Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Електронної та біомедичної інженерії
(повна назва)

Кафедра Фізичних основ електронної техніки
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти другий (магістерський)
СТВОРЕННЯ ВІРТУАЛЬНОГО СТЕНДУ КВАНТОВОЇ КРИПТОГРАФІЇ ДЛЯ ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНИХ ТЕХНОЛОГІЙ
(тема)

Виконав:
студент 2 курсу, групи ФТОІм-22-1
Куценко В.І.
(прізвище, ініціали)

Спеціальність 152 Метрологія та інформаційно-вимірювальна техніка
(код і повна назва спеціальності)
Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)
Освітня програма «Фотоніка та оптоінформатика»

(повна назва освітньої програми)

Керівник зав. каф. ФОЕТ Гнатенко О.С.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ Гнатенко О.С.
(підпис) (прізвище, ініціали)

2024 р.

Харківський національний університет радіоелектроніки

Факультет Електронної та біомедичної інженерії
(повна назва)
Кафедра Фізичних основ електронної техніки
(повна назва)
Рівень вищої освіти перший (бакалаврський)
Спеціальність 152 Метрологія та інформаційно-вимірювальна техніка
(код і повна назва)
Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)
Освітня програма «Фотоніка та оптоінформатика»
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«____»_____ 20 ___ р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентові Куценку Владиславу Ігоровичу
(прізвище, ім'я, по батькові)

1. Тема роботи Створення віртуального стенду квантової криптографії для інформаційно-вимірювальних технологій
затверджена наказом університету від « 03 » листопада 2023 р. № 1285 Стз
2. Термін подання студентом роботи до екзаменаційної комісії 23 січня 2024 р.
3. Вихідні дані до роботи фізичні основи квантової криптографії; демонстраційний комплекс EDU-QCRY1; алгоритм квантової криптографії.

4. Перелік питань, що потрібно опрацювати в роботі:
1 Дослідити принципи роботи та конструкцію демонстраційого комплексу EDU-QCRY1 EDU-QCRY1/M.
2 Спроектувати віртуальний стенд квантової криптографії для інформаційно-вимірювальних технологій.
3 Розробити WEB-додаток, емулюючий роботу демонстраційого комплексу EDU-QCRY1

5. Перелік графічного матеріалу із зазначенням кресленików, схем, плакатів, комп'ютерних ілюстрацій
Демонстраційний матеріал – 15 шт.
Код програми – 7 арк.

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	Інформаційно-тематичний пошук та огляд літературних джерел про демонстраційний комплекс EDU-QCRY1	01.09.23–30.09.23	Виконано
2	Дослідження конструкції, можливостей та прикладів використання демонстраційного комплексу	01.10.23–20.10.23	Виконано
3	Вибір технологій, розбір алгоритму, створення архітектури для розробки застосунку	21.10.23–04.11.23	Виконано
4	Розробка інтерфейсу та розрахункової логики застосунку	05.11.23–11.12.23	Виконано
5	Оформлення пояснювальної записки	12.12.23–04.01.24	Виконано
6	Оформлення графічних та демонстраційних матеріалів	10.01.24–12.01.24	Виконано
7	Проходження нормоконтролю і отримання рецензії	13.01.24–15.01.24	Виконано
8	Проходження перевірки на плагіат	20.01.24–21.01.24	Виконано
9	Підготовка та захист кваліфікаційної роботи	22.01.24–24.01.24	

Дата видачі завдання 01 вересня 2023 р.

Студент _____
(підпис)

Керівник роботи _____ зав. каф. ФОЕТ Гнатенко О.С.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 33 с., 7 рис., 3 табл., 2 додатки, 14 джерел.

АЛГОРИТМ ОПТИЧНОГО ШИФРУВАННЯ, ВІРТУАЛЬНИЙ СТЕНД КВАНТОВОЇ КРИПТОГРАФІЇ, КВАНТОВА КРИПТОГРАФІЯ, ПРИНЦИП ОПТИЧНОЇ КРИПТОГРАФІЇ, РОЗГЛЯД СТЕНДУ EDU-QCRY1 EDU-QCRY1/M.

Об’єкт дослідження – демонстраційний комплекс EDU-QCRY1 EDU-QCRY1/M.

Метою кваліфікаційної роботи є розробка віртуального стенду квантової криптографії для інформаційно-вимірювальних технологій на основі демонстраційного комплексу EDU-QCRY1 EDU-QCRY1/M, дослідження фізичних основ, конструкції, а також тенденції розвитку систем оптичної криптографії.

Метод дослідження – практичний.

Для досягнення мети в роботі поставлено та вирішено наступні завдання.

1. Дослідити фізичні основи оптичної криптографії.
2. Дослідити конструкцію демонстраційного комплексу оптичної криптографії.
3. Дослідити алгоритми оптичного шифрування.
4. Розробити віртуальний стенд (WEB-додаток), емулюючий роботу демонстраційного комплексу оптичної криптографії EDU-QCRY1 EDU-QCRY1/M.

ABSTRACT

Explanatory note of the qualification work: 33 pp., 7 figures, 3 tables, 2 application, 14 sources.

OPTICAL ENCRYPTION ALGORITHM, PRINCIPLE OF OPTICAL CRYPTOGRAPHY, OPTICAL ENCRYPTION ALGORITHM, QUANTUM CRYPTOGRAPHY, REVIEW OF THE EDU-QCRY1 EDU-QCRY1/M STAND, VIRTUAL STAND OF QUANTUM CRYPTOGRAPHY.

The research object is the demonstration complex EDU-QCRY1 EDU-QCRY1/M.

Research method – practical.

The aim of the qualification work is to develop a virtual stand for quantum cryptography for information and measurement technologies based on the demonstration complex EDU-QCRY1 EDU-QCRY1/M, investigate the physical foundations, design, and trends in the development of optical cryptography systems.

To achieve the goal, the following tasks were set and solved in the work:

1. Investigate the physical foundations of optical cryptography.
2. Study the design of the demonstration complex of optical cryptography.
3. Investigate algorithms for optical encryption.
4. Develop a virtual stand (WEB application) emulating the operation of the demonstration complex of optical cryptography EDU-QCRY1 EDU-QCRY1/M.

ЗМІСТ

ВСТУП

В сучасному світі, що стрімко розвивається в галузі інформаційних технологій, концепція захисту даних стає все більш актуальною та складною. З інтенсивним використанням кіберпростору та зростанням обсягів обробки інформації, виникають нові виклики для забезпечення конфіденційності та цілісності даних. У цьому контексті особливу вагу набуває захист квантової інформації.

З одного боку квантова інформація надає безпрецедентні можливості для розвитку нових технологій, з іншого боку, вона стає об'єктом підвищеної уваги щодо безпеки. Швидкісна передача інформації на великі відстані породила напрямок квантової криптографії [1]. Важливість захисту квантової інформації полягає в розпізнанні унікальних властивостей квантових систем, які можуть бути використані для створення надійних методів криптографічного захисту.

Однією з ключових особливостей квантової інформації є принцип невизначеності Гейзенберга, що гарантує, що будь-яке спостереження частинки може вплинути на її стан. Цей принцип ускладнює спроби несанкціонованого доступу до інформації, оскільки будь-яка спроба її вимірювання може бути виявлена. Крім того, квантові біти, або кубіти, можуть існувати в суперпозиції станів, що дозволяє створювати системи квантового шифрування, які надійно захищають інформацію від атак з використанням сучасних обчислювальних методів.

Забезпечення безпеки квантової інформації відкриває нові перспективи для створення квантових комунікаційних мереж та розвитку квантових комп'ютерів. Квантові комп’ютери не працюють швидше ніж класичні комп'ютери, але працюють цілком інакше, вони досягають безпрецедентного прискорення, уникаючи непотрібних обчислень [2]. Проте, існує важливий виклик – розвиток криптографічних протоколів, які будуть стійкими до квантових обчислювачів. Існуючі криптографічні алгоритми можуть бути

легко розгадані квантовими комп'ютерами, що вимагає розробки нових методів шифрування.

Отже, важливість захисту квантової інформації полягає не лише в забезпеченні конфіденційності сучасних даних, але й у підготовці до нового етапу розвитку технологій, де квантова інформатика стане неодмінною частиною нашого цифрового майбутнього. Сприяючи розвитку квантової криптографії та створюючи ефективні методи захисту, ми визначаємо напрямок для безпечного та надійного використання квантової інформації в епоху зростаючого цифрового впливу.

У світі наближення науки до квантової переваги, технологічно розвинені держави все більше усвідомлюють, який прорив подарує їм повноцінний квантовий комп'ютер та розвивають квантові криптографічні системи. Національні стратегії квантового розвитку та відповідні бюджети були ухвалені США, Великобританією, Австралією, Китаєм, Японією та іншими державами [3]. Тому Україна також вимагає розвитку квантових технологій та квантової криптографії зокрема.

1 ЗАХИСТ ІНФОРМАЦІЇ

1.1 Методи захисту інформації

Захист інформації – це важлива складова сучасного суспільства, оскільки інформація стала ключовим ресурсом. Ось кілька основних аспектів, які варто враховувати при розгляді заходів захисту інформації:

– шифрування даних: використання шифрування дозволяє перетворити інформацію в незрозумілу форму для осіб, які не мають права доступу. Застосування сучасних шифрувальних алгоритмів є важливим для захисту конфіденційної інформації;

– аутентифікація та авторизація: використання механізмів аутентифікації (підтвердження особи) та авторизації (визначення прав доступу) допомагає контролювати, хто має доступ до конкретної інформації та як це використовується;

– фізичний захист: захист фізичного обладнання та інфраструктури, яка зберігає чи оброблює інформацію, також є важливим. Це може включати контроль доступу до приміщень, захист пристроїв від крадіжок, а також вживання заходів проти знищення обладнання;

– захист від програмного забезпечення: використання антивірусного програмного забезпечення, файрволів та інших інструментів для захисту систем від вторгнень та шкідливих програм;

– навчання персоналу: засвоєння засобