформації по волоконно-оптичним лініям зв’язку шляхом впровадження додаткових методів захисту.

Захист інформації у волоконно-оптичних лініях зв’язку розглядається в роботах [33-37]. Запропоновано та отримано патент на спосіб захисту інформації у волоконно-оптичних лініях зв’язку від несанкціонованого доступу з поліпшеними характеристиками, тобто з підвищеною захищеністю, надійністю та з покращеною якістю інформаційного сигналу на приймальній стороні, які досягаються шляхом технічних удосконалень.

Поля і хвилі в задачах технічного захисту інформації розглядається в роботах [38-41]. Хвильовим процесом називають будь яку зміну (збурення) стану суцільного середовища, що поширюється з кінцевою швидкістю і переносить енергію. Проведено дослідження нових типів метаматеріалів на базі спіральних структур та виявлено нові електродинамічні явища прі взаємодії електромагнітної хвилі з шаром метаматеріалу.

Стрімкий розвиток систем безпілотних літальних апаратів в Україні та за кордоном і розвиток радіоелектроніки змушують постійно переглядати вимоги до каналу зв’язку між безпілотним літальним апаратом і наземним комплексом управління. Проблемам захисту інформації, що передається з безпілотних літальних апаратів, присвячено роботи [42-43]. Запропоновано криптографічний протокол захисту інформації в радіоканалах безпілотних літальних апаратів. Для цього розроблений комбінований алгоритм генерації загального сеансного ключа і поточного шифрування, який поєднує в собі переваги симетричних і асиметричних криптосистем.

Сучасне життя неможливе без комп’ютерних систем та мереж. Тому захист інформації в таких мережах набуває все більшої актуальності. Роботи [44-47] присвячені побудові комплексних систем захисту інформації. Проведено опис компонентів автоматизованої системи та технології обробки інформації. Після обстеження автоматизованої системи були визначенні основні загрози для інформації та побудована модель порушника. Для побудови комплексної системи захисту автоматизованої системи було впроваджено комплекси засобів захисту від несанкціонованого доступу «Гриф», «Лоза-1» та «Лоза-2».

Проблеми безпеки Інтернету речей розглядаються в роботах [48-49]. Авторами розроблений проект Friends Reminder, якій допомагає спілкуватися більше зручніше та безпечніше.

В даний час все більш широко застосовується технологія Near Field Communication. Це технологія бездротового високочастотного зв’язку малого радіусу дії, яка дає можливість обміну даними між пристроями, що знаходяться на відстані близько 15 сантиметрів.

Захист передачі конфіденційних повідомлень розглядається в роботах [50-52]. Пропонується для захисту передачі конфіденційних повідомлень використання завадостійкого кодування для та введення шифрування як додаток до відомих мережевих протоколів. Для забезпечення безпеки технології Near Field Communication пропонується побудувати стек протоколів, в якому на потрібний рівень будуть вбудовані криптографічні протоколи.

1ДОСЛІДЖЕННЯ ТЕХНІЧНИХ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ

1.1 Стратегія кіберзахисту України

1.1.1 Аналіз національної стратегії кіберзахисту України

В даний час розвиток інформаційних технологій, їх поширення в усі сфери життєдіяльності людини та суспільства стали нормою подальшої еволюції цивілізації.

Рада національної безпеки і оборони ухвалила стратегію кібербезпеки України [53]. Стратегія кібербезпеки передбачає розбудову національної системи забезпечення захисту кіберпростору, своєчасне виявлення та нейтралізацію кіберзагроз, а також запобігання їм з урахуванням практики провідних держав-членів НАТО та ЄС.

У стратегії йдеться про координацію, взаємодію і розподіл повноважень та відповідальності органів сектора безпеки й оборони України в питаннях кібербезпеки, кіберзахисту та протидії кібертероризму й кіберзлочинності. Доповідь складається з чотирьох частин: ситуація в Україні, термінологія; різновиди та приклади кібератак; основні напрямки забезпечення кіберзахисту України; шляхи вирішення питання кібербезпеки України.

Аналітична складова доповіді основана на розгляді та аналізі стратегії кібербезпеки України. Необхідно мати на увазі, що у Сполучених Штатах Америки добре розуміють, що військові переваги в кіберпросторі роблять Америку найпотужнішою глобальною державою світу. Однак разом із перевагами посилюються численні загрози кіберпростору. Саме тому у XXI ст. кіберпростір стає чи не найважливішою сферою державних і глобальних інтересів усіх розвинутих країн, у тому числі вирішення питання кібербезпеки України.

1.1.2 Особливості розробки політики безпеки в державних установах України

В провідних країнах світу, у тому числі країнах-членах ЄС, розвиток інформаційного суспільства визначено одним з головних пріоритетів державної політики.

Формування та реалізація ефективної державної політики в цій сфері обумовлена наступними факторами: зростаючим значенням інформації для будь-якої сфери життєдіяльності особи, суспільства та держави; прагнення України набути статусу асоційованого члена ЄС; входженням нашої країни в світовий інформаційний простір; появою нових та зростанням рівня традиційних загроз в інформаційній сфері; агостренням комплексу проблем в інформаційній сфері; недосконалістю чинного законодавства; важливістю державного регулюючого впливу на інформаційну сферу та реалізації державної політики у сфері інформаційного суспільства.

Концепція державної політики у сфері інформатизації та розвитку інформаційного суспільства визначено законодавчим актом, в якому позначені головна мета, основні завдання, шляхи розв’язання проблем, завдання та функції органів влади, механізми взаємодії їх між собою та суспільством.

З метою вирішення проблеми захисту національних інтересів України доцільно створити Центральний орган виконавчої влади в сфері телекомунікації та інформатизації. Очолити цей орган має висококваліфікована, порядна та досвідчена в цій галузі людина-науковець.

Основним завданням цієї державної структури мають бути: всебічний розвиток та захист галузі ІТ; заходи щодо її інвестиційної привабливості; вихід нашої держави в світові лідери в ІТ галузі; стимулювання впровадження новітніх ІТ і виробництва конкурентоспроможного національного інформаційного продукту, зокрема сучасних засобів і систем захисту інформаційних ресурсів;

Крім цього, вайжливішем завданням є забезпечення безпеки інформаційно-телекомунікаційних систем, що функціонують в інтересах управління державою, забезпечують потреби оборони та безпеки держави, кредитно-банківської та інших сфер економіки, систем управління об’єктами критичної інфраструктури; розробка та впровадження національних стандартів і технічних регламентів застосування інформаційних стандартів і технічних регламентів застосування інформаційно-комунікаційних технологій, гармонізованих із відповідними стандартами держав – членів ЄС, у тому числі, згідно з вимогами Конвенції про кіберзлочинність; створення національної системи кібербезпеки; розбудова сучасної, заможної України.

1.1.3 Огляд ефективних заходів протидії кіберзагрозам

Сучасний кіберпростір розширює свободу і можливості людей, збагачує суспільство, створює глобальний ринок ідей, досліджень та інновацій.

Стрімкий розвиток інформаційних технологій обумовлює появу нових загроз національній та міжнародній безпеці. Зростає кількість та потужність кібератак, мотивованих інтересами окремих держав, груп та осіб. З цього випливає актуальність розробки, вибору і правильного використання методів, засобів і заходів ефективної протидії ним.

Мета роботи полягає у аналізі поняття кіберзагроз [54], огляді методів їхньої реалізації на сучасному етапі розвитку інформаційних систем та ефективних заходів протидії.

Існують 3 основні підходи до пояснення терміну «кібербезпека».

Кібербезпека – безпека кібернетичних систем. Кібернетика охоплює багато дисциплін, деякі з яких можуть стати цілями для кібератак: штучний інтелект, робототехніка, системи керування, соціальні системи тощо.

Згідно з аналітичним терміном, кібербезпека охоплює широке коло дій, засобів і концепцій, що пов’язані з забезпеченням інформаційної безпеки.

За стандартом ISO/IEC 27032 кібербезпека - стан захищеності інформації від кіберзагроз, тобто загроз доступності, повноті, цілісності, достовірності інформації, яка циркулює в об’єктах національної інформаційної інфраструктури.

Ще в 2010 році було виявлено шкідливе програмне забезпечення Stuxnet, яке продемонструвало реальність загроз, які раніше вважалися лише уявними. Ця програма мала наступні важливі особливості. Вона здатна атакувати локальні мережі, не підключені до Інтернету, і також призначена для атаки на промислове обладнання ядерного об’єкта.

Пізніше спеціалістами були виявилені зразки програмного забезпечення, яке мало розвідувальні функції. Найбільш відомими прикладами є DuQu, Flamer, Red October. Як з’ясувалось, деякі з масштабних розвідувальних операцій у кіберпросторі проводились протягом майже десяти років. Цілями були США, Західна Європа, Росія, Казахстан, Білорусь, Україна.

Останнім часом вищенаведений список програм, які можуть становити загрозу кібербезпеці, в тому числі і національній, стрімко поповнюється. Також зростає кількість і частота кібератак, що проводяться організованими групами кіберзловмисників.

Для протистояння кіберзагрозам використовуються наступні засоби: антивірусний захист, комплексні системи захисту інформації, системи управління інформаційною безпекою, навчання користувачів і підготовка фахівців тощо.

Антивірусний захист полягає в виявленні та знешкодженні програм, які створені для того, щоб порушити безпеку інформації у системі. Антивірусний захист є одним із базових компонентів захисту сучасних інформаційно-телекомунікаційних систем.

Наступним засобом забезпечення кібербезпеки є комплексні системи захисту інформації (КСЗІ), які є необхідним компонентом будь-якої інформаційної системи, в яких обробляється інформація, що належить державі. Розробка і впровадження КСЗІ передбачає декілька етапів: обстеження об’єкта,

розробка моделі загроз, оцінка ризиків, розробка політики безпеки, державна експертиза з метою підтвердження відповідності КСЗІ.

Будь-які зміни у системі вимагають повторного обстеження і внесення змін у модель загроз, переоцінки ризиків, коригування політики безпеки тощо.

Одним із ефективних засобів забезпечення безпеки інформаційних об’єктів є використання системи управління інформаційною безпекою (СУІБ), в основу якої покладено модель PDCA: планування (Plan) — етап розроблення СУІБ, оцінювання ризиків і підбір заходів; дія (Do) — етап реалізації і впровадження обраних заходів; перевірка (Check) — етап оцінювання ефективності та продуктивності СУІБ, що переважно виконують внутрішні аудитори; удосконалення (Act) — виконання коригуючих дій.

Таким чином, кіберпростір є територією активного протистояння, в якому спеціалісти з кібербезпеки поки що програють. Атаки здійснюються за допомогою спеціально розробленого програмного забезпечення, що використовує вразливості комп’ютерних систем. Виявлення таких атак ускладнюється тим, що вони здійснюються на обмежену кількість спеціально визначених цілей, не викликають збоїв і відмов комп’ютерів і тому тривалий час не потрапляють у поле зору дослідників з антивірусних лабораторій.

Для розробки дієвого механізму протидії кіберзагрозам Україні варто взяти за приклад існуючу практику зарубіжних країн і міжнародної спільноти та привести її у відповідність до українських реалій.

1.2 Дослідження захищеності інформації в мережах

1.2.1 Дослідження захищеності закритих Wi-Fi мереж

Дослідження бельгійського університету KU Leuven знайшли серйозні недоліки WPA2-протоколу, що забезпечує захист сучасних захищених мереж Wi-Fi. Зловмисник, який знаходиться у зоні дії жертви, може використовувати

ці недоліки та застосовувати для атаки на повторну установку ключів. Таким чином, може бути викрадена конфіденціальна інформація, що вважалась раніше захищеною: номери кредитних карток, паролі, повідомлення чату, електронні листи, фотографії і т.д.

Зловмисник може розшифрувати всі дані, що передає жертва, використовуючи повторну установку універсального ключа шифрування. При криптографічному рукостисканні не гарантується безпека одноразового використання параметрів, що пов’язані з використовуваним ключем. Зловмисник при перехваті ключа шифрування компрометує жертву переустановкою вже використовуваного ключа. Зв’язані параметри (інкрементний номер пакету що передається (nonce) та номер пакету що приймається (лічильник повторів)) скидаються до початкового значення.

Коли новий клієнт приєднується до мережі, він виконує чотиристоронне рукостискання для узгодження нового ключа шифрування. Як тільки ключ встановлено, він буде використовуватись для шифрування нормальних фреймів даних з використанням протоколу шифрування. Так як повідомлення можуть бути втрачені чи скинуті, точка доступу повторно передає повідомлення про підтвердження сеансу, якщо воно не отримало відповідного пакета для підтвердження. Тому клієнт може отримувати це повідомлення декілька разів. Зловмисник може змусити повідомлення некоректно скидатися, в результаті чого клієнт отримує його і перевстановлює той самий ключ шифрування та скидає інкрементний номер пакету передачі (nonce), отримуючи лічильник повтору, що використовується протоколом шифрування. Таким чином, викликаючи навмисне повторне використання, пакети можуть бути відтворені, дешифровані та/або підроблені. Цей метод можливий для використання в атаці групового ключа, PeerKey, TDLS і узгодження швидкого переходу BSS.

Дешифрування потоку можливе тому, що атака перевстановлення ключа приводить до відновлення nonce (також відомих як номери пакетів чи вектори ініціалізації) до початкового значення. Тобто один і той же ключ шифрування використовується із повторюваним декілька разів значенням nonce. Це

призводить до того що всі протоколи WPA2 повторно використовують кеш-потік при шифруванні пакетів.

Можливість дешифрування пакетів може бути використана для дешифрування пакетів TCP SYN, що дозволяє зловмиснику отримати порядкові номери TPC з'єднання та захопити його. Після цього зловмисник може не зважати на використання WPA2 та виконати найбільш розповсюджену атаку на мережі Wi-Fi: внесення шкідливих даних в незашифровані HTTP-з'єднання (вводити вимагання чи шантаж, тобто шкідливе програмне забезпечення на сайти, що відвідує жертва).

В небезпеці знаходяться жертви, що використовують протокол шифрування WPA-TKIP чи GCMP замість AES-CCMP.

Проти цих протоколів шифрування можливе не тільки розшифрування, а й підробка та введення пакетів, так як ці протоколи використовують повторне використання nonce. GCMP використовує один і той же ключ аутентифікації в обидві сторони зв'язку, тому ключ може бути відновлено. Як рішення цієї проблеми, підтримка GCMP на даний момент розвертається під назвою Wireless Gigabit (WiGig) та очікується її прийняття в найближчі декілька років.

Напрям, в якому пакети можуть бути дешифровані чи підроблені, залежить від атаки на рукостискання. Якщо спрощено атакувати чотиристоронє рукостискання, зловмисник може дешифрувати і підробити пакети, відправлені клієнтом. Коли атака відбувається на рукостискання Fast BSS Transition (FT), є можливість розшифрувати і підробити пакети відправлені клієнту. Більшість атак також здатні відновлювати одноадресні, широкомовні чи багатоадресні кадри.

Важливою деталлю є той факт, що наведені атаки не відновлюють пароль від мережі Wi-Fi, не відновлюють будь-які частини нового ключа шифрування що узгодився під час чотиристоронього рукостискання. На даному етапі розслідування можливість KRACK можна нейтралізувати за допомогою оновлень безпеки пристроїв, які дозволять встановлювати ключ шифрування тільки раз. Постачальники, чиї продукти протестували дослідники, отримали

повідомлення про недоліки ще в липні 2017 року. У серпні до процесу також підключилася координаційний центр CERT-CC, який розіслав повідомлення про вразливості.

Оновлення безпеки гарантують, що ключ встановлюється тільки один раз, що запобігає атаці. Тому користувачі повинні переконатися, що всі пристрої оновлені, а також повинні оновити прошивку маршрутизатора. Що робити, якщо немає оновлень безпеки для мого маршрутизатора або точки доступу, або якщо він не підтримує 802.11r? Домашні маршрутизатори або AP, ймовірно, не вимагають оновлень безпеки. Замість цього, головним чином, корпоративні мережі повинні будуть оновити свою мережеву інфраструктуру.

Є можливість спробувати зменшити атаки на маршрутизатори і точки доступу, відключивши клієнтські функції (наприклад, використовувані в режимах ретранслятора) і 802.11r (швидкий роумінг).

1.2.2 Аналіз брандмауерів на захищеність

Системи захисту інформації в комп'ютерних мережах повинні забезпечувати цілеспрямовану роботу останніх. Тобто вся інформація повинна бути прихованою і цілісною. В більшості випадків всі мережі офісів і компаній підключаються до всесвітньої павутини.

Для захисту локальних мереж, використовують міжмережеві екрани, які називаються брандмауерами. Даний екран є засобом диференціального доступу. Це означає, що мережа розосереджена на дві половини. Тобто є межа між інтернет-мережею і локальною мережею.

Брандмауери бувають програмними та апаратними.

Для аналізу брандмауерів на захищеність використовують утиліти з сайту www.testmypcsecurity.com, а саме Jumper, DNStester і CPIL Suite (розробка компанії Comodo). Ці утиліти використовують такі ж самі методи, що і

шкідливі програми, роботу яких вони симулюють. Під час тестування всі засоби антивірусного захисту повинні бути деактивовані.

Розглянемо наступні утиліти.

Утиліта Jumper дозволяє обійти брандмауер, використовуючи методи «DLL injection» і «thread injection».

Утиліта DNS Tester використовує рекурсивний DNS-запит, щоб обійти брандмауер.

Утиліта CPIL Suite надає набір тестів від компанії Comodo.

Всі ці утиліти потрібно запускати безпосередньо з досліджуваних комп'ютерів, а з зовні потрібно сканувати мережу за допомогою програми nmap.

Апаратні брандмауери використовують для ефективного захисту кожного вузла мережі. До їх недоліків можна віднести те, що вони не можуть забезпечити захист кожної окремої робочої станції, безсилі при атаках всередині мережі, а також не можуть виконувати розмежування інформаційної системи персональних даних.

Програмні брандмауери використовують для захисту всієї мережі в цілому. Їх стандартні настройки не можуть забезпечити максимальний захист від усіх типів загроз, тому правильно налаштовані програмні брандмауери дають більш гарантовану безпеку роботи в мережі.

Для досягнення найбільшої ефективності захист інформаційної системи повинен бути комплексним та включати програмні і апаратні брандмауери, антивіруси і правильні налаштування операційної системи.

1.3 Дослідження засобів прихованого підключення до інформаційних мереж

Засоби прихованого підключення розглядаються в роботах [9-11]. Ці засоби можуть бути як суто апаратними, наприклад, закладні пристрої, так і програмними, тобто замаскованими в лігальні програмні продукти.

1.3.1 Сучасні радіозакладні пристрої

Радіоелектронні закладні пристрої (ЗП) являють собою пристрої, що створюють канал несанкціонованого отримання і передачі в пункт прийому аудіо-, аудіовізуальної або оброблюваної радіоелектронної апаратурою та переданої в мережах зв'язку інформації.

ЗП можна поділити за кількома ознаками: радіозакладні пристрої, що випромінюють в ефір; закладні пристрої, які не випромінюють в ефір (з передачею перехопленої інформації по мережах зв'язку, управління, електроживлення, сигналізації і т.п.); радіозакладні пристрої з перевипромінюванням; закладні пристрої з передачею перехопленої інформації по стандартному телефонному каналу.

Для виявлення випромінюючих в ефір радіозакладок необхідно визначити можливий частотний діапазон їх роботи і види модуляції. Як випливає з аналізу існуючих радіозакладних пристроїв (РП), діапазон їх роботи досить широкий і має тенденцію до просування в більш високі частоти. Також існують пристрої із "стрибаючими" частотами. Це істотно ускладнює пошук РП по їх випромінюванням. Серйозне ускладнення в пошуку ЗП викликають і зміни та удосконалення видів модуляції, що використовуються. З'явився принципово новий клас РП з дельта-модуляцією. Крім того, в найбільш професійних радіозакладках використовують такі складні сигнали, як шумоподобні або з псевдовипадковою перестановкою несучої частоти. При кодуванні перехопленої інформації часто застосовується аналогове скремблювання, що змінює характеристики мовного сигналу таким чином, що він стає нерозбірливим.

Пошук таких пристроїв досить клопітка і головне дуже складна робота. Вони можуть бути закамуфльовані або вбудовані в предмети, що знаходяться у приміщенні.

Найбільшого поширення набули радіомікрофони. Цьому сприяв ряд причин. По-перше, простота установки і знімання інформації без необхідності

застосування складного обладнання: необхідно лише сам ЗП і приймач для прийому радіосигналів. По-друге, можливість отримання інформації «з перших рук» в режимі реального часу.

Сучасні «прослушки» по радіоканалах мають широке розповсюдження тому що мають невеликі розміри і досить високу потужність; високу якість звуку, завдяки багаторівневим мікрофонам; тривалий час роботи без підзарядки; наявність функції голосової або іншої активації; відсутність необхідності оплачувати послуги мобільного оператора для передачі аудіоінформації; доступну ціну.

Найсучасніші радіомікрофони, мають габарити не більше чверті олівцевої гумки та здатні протягом року сприймати і передавати на приймальний пристрій, розташований за півтора кілометра, розмову, яка ведеться в приміщенні пошепки. Він відноситься до класу пристроїв типу «клоп». Крім цього, вже зараз виробляються "клопи", які можуть записувати перехоплену інформацію, зберігати її протягом доби або тижня, а потім передати її в режимі швидкодії за дуже короткий час, стерти запис і почати процес знову.

Такі пристрої негласного знімання інформації можуть бути вмонтовані, наприклад, в брелки, кулькові ручки, мережеві фільтри, окуляри або годинник, елементи одягу, тощо.

Із зазначеного вище можна зробити висновок, що боротьба із радіозакладними пристроями в сучасних умовах набуває все більшої актуальності.

1.3.2 Прихований майнінг

Майнінг - це діяльність по створенню нових структур для забезпечення функціонування криптовалютних платформ. Для видобутку криптовалюти можливо не тільки використання власного комп’ютера, але і безлічі чужих машин [55].

Наприклад, у магазині Google Play знайшли додаток під назвою Vilny.net, що працює як VPN-сервіс, проте в той же час використовує ресурси смартфонів, щоб майніти криптовалюту Monero.

На сьогоднішній день прихований майнінг може зробити будь-який користувач. Для цього досить лише завантажити готову програму, написати номер свого електронного гаманця і все. Програма модифікована так, що вона не відрізняється від троянського вірусу: вона може поширюватися в мережі, копіювати сама себе на зовнішній накопичувач, приховувати свої процеси в диспетчері завдань і використовувати комп'ютер коли ним ніхто не користується.

Для прихованого видобутку криптовалюти не потрібно зламувати комп'ютер і встановлювати троян. Поки у користувача в браузері відкрита сторінка з шкідливим скриптом, процесор буде непомітно майніти.

І необов'язково, що навантаження на відеокарту або процесор має зрости до 100% - зловмисники обережні і не стануть навантажувати машину учасника своєї мережі в нерозумних межах. Ви можете, в принципі, і не помітити великої різниці, якщо у вас досить потужна техніка. Це важлива умова для збереження прихованої роботи майнера.

"Підвисання" на комп'ютері, які зникають, якщо розірвати з'єднання з інтернетом є ознакою, що ресурси вашого комп'ютера витрачаються із зовні. Варто обірвати з'єднання і шукати проблеми в системі.

Найчастіше програму майнінг ховають під системний процес svchost.exe. Для того, щоб знайти цю програму необхідно зробити наступне [56].

Svchost.exe повинен завжди виконуватися від імені системи, network і local сервісів. Якщо він запущений від імені будь-якого користувача, то варто перевірити його директорію на жорсткому диску. Істинний файл знаходиться у папці Windows/system32 і ніяк інакше.

Слід перевірити таблицю автозавантаження Windows. У цій таблиці не повинен знаходитися файл svchost.exe. Цей процес операційна система повинна

запускати самостійно, без участі користувача або шкідливої програми, яка занесла цю програму до списку автозавантажень.

Якщо програму майнінг знайдено, необхідно її видалити. Для цього слід використовувати програму Process Hacker. Криптовані процеси або упаковані процеси - найчастіше приховані. Майнер виступає саме як "упакований процес" в svchost.exe або іншій програмі, який відображається рожевим кольором в Process Hacker (packet procces). Слід відшукати такі процеси і проаналізувати їх директорію на жорсткому диску. Найчастіше вони ховаються від імені cmd.exe (прихованого командного рядка). Коли цей процес знайдено, перед тим як його зупинити, слід знайти місце розташування цього процесу. Після того, як ця програма зупинена, необхідно її видалити з жорсткого диску і, бажано, просканувати системний реєстр на посилання на цю директорію.

Якщо програму майнінгу модифікувати, то можливе знімання інформації про всі дії користувача. Тому, для захисту інформації, слід обов’язково знищувати програми майнінгу.

1.3.3 Приховане під’єднання до оптоволоконної лінії зв’язку

На противагу загальним уявленням, оптоволокно, по суті, не має захисту від сторонніх підключень і прослуховування. В даний час оптичними каналами зв’язку передається велика кількість критичної і чутливої інформації, і є ризик того, що вона може потрапити в руки певних осіб, які мають необхідні ресурси і обладнання.

Підключення до оптоволокна – процес, при якому безпека оптичного каналу компрометується вставкою або витягом світлової інформації [57].

Підключення до оптоволокна може бути інтрузивним або не інтрузивним. Перший метод вимагає перерізування волокна і приєднання його до проміжного пристрою для знімання інформації, в той час як при використанні другого методу, підключення виконується без порушення потоку даних і

переривання сервісу. В даному випадку мова буде йти саме про неінтрузивні технології.

Існує ряд відомих методів, що використовуються для отримання або вставки інформації в оптичний канал і дозволяють уникнути виявлення підключення. В основному буде розглядатися метод підключення заснований на згинанні оптоволокна.

При цьому методі підключення, кабель розбирається до волокна. Даний спосіб заснований на принципі поширення світла через волокно за допомогою повного внутрішнього відбиття. Для досягнення даного явища кут падіння світла на переході між власне ядром волокна і його оболонкою повинен бути більшим, ніж критичний кут повного внутрішнього відбиття. При згинанні волокна, воно викривляється таким чином, що кут відбиття стає меншим ніж критичний, і світло починає проникати через оболонку.

Під час під'єднання волокно розбирається до оболонки і поміщається в оптичний куплер, де волокно згинається, викликаючи випромінювання певної кількості світла, що порушує принцип повного внутрішнього відбиття. Таким чином інформація зчитується з волокна.

Є три основні категорії методів, які запобігають або знижують до мінімуму вплив сторонніх підключень: спостереження за кабелем і моніторинг, використання гнучкого волокна, шифрування інформації.

Підключення до оптоволокна є вельми відчутною загрозою інтересам національної безпеки України, фінансовим організаціям, а також приватним особам.

1.4 Дослідження захищеності мовної інформації в інформаційних системах

1.4.1 Аналіз факторів, що впливають на захищеність мовної інформації в розподілених інформаційних системах

Розробка будь-якої системи інформаційної безпеки повинна ґрунтуватися на певному переліку потенційних загроз безпеці та встановленню можливих джерел їх виникнення. У випадку, коли в системі існують загрози, для яких не передбачені які-небудь заходи протидії – це може призвести до того, що всі зусилля, витрачені на створення системи захисту, до очікуваного результату не приведуть. Тому при проектуванні системи захисту мовної інформації в розподілених інформаційних системах (РІС), як і для будь-яких інших систем, необхідно провести всебічне врахування загроз і для кожної з них реалізувати відповідний метод захисту.

Якісне вирішення даної проблеми можливе тільки в разі початкового визначення природи виникаючих загроз, тобто умов і факторів, які сприяють появі тієї чи іншої загрози.

Повне врахування дестабілізуючих факторів (ДФ) безпосередньо залежить від характеристики об’єкту захисту – структури об’єктів інформаційної діяльності (ОІД) [58], які в сукупності і створюють РІС.

В роботі запропоновано два підходи класифікації ДФ, що впливають на захищеність мовної інформації: за видовою ознакою та ієрархічний.

Фактори загроз за видовою ознакою поділяються на політичні, економічні та організаційно-технічні.

Під політичними факторами загроз безпеці мовній інформації розуміють: зміни геополітичної обстановки в Україні та в регіонах світу, інформаційна експансія розвинених країн, які здійснюють глобальний моніторинг світових політичних, економічних, воєнних, екологічних та інших процесів [59].

Основними економічними факторами загроз безпеці мовній інформації є: поява на ринку великої кількості вітчизняних та зарубіжних комерційних структур – виробників та споживачів інформації, засобів інформатизації та захисту інформації, критичний стан вітчизняних галузей промисловості, яка виробляє засоби інформатизації та захисту мовної інформації;

Основними організаційно-технічними факторами є: недостатня нормативно-правова база у сфері інформаційних відносин, у тому числі в галузі захисту мовної інформації, широке використання у сфері державного управління незахищених від витоку інформації імпортних технічних засобів для обробки та передавання мовної інформації.

За ієрархічним принципом ДФ можливо поділити на три групи.

Глобальні ДФ: недружня політика іноземних держав у галузі глобального інформаційного моніторингу, розповсюдження інформації, розповсюдження нових інформаційних технологій; діяльність іноземних розвідувальних та спеціальних служб.

Регіональні ДФ: використання інформаційної інфраструктури колишнього СРСР для передавання конфіденційної інформації, відставання від розвинених країн світу з темпів та масштабів розробки та впровадження нових інформаційних технологій.

Локальні ДФ: перехоплення електронних випромінювань, застосування підслуховуючих пристроїв або закладок, незаконне приєднання до апаратури та ліній зв’язку і т. ін.

1.4.2 Порівняльний аналіз методів захищеності мовної інформації

Найчастіше обмін конфіденційною інформацією відбувається у закритих приміщеннях, де акустичні хвилі поширюються заповнюючи увесь його простір. Приміщення істотно впливає на процес поширення звукових хвиль через багаторазові відбиття звукових хвиль від меж приміщення (стін, стелі і

підлоги), а також від предметів інтер'єру. На відміну від відкритого простору структура акустичного поля у приміщенні є складною і залежить не лише від джерела звуку, але також від геометричних розмірів і форми приміщення, властивості стін, дверей, вікон відбивати та поглинати акустичну енергію.

У зв'язку із наявністю високоефективних технічних засобів підслуховування розмов актуальним є розроблення і застосування адекватних заходів захисту мовної інформації від витоку технічними каналами.

Захист мовної інформації від витоку є досить складним та дорогим заходом. Багато організацій для ведення конфіденційних розмов обладнують спеціальні виділені приміщення, що забезпечують гарантований рівень захисту мовної інформації. З метою документального підтвердження захищеності виділених приміщень проводять спеціальні інструментальні вимірювання рівня небезпечних сигналів у можливих технічних каналах витоку мовної інформації. За відсутності спеціальної контрольно-вимірювальної апаратури або задля оперативного оцінювання рівня захищеності приміщення застосовують спеціальні методики розрахунку. Підвищення точності таких розрахунків є актуальним завданням інформаційної безпеки, вирішення якого може підвищити достовірність результатів оцінки акустичної захищеності виділених приміщень, виявити вразливості та удосконалити методики інструментального контролю, а на етапі організації виділених приміщень – виробити рекомендації щодо розташування елементів інтер'єру, в тому числі засобів передавання та оброблення інформації.

В роботі проведено порівняльний аналіз статистичної та хвильової теорій поширення звукових хвиль, які лежать в основі оцінки розбірливості мовної інформації [60]. Показано переваги хвильової теорії при розрахунку основних параметрів акустичного поля та перспективи застосування сучасних систем фізико-технічного моделювання для оцінки захищеності виділених приміщень.

Для акустичного розрахунку приміщень, зокрема і у сфері інформаційної безпеки користуються статистичною теорією реверберації. В основу цієї теорії покладено модель ідеального приміщення, за якою акустичне поле після

припинення дії джерела звуку розраховується на основі статистичного опису процесу згасання звукових хвиль. При цьому припускається, що амплітуди і фази відбитих звукових хвиль розподілені хаотично, тобто у хвильовому русі немає переважаючих напрямків потоків і симетрії в розподілі амплітуд, тобто акустичне поле є дифузним.

У рамках статистичної теорії є можливість розрахувати основні акустичні характеристики приміщення: акустичне співвідношення, за яким оцінюється вплив приміщення на сприйняття звуку; коефіцієнт чіткості, який дає змогу оцінити погіршення розбірливості мови, через створення реверберацій ним сигналом перешкоджаючого фону.

У теорії хвильової акустики виділяються три основні питання: взаємодія між звуковою хвилею і межами – стінками приміщення, стаціонарний (усталений) звуковий режим у приміщенні і характер процесів установлення, зокрема реверберації. У рамках цієї теорії приміщення розглядається як об’ємний резонатор із великою кількістю власних (резонансних) частот, а акустичні процеси в ньому – як збудження власних коливань, їх встановлення і поступове спадання після вимикання джерела збудження [61].

Статистична та хвильова теорії акустики приміщень доповнюють одна одну, проте, хвильова теорія є точнішою і дає достовірніші результати, хоча математичні моделі акустики приміщень є громіздкими. Сучасні системи фізико-технічного моделювання такі як Femlab і COMSOL Multiphysics дозволяють розраховувати акустичні властивості приміщень за цією теорією, у тому числі і у сфері захисту інформації.

Окрім можливості визначення резонансних частот приміщення, часу реверберації з урахуванням поглинання звукових хвиль різними поверхнями, за допомогою хвильової теорії можна досліджувати стаціонарні та динамічні процеси в приміщеннях, тобто розраховувати розподіл акустичного поля у просторі.

1.5 Дослідження методів розпізнавання зображень

1.5.1 Використання технологій штучних нейронних та капсульних мереж для розпізнавання зображень

Штучні нейронні мережі – це паралельно розподілена система обробки інформації, утворена тісно зв’язаними простими обчислювальними вузлами (однотипними або різними), що має властивість накопичувати експериментальні знання, узагальнювати їх і робити доступними для користувача у формі, зручній для інтерпретації й прийняття рішень.

Штучні нейронні мережі знаходять сьогодні широке застосування у будь-яких галузях. Зокрема, штучні нейронні мережі демонструють надлюдські можливості у задачах розпізнавання обличь і зображень. Роль нейронних мереж буде найбільшою для систем відеоспостереження, аудіо аналітики, забезпечення кібербезпеки, а також для систем управління доступом. Особливу роль нейромережеві технології будуть відігравати в інтеграції та обробці різнорідної інформації від різноманітних типів сенсорів та датчиків. Це дозволить створити інтелектуальні автономні системи безпеки нової якості.

Недоліком сучасних нейронних мереж є потреба у великій кількості даних. Програмне забезпечення для розпізнавання зображень, яке сьогодні використовується Google та іншими, потребує великої кількості прикладів фотографій, щоб навчитись надійно розпізнавати об’єкти у всіх ситуаціях. Це пов’язано з тим, що програмне забезпечення не вміє узагальнювати те, що вивчається у нових ситуаціях, наприклад, розуміння того, що об’єкт є одним і тим же, якщо дивитися на нього з нової точки зору.

Капсульні мережі направлені на усунення недоліків сучасних систем машинного навчання, які обмежують їх ефективність. В цьому підході використовуються невеликі групи нейронів, які називаються капсулами. В свою чергу, капсули складають шари для ідентифікації об’єктів на відео або зображеннях. Коли декілька капсул в одному шарі приймають однакове

рішення, вони активують наступну капсулу, що знаходиться на рівень вище. Цей процес продовжується доки мережа не зможе зробити висновок про те, що вона бачить. Кожна із капсул капсульної мережі створена таким чином, що здатна виявляти у зображенні конкретну ознаку і розпізнавати її під різним кутом.

Капсульні мережі потребують менший об’єм даних для навчання та розпізнавання об’єктів у нових ситуаціях. Вони не поступаються звичайним штучним нейронним мережам у розпізнаванні рукописних символів. Капсульні мережі пройшли тест на розпізнавання об’єктів, що були зображені з різних ракурсів, та зробили в два рази менше помилок ніж інші мережі.

Проте на даному етапі розвитку капсульних мереж поступаються традиційним штучним нейронним мережам у швидкості обробки даних, що потребує подальшого вивчення та вдосконалення технології капсульних мереж.

1.5.2 Аналіз алгоритму розпізнавання обличь Eigenface і його реалізація

В наш час все більшого поширення набувають технології автоматичного розпізнавання особи. Вони використовуються в таких системах як: біометрична ідентифікація, зір роботів, відеоконференції і т.д. Технологія ідентифікації особистості на основі зображення обличчя, на відміну від використання інших біометричних показників, не вимагає фізичного контакту з пристроєм і з урахуванням стрімкого розвитку цифрової техніки є найбільш прийнятною для масового застосування.

В роботі аналізується сучасний метод розпізнавання облич - метод головних компонентів (Principal Component Analysis, PCA). Ідея методу полягає в поданні зображень облич у вигляді набору (вектора) головних компонентів зображень, що називаються «власні обличчя» (Eigenfaces). Обличчя, мають корисну властивість: зображення, відповідне кожному такому вектору, має лицеподібну форму.

У роботі представлено побудову та архітектуру алгоритму розпізнавання Eigenface та його навчання у середовищі Matlab.

Зображення представляється як сума базисних компонент (зображень).

Зазвичай береться від 5 до 200 головних компонентів. Процес розпізнавання полягає в порівнянні головних компонент невідомого зображення з компонентами всіх відомих зображень. При цьому передбачається, що зображення облич, що відповідають одній людині, згруповані в кластери у власному просторі. З бази даних вибираються зображення-кандидати, що мають найменшу відстань від вхідного (невідомого) зображення.

Метод головних компонент добре зарекомендував себе в практичних додатках. Однак, в тих випадках, коли на зображенні обличчя присутні значні зміни в освітленості або виразі обличчя, ефективність методу значно падає. Вся справа в тому, що PCA вибирає підпростір з такою метою, щоб максимально апроксимувати вхідний набір даних, а не виконати дискримінацію між класами обличь.

2 ДОСЛІДЖЕННЯ І РОЗРОБКА КРИПТОГРАФІЧНИХ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ

2.1Протоколи цифрового підпису різного призначення

Одна з особливостей сучасного етапу розвитку систем електронного документообігу полягає в тому, що існуючі системи підтримують лише двоточковий варіант протоколу електронного цифрового підпису, до якого прив'язаний і український стандарт ДСТУ 4145-2002.

Однак існує велика кількість різних схем електронного цифрового підпису,що допускають участь у протоколі більше двох сторін [62].

На практиці часто виникає необхідність мати колективний підпис. Колективний підпис дозволяє відмовитися від використання кратного підпису при одноразовому підписанні документа групою відповідальних осіб. Концепція групового підпису реалізує метод, що дозволяє членам групи анонімно підписати повідомлення від імені всієї групи.

Кільцевий підпис уможливлює специфікувати набір можливих осіб, що підписують, без викриття, хто саме з них дійсно зробив підписання. Схема підпису із призначеним одержувачем–це схема підпису, де підпис може бути перевірений тільки єдиним «призначеним одержувачем», обраним підписувачем.

Незаперечний цифровий підпис може бути перевірений тільки в присутності підписувача. Схема підпису на ідентифікаторах дозволяє будь-якій парі користувачів перевіряти підпис один одного без обміну особистими або відкритими ключами, без зберігання ключів у каталогах, без використання послуг третьої сторони.

Сліпий електронний підпис запропоновано для захисту від підробки електронних грошей. За допомогою використання так званого «цифрового конверта» у такій системі одночасно з рішенням задач ідентифікації, автентифікації й авторизації претендента вирішена задача забезпечення

анонімності останнього, інакше кажучи, невідстежуваності електронних документів, зокрема електронних грошей.

В схемі мультипідпису із груповою перевіркою чинності можливо перевіряти цифрові мультипідписи із використанням лише однієї перевірки замість декількох.

Схемирозподілення секрету дозволяють розділити секрет проміж групи учасників, кожен з яких володіє тільки своєю часткою секрету. Секрет може бути відтворений тільки за умови одночасної присутності всіх або певної кількості учасників протоколу.

На сьогодні в Україні прийнято низку стандартів на криптографічні алгоритми серед яких, окрім стандарту цифрового підпису, прийняті стандарт на алгоритм симетричного блокового перетворення ДСТУ 7624:2014 та стандарт на функцію гешуванняДСТУ 7564-2014. Однак, незважаючи на те, що розглянуті схеми цифрового підпису мають вже поважний вік, їх математичний апарат та доказ криптографічної стійкості є недостатньо опрацьованими для прийняття відповідних державних стандартів, що надає широке поле для наукових досліджень.

Напрямком подальших досліджень є аналіз математичного апарату та криптографічної стійкості розглянутих схем цифрового підпису, пошук можливих областей використання та розробка відповідного програмного забезпечення.

2.1.1 Підхід до формування схем сліпого підпису

Актуальною задачею на сучасному етапі розвитку суспільства є переведення звичних офіційних та соціальних процедур в онлайн. Не останню роль в її вирішенні відіграє криптографічний механізм електронного цифрового підпису (ЕЦП). Традиційні схеми ЕЦП вже давно застосовуються на практиці в системах електронного документообігу як на рівні окремих підприємств чи

відомств, так і на рівні держави. Втім, коло задач, які можуть бути вирішені за допомогою схем ЕЦП не обмежується підтвердженням приналежності електронного документа учаснику системи електронного документообігу та засвідченням його цілісності. Існують схеми ЕЦП різного призначення, зокрема, сліпий підпис, який може бути використано в системах електронного голосування та для забезпечення обігу електронної готівки.

На часі розроблено велику кількість схем ЕЦП, а в багатьох розвинених країнах діють національні чи міждержавні стандарти ЕЦП. Криптостійкість таких схем, як правило, перевірена і доведена їхніми авторами та експертною спільнотою. Натомість, схеми ЕЦП іншого призначення, зокрема сліпого підпису, ще не стандартизовані.

Існують два підходи до формування схем сліпого підпису – розробка нової схеми та модифікація існуючої схеми ЕЦП. Другий підхід видається авторам більш виправданим, оскільки в цьому випадку криптостійкість основних перетворень схеми забезпечується базовою схемою ЕЦП. Також модифіковану схему легко інтегрувати до системи електронного документообігу чи інфраструктури відкритих ключів, де використовується базова схема ЕЦП.

Модифікація схеми ЕЦП в рамках другого підходу передбачає перетворення алгоритму постановки підпису, розрахованого на одного учасника, на протокол взаємодії двох учасників. Алгоритм перевірки підпису має залишитись без змін.

Новостворений протокол має передбачати обмін між емітентом документа і підписантом. При цьому емітент має засліпити параметри, які він надсилає підписанту, і зняти засліплення з отриманого від підписанта компонента підпису. Засліплення, як правило, відбувається за допомогою декількох випадкових коефіцієнтів, які емітент обирає окремо для кожної сесії постановки підпису. При розробці співвідношень для засліплення параметрів і його зняття можуть використовуватись тимчасові коефіцієнти, які потім мають бути виражені через коефіцієнти засліплення шляхом вирішення відповідної

системи рівнянь. Також треба враховувати необхідність забезпечення захищеності схеми сліпого підпису за критерієм анонімності, оскільки криптостійкість базової схеми ЕЦП на нього не розрахована.

Авторами продемонстровано дієвість такого підходу, зокрема, на прикладі модифікації німецького стандарту ЕЦП ECGDSA. Отримане сімейство схем сліпого підпису захищене за критерієм анонімності і може бути використане за призначенням.

2.1.2 Протоколи групової підписи

Аутентифікація інформації за допомогою двохключового схем електронного цифрового підпису знайшла широке застосування в інформаційних технологіях, пов’язаних з циркуляцією електронних повідомлень і документів, що мають юридичне значення. У різноманітних практичних додатках використовуються протоколи електронного цифрового підписи різного типу: звичайна (індивідуальна) цифровий підпис, колективна цифровий підпис, сліпа цифровий підпис та ін. Одним з цікавих проток є групова цифровий підпис.

Протокол групового електронного цифрового підпису забезпечує можливість формування цифрового підпису від імені деякого колегіального органу - групи підписантів, один з яких є лідером (керівником). В даному протоколі реалізуються наступні властивості: підписати документ має можливість будь-який член групи; лідер за значенням електронного цифрового підпису та відповідного їй документу може визначити особу, сформувало дану конкретну підпис; особи, які не перебувають в штаті органу, не можуть встановити, хто конкретно сформував групову підпис до заданого документу.

Розглядається протокол групової цифрового підпису, що задовольняє додатковим вимогам: особисті секретні ключі підписувати не розголошуються кому б то не було; формування групової підпису здійснюється в два етапи;

предподпісь може бути сформована будь-яким підписує або будь-яким підмножиною підписують; по деякому документу і груповий підписи до нього ідентифікувати підписала або підмножина підписали може тільки лідер.

У протоколі даного типу питання про те, хто підписує конкретний документ, є прерогативою керівника (лідера), який розподіляє роботу з підготовки електронних документів.

При формуванні підпису на першому етапі виконавцем або декількома виконавцями формується «групова предподпісь», яка фактично є їх цифровим підписом, що додається до цього документу. Якщо керівник вирішує затвердити документ, то на другому етапі він з «предподпісі» обчислює значення групової підписи, т. е. виконує процедуру затвердження підписаного документа.

Таким чином, групова підпис в запропонованому протоколі включає в себе підписи розробників документа і яка стверджує підпис керівника.

Розглянутий протокол групової цифрового підпису забезпечує роботу з електронними документами в близькій аналогії з традиційною процедурою підготовки, підписання та затвердження паперових документів. Це робить його досить цікавим для практичного використання в технологіях електронного документообігу. Перевагою є також і можливість використання стандартної інфраструктури відкритих ключів, яка в даний час є і використовується для реалізації протоколів індивідуальної цифрового підпису. Це дозволяє легко розширювати групу підписують, а також змінювати лідера, якщо виникне в цьому необхідність.

Протокол також досить гнучко реалізує і властивість «порогового».

Гнучкість полягає в тому, що не потрібно участь довірених осіб і лідер вирішує самостійно, скільки і які виконавці повинні бути залучені для роботи над тим чи іншим документом.

Завдання забезпечення неотслежіваемості учасників процедури формування конкретної групової підпису вирішується шляхом маскування

відкритих ключів, які підписують в залежності від значення хеш-функції від підписується документа і від додаткового секретного ключа лідера.

Запропонований протокол групової цифрового підпису відрізняється від відомих раніше набором додаткових властивостей. На відміну від індивідуальної електронного цифрового підпису групова цифрова підпис містить три елементи, що істотно збільшує розмір підписи в порівнянні з випадком протоколів індивідуальної цифровий підписи, заснованих на складності завдання дискретного логарифмування.

Однак розмір груповий цифрового підпису (1344 біт) незначно перевищує розмір індивідуальної цифрового підпису в криптосистеме RSA (1024 біт) при заданому рівні стійкості.

Конструктивна схема розглянутого протоколу і її основні механізми дозволяють розробляти нові протоколи груповий електронного цифрового підпису із застосуванням інших перевірочних рівнянь і інших кінцевих груп.

2.1.3 Протокол колективного цифрового підпису на основі EC-GDSA для використання в телемедицині

Важливим напрямом розвитку сучасної медицини є Digital med (телемедицина, цифрова радіологія, e-health). При цьому важливо дотримуватись вимог щодо дотримання конфіденційності медичної інформації при застосуванні інструментів телемедицини. Безпека та автентичність даних, що передаються каналами зв’язку, забезпечується використанням криптографічних методів в умовах функціонування загальної на рівні держави інфраструктури відкритих ключів. В ЄС кожна країна – член ЄС має створювати власну інфраструктуру відкритих ключів, але при цьому дотримуватися вимог європейського законодавства з метою забезпечення інтероперабельності.

Існуючі стандарти електронного цифрового підпису в більшості ґрунтуються на арифметиці еліптичних кривих. Німеччина є однією з найбільш

розвинених держав європейського союзу з високим рівнем розвитку ринку послуг телемедицини, потенціально найбільш готовою до впровадження нових технологій. Тому розглянемо можливість модифікації сучасного стандарту електронного цифрового підпису Німеччини EC-GDSA для реалізації колективного підпису, який може бути корисним для забезпечення безпечної автентифікації загального медичного висновку при проведенні консиліуму лікарів.

2.2 Дослідження клептографічних атак на криптосистеми

Сучасні комп'ютерні технології та нові математичні методи дають можливість крипто- аналітикам створювати різного роду небезпечні програми і впроваджувати шкідливі крипто- алгоритми в криптосистеми.

Вперше поняття клептографії ввели А. Янг та М. Юнг [63], як метод використання криптографії проти криптографії з метою отримання секретної інформації.

Існують різні клептографічні атаки, в ході яких зловмисник використовує асиметричну систему криптографії для здійснення злому.

При здійсненні клептографічних атак створюються приховані канали, які є частиною криптоалгоритму і дозволяють непомітно передавати інформацію з криптографічної системи або, навпаки, в криптографічну систему. Наприклад, додаткова інформація може міститися в цифровому підпису або у відкритому ключі шифрування.

2.2.1 Клептографічна атака на ECDSA

Клептографічна атака – це створення "закладки", що впроваджується в криптосистему, що розробляється, яка може бути реалізована у вигляді апаратного пристрою (наприклад, смарт-карти) або програми (наприклад, Web-

сервера або поштового клієнта). При цьому не повинно існувати можливості виявити наявність закладки за зовнішніми ознаками. Інакше кажучи, якщо розглядати криптосистему як "чорний ящик", неможливо визначити, здійснив розробник клептографичну атаку чи ні.

Крім того, атакуюча сторона, що створює "закладку", отримує ексклюзивне право її використання, тобто навіть за наявності у третьої сторони вичерпної інформації про реалізацію системи, вона у кращому разі зможе виявити наявність прихованого каналу, але не зможе їм скористатися.

Базовими елементами будь-яких клептографічних атак є приховані канал передачі інформації. Саме вони в поєднанні з додатковими криптографічними методами забезпечують секретність цих атак. Клептографічні методи дозволяють довести до досконалості приховання факту передачі додаткової інформації. У цьому сенсі простежується схожість з стеганографією.

Приховані клептографичні канали є частиною крипто-алгоритма і дозволяють непомітно передавати інформацію з криптографічної системи або, навпаки, в криптографічну систему. Наприклад, додаткова інформація може міститися в цифровому підписі або у відкритому ключі шифрування.

При аналізі роботи клептографічних систем слід виділити наступних учасників.

Розробник має інформацію про модифікацію алгоритма, володіє секретним ключем прихованого каналу передачі інформації, не володіє секретним ключем користувача.

Користувач володіє секретним ключем користувача, у разі успішного реверс-инжиниринга (reverse engineering - зворотнє проектування) має інформацію про модифікацію криптосистеми, але не володіє секретним ключем прихованого каналу.

Зловмисник у разі успішного реверс-інжиниринга володіє информаций про модифікацію алгоритму, але не володіє секретним ключем прихованого каналу передачі інформації і секретним ключем користувача.

Метою даної роботи є ознайомлення та аналіз клептографічної SETUP–атаки (Secretly Embedded Trapdoor with Universal Protection) на алгоритм цифрового підпису на еліптичних кривих ECDSA, а також реалізація цієї атаки.

В цій роботі наведені принципи клептографічного атакування на асиметричні криптографічні алгоритми. Зокрема описано SETUP-атака

Практична реалізація клептографічної SETUP – атаки була здійснена на 2-х різних еліптичних кривих над простим полем

В результаті атаки знайдено секретний ключ, за допомогою якого був сформований цифровий підпис за алгоритмом ECDSA.

Для здійснення цієї атаки крипто аналітику необхідно створити додаткові параметри, які використовуються при формуванні цифрового підпису, а також прихований канал для зберігання необхідних параметрів.

Аналіз SETUP–атаки на алгоритм ECDSA показав, що ця атака може бути здійснена при умові лише разового доступу до модифікації програмного забезпечення.

2.2.2 Захист від клептографічних атак на криптосистеми

В ході проведених експериментів та після аналізу клептографічних атак авторами запропоновано заходи до реалізації захисту від клептографічних атак зображено на рисунку 2.1.

У загальному випадку як показано на рисунку 1 методи і моделі захисту криптосистем повинні дозволяти проведення: аналізу сценаріїв, способів реалізації та розпізнавання образів клептографічних атак потенційного порушника; ідентифікації стану криптосистем; апріорного опису процесів протидії атакам на криптосистеми; попередження, виявлення та аналізу атак на основі математично формалізованих і узгоджених логічних правил; експериментальної оцінки ефективності застосування засобів протидії клептографічним атакам; обґрунтування оцінки методів, моделей і засобів

протидії атакам; обґрунтування вимог і пропозицій щодо розроблення засобів протидії атакам.

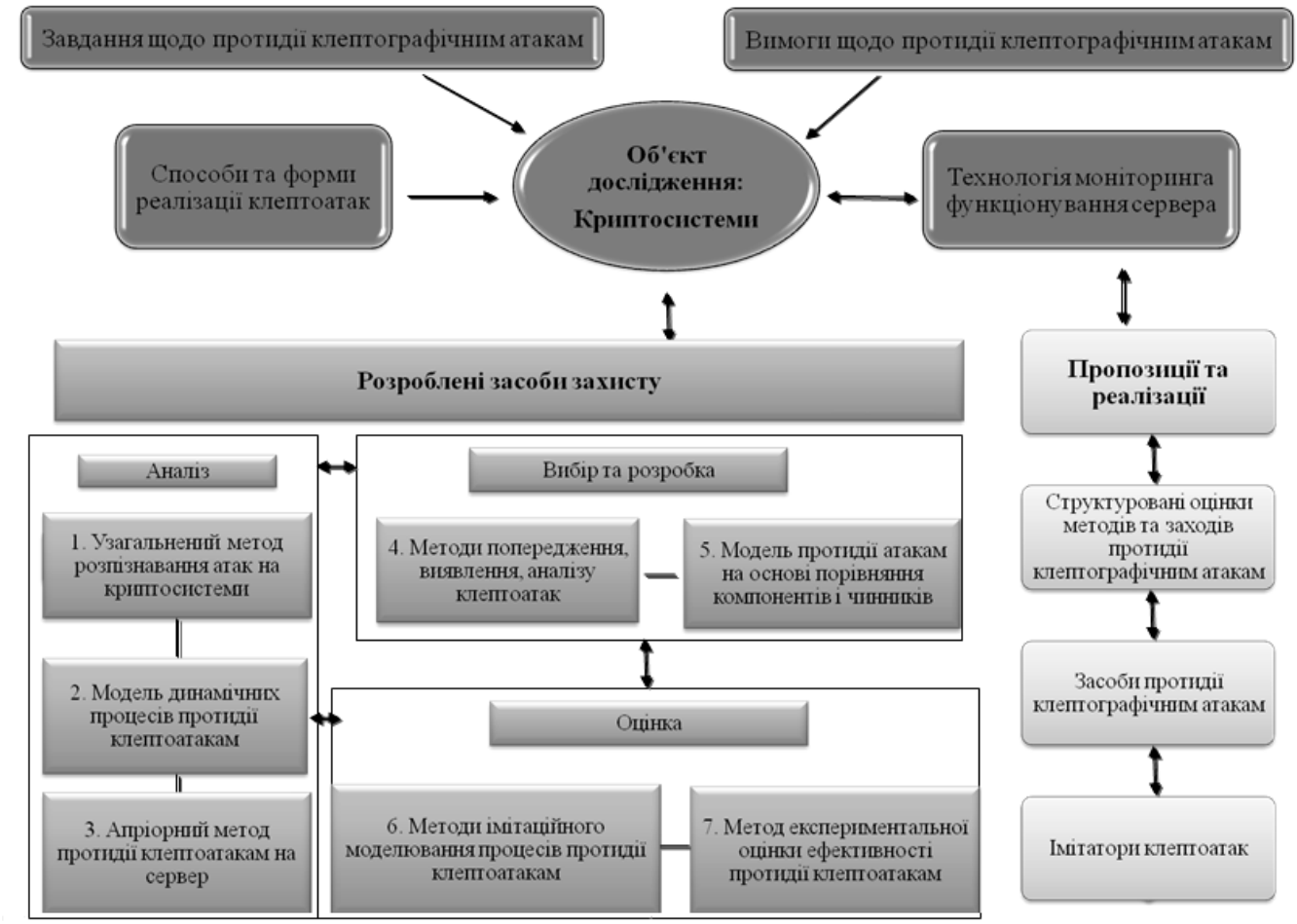

Рисунок 2.1 – Структурна модель методів протидії клептографічним атакам

На сьогодні криптографічні методи захисту інформації вважаються стійкими до порушення конфіденційності інформації, і використовуються для більш надійної передачі повідомлень користувачів. Але клептографія доводить протилежне, тобто що при можливості зловмисника ввести модифікації перед тим як криптографічний алгоритм стане «чорним ящиком» тоді криптографічні методи будуть «працювати» на зловмисника.

На основі практичної реалізації можна зробити висновок що зловмисник не знаючи параметрів користувача, але маючи можливість впровадження додаткового алгоритму в криптосистему може дізнатися секретний ключ користувача за допомогою SETUP атаки, та троянських впроваджень.

2.3 Алгоритми заперечуваного шифрування

2.3.1 Дослідження алгоритмів заперечуваного шифрування

Останнім часом зростає кількість кіберзлочинів, які охопили майже всі мережевої інфраструктури. Існуючі засоби криптографічного захисту хоча й забезпечують криптографічну стійкість до зламу збоку зловмисників, але вони винаходять все більш тонкі способи їх обходу шляхом впливу безпосередньо на користувачів цих засобів. Тому криптографічна стійкість сучасних алгоритмів шифрування вже не забезпечує абсолютну стійкість до зламу.

Для вирішення цієї проблеми було винайдено метод заперечуваного шифрування [64], який зустрічається в сучасній літературі під назвою «неоднозначне» шифрування.

Метод заперечуваного шифрування має на меті не скільки приховати секретну інформацію, скільки заперечити сам факт її існування. Власник секретної інформації має можливість не лише заперечувати факт існування криптограми, а й саму ймовірність існування в ній будь-якої секретної інформації. При дешифруванні криптограм, сформованих за одним із алгоритмів заперечуваного шифрування, користувач може отримати декілька варіантів секретного повідомлення.

Такий підхід дозволяє виключити можливість компрометації секретної інформації зловмисником, навіть при повному зламі криптографічної схеми алгоритму.

Авторами були досліджені алгоритми,яки запропоновали М.А. Молдовян, Г. Ібрахім, JingQing Wang і Bo Meng.

В результаті досліджень цих алгоритмів були перевірені їх криптографічна стійкість та стійкість до впливу на абонентів, які визначають ефективність роботи алгоритмів.

Аналізуючи результати досліджень можна зробити висновок, що алгоритми заперечуваного шифрування запропоновані JingQing Wang, Bo Meng

і Г. Ібрахімом мають оптимальну стійкість не лише до атак на основі обчислень, але й до атак на основі впливу на абонента.

Алгоритм заперечуваного шифрування, запропонований М.О. Молдовяном, хоча й має дещо меншу стійкість, але на відміну від попередніх він має досить просту реалізацію, що робить його більш перспективний для практичного застосування.

Проте недоліками цих алгоритмів є обмежена кількість повідомлень, які можуть бути зашифровані в криптограмі (фіктивних повідомлень).

Отже, усі досліджені алгоритми заперечуваного шифрування є досить перспективними для подальшого вивчення та практичного застосування для захисту інформації в комп'ютерних системах і мережах.

2.3.2 Модифікація алгоритму заперечуваного шифрування Менга

Алгоритм заперечуваного шифрування Менга вирішує проблему щодо атак на основі примушування, яке застосовується як до відправника та одержувача, так і до обох одночасно. Таким чином виключається будь – яка можливість отримання секретної інформації зловмисником.

Оскільки на етапі генерації ключів виникає проблема, яка пов'язана з розподілом ключів між абонентами, то її вирішення полягає у модифікації первісного алгоритму шляхом функціональної заміни задачі дискретного логарифмування на протокол «непомітної» передачі *OTn*1 [25].

Згідно з результатами експериментів можна зробити висновок, що застосування протоколу «непомітної» передачі *OTn*1 в процедурі розподілу ключів алгоритму заперечуваного шифрування Менга має більш оптимальний час і спрощує його технічну реалізацію.

Моделювання роботи модифікованого алгоритму заперечуваного шифрування Менга було виконано за допомогою 128-бітного ключа та продемонстровано його особливості, які забезпечують надійний захист

інформації від атак на основі примусу. Для оцінки ефективності виконаних модифікацій алгоритму авторами проведено експерименти щодо визначення оптимальної швидкодії його роботи шляхом порівняння швидкодії первісного та модифікованого алгоритмів.

Оскільки модифікація полягала в покращенні часових характеристик процедури генерації та розподілу ключів, то для спрощення експериментів було досліджено швидкодії процедур генерації ключів: на основі задачі дискретного логарифмування та протоколу «непомітної» передачі *OTn*1.

Для виконання експериментів було використано структурні схеми первісного та модифікованого алгоритмів заперечуваного шифрування Менга.

Основний показник, який досліджувався в ході експериментів – це швидкодія виконання процедури генерації ключів. За результатами проведених експериментів автори виконали порівняльну характеристику швидкодії процедур генерації ключів і визначили оптимальний час для виконання процедури генерації ключів, а також метод за допомогою якого вона виконана.

В ході проведення експерименту експериментальні дані, отримані авторами, носять практично константний характер, тобто одне й те саме значення для ключів, яке складає 15–16 мс для ключів розрядністю до 2048 біт і більше (коливання часу на рівні 1 мс).

2.4 Використання паралельних та квантових обчислень при реалізації криптографічних алгоритмів

На сьогоднішній день паралельні та квантові технології, такі як розподілені системи, квантові системи та комунікації, квантове шифрування, квантові алгоритми, квантові лінії зв’язку та ін. мають високий потенціал в системі захисту інформації. Саме тому квантові системи передачі інформації викликають інтерес у фахівців із захисту інформації.

2.4.1 Розпаралелювання та порівняльний аналіз методів дискретного логарифмування на GPGPU

Стійкість криптосистем, що побудовані за принципом задачі Діффі-Хеллмана, ґрунтується на високій обчислювальній складності задачі дискретного логарифмування в скінченому полі Галуа. Найбільш ефективні на сьогодні алгоритми дискретного логарифмування мають вже субекспоненційну складність. Також існують квантові алгоритми вирішення цієї задачі, які чекають свого часу.

В роботі проведено розпаралелювання та реалізація відомих алгоритмів дискретного логарифмування (index-calculus, ρ − Полларда, Шенкса, COS та інш.), включаючи метод повного перебору для різної довжини вхідних параметрів.

Для проведення дослідження авторами було розроблено бібліотеку MINI-GMP-CUDA для масивно паралельних пристроїв GPGPU, яка повністю повторює програмний інтерфейс бібліотеки GMP і сумісна з нею на рівні структур даних, що дозволяє використовувати засновані на GMP алгоритми в середовищі графічного процесора без необхідності зміни кодової бази. Сумісність портованої бібліотеки з GMP на рівні структур даних дозволяє використовувати її в CPU / GPU-гібридних кластерних системах.

Для портування на CUDA було обрано скорочену версію MINIGMP бібліотеки GMP, яка за даними різних досліджень визнана однією з найбільш високопродуктивних бібліотек довгої арифметики. Однак повна версія GMP, крім базових структур даних і алгоритмів, містить також велику кількість оптимізацій під різні процесорні архітектури. В складі MINI-GMP збережено всі основні функції повної версії, але вона позбавлена при цьому ряду архітектурно-залежних частин коду.

Процес перенесення коду, орієнтованого на CPU, в код для графічного процесора можна умовно розділити на кілька етапів.

Перший етап зводиться до простого синтаксичному прийому, який визначає для яких функцій потрібно генерувати при компіляції GPU-орієнтований машинний код. У складі SDK CUDA присутній компілятор NVCC, який дозволяє за допомогою спеціальних модифікаторів вказувати середу виконання кожної функції.

Другий етап полягає у виключенні з коду функцій і системних викликів, для яких немає аналогів в середовищі графічного процесора. У випадку з бібліотекою MINI-GMP до таких функцій відносяться функції роботи з пристроями введення-виведення і функції роботи з файлами.

Третій етап полягає в зміні функцій роботи з пам’яттю. Архітектура CUDA не передбачає можливість динамічного розподілу пам’яті в процесі обчислень. Вся пам’ять, що використовується обчислювальними ядрами, повинна бути виділена до початку процесу обчислень, в той час як в бібліотеці MINI-GMP часто застосовується динамічне виділення пам’яті у тілі обчислювальних функцій. У портованій версії бібліотеки кількість пам’яті, що виділяється для зберігання даних, вказується на етапі компіляції.

Інтерес для даного дослідження алгоритми дискретного логарифмування представляють як основа більш стійких алгоритмів дискретного логарифмування на еліптичних кривих, які планується дослідити за аналогічною методикою в подальших експериментах.

2.4.2 Розробка паралельних моделей протоколів квантової криптографії під технологію GPGPU

Квантова технологія – здатність керувати складними квантовими системами на основі їх індивідуальних компонентів. В квантовому комп’ютері необхідно управляти окремими квантовими елементами – квантовими бітами (кубітами) щоб здійснювати квантові обчислення.

Квантові комп’ютери працюють за кардинально іншим принципом, ніж класичні комп’ютери, де вся інформація закодована послідовністю бітів (нуль

або одиниця). Якщо три звичайних біта можуть передавати будь-яке із восьми значень (два в третього ступеня), то три кубіта можуть теоретично представляти всі вісім значень. Це означає більш швидкі обчислення в порівнянні з класичними комп'ютерами.

Квантова криптографія є новим етапом в еволюції інформаційного захисту, заснованим на законах квантової фізики. Кожен біт коду передається за допомогою квантового стану елементарної частинки світла-фотона. Як відомо, аксіома квантової фізики свідчить, що квантовий стан неможливо виміряти не порушивши його. Таким чином, виключається спроба зловмисника заволодіти інформацією, що виводить криптографію як науку на принципово новий рівень.

Однак, квантова технологія має і певні недоліки.

Через нестійкість поляризації одиночного фотона основна кількість помилок в сирому ключі спостерігається через втрату поляризації фотонів після проходження по інформаційному каналу. Через нестійкість поляризації системи даного типу обмежені довжиною лінії передачі. Процес виправлення помилок детектування поляризації робить систему громіздкою і зменшує її швидкість.

Існуюча елементна база лавинних фотодіодів має низьку швидкість і низьку квантова ефективність.

Складні методики контролю поляризації зазвичай не виправдовують себе, що призводить до збільшення помилок в ключі.

Незважаючи на труднощі апаратного втілення квантових технологій корпорація IBM зовсім недавно вже відкрила тестовий доступ до свого хмарного квантового комп'ютера, що на їх думку допоможе дослідникам усього світу працювати над інноваційними технологіями [65].

Привабливість досліджень в області квантових комп'ютерів забезпечується природним паралелізмом таких обчислень, який можна змоделювати на сучасних масивно- паралельних пристроях ще до використання реального квантового комп'ютера.

На сьогоднішній день набирає обертів парадигма GPGPU-неспеціалізовані обчислення на графічних процесорах – метод використання графічного процесора відеокарти (масивно-паралельного пристрою) для виконання не тільки графічних, а й загальних обчислень.

Однією з платформ для таких обчислень є технологія CUDA.

CUDA будується на концепції, що GPU (званий пристроєм, device) виступає в ролі масивно-параллельного співпроцесора до CPU (званому host). Программа на CUDA задіє як CPU, так і GPU. При цьому звичайний (послідовний, тобто не паралельний) код виконується на CPU, а для масивно-паралельних обчислень відповідний код виконується на GPU як набір ниток (потоків, threads), що виконуються одночасно. Таким чином, GPU розглядається як спеціалізований обчислювальний пристрій, який: є співпроцесором до CPU; володіє власною пам'яттю; має можливість параллельного виконання огромного кількості окремих ниток.

Метою дослідження є розробка програмних моделей протоколів квантової криптографії на GPU з використанням технології CUDA дозволяє виключти недоліки криптографічних протоколів ще на етапі моделювання, що дає позитивний економічний ефект.

2.4.3 Порівняльний аналіз протоколів квантового розподілення ключів

Порівняльний аналіз спрямований на вивчення сучасної квантової теорії в системі захисту інформації, ознайомлення з історією виникнення та розвитку квантової криптографії та криптографічних протоколів. Висвітлюються проблеми та недоліки практичної реалізації квантових протоколів, перелік атак на криптосистеми та методи їх усунення. Проводиться аналіз протоколів квантового розподілення ключів (КРК) таких як BB84, B92, протокол КРК з шістьма станами, BB84(4+2), Гольденберга-Вайдман, Коаші-Імото, E91, протоколи SARG04 та Lo05.

Зараз число фотонів, потрібне для успішної передачі, дуже велике, порядку мільярдів. Необхідна деяка оптимізація, яка значно скоротить це число. У більш довгостроковій перспективі присутній інтерес до розробки однофотонних джерел. Однофотонні джерела знайдуть корисне застосування в області квантових комп'ютерів, заснованих на лінійній оптиці. Незважаючи на те, що вони не строго необхідні для КРК, вони можуть збільшити частоту зміни ключа при ньому. Ідеальне однофотонне джерело – те, що по команді випускає один фотон: людина натискає кнопку - один фотон вилітає.

Неефективність реєстрації станів фотонів є платою за секретність. Слід враховувати, що при роботі в однофотонному режимі виникають чисто квантові ефекти. При горизонтальній поляризації (H) і використанні вертикального поляризатора (V) результат очевидний – фотон не буде зареєстрований. При 45-градусній поляризації фотона і вертикальному поляризаторі (V) ймовірність реєстрації 50%. Саме ця обставина і використовується в квантової криптографії.

Квантова криптографія [66] наразі знаходиться на етапі свого активного розвитку. Зокрема активно проводиться проектування квантових оптичних криптографічних систем з використанням різноманітних модифікацій апаратури та криптографічних протоколів. Найкращим каналом передачі квантових кодів вважаються волоконно-оптичні лінії зв'язку, оскільки їх зручно будувати, вони вважаються найбільш захищеними та швидкими.

Протоколи квантового розділення ключів вже проходять етап тестування на реальних системах, створюються канали передачі на невеликих дистанціях.

При аналізі перерахованих вище протоколів квантового розподілення ключів за основу бралися їх фізичні перетворювання, властивості и реалізація, а також складність проектування криптографічних систем з цими протоколами КРК і їх криптостійкість. Основним параметром, який їх об'єднує поки є недолік короткої безпечної дистанції передачі. На разі робота з цими протоколами не закінчена, продовжуються вдосконалення в методиці кодування сигналів та йдуть роботи по покращенню фізичної реалізації таких каналів передачі інформації.

Виходячи з результатів аналізу можна зробити висновок, що найбільш популярними протоколами КРК є BB84 та B92. Вони прості в алгоритмі кодування, мають значну швидкодію та результативність реєстрації отриманих фотонів при передачі відкритим каналом. Для фізичної реалізації не потребують дорогої апаратури. Обов'язкова наявність волоконно-оптичної лінії зв'язку, лазеру та фотодетекторів.

Але дані протоколи в своєму звичайному вигляді криптоламкі. Вже в експериментальних умовах успішно проведені декілька атак на ці протоколи. Тому у «сирому» вигляді їх використовувати небажано. Для підвищення захищеності окрім самих протоколів також бажано робити перемішування коду.

2.4.4 Моделювання протоколів квантової криптографії на платформі CUDA

Квантова криптографія є новим етапом в еволюції інформаційного захисту, заснованим на законах квантової фізики. Кожен біт коду передається за допомогою квантового стану елементарної частинки світла-фотона. Як відомо, аксіома квантової фізики свідчить, що квантовий стан неможливо виміряти не порушивши його. Таким чином, виключається спроба зловмисника заволодіти інформацією.

В даний час квантова криптографія включає кілька напрямків, одним з яких є квантові протоколи розподілу ключів. Існує декілька протоколів розподілу ключів. У дослідженні розглядається принцип роботи квантового протокола розподілу ключів і проводитися порівняльний аналіз на прикладі двох протоколів: протоколу BB84 і протоколу з шістьма станами.

Однією з причин привабливості досліджень в області квантових комп'ютерів є їх природний паралелізм обчислень.

На сьогоднішній день набирає обертів парадигма GPGPU-неспеціалізовані обчислення на графічних процесорах – метод використання

графічного процесора відеокарти (масивно-паралельного пристрою) для виконання не тільки графічних, а й загальних обчислень. Однією з платформ для таких обчислень є технологія CUDA. Вона дозволяє істотно збільшити обчислювальну продуктивність в результаті використання графічних процесорів.

Метою даного дослідження є розробка програмних моделей протоколів квантової криптографії на масивно-паралельних пристроях з використанням технології CUDA. Це дозволить виключити недоліки протоколів на етапі моделювання до створення реального квантового комп’ютера.

ЗРОЗРОБКА ТЕХНІЧНИХ МЕТОДІВ ЗАХИСТУ

3.1 Захист інформації у волоконно-оптичних лініях зв'язку

В даний час все більше конфіденційної інформації передається саме волоконно-оптичними мережами зв'язку. Це пояснюється тим, що з точки зору надійності та захищеності волоконно-оптичні лінії посідають провідне місце серед безпечних мереж передачі інформації, при цьому зберігається надвисока пропускна здатність каналу передачі, висока завадостійкість та інші позитивні властивості. Але, при певних умовах, за яких зловмисник має безпосередній доступ до волоконно-оптичної лінії, перехоплення інформації та її трактування стає цілком можливим [67-68]. Тому, виникає актуальна задача створення більш надійного способу передачі інформації по волоконно-оптичним лініям зв'язку шляхом впровадження додаткових методів захисту.

3.1.1 Захист інформації у волоконно-оптичних лініях зв'язку від несанкціонованого доступу

Запропоновано розробка способу захисту інформації у волоконно-оптичних лініях зв'язку від несанкціонованого доступу з поліпшеними характеристиками, тобто з підвищеною захищеністю, надійністю та з покращеною якістю інформаційного сигналу на приймальній стороні, які досягаються шляхом технічних удосконалень.

Поставлена задача вирішується тим, що виконується маскування інформаційного сигналу перед передачею по волоконно-оптичній лінії зв'язку, тобто забезпечується однакова форма заповнення кожної частини тактового інтервалу Т як при передачі двійкового нуля, так і при 5 передачі двійкової одиниці, а на приймальній стороні виконуються зворотні перетворювальні дії.

При цьому виконують наступні перетворювальні дії. Перед передаванням інформації вона проходить етап маскування, а саме, інформацію, яку треба

захистити, розподіляють за кодом RZ-1/4, тобто на чотири частини тактового інтервалу Т, причому двійкова одиниця передається однією чвертю тактового інтервалу Т на його початку, затримується на час, рівний 1/2 частині 10 тактового інтервалу, та передається як на початку тактового інтервалу, так і у третій його чверті разом протягом кожного тактового інтервалу Т.

Маскування інформації виконується також при передачі двійкового нуля, передавання якого відбувається заміною відсутнього в тактовому інтервалі Т нульового посилання на посилання імпульсів відповідних двійковій одиниці.

Виконуються такі ж перетворювальні дії як для двійкових одиниць, передача замаскованих 15 двійкових одиниці та нуля відбувається на двох обов'язково сусідніх довжинах хвиль стандартного частотного плану WDM, які мультиплексуються і передаються одночасно, на приймальному боці після демультиплексування інформація маскованих двійкових нулів відкидається, а двійкових одиниць передається для подальшої обробки, в процесі якої інформація на 1/4 та 3/4 частинах кожного тактового інтервалу Т коду RZ-1/4 затримується на 20 час, що дорівнює 1/4 частині тактового інтервалу, відповідно інформація відображається на 2/4 та 4/4 частинах у кожному тактовому інтервалі при передаванні двійкової одиниці, а на виході приймача отримується інформація в коді NRZ.

Запропонований спосіб захисту інформаційного сигналу від несанкціонованого доступу у волоконно-оптичних лініях зв'язку дозволяє передавати інформаційні сигнали як двійкових 25 нулів, так і двійкових одиниць в однаковій формі. При цьому досягається позитивний технічний результат – надійне маскування інформації, що передається у волоконно-оптичних лініях зв'язку та чітке її розпізнавання на приймальній стороні.

Таким чином, нові ознаки при взаємодії з відомими ознаками забезпечують виявлення нових властивостей – шляхом технічних удосконалень розроблений спосіб захисту інформації у 30 волоконно-оптичних лініях зв'язку від несанкціонованого доступу з поліпшеними характеристиками, тобто з

підвищеною захищеністю, надійністю та з покращеною якістю інформаційного сигналу на приймальній стороні.

Спектральний спосіб маскування інформаційних сигналів при передачі інформації у волоконно-оптичних лініях зв'язку працює наступним чином. Наприклад, необхідно безпечно, швидко та якісно передати конфіденційну інформацію від мікрофона, що являє собою сигнал в аналоговій формі.

Для цього виконуються наступні перетворювальні дії.

Перш за все отримуємо інформацію у вигляді інформаційних сигналів, що являються наслідком перетворення сигналів з аналогової форми в цифрову, а потім в оптичні та представляють собою набір двійкових одиниць і нулів, 45 розподіляємо їх у коді RZ-1/4 на певній довжині хвилі Л1.

Наступним кроком отримані у коді RZ-1/4 інформаційні сигнали затримуються на час, що дорівнює половині тактового інтервалу, що для коду RZ-1/4 представляє собою чотири окремих частини, тобто на час, рівний Т-1/2, та поєднуються з першою його чвертю, що передається за час Т-1/4, в результаті чого у кожному тактовому інтервалі Т передаються сигнали на 50 довжині хвилі ЛІ при передачі двійкової одиниці у часі Т-1/4 та Т-3/4, а при передачі двійкових нулів інформаційні сигнали відсутні.

Для забезпечення більш високої захищеності передаваних сигналів переходимо до етапу маскування інформаційних сигналів двійкових нулів, де допоміжний маскований сигнал, що генерується на сусідній довжині хвилі частотного плану WDM, тобто на довжині хвилі Л2 при 55 передачі двійкового нуля, передається на першій чверті тактового інтервалу Т-1/4, далі затримується на час, рівний Т-1/2, та відображається у третій чверті тактового інтервалу, тобто у часі Т-3/4, та поєднується з першою його чвертю, що передається за час Т-1/4.

Отримані сигнали мультиплексуються, в результаті чого у кожному тактовому інтервалі Т передаються сигнали на довжині хвилі Л1 та Л2 при передачі як двійкової одиниці, так і двійкового нуля у часі Т-1/4 та Т-3/4 рівномірно протягом кожного тактового інтервалу Т, тобто інформаційний та

маскований сигнали передаються у вигляді суцільного потоку даних коду RZ-1/4, що унеможливлює зрозуміти перехоплювачеві, де нуль, а де одиниця.

На приймальному боці після демультиплексування допоміжні масковані сигнали при передачі двійкового нуля відкидаються і залишаються лише інформаційні сигнали при передачі двійкової одиниці в моменти часу Т-1/4 і Т-3/4 (кодограма 8), які затримуються у часі на 1/4 тактового інтервалу та передаються відповідно у моменти часу Т-2/4 і Т-4/4.

Усі отримані чотири інформаційні сигнали у кожній частині тактового інтервалу Т-1/4, Т-2/4, Т-3/4, Т-10 4/4 підсумовуються, в результаті чого виходить сигнал чітко переданий протягом всього тактового інтервалу Т при отриманні двійкової одиниці. Так як допоміжні масковані сигнали при передачі двійкового нуля відкинуті, то у відповідних чвертях тактового інтервалу відсутні інформаційні сигнали і на приймальному боці потрапляє інформація у чітко розрізнюваному форматі коду NRZ.

Таким чином конфіденційна інформація у чіткому форматі 15 швидко знайшла свого адресата, причому введене маскування забезпечило її надійний захист.

3.1.2 Вдосконалений спосіб маскування лінійного коду в ВОЛЗ

Метою роботи є розробка більш надійного способу передачі конфіденційної інформації в волоконно-оптичній лінії зв’язку для ефективного захисту від несанкціонованого доступу шляхом впровадження додаткового маскування лінійного коду перед його передачею та демаскування на приймальному боці, а також розробка пристрою, що реалізує цей спосіб.

Аналізуючи існуючі методи маскування лінійного коду стало зрозуміло, що в ціх методах кодуються лише біти інформаційного сигналу, що містять двійкову одиницю, двійкові нулі передаються по лінії без зміни. У зв’язку з цим зловмиснику легко відрізнити передачу незамаскованих "0" і видозмінені "1".

Саме тому на кафедрі Захисту інформації ЗНТУ було проведено доопрацювання вказаних методів маскування інформації, враховуючи їх недоліки. Був запропонований новий спосіб маскування, що істотно ускладнює розшифровку повідомлення, а також пристрій, що реалізує цей метод.

Для подальшого захисту інформації в лінії зв'язку при передачі імпульсів двійкового нуля ці імпульси перетворюються в таку саму форму, як і імпульси при передаванні двійкової одиниці, а на приймальній стороні замасковані імпульси «нуля» відкидаються.

У запропонованому способі перетворення і кодування інформації в ВОЛЗ ступінь захищеності від НЗІ досить висока, оскільки важко виявити зміст інформації, що передається, яка складається з двох частин - корисною і маскувальною інформації, при передачі якої в лінію надходять однакові імпульси як при передачі "одиниці", так і при передачі "нуля".

Крім того, для НЗІ необхідне використання спеціального обладнання, яке дозволило б з'ясувати довжини хвиль переданих оптичних сигналів, налаштувати на них апаратуру.

Розроблені спосіб і пристрій маскування лінійного коду призначені для забезпечення безпечного каналу передачі інформації шляхом технічних вдосконалень. Результати роботи можуть бути використані фахівцями для удосконалення систем передачі інформації в волоконно-оптичних лініях зв'язку з метою підвищення їх захищеності, надійності та якості передаваної інформації.

3.2 Поля і хвилі в задачах технічного захисту інформації

Хвильовим процесом називають будь яку зміну (збурення) стану суцільного середовища, що поширюється з кінцевою швидкістю і переносить енергію. Існує велике різноманіття хвильових процесів (різновидів хвиль): звукові хвилі, сейсмічні, хвилі, що виникають на поверхні води, хвилі

механічних коливань в кристалах, радіохвилі, оптичні хвилі. В усіх різновидах хвильових процесів спостерігаються схожі закономірності поведінки у просторі і в часі; вони описуються однаковими математичними моделями і досліджуються загальними методами. Виділяють два основних типи хвиль: пружні і електромагнітні. Пружні (друга назва акустичні, від грецького слова acustikos – слуховий) хвилі – це хвилі, які зв'язано з коливаннями частинок при механічній деформації пружного середовища (рідкого, газоподібного, твердого). При цьому має місце перенесення енергії при відсутності переносу речовини. В акустичній хвилі частинки здійснюють коливання навколо точки спокою. Хвиля, у якої частки середовища здійснюють коливання уздовж напрямку поширення, називається поздовжньою хвилею. Якщо частки середовища коливаються перпендикулярно до напрямку поширення хвилі, акустична хвиля називається поперечною або зсувною. Це ті хвилі, які чує людське вухо. Вони займають діапазон частот від 17 Гц до 20 кГц. Більш низькі за частотою (інфразвукові, частоти нижче 17 Гц) та більш високі (ультразвукові, частоти від 20 КГц до 1 МГц) людське вухо не сприймає.

Електромагнітні хвилі – це змінні в часі електромагнітні поля, які мають властивість поширюватися в оточуючому просторі. Електромагнітні хвилі в вільному просторі завжди мають поперечні до напрямку поширення складові векторів напруженостей електричного і магнітного полів. Поздовжні складові цих векторів можуть існувати лише за певних умов (біля меж розділу різних середовищ, поблизу збуджуючих джерел, в лініях передачі). Чисто поздовжніх електромагнітних хвиль не існує. Часто електромагнітні хвилі звуть радіохвилями, підкреслюючи цим їх зв'язок з радіотехнічними процесами. Звичайно до радіохвиль відносять електромагнітні хвилі з частотами від $3\cdot10^3$ Гц до $3\cdot10^{11}$ Гц. Далі за частотою розташовано оптичний діапазон з частотами від $3\cdot10^{11}$ Гц до $1.5\cdot10^{17}$ Гц; до нього відносять інфрачервоне, видиме і ультрафіолетове випромінення. Ще більш високі частоти відповідають рентгенівському і гамма – випроміненню.

3.2.1 Моделювання взаємодії плоскої хвилі зі шаром метаматеріалу

Запроновано чисельне моделювання взаємодії плоскої хвилі із шаром метаматеріалу на прикладі структури, яка складається з дротяних елементів у вигляді спіралей з різноспрямованим намотуванням, періодично розташованих у вільному просторі. При моделюванні використовувалася програма для аналізу дротяних структур, розроблена на основі інтегрального рівняння Поклінгтона. Програма обчислює невідоме розподілення струму в дротяних елементах і далі знаходяться всі необхідні електродинамічні характеристики структури, зокрема, діаграми спрямованості розсіяного поля. Тестування програми шляхом порівняння результатів моделювання з експериментом, присвяченому проблемі подолання дифракційної межі, підтвердило не тільки адекватність моделі на основі рівняння Поклінгтона, але і показало повний збіг результатів розрахунку і експерименту [69]. Крім того, ретельне тестування програми на різних прикладах показало високу точність розрахунків полів як в далекій, так і в близькій зонах.

Шар метаматеріалу розташовувався в площині X0Z і збуджувався плоскою хвилею, що розповсюджувалася вздовж осі Y з електричним полем, поляризованим вздовж осі Z.

При моделюванні використовувалися параметри структури, що в точності відповідами експериментально перевіреним даним: діаметр витка спіралі 9 мм, період структури (вздовж осі X) 20 мм.

Спіраль має 2 витка, крок спіралі 0,16 мм, діаметр провідника 0,2 мм. Кожен виток спіралі апроксимувався 6 прямолінійними сегментами.

Проведений в даній роботі чисельний аналіз показав наявність резонансних явищ в структурі в околиці частоти f≈2 ГГц і виявив ряд частотних точок, в яких поведінка досліджуваної структури відповідала розглянутим вище властивостями.

Зокрема, на певних частотах виявлені ефекти повного відображення і повного проходження хвилі. Крім того, зафіксовано явище відхилення напрямку поширення електромагнітної хвилі.

При зміні частоти в межах від 2 ГГц до 2,8 ГГц діаграма спрямованості деформується і на частоті 2,39 ГГц приймає форму, що ілюструє ефект зміни напрямку поширення електромагнітної хвилі.

Це дає лише якісне уявлення про просторовий розподіл енергії хвилі. Кількісну оцінку можна отримати в полярній системі координат, з яких випливає, що шар метаматеріалу відхиляє падаючу хвилю переважно у верхній напівпростір (в напрямку осі Z). Дослідження поляризаційних властивостей цієї хвилі показало, що вона залишається лінійно поляризованою. Однак вектор поляризації нахилений до осі У під деяким кутом, що характерно для гіротропному магнітному середовищі.

Розташування спіралей по відношенню до обраного напряму поширення і поляризації падаючої хвилі відповідає випадку, коли структура виявляє переважно магнітні властивості. При цьому діелектрична проникність шару мало відрізняється від діелектричної проникності вільного простору.

Аналіз отриманих результатів показує, що розглянута структура шару метаматеріалу володіє частотно залежною анізотропією, яка на певних частотах призводить до ефектів повного відображення, повного проходження, або відхилення електромагнітної хвилі.

Також розглянуто властивості електрофізичних параметрів шару метаматеріалу при взаємодії з нормально падаючою на шар плоскою електромагнітною хвилею. Показано, що в режимах повного проходження та повного відбиття хвилі властивості метаматеріалу схожі з властивостями SRR-структур. Крім того показано, що при повному проходженні товщина шару є кратною цілому числу півхвиль в матеріалі шару. Проведено чисельне моделювання шару метаматеріалу, структура якого представляє собою періодично розташовані у вільному просторі дротяні спіралі з різноспрямованим намотуванням.

Аналіз результатів чисельних експериментів показав, що досліджуваний шар метаматеріалу володіє частково залежною магнітною анізотропією, однак при повороті вектора поляризації збуджуючого поля на 90 градусів ефекти анізотропії зникають. Один з напрямків подальших досліджень пов'язаний з розробкою ефективних методів безпосереднього розрахунку електрофізичних параметрів метасередовищ, побудованих з дротяних елементів довільної форми.

3.2.2 Нелінійна локація

Однією з найбільш складних задач в області захисту інформації є виявлення та пошук тих закладних пристроїв, які або взагалі не використовують радіоканал для передачі, наприклад, цифрові диктофони, або знаходяться в пасивному (невипромінювальному) стані. В цьому випадку застосування традиційних засобів виявлення закладних пристроїв (панорамні радіоприймачі, аналізатори спектру або детектори поля) взагалі неможливе, бо відсутній сам факт випромінення. Візуальний же пошук також не гарантує виявлення, бо сучасні технології дозволяють виготовляти їх з будь-яким видом камуфляжу, ховати в елементах будівельних конструкцій, інтер'єру і т.і.

Дослідження та зусилля, які було здійснено для вирішення саме цих задач і привели до появи пошукового пристрою, який отримав назву нелінійний локатор. Своєю назвою він зобов'язаний закладеному в ньому фізичному принципу виявлення підслуховувальних пристроїв.

3.2.3 Джерела завад при роботі нелінійного локатору

В практиці застосування нелінійних локаторів було виявлено, що відгуки на гармоніках сигналу опромінення можуть створюватися не тільки напівпровідниковими елементами із складу закладних пристроїв, але і такими

металевими елементами конструкцій, які контактують між собою. Для нелінійного локатору сигнали цих відгуків будуть завадами.

Найбільш типовими структурами, що створюють завади, є контактуючі між собою складові металевого каркасу і арматури залізобетонних будинків, металеві конструкції віконних і дверних коробок, арматура підвісних стель і т.і. Річ у тому, що в області контакту двох металів можуть утворюватися структури, які за своїми властивостями є деякими аналогами p-n переходів в напівпровідниках.

Таким чином утворюються хибні нелінійні елементи. Відгуки від цих нелінійних елементів сприймаються нелінійним локатором аналогічно відгукам від справжніх напівпровідників зі складу розшукуваного закладного пристрою, але за своєю сутністю такі відгуки є завадами.

Джерелами завад для роботи нелінійного локатору також може слугувати контакт двох металів зі слабким стисненням, якщо один із них (або обидва) мають проміжний оксидний шар (складені разом канцелярські скріпки, монети, плетені сітки), або просто піддані корозії метали. Рідко (при великій потужності опромінення) небажаний ефект можуть дати паяні та зварні з'єднання. Такі структури являють собою квазілінійні елементи зі стійким (інколи нестійким) *p-n*-переходом.

У фізиці напівпровідників такі поєднання звуть структурами типу метал-оксид-метал, а нелінійні елементи – МОМ-структурами. Вольт-амперна характеристика (ВАХ) такої випадкової МОМ - структури, на відміну від характеристики *p-n*-переходу, зазвичай симетрична.

При достатньо малій товщині оксидної плівки (менше десятків ангстрем) основним механізмом переносу носіїв через контакт є тунельний ефект. При невеликих напругах (менше 1В) і однакових металах, ВАХ контакту можна апроксимувати поліномом третього ступеню. При напрузі на контакті більше 1,5В ВАХ стає більш крутою, а при подальшому збільшенні – нестійкою і в більшості випадків настає незворотній пробій контакту.

Суттєвою особливістю ВАХ таких МОМ - структур є їхня нестійкість при деяких механічних впливах. Серед досить широкого розмаїття таких впливів в першу чергу виділяють зміну тиску на контакт.

3.3 Захист інформації в радіоканалах безпілотних літальних апаратів

Розвиток сучасних технологій управління і передачі інформації призводить до значного зростання інформаційних потоків в радіоканалах. Інформація, що циркулює по радіоканалах управління і інформаційного обміну, може мати критичне значення для користувача, тобто розкриття інформації стороннім особам може привести до значного збитку для користувача. Така інформація є конфіденційною і вимагає захисту від різних загроз.

З огляду на просторову доступність радіоканалів управління і інформаційного обміну з безпілотного літального апарату (БПЛА), значна увага необхідно приділяти питанням захисту інформації від несанкціонованого доступу до її смисловим змістом. Основним інструментом захисту інформації в цьому випадку є криптографічний захист, побудована на основі різних алгоритмів шифрування.

3.3.1 Проблеми захисту інформації в радіоканалах БПЛА

Стрімкий розвиток систем безпілотних літальних апаратів в Україні та за кордоном і розвиток радіоелектроніки змушують постійно переглядати вимоги до каналу зв’язку між БПЛА і наземним комплексом управління (НКУ).

На сьогоднішній день стало можливим здійснення літаководіння автопілотом при повній відсутності зв’язку між бортом літального апарату та наземним комплексом управління. При цьому льотне завдання виконується в автономному режимі. Тим не менш, це не дозволяє говорити про те, що командно-телеметрична радіолінія зв’язку може бути виключена зі складу

БПЛА. У силу підвищеної складності та вартості комплексу при його експлуатації потрібен постійний контроль за станом БПЛА, що знаходяться в повітрі. Крім того, іноді виникає необхідність коригування параметрів польоту БПЛА.

Актуальним завданням також є передача даних корисного навантаження БПЛА на НКУ. У цьому випадку потрібно забезпечити передачу великого обсягу даних при заданих вимогах по смузі пропускання, ймовірності бітової помилки та ін.

Вибір робочого частотного діапазону радіоканалу зв'язку обумовлюється декількома факторами: вимогами до маси, габаритів і споживанню приймально-передавального пристрою БПЛА; необхідною дальністю роботи при заданій ймовірності бітової помилки; можливістю отримання ліцензії на роботу в необхідному діапазоні або можливістю безліцензійної роботи.

Доцільним є вибір діапазону надвисоких частот, при цьому вдається створити антену малих розмірів, здатну розміститися в профілі крила. Щільна компоновка устаткування усередині малого БПЛА не дозволяє ефективно використовувати прийомопередавач великої потужності з укороченими антенами ультракороткохвильового діапазону внаслідок проблем з електромагнітною сумісністю і великим впливом навколишніх об'єктів на характеристики антени. Одним з відповідних частотних діапазонів є діапазон 2,4 ГГц.

До систем зв'язку БПЛА середнього і великого класу пред'являються більш жорсткі вимоги по дальності роботи, перешкодозахищеності та ймовірності бітової помилки. У цьому випадку є можливим і оптимальним комплексування декількох каналів зв'язку, що працюють в різних частотних діапазонах.

Використання декількох каналів зв'язку підвищує надійність системи передачі даних і в той же час є надлишковим з точки зору ефективного використання радіочастотного спектру. Одним із способів підвищення ефективності комплексированної системи зв'язку є адаптивна робота системи,

яка має на увазі передачу по командно-телеметричним каналах зв’язку частини даних корисного навантаження, обсяг яких варіюється залежно від поточних умов передачі радіосигналу.

Перспективним напрямком у розвитку систем зв’язку з БПЛА є використання частотних діапазонів вище 5 ГГц. При цьому стає можливою передача великого обсягу даних корисного навантаження в режимі реального часу. Факторами, що різко обмежують радіус дії радіосистеми зв’язку при використанні даних діапазонів, є сильна залежність умов поширення електромагнітних хвиль від погодних умов, необхідність прямої видимості.

Для забезпечення зв’язку на великих відстанях необхідно збільшувати відстань до радіогоризонта для наземної та бортової антен. Максимальна дальність радіозв’язку буде визначатися сумою діяльностей радіогоризонта для антен НКУ та БПЛА. При цьому зони повітряного простору можна умовно розділити на зону освітленості, зону півтіні і зону тіні. Зона півтіні є перехідною між зоною освітленості, в якій ще можливий впевнений прийом, і зоною тіні, прийом в якій може бути здійснений тільки завдяки дифракції сигналу навколо земної кулі.

Серед безліч загроз безпеці інформації в безпілотних системах можна виділити: перехоплення в радіоканалі (контроль трафіку); вплив навмисних перешкод; несанкціоноване декодування і дешифрування інформації; інформаційне перевантаження за рахунок передачі великої кількості фрагментів неправдивої інформації; передачу неправдивої інформації, постановку імітуючих перешкод; фізичний вплив на кінцеві пристрої.

Крім того, всі атаки можна розділити на пасивні та активні.

Пасивна атака на передачу даних з борту безпілотника може реалізовуватися по-різному в залежності від типу лінії передачі даних. Приміром, при передачі даних на частоті 2,4 ГГц (стандарт 802.11) для її реалізації необхідний програмний сніфер, що перехоплює трафік, а також мережева плата бездротового зв’язку з набором мікросхем Prism. Іншим способом передачі даних є супутниковий канал зв’язку. Існує певне програмне

забезпечення, що дозволяє перехоплювати трафік з супутника і зберігати його на персональний комп'ютер, приміром, продукт SkyGrabber, знову ж, при використанні відповідного апаратного забезпечення. Саме його, за твердженнями командування американської армії в Іраку, використовували повстанці для отримання зображення з розвідувальних БПЛА.

Для передачі відеопотоку більш низької якості може використовуватися канал бездротового зв'язку на частоті 2.4 ГГц. При використанні даного виду зв'язку на канал можуть бути проведені як пасивні, так і активні атаки. Програмне забезпечення, що використовується для проведення такого роду атак, також широко поширене в Інтернеті.

Приміром, може використовуватися сніфер Wireshark, що дозволяє перехоплювати пакети, передані по бездротовій мережі, а також зберігати їх на персональний комп'ютер для подальшої обробки. Одним з плюсів даної програми є можливість провести атаку на зашифрований бездротовий канал зв'язку.

Бездротові мережі беззахисні перед атаками на перший рівень. Єдине, що можна зробити - спробувати виявити джерело перешкод. Це можна зробити методом тріангуляції, тобто шляхом заміру рівня сигналу в декількох точках. На підставі отриманих даних можна спробувати визначити місцезнаходження придушуючого пристрою.

Враховуючи просторову доступність радіоканалів управління та інформаційного обміну з БПЛА, значну увага необхідно приділяти питанням захисту інформації від несанкціонованого доступу до її смислового зміста. Основним інструментом в цьому випадку є криптографічний захист, побудований на основі різних алгоритмів шифрування. Крім того, при здійсненні передачі конфіденційної інформації по зв'язку БПЛА принципово необхідно виконання процедури аутентифікації – підтвердження дійсності абонента.

3.3.2 Протокол захисту інформації в радіоканалах БПЛА

У загальному випадку системи управління і інформаційного обміну з безпілотним літальним апаратом можуть бути різнорідними і використовувати різні протоколи на різних рівнях моделі взаємодії відкритих систем.

У таких мережах можуть бути використані різні канали передачі інформації, в тому числі провідні, радіо, оптичні та ін. Крім того, в інтересах управління і інформаційного обміну з безпілотним літальним апаратом можливе використання мережевих супутникових систем зв'язку загального користування.

У зв'язку з цим найбільш доцільно розміщувати криптографічні функції на рівні уявлення або прикладному рівні семиуровневой моделі взаємодії відкритих систем OSI (open systems interconnection basic reference model), що аналогічно «тунелювання» при створенні закритих каналів в комп'ютерних мережах.

Шифрування всієї інформації, що передається в цьому випадку здійснюється до її надходження в термінальну абонентську апаратуру. За рахунок цього стає можливою аутентифікації абонентів подальшим переходом до інформаційного обміну в закритому режимі роботи.

У безпілотних системах доцільніше використовувати асиметричні криптосистеми. Асиметричні криптосистеми дозволяють будувати ефективні алгоритми аутентифікації. Використання для захисту інформації тільки симетричних криптосистем вимагає поширення великої кількості ключової інформації, а асиметричні криптосистеми вільні від даного недоліку.

Розроблено комбінований алгоритм генерації загального сеансного ключа і поточного шифрування, який поєднує в собі переваги симетричних і асиметричних криптосистем. Алгоритм визначає порядок вироблення загального сеансного ключа на основі протоколу Діффі-Хеллмана з використанням еліптичних кривих (асиметрична частина) з подальшим шифруванням потоку інформації методом гамування (симетрична частина).

Початкові стани обох генераторів визначаються ключем, отриманим в результаті алгоритму генерації сеансного ключа.

Шифрування переданих повідомлень в цьому випадку проводиться тільки кінцевими абонентами. Зашифрований пакет інформаційного обміну абонентів инкапсулируется в пакет за стандартом, прийнятим в використовуваної мережі зв'язку.

3.4 Побудова комплексних систем захисту інформації

Сучасне життя неможливе без комп'ютерних систем та мереж. Тому захист інформації в таких мережах набуває все більшої актуальності.

3.4.1 КСЗІ типового робочого місця АС-1 4-ої категорії на базі системи «Лоза-1»

Одним з механізмів захисту інформації є система «Лоза-1». «Лоза-1» - це програмний засіб захисту інформації від несанкціонованого доступу в автоматизованих системах класу «1». Ця система призначена для захисту інформації, що обробляється у відокремлених комп'ютерах і може працювати під керуванням операційних систем Windows XP/Vista/7/8/8.1/10/2003/2008/ 2012 (32- та 64-розрядних версіях).

«Лоза-1» реалізує всі стандартні функції, необхідні для надійного захисту інформації від несанкціонованого доступу і тому може бути використана для побудови комплексної системи захисту інформації.

Використання системи «Лоза-1» в автоматизованих системах класу «1» має наступні переваги: захист від несанкціонованого доступу до інформації (забезпечує надійний захист документів Microsoft Word та Microsoft Excel за рахунок тісної інтеграції з Microsoft Office за рахунок відключення небезпечних команд, макросів, шаблонів тощо); контроль друку та експорту (забезпечує

можливість встановлення дозволу/заборони друку та експорту на рівні окремих документів); контроль входу користувачів до системи; реєстрація подій (веде захищений журнал, в якому реєструються всі події, важливі для захисту інформації).

Таким чином, використання системи «Лоза-1» є надійним засобом для забезпечення комплексної безпеки в автоматизованій системі класу «1».

3.4.2 КСЗІ типового робочого місця АС-1 4-ої категорії на базі комплексу «Гриф»

Питання забезпечення безпеки інформації відіграють важливу роль у житті суспільства , а в деяких випадках і визначальну.

Автоматизована система (АС) являє собою організаційно-технічну систему, що об’єднує фізичне середовище, персонал і оброблювану інформацію. Вимоги до функціонального складу комплексної системи захисту залежать від характеристик оброблюваної інформації, фізичного середовища, персоналу і організаційної підсистеми. Вимоги до гарантій визначаються насамперед характером (важливістю) оброблюваної інформації і призначенням автоматизованих систем.

Для забезпечення інформаційної безпеки в автоматизованих системах застосовують комбіновані методи захисту: захист інформації від несанкціонованого доступу засобами перевірки повноважень користувачів та обслуговуючого персоналу на використання інформаційних ресурсів; ідентифікацію та автентифікацію сторін, що здійснюють обмін інформацією (підтвердження автентичності відправника та одержувача); розмежування прав користувачів і обслуговуючого персоналу при доступі до інформаційних ресурсів, а також при зберіганні та наданні інформації з обмеженим доступом; розподіл інформації за ступенями захищеності і за категоріями доступу, сертифікація технічних і програмних засобів та інші методи.

Надійним засобом забезпечення інформаційної безпеки в АС класу «1» є комплекс засобів захисту інформації від несанкціонованого доступу «Гриф» версії 3. Він призначений для забезпечення захисту інформації з обмеженим доступом (включаючи інформацію, що являє собою державну таємницю, службову інформацію, конфіденційну інформацію (персональні дані), інформацію, що становить комерційну таємницю, та інше) при її обробці в АС класу «1», що будуються на базі персональних електронних обчислювальних машин.

Таким чином, використання комплексу «Гриф» в АС класу «1» має наступні переваги: запобігання неконтрольованому і несанкціонованому ознайомленню, копіюванню та відновленню інформації; запобігання неконтрольованій та несанкціонованій модифікації та видаленню інформації; надання доступу до інформації тільки за умови достовірного розпізнавання користувачів і з урахуванням повноважень, наданих згідно службової необхідності; контроль дій користувачів і реєстрацію спроб порушення встановленого порядку доступу до інформації, включаючи блокування доступу до інформації в разі виявлення таких спроб, а також можливість здійснення контролю за доступом до інформації з боку уповноважених осіб.

Ці переваги обумовлюють широке та успішне застосування комплексу «Гриф» в АС класу «1».

3.4.3 КСЗІ типової локальної мережі АС класу 2 на базі Windows

Розгортання комплексної системи захисту інформації в інформаційно-телекомунікаційних системах (ІТС) вимагає значних витрат на проведення державних експертиз. При цьому багато ІТС мають схожі середовища функціонування та вимоги до захисту інформації. Це зумовлює необхідність в уніфікованих КСЗІ для типових ІТС.

У цій роботі розглядається процес створення КСЗІ для типової локальної мережі АС класу 2 на базі Windows Server 2012 згідно з вимогами існуючих нормативних документів.

Ці нормативні документи встановлюють порядок проведення робіт із створення КСЗІ в ІТС та вимоги із захисту службової інформації від несанкціонованого доступу (НСД) під час оброблення в АС класу 2, а також стандартні функціональні профілі захищеності оброблюваної інформації від НСД.

Створення КСЗІ було розпочато із обстеження середовищ функціонування досліджуваної АС.

При обстеженні обчислювальної системи були проаналізовані та описані загальна структурна схема і склад АС, види і характеристики каналів зв'язку, визначені особливості взаємодії окремих компонентів АС, їх взаємний вплив один на одного, описані існуючі засоби захисту АС та їх можливості.

При обстеженні інформаційного середовища було проаналізовано види інформації, що обробляється в АС, проведена її класифікація за режимом доступу, визначені види її представлення в ІТС та властивості захищеності, яким вони повинні задовольняти.

В ході аналізу технології обробки інформації визначено інформаційні потоки і середовища, через які вони передаються, джерела утворення потоків та місця їх призначення, складені структурні схеми потоків.

При обстеженні фізичного середовища було здійснено аналіз взаємного розміщення засобів обробки інформації ІТС на об'єктах інформаційної діяльності, комунікацій, систем життєзабезпечення та зв'язку, а також режим функціонування цих об'єктів.

За результатами обстеження середовищ функціонування ІТС виконано розробку політики безпеки інформації в ІТС. Визначені потенційні загрози для інформації та розроблені модель загроз та модель порушника. Сформовані вимоги, правила, обмеження, рекомендації, які регламентують використання

захищених технологій обробки інформації в ІТС, окремих заходів і засобів захисту інформації, діяльність користувачів всіх категорій.

Завершальним етапом роботи є розробка технічного завдання на створення КСЗІ.

Результатом роботи є комплект нормативних документів, необхідних при побудові КСЗІ для типової локальної мережі АС класу 2 на базі Windows Server 2012. Цей комплект може використовуватись як основа для побудови КСЗІ в реальних локальних мережах, значно знижуючи витрати на проведення державних експертиз.

3.4.4 КСЗІ типової локальної мережі АС класу 2 на базі «Лоза-2»

Розгортання комплексної системи захисту інформації в інформаційно-телекомунікаційних системах вимагає значних витрат на розробку документації та проведення державних експертиз. При цьому багато ІТС мають схожі середовища функціонування та вимоги до захисту інформації, що зумовлює необхідність в уніфікованих КСЗІ для типових ІТС.

У цій роботі розглядається процес створення КСЗІ для типової локальної мережі АС класу 2 (звичайно це локальна обчислювальна мережа) на базі програмного засобу захисту інформації від несанкціонованого доступу «Лоза-2».

Така КСЗІ повинна розроблятися згідно з вимогами існуючих нормативних документів. Ці документи встановлюють порядок проведення робіт із створення КСЗІ в ІТС та вимоги із захисту службової інформації від несанкціонованого доступу під час оброблення в АС класу 2, а також стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

Першим етапом авторами було проведено аналіз нормативно-правових актів, на підставі яких може встановлюватись обмеження доступу до певних

видів інформації. Було визначено наявність у складі інформації таких її видів, що потребують обмеження доступу або забезпечення цілісності чи доступності.

Наступний етап створення КСЗІ - це обстеження середовищ функціонування ІТС для підготовки засадничих даних для формування вимог до КСЗІ у вигляді опису кожного середовища функціонування ІТС. Були виявлені елементи середовищ функціонування, які безпосередньо чи опосередковано можуть впливати на безпеку інформації. Досліджено взаємний вплив елементів різних середовищ. Результати обстеження були задокументовані та включені до плану захисту інформації для використання на наступних етапах робіт.

За результатами обстеження середовищ функціонування ІТС виконано розробку політики безпеки інформації в ІТС. Визначені потенційні загрози для інформації та розроблені модель загроз та модель порушника. Побудову моделей здійснено відповідно до положень НД ТЗІ 1.1-002, НД ТЗІ 1.4-001 та НД ТЗІ 1.6-003, та оформлено у вигляді окремих документів плану захисту. Здійснено вибір основних рішень з протидії всім суттєвим загрозам. Сформовані вимоги, правила, обмеження та рекомендації, які регламентують використання захищених технологій обробки інформації в ІТС, окремих заходів і засобів захисту інформації, діяльність користувачів всіх категорій.

Завершальним етапом роботи є розробка технічного завдання на створення КСЗІ.

Результатом роботи є комплект нормативних документів, необхідних при побудові КСЗІ для типової локальної мережі АС класу 2 на базі «Лоза-2». Цей комплект може використовуватись як основа для побудови КСЗІ в реальних локальних мережах, значно знижуючи витрати на проведення державних експертиз.

3.5 Безпека систем Інтернету речей

Інтернет речей (Internet of Things, IoT) – динамічна глобальна мережна інфраструктура з можливістю самонастроювання на основі стандартних і сумісних протоколів зв'язку, де фізичні та віртуальні «речі» мають ідентифікатори, фізичні атрибути, використовують інтелектуальні інтерфейси та інтегруються в інформаційну мережу [70].

З логічної точки зору, система IoT може бути представлена як сукупність спільно взаємодіючих інтелектуальних пристроїв. З технічної точки зору, IoT може використовувати різні шляхи обробки даних, комунікації, технології та методології, ґрунтуючись на їх цільове призначення.

3.5.1 Інтернет речей: проблеми безпеки

Розглянемо три ключові вимоги безпеки з акцентом на системи Інтернету речей: автентифікація, конфіденційність, масштабованість.

Основними проблемами, що пов'язані з безпекою IoT, є наступні.

Високий рівень неоднорідності в поєднанні з широкою гамою систем IoT збільшило число загроз безпеки власників пристроїв, які все частіше використовуються для взаємодії людей, машин і речей в будь-який варіації.

Традиційні заходи забезпечення безпеки і дотримання конфіденційності не можуть бути застосовані до технологій IoT, зокрема, через їх обмежену обчислювальну потужність.

Велика кількість підключених пристроїв породжує проблему масштабованості. У той же час для досягнення визнання з боку користувачів необхідно в обов'язковому порядку забезпечити дотримання безпеки, конфіденційність і моделі довіри, які підходять для контексту IoT.

Довіра – це основна проблема, оскільки IoT-середовище характеризується різними типами пристроїв, які повинні обробляти дані відповідно до потреб і правами користувачів.

Крім цього, існують проблеми, пов’язані з контролем доступу в сценарії IoT.

Для вирішення ціх проблем в технології IoT використовується традиційні і нові підходи.

Для автентифікації передбачають використання налаштування користувачем механізму інкапсуляції, а саме протокол прикладного рівня для IoT під назвою – «інтелектуальна служба забезпечення безпеки». Він поєднує в собі крос-платформні зв’язку з шифруванням, підписом і автентифікації для підвищення ефективності розробки додатків IoT шляхом створення системи захищеного зв’язку між різними речами.

Підхід, який усуває проблему автентифікації зовнішніх потоків даних з використанням безперервної перевірки автентичності в потоках даних [71], тут передбачається наявність постачальника послуг, який збирає дані від одного або декількох власників разом з інформацією автентифікації і при цьому одночасно обробляє запити багатьох клієнтів. Постачальник послуг повертає клієнтам результати запитів, а також інформацію про перевірку, що дозволяє їм перевірити справжність і повноту отриманих результатів на основі інформації автентифікації, наданої власником даних.

Конфіденційність і цілісність в контексті IoT можна забезпечити за допомогою існуючих систем управління ключами. Це дозволяє класифікувати протоколи систем управління ключами [72] за чотирма основними категоріями: структура пулу ключів, математична база, механізм взаємодії і структура відкритого ключа.

Вимоги до обчислювальної потужності можна забезпечити за допомогою методу перевірки автентичності і контроль доступу, спрямованого на створення ключа сеансу із застосуванням еліптичної криптографії.

При вирішенні проблеми довіри потрібно звернути увагу також на аутсорсинг даних. Через велику кількість потокових даних компанії можуть не купувати ресурси, необхідні для розгортання систем управління потоками даних. Постає питання довіри: третя особа може діяти зловмисно, наприклад, з метою збільшення свого прибутку.

Рішення полягає в тому, що метод прийнятий так, для автентифікації потоку, що клієнти можуть перевіряти цілісність і актуальність отриманих від сервера даних. При цьому метод задовольняє вимогам IoT пристроїв, що характеризуються обмеженими ресурсами з точки зору енергоспоживання, обчислювальної потужності і захисту пристроїв.

Проведений аналіз безпеки інтернет речей показує, що поширення послуг IoT вимагає гарантування автентифікації, масштабованості, конфіденційності, сумісності та відповідності протоколам безпеки. Він проливає світло на напрямки досліджень в області поширення IoT.

3.5.2 Стартап Friends-Reminder в області Інтернет-речей

Сьогодні інтернет речей став популярним терміном для опису сценаріїв, у яких інтернет з’єднання і обчислювальна здатність поширюються на множину об’єктів, пристроїв, сенсорів і повсякденних об’єктів. Крім сенсорів, мережа може мати виконавчі пристрої, вбудовані у фізичні об’єкти і пов’язані між собою через дротові і бездротові мережі. Ці взаємопов’язані об’єкти (речі) мають можливість зчитування та приведення в дію, функцію програмування та ідентифікації, а також дозволяють виключити необхідність участі людини, за рахунок використання інтелектуальних інтерфейсів.

У сучасному світі, спілкування має дуже велике значення, і за допомогою сучасних інформаційних технології робити це стає дедалі простіше. З урахуванням того що сьогодні пристроєм комунікації може бути як стаціонарний пристрій, смартфон, так і смарт-годинник або браслет, то

розроблений авторами проект Friends Reminder допомагає спілкуватися ще більше та зручніше.

Ідея полягає в тому щоб група людей (друзів) заздалегідь домовившись про зустріч, змогли через Friends Reminder налаштувати синхронне нагадування. Воно буде заздалегідь (в залежності від налаштування) оповіщати про майбутню зустріч через записаний друзями звуковий сигнал, текстове повідомлення або короткий відеоролик.

Елементною базою для розробки апаратної складової Friends Reminder виступає Arduino kit, а саме: монтажна плата, сенсорний екран, бездротові передавачі, приймачі та ін.

Friends Reminder працює через мережу інтернет, і організований на хмарному сервері. Реєстрація проводиться через веб-сайт, там також створюються групи друзів (користувачів). Після реєстрації користувачі зможуть створювати свої групи і за допомогою групових політик, реалізованих на сервері, регулювати налаштування і комунікацію між членами кожної групи. Апаратно ідея такого комунікаційного пристрою може бути втілена у вигляді домашнього стаціонарного пристрою, мобільного інтернет-додатку на смартфонах або браслетах-годинниках.

3.6 Захист передачі конфіденційних повідомлень

3.6.1 Використання завадостійкого кодування для передачі конфіденційних повідомлень

В даний час засоби обчислювальної техніки та мережі зв’язку одержали настільки широке поширення, що відмовитися від їх використання виявляється абсолютно неможливо, хоча більше 80 % компаній несуть збитки через різні порушення цілісності даних. Тому проблема захисту інформації практично в усіх обчислювальних системах і системах зв’язку стала дуже актуальною.

Саме поняття захисту інформації є досить багатогранним. Воно включає в себе, принаймні, три аспекти: захист від отримання інформації противником, захист від зміни інформації та захист від руйнування інформації незаконним користувачем. В представленій роботі розглядаються деякі аспекти захисту від перехоплення інформації противником [73-74].

Робота засобів обчислювальної техніки і зв'язку супроводжується електромагнітними випромінюваннями і наведеннями на різні радіотехнічні ланцюги. Перехоплення сигналів наведень і випромінювань відкриває противнику доступ до інформації, що циркулює в інформаційно-обчислювальних мережах. Канали витоку інформації такого виду складають основу математичних моделей каналів з перехопленням, що досліджуються в даній роботі.

Для захисту інформації від витоку каналами наведень і електромагнітних випромінювань використовуються різні способи. Серед них повна ізоляція всіх технічних засобів від можливого перехоплення територіально і за допомогою спеціальних екранів і фільтрів, використання методів шифрування, використання зашумлення електромагнітних випромінювань спеціальними генераторами супроводжуючого шуму і т. п. Всі ці способи вимагають додаткових значних витрат різних ресурсів.

Однак є інший підхід до цієї проблеми, заснований на досягненнях сучасної теорії інформації і кодування [75], що дозволяє передавати конфіденційні повідомлення по відкритих каналах без небезпеки їх компрометації. В такому підході захист інформації забезпечується не за рахунок впливу на параметри каналів витоку, а за рахунок ймовірнісного перетворення інформації перед передачею по каналу зв'язку. Неможливість відновлення інформації противником заснована на тій властивості, що канал витоку має меншу пропускну здатність, ніж канал законного користувача. Спосіб кодування вибирається так, щоб в каналі витоку кількість виникаючих помилок сильно зростала, забезпечуючи ефект зашумлення переданого сигналу, в той час як в основному каналі забезпечувалася надійна зв'язок.

Розглянемо модель двійкового каналу з перехопленням. Передбачається, що основний канал, по якому передаються повідомлення від легального відправника до легального одержувачу, вільний від помилок, а канал перехоплювача є двійковим симетричним каналом з перехідною ймовірністю помилки.

Показано, що випадкове кодування переданого повідомлення змінює канал. Легальний користувач отримуємо синдром послідовності з деякого суміжного класу розкладання векторного простору за використовуваним кодом. Приймач-перехоплювач також отримує цей синдром плюс синдром вектора помилки двійкового симетричного каналу. Високий рівень захисту від перехоплення досягається, якщо синдроми, одержувані від помилкових векторів каналу мають близький до рівномірного розподіл.

3.6.2 Удосконалення безпеки персональних даних при їх передачі інтерфейсом NFC

В даний час все більш широко застосовується Near Field Communication (NFC) – технологія бездротового високочастотного зв’язку малого радіусу дії, яка дає можливість обміну даними між пристроями, що знаходяться на відстані близько 15 сантиметрів [76]. На відміну від такої технології, як Bluetooth, вона дозволяє швидше обмінюватися маленькими обсягами інформації та підтримує пасивні пристрої (мітки, карти), дешевше в реалізації - що істотно збільшує область застосування.

NFC широко застосовується в бездротових смарт-картах і бездротових мітках. Область активно розширюється за рахунок емуляції смарт-карт, або міток в пристроях: телефон, планшет, бездротова платіжна картка, бездротова картка для контролю доступу, універсальні картки, пасивні мітки, імплантовані мітки, зчитувачі, тощо.

Аналіз показав, що NFC працює в 2 режимах передачі даних: пасивний - коли одне з них не створює свого поля, а тільки відповідає на поле іншого

пристрою і активний - коли обидва взаємодіючих пристрої створюють свої поля. Найбільш універсальні в цій частині телефони та планшети з підтримкою NFC - вони можуть виступати як пасивні NFC пристрої, як зчитувачі для пасивних пристроїв, а також брати участь в активній взаємодії двох пристроїв.

Дана технологія застосовується в наступних напрямках: контроль доступу в приміщення, на територію (великі об’єкти - заводи, готелі, аквапарки, публічні заходи - концерти, виставки, саміти в тому числі заходи щодо інформаційної безпеки, гірськолижні курорти, олімпіади та інші спортивні заходи), банківські платежі, мобільні платежі, оплата транспорту (транспортні карти, електронні квитки), оплата товарів, відстеження переміщення товарів, посвідчення особи, отримання інформації.

Аналіз показав, що з точки зору інформаційної безпеки основні слабкості і недоліки NFC пов’язані з тим, що стек протоколів NFC не передбачає криптографії при передачі. Стандарти зберігання даних в мітках і картах, а також їх емуляції - не передбачають криптографічного захисту при зберіганні. У реалізаціях багатьох карт, смарт-карт і їх емуляції застосовуються слабкі криптографічні алгоритми.

Крім того, в NFC сервісах традиційно закладається надмірна довіра до інформації, що зберігається на картках і мітках, в результаті фактично не виконується фільтрація даних. Для сучасних NFC смартфонів можна легко створити емуляцію карти і записати туди довільні дані.

В результаті дослідження засобів атак, слід виділити наступні способи порушення безпеки протоколу: прослуховування інформації при передачі по NFC; несанкціоноване (приховане / не помітне для користувача) зчитування інформації з NFC пристроїв; lockAttack (переклад імітованої картки / мітки в режим тільки читання і блокування запису інформації зчитувачем); timeAttack (в разі якщо термін дії картки або послуг прописаний на самій картці, можна поміняти цю дату); класичні атаки на серверну та інфраструктурну частину NFC сервісів.

Найбільш небезпековою для користувача є replyAttack (перехоплення інформації і багаторазове її повторення або застосування - дозволяє отримувати послуги, товари, отримувати доступ від імені іншої особи), яка схожа з наведеної вище атака клонування NFC пристроїв Relayattack. В цієї атаці зловмисник використовує 2 NFC пристрої, одне з яких зчитує дані з пристрою жертви, передає дані на друге, а другий пристрій видає отримані дані зчитувача і отримуємо послугу від імені жертви.

Для забезпечення безпеки NFC пропонується побудувати стек протоколів, в якому на потрібний рівень будуть вбудовані криптографічні протоколи, що забезпечать обмін ключами і шифрування трафіку при передачі по інтерфейсу NFC.

3.6.3 Реалізація захищеного мережного сервісу обміну повідомленнями

Сучасні технології та програмне забезпечення розвиваються дуже стрімко, як у сфері захисту інформації, так і в сфері тестування вразливостей. Другі можуть використовуватися зловмисниками в своїх корисливих цілях. Як наслідок, інформація, що представляє певну цінність, яка циркулює в засобах обчислювальної техніки підлягає захисту. Одним із засобів захисту є захист програмного забезпечення, що приймає участь в обробці та зберіганні цінної інформації.

В даному випадку йдеться про конфіденційні переговори за допомогою мережного додатку для обміну текстовими повідомленнями. У програмах подібного типу для відправки і прийому повідомлень використовується протокол TCP [77].

Однак даний протокол не передбачає засобів захисту, а є лише способом передачі. Для забезпечення безпеки переданих пакетів з даними, пропонується використовувати програмний додаток, який додатково шифруватиме повідомлення.

Шифрування даних є найбільш ефективним способом захисту інформації. Так як в протоколі TCP відсутнє шифрування даних, що передаються, то виникає необхідність запровадити шифрування на етапі формування TCP пакетів.

Запропонований програмний додаток працює без виділеного сервера для приватних (не систематичних) переговорів, з шифруванням переданих даних. Шифрування даних проводиться алгоритмом AES256.

Advanced Encryption Standard (AES), також відомий як Rijndael — симетричний алгоритм блочного шифрування (розмір блоку 128 біт, ключ 128/192/256 біт), прийнятий в якості стандарту шифрування урядом США. Станом на 2017 рік AES є одним з найпоширеніших алгоритмів симетричного шифрування. При використанні 128-бітного ключа для злому шифрування, за заявою уряду США, буде потрібно 149 трильйонів років. Підтримка AES (і тільки його) запроваджена фірмою Intel в сім'ї процесорів x86 починаючи з Intel Core i7-980X Extreme Edition, а потім на процесорах Sandy Bridge.

ВИСНОВКИ

Запропоновано та отримано патент на спосіб захисту інформації у волоконно-оптичних лініях зв’язку від несанкціонованого доступу з поліпшеними характеристиками, тобто з підвищеною захищеністю, надійністю та з покращеною якістю інформаційного сигналу на приймальній стороні.

Побудовано та впроваджено комплексні системи захисту інформації, в яких використано комплекси засобів захисту від несанкціонованого доступу «Гриф», «Лоза-1» та «ЛОЗА-2».

Запропоновано протокол колективного цифрового підпису на основі EC-GDSA для забезпечення безпечної автентифікації загального медичного висновку при проведенні консиліуму лікарів.

Побудована модифікація алгоритму заперечуваного шифрування Менга, яка забезпечує надійний захист інформації від атак на основі примусу.

Для безпеки Інтернету речей розроблений проект Friends Reminder, якій допомагає спілкуватися більше зручніше та безпечніше.

Запропоновано криптографічний протокол захисту інформації в радіоканалах безпілотних літальних апаратів. Для цього розроблений комбінований алгоритм генерації загального сеансного ключа і поточного шифрування, який поєднує в собі переваги симетричних і асиметричних криптосистем.

Наведено вимоги щодо криптосистем з метою захищення від клептоатак.

Побудовані моделі протоколів квантової криптографії на платформі CUDA.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Лех В.О. Аналіз національної стратегії кіберзахисту України / Лех В.О., Нікуліщев Г.І. // Тиждень науки: щорічна наук.-практ. конф. викладачів, науковців, молодих учених і аспірантів, 18-22 квітня 2016 р.: збірник тез доповідей в 5 томах. – Запоріжжя, 2016. – Т.1. – С. 328.

2. Касьяненко Є.М. Особливості розробки політики безпеки в державних установах України / Касьяненко Є.М., Воскобойник В.О. // Тиждень науки: щорічна наук.-практ. конф. викладачів, науковців, молодих учених і аспірантів, 18-22 квітня 2016 р.: збірник тез доповідей в 5 томах. – Запоріжжя, 2016. – Т.1. – С. 325-326.

3. Чуницька, В.В. Аналіз Закону «Про основні засади забезпечення кібербезпеки України» [Текст] / В.В. Чуницька, Є.В. Гайтота, Г.І. Нікуліщев // Кібербезпека та системи захисту інформації: виклики сьогодення: науковий круглий стол, 26 жовтня 2017 р. : збірник матеріалів. – Маріуполь.: МДУ, 2017. – С.30-33.

4. Шкарупа І.В. Огляд ефективних заходів протидії кіберзагрозам / Шкарупа І.В., Нікуліщев Г.І. // Використання сучасних інформаційних технологій в діяльності Національної поліції України: всеукр. наук.-практ. семінар, 24 листопада 2017 р.: тези доп. – Дніпро, 2017. – С.189-191.

5. Воскобойник В. А. Один из подходов обеспечения устойчивости и стабильности функционирования технических средств передачи-приема информации / Воскобойник В. А. // Системи управління, навігації та зв’язку. – 2015. – Випуск 1 (33). – С.70-73.

6. Лізунов, С.І. Дослідження захищеності закритих Wi-Fi мереж / Лізунов С.І., Вовкостріл А.І. // Використання сучасних інформаційних технологій в діяльності Національної поліції України: всеукр. наук.-практ. семінар, 24 листопада 2017 р.: тези доп. – Дніпро, 2017. – С.64-66.

7. Верещака М.П. Тестирование Wi-FI сетей с помощью KALI LINUX [Електронний ресурс] / Верещака М.П., Лизунов С.И. // Тиждень науки: щоріч. наук.- практ. конф., 18-21 квітня 2017 р.: тези доп. / Редкол.: В.В. Наумик (відпов. ред.) Електрон. дані.- Запоріжжя : ЗНТУ, 2017. - С. 598-599 - 1 електрон. опт. диск (DVD-ROM). - назва з тит. екрана.

8. Лізунов, С.І. Аналіз брандмауерів на захищеність / Лізунов С.І., Верещака М.П. // Використання сучасних інформаційних технологій в діяльності Національної поліції України: всеукр. наук.-практ. семінар, 24 листопада 2017 р.: тези доп. – Дніпро, 2017. – С.66-67.

9. Лізунов, С.І. Сучасні радіозакладні пристрої / Лізунов С.І., Абраменко Л.О. // Використання сучасних інформаційних технологій в

діяльності Національної поліції України: всеукр. наук.-практ. семінар, 24 листопада 2017 р.: тези доп. – Дніпро, 2017. – С.59-61.

10. Лізунов, С.І. Прихований майнінг та захист від нього / Лізунов С.І., Верещака М.П. // Тиждень науки: щорічна наук.-практ. конф. викладачів, науковців, молодих учених і аспірантів, 16-20 квітня 2018 р.: тези доповідей. – Запоріжжя, 2018.

11. Войтіх М.І. Приховане під'єднання до оптоволоконної лінії зв'язку [Електронний ресурс] / Войтіх М.І., Грицев.В.І., Куцак С.В. // Тиждень науки: щоріч. наук.- практ. конф., 18-21 квітня 2017 р.: тези доп. / Редкол.: В.В. Наумик (відпов. ред.) Електрон. дані.- Запоріжжя : ЗНТУ, 2017. - С.612-613 - 1 електрон. опт. диск (DVD-ROM). - назва з тит. екрана.

12. Пшеничний П.В. Аналіз факторів, що впливають на захищеність мовної інформації в розподілених інформаційних системах [Електронний ресурс] / Пшеничний П.В., Куцак С.В. // Тиждень науки: щоріч. наук.- практ. конф., 18-21 квітня 2017 р.: тези доп. / Редкол.: В.В. Наумик (відпов. ред.) Електрон. дані.- Запоріжжя : ЗНТУ, 2017. - С.628-629 - 1 електрон. опт. диск (DVD-ROM). - назва з тит. екрана.

13. Пшеничний П.В. Порівняльний аналіз методів оцінки захищеності мовної інформації / Пшеничний П.В., Куцак С.В. // Тиждень науки: щорічна наук.-практ. конф. викладачів, науковців, молодих учених і аспірантів, 16-20 квітня 2018 р.: тези доповідей. – Запоріжжя, 2018.

14. Кузьменко А.В. Використання технологій штучних нейронних та капсульних мереж у системах захисту інформації / Кузьменко А.В., Матвейчук О.В., Корольков Р.Ю. // Використання сучасних інформаційних технологій в діяльності Національної поліції України: всеукр. наук.-практ. семінар, 24 листопада 2017 р.: тези доп. – Дніпро, 2017. – С.128-129.

15. Морозовський І.В. Аналіз алгоритму розпізнавання обличь Eigenface і його реалізація в середовищі MATLAB [Електронний ресурс] / Морозовський І.В., Корольков Р.Ю. // Тиждень науки: щоріч. наук.- практ. конф., 18-21 квітня 2017 р.: тези доп. / Редкол.: В.В. Наумик (відпов. ред.) Електрон. дані.- Запоріжжя : ЗНТУ, 2017. - С.614-615 - 1 електрон. опт. диск (DVD-ROM). - назва з тит. екрана.

16. Неласа, Г.В. Особливості використання схем цифрового підпису / Неласа Г.В., Козіна Г.Л. // Кібербезпека в системі національної безпеки України: пріоритетні напрямки розвитку: науковий круглий стіл, 26 квітня 2018 р.: збірник матер. – Маріуполь, 2018. – С. 43-45.

17. Неласа, Г.В. Про реалізацію різних схем цифрового підпису / Неласа Г.В., Козіна Г.Л. // Тиждень науки: щорічна наук.-практ. конф. викладачів, науковців, молодих учених і аспірантів, 16-20 квітня 2018 р.: тези доповідей. – Запоріжжя, 2018.

18. Козина Г.Л. Схемы цифровой подписи разного назначения / Козина Г.Л., А.В. Неласая, Н.А. Молдовян / Математическое моделирование, оптимизацияи информационные технологи. 5-я Международная конференція. Кишинев, 22-25 марта 2016 г.: Материалы конференции/ Evrica – Chisinau, 2016. – С. 209-214.

19. Нікуліщев Г.І. Підхід до формування схем сліпого підпису / Нікуліщев Г.І., Козіна Г.Л. // Тиждень науки: щорічна наук.-практ. конф. викладачів, науковців, молодих учених і аспірантів, 18-22 квітня 2016 р.: збірник тез доповідей в 5 томах. – Запоріжжя, 2016. – Т.1. – С. 336-337.

20. Семеренко Т.Ю. Протоколы групповой подписи / Семеренко Т.Ю., Козина Г.Л. // Тиждень науки: щорічна наук.-практ. конф. викладачів, науковців, молодих учених і аспірантів, 18-22 квітня 2016 р.: збірник тез доповідей в 5 томах. – Запоріжжя, 2016. – Т.1. – С. 319-320.

21. Неласа, Г. Протокол колективного цифрового підпису на основі EC-GDSA для використання в телемедицині [Текст] / Г Неласа, Р. Шовгенюк, О. Королькова // Перспективні напрямки сучасної електроніки, інформаційних і комп'ютерних систем (MEICS-2017): II всеукр. наук.-практ. конф., 22–24 листопада 2017 р.: тези доп. – Дніпро, 2017. – С.123-124.

22. Лех, В.О. Клептографічна атака на алгоритм цифрового підпису ECDSA [Електронний ресурс] / Лех В.О., Козіна Г.Л. // Тиждень науки: щоріч. наук.- практ. конф., 18-21 квітня 2017 р.: тези доп. / Редкол.: В.В. Наумик (відпов. ред.) Електрон. дані.- Запоріжжя : ЗНТУ, 2017. - С.595-596 - 1 електрон. опт. диск (DVD-ROM). - назва з тит. екрана.

23. Лех В.О. Захист від клептографічних атак на криптосистеми / Лех В.О., Козіна Г.Л. // Майбутній науковець-2017: VIII всеукр. наук.-практ. конф., 1 грудня 2017 р.: тези доп. – Сєвєродонецьк, 2017. – С. 180.

24. Козіна Г.Л. Дослідження властивостей алгоритмів заперечуваного шифрування / Козіна Г.Л., Гальченко А.В. // Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій: VIII Міжн. наук.-практ. конф., 21-23 вересня 2016 р. : тези доповідей.– Запоріжжя, 2016. – С.238-240.

25. Гальченко А.В. Модифікація алгоритму заперечуваного шифрування Менга / Гальченко А.В., Козіна Г.Л. // Радіоелектроніка. Інформатика. Управління. – 2016. – №2. – С.77-86.

26. Неласа Г.В. Розпаралелювання та порівняльний аналіз методів дискретного логарифмування на GPGPU / Неласа Г.В., Верещак М.І. // Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій: VIII Міжн. наук.-практ. конф., 21-23 вересня 2016 р. : тези доповідей.– Запоріжжя, 2016. – С.240-241.

27. Неласа, Г.В. Використання паралельних обчислень при реалізації криптографічних алгоритмів [Текст] / Неласа Г.В. Верещак М.І. // Кібербезпека та системи захисту інформації: виклики сьогодення: науковий круглий стол, 26 жовтня 2017 р. : збірник матеріалів. – Маріуполь.: МДУ, 2017. – С.9-10

28. Неласа Г.В. Розробка паралельних моделей протоколів квантової криптографії під технологію GPGPU / Неласа Г.В., Сидоренко Т.С. // Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій: VIII Міжн. наук.-практ. конф., 21-23 вересня 2016 р. : тези доповідей.– Запоріжжя, 2016. – С.242-243.

29. Неласая А.В. Моделирование квантового алгоритма Шора факторизации натуральных чисел / Неласая А.В., Сидоренко Т.С. // Актуальні задачі та досягнення у галузі кібербезпеки: Всеукраїнська науково-практична конференція студентів і молодих вчених, 23-25 листопада 2016 р.: матеріали конф. – Кропивницький, 2016. – С.145.

30. Абраменко Л.О. Моделювання квантового алгоритму Шора для факторизації натуральних чисел / Абраменко Л.О., Неласа Г.В. // Комп'ютерні технології: теорія і практика: міжвуз. інтернет-конф. молодих вчених, 12 грудня 2017 р.: тезі доп. – Харків, 2017. – Режим доступу: http://pmit.kname.edu.ua/index.php/main/internet-conference

31. Литовка, Т.В. Порівняльний аналіз протоколів квантового розподілення ключів / Литовка Т.В., Неласа Г.В. // Тиждень науки: щорічна наук.-практ. конф. викладачів, науковців, молодих учених і аспірантів, 16-20 квітня 2018 р.: тези доповідей. – Запоріжжя, 2018.

32. Сидоренко Т.С. Моделювання протоколів квантової криптографії на платформі CUDA / Сидоренко Т.С., Неласа Г.В. // Тиждень науки: щорічна наук.-практ. конф. викладачів, науковців, молодих учених і аспірантів, 18-22 квітня 2016 р.: збірник тез доповідей в 5 томах. – Запоріжжя, 2016. – Т.1. – С. 321.

33. Пат. 123836 Україна, МПК H04K 1/10 (2006.01), H04B 10/25 (2013.01). Спосіб захисту інформаціїу волоконно-оптичних лініях зв'язку від несанкціонованого доступу / О.В. Щекотихін, Л.М. Карпуков, Д.К. Савченко, Т.В. Литовка. – № u2017 09443, заявл. 29.09.2017, опубл. 12.03.2018, Бюл.№ 5, 2018 р. – 4 с.

34. Щекотихин О.В. Пассивные оптические сети доступа: монографія / Щекотихин О.В., Сметанин И.В., Піза Д.М. – Запоріжжя: ЗНТУ, 2016. – 276 с.

35. Карпуков Л.М. Защита информации в ВОСПИ / Карпуков Л.М., Щекотихин О.В., Савченко Д.К. // Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій: VIII Міжн. наук.-практ. конф., 21-23 вересня 2016 р. : тези доповідей.– Запоріжжя, 2016. – С.236-238.

36. Михалко, В.В. Методы съема информации в оптоволоконных линиях связи / Михалко В.В., Щекотихин О.В. // Тиждень науки: щорічна наук.-практ. конф. викладачів, науковців, молодих учених і аспірантів, 16-20 квітня 2018 р.: тези доповідей. – Запоріжжя, 2018.

37. Литовка Т.В. Вдосконалений спосіб маскування лінійного коду в ВОЛЗ / Литовка Т.В., Савченко Д.К., Щекотихін О.В. // Майбутній науковець-2017: VIII всеукр. наук.-практ. конф., 1 грудня 2017 р.: тези доп. – Сєвєродонецьк, 2017. – С. 329 – 331.

38. Романенко С.М. Поля і хвилі в задачах технічного захисту інформації : навч. посібник / Романенко С.М., Дмитренко В.П., Карпуков Л.М. – Запоріжжя: ЗНТУ, 2016. – 282 с.

39. Тверденко А.В. Моделювання взаємодії плоскої хвилі зі шаром метаматеріалу / Тверденко А.В., Романенко С.М. // Майбутній науковець-2017: VIII всеукр. наук.-практ. конф., 1 грудня 2017 р.: тези доп. – Сєвєродонецьк, 2017. – С. 247 – 250.

40. Романенко С.Н. Шлейфне ответвители на комбинациях МПЛ и ЩЛ / Романенко С.Н., Дмитренко В.П., Тверденко А.В. // Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій: VIII Міжн. наук.-практ. конф., 21-23 вересня 2016 р. : тези доповідей.– Запоріжжя, 2016. – С.63-66.

41. Романенко, С.Н. Широкополосная антенна для приема беспроводной энергии / Романенко С.Н., Тверденко А.В. // Тиждень науки: щорічна наук.-практ. конф. викладачів, науковців, молодих учених і аспірантів, 16-20 квітня 2018 р.: тези доповідей. – Запоріжжя, 2018.

42. Карпуков Л.М. Захист інформації в радіоканалах БПЛА / Л.М. Карпуков, С.І. Лізунов // Використання сучасних інформаційних технологій в діяльності Національної поліції України: Всеукр. науково-практ. семінар, 25 листопада 2016 р.: матеріали семінару – Дніпро, 2016. – С.17-22.

43. Панкова Т.Б. Криптографический протокол защиты информации в радиоканалах БПЛА / Панкова Т.Б., Лизунов С.И. // Тиждень науки: щорічна наук.-практ. конф. викладачів, науковців, молодих учених і аспірантів, 18-22 квітня 2016 р.: збірник тез доповідей в 5 томах. – Запоріжжя, 2016. – Т.1. – С. 312-314.

44. Ігнатенко К.В. Комплексна СЗІ типового робочого місця АС-1 4-ої категорії на базі системи «Лоза-1» [Електронний ресурс] / Ігнатенко К.В., Лізунов С.І., Лапутько А.В. // Тиждень науки: щоріч. наук.- практ. конф., 18-21 квітня 2017 р.: тези доп. / Редкол.: В.В. Наумик (відпов. ред.) Електрон. дані.- Запоріжжя : ЗНТУ, 2017. - С.630-631 - 1 електрон. опт. диск (DVD-ROM). - назва з тит. екрана.

45. Таган Д.А. Комплексна СЗІ типового робочого місця АС-1 4-ої категорії на базі комплексу «Гриф» [Електронний ресурс] / Таган Д.А., Лізунов С.І., Лапутько А.В. // Тиждень науки: щоріч. наук.- практ. конф., 18-21 квітня 2017 р.: тези доп. / Редкол.: В.В. Наумик (відпов. ред.) Електрон. дані.- Запоріжжя : ЗНТУ, 2017. - С.631-632 - 1 електрон. опт. диск (DVD-ROM). - назва з тит. екрана.

46. Гужва А.А. КСЗІ типової локальної мережі АС класу 2 на базі Windows [Електронний ресурс] / Гужва А.А., Лізунов С.І., Лапутько А.В. // Тиждень науки: щоріч. наук.- практ. конф., 18-21 квітня 2017 р.: тези доп. / Редкол.: В.В. Наумик (відпов. ред.) Електрон. дані.- Запоріжжя : ЗНТУ, 2017. - С.632-633 - 1 електрон. опт. диск (DVD-ROM). - назва з тит. екрана.

47. Першин Є.О. КСЗІ типової локальної мережі АС класу 2 на базі «ЛОЗА-2» [Електронний ресурс] / Першин Є.О., Лізунов С.І., Лапутько А.В. // Тиждень науки: щоріч. наук.- практ. конф., 18-21 квітня 2017 р.: тези доп. / Редкол.: В.В. Наумик (відпов. ред.) Електрон. дані.- Запоріжжя : ЗНТУ, 2017. - С.634-635 - 1 електрон. опт. диск (DVD-ROM). - назва з тит. екрана.

48. Безрук Є.А. Інтернет речей: проблеми безпеки / Безрук Є.А., Брусенський В.Р., Куцак С.В. // Використання сучасних інформаційних технологій в діяльності Національної поліції України: всеукр. наук.-практ. семінар, 24 листопада 2017 р.: тези доп. – Дніпро, 2017. – С.95-97

49. Дьяченко А.В. Стартап Friends-Reminder в області Інтернет-речей [Електронний ресурс] / Дьяченко А.В., Неласа Г.В. // Тиждень науки: щоріч. наук.- практ. конф., 18-21 квітня 2017 р.: тези доп. / Редкол.: В.В. Наумик (відпов. ред.) Електрон. дані.- Запоріжжя : ЗНТУ, 2017. - С.602 - 1 електрон. опт. диск (DVD-ROM). - назва з тит. екрана.

50. Корольков Р.Ю. Використання завадостійкого кодування для передачі конфіденційних повідомлень [Електронний ресурс] / Корольков Р.Ю., Куцак С.В., Логачова Л.М. // Тиждень науки: щоріч. наук.- практ. конф., 18-21 квітня 2017 р.: тези доп. / Редкол.: В.В. Наумик (відпов. ред.) Електрон. дані.- Запоріжжя : ЗНТУ, 2017. - С.626-627 - 1 електрон. опт. диск (DVD-ROM). - назва з тит. екрана.

51. Брусенський, В.Р. Удосконалення безпеки персональних даних при їх передачі інтерфейсом NFC / Брусенський В.Р., Воскобойник В.О. // Тиждень науки: щорічна наук.-практ. конф. викладачів, науковців, молодих учених і аспірантів, 16-20 квітня 2018 р.: тези доповідей. – Запоріжжя, 2018.

52. Данілов А.І. Реалізація захищеного мережного сервісу обміну повідомленнями [Електронний ресурс] / Данілов А.І., Куцак С.В. // Тиждень науки: щоріч. наук.- практ. конф., 18-21 квітня 2017 р.: тези доп. / Редкол.: В.В. Наумик (відпов. ред.) Електрон. дані.- Запоріжжя : ЗНТУ, 2017. - С.608-610 - 1 електрон. опт. диск (DVD-ROM). - назва з тит. екрана.

53. Стратегія кібербезпеки України: Указ Президента України № 96/2016 від 15.03.2016 р. [Електронний ресурс]. - Режим доступу: http://zakon3.rada.gov.ua/laws/show/96/2016.

54. Поняття та зміст кіберзагроз на сучасному етапі [Електронний ресурс]. - Режим доступу: http://goal-int.org/ponyattya-ta-zmist-kiberzagroz-na-suchasnomu-etapi/

55. Скрытый майнинг: найти и уничтожить [Електронний ресурс]. – Режим доступу: https://bitnovosti.com/2017/08/16/skritiy-mayning-nayti-unichtojit/.

56. Как обезопасить себя от скрытого майнинга криптовалют [Електронний ресурс]. – Режим доступу: https://tjournal.ru/59579-kak-obezopasit-sebya-ot-skrytogo-mayninga-kriptovalyut.

57. Щекотихін О.В. Компоненти та пристрої волоконно-оптичних ліній зв'язку [Текст]: навчальний посібник / О.В. Щекотихін, Д.М. Піза, Т.І. Бугрова. – Запоріжжя: ЗНТУ, 2012. – 308 с.

58. Місюра С.М. Варіант захисту мовної інформації на об'єктах інформаційної діяльності [Текст] / С.М. Місюра, В.В. Овсянніков, І.Р. Мальцева // Збірник наукових праць ВІТІ НТУУ „КПІ".– 2011.– №2. – С. 84-93.

59. Федоренко Р.М. Контент-моніторинг інформаційного простору як чинник забезпечення інформаційної безпеки держави у воєнній сфері [Текст] / Р.М.Федоренко // Сучасний захист інформації. – 2015. – №2. – С. 21-25.

60. Кеньо Г. В. Акустична захищеність виділених приміщень у світлі статистичної та хвильової теорій / Г. В. Кеньо, В. В. Хома // Вісник НУ "Львівська політехніка". – 2011. – № 695. – С. 22–29.

61. Ефимов А.П. Три взгляда на акустику помещений [Електронний ресурс]: – Режим доступу: http://www.acoustic.ua/.

62. КозінаГ.Л. Криптопротоколи: схеми цифрового підпису : навч. посіб. / Г.Л. Козіна, М. А. Молдов'ян, Г. В. Неласа. –Запоріжжя : ЗНТУ, 2014. – 158 с.

63. Young A. Kleptography: Using Cryptography against Cryptography/ Young A., Yung M. // Advances in Cryptology – EUROCRYPT '97 Proceedings, Springer-Verlag, 1997. – pp. 62–74.

64. Wang J. A Receiver Deniable Encryption Scheme / J. Wang, Bo Meng // Proceedings of the 2009 International Symposium on Information Processing (ISIP'09), 21–23 August 2009: proceedings. – Huangshan : P. R. China, 2009. – pp. 254–257.

65. IBM открыла доступ к своему облачному квантовому комп'ютеру [Електроний ресурс]: / Ольга Карпенко / Новини від 05.05.2016– Назва з титул. екрану, Режим доступу: http://ain.ua/2016/05/05/646763

66. Востоков Н.А. Квантовая криптография / Востоков Н., Борисова С.Н. // Успехи современного естествознания. – 2012. – № 6. – С. 88-90,

[Електронний ресурс]: – Режим доступу: https://www.natural-sciences.ru/ru/article/view?id=30414

67. Яковлєв А. В. Волоконно-оптичні системи передачі конфіденційної інформації / Яковлєв А. В. // Електрозв'язок. – 2016. – №10.– С 11-13.

68. Манько О. Використання пасивних оптичних пристроїв для захисту інформації у волоконно-оптичних лініях зв'язку та мережах [Текст] / Манько О., Шматок О., Петренко А. // Захист інформації. – 2017. – Том 19, №2. – С. 143-147.

69. Романенко С.Н. Поверхностные волны на границах раздела метасред. Моделирование эффектов сверхразрешения [Текст] / С.Н. Романенко, Л.М. Карпуков, В.А. Борисенко, А.С. Львов // Радіоелектроніка. Інформатика. Управління. – 2011. – №2. – С. 7-13.

70. Internet of Things Global Standards Initiative [Електронний ресурс]: – Режим доступу: http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx.

71. Paradopulus S. Continuous authentication on relational data streams / S. Paradopulus, Y. Yang, D. Papadias // VLDB Journal. – 2010. – Vol. 19.– №1 – pp.161-180.

72. Understanding KMS [Електронний ресурс]: – Режим доступу: https://technet.microsoft.com/ru-ru/library/ff793434.aspx.

73. Юдін О.К. Кодування в інформаційно-комунікаційних мережах [Текст]: Монографія / О.К. Юдін. – К.: Книжкове видавництво НАУ, 2007. – 302 с.

74. Майданюк В.П. Кодування та захист інформації [Текст]: навчальний посібник / В.П. Майданюк. – Вінниця: ВНТУ, 2009. – 164 с.

75. Жураковський Ю.П. Теорія інформації та кодування [Текст]: Підручник / Ю.П. Жураковський, В.П. Полторак. – К.: Вища школа, 2001. – 255 с.

76. NFC controller PN544 for mobile phone sand portable equipment [Електронний ресурс]. – Режим доступу: http://www.nxp.com/documents/leaflet /75016890.pdf.

77. Буров Є. В. Комп'ютерні мережі [Текст] : підручник / Є. В. Буров. – Львів: Магнолія, 2013. – 262 с.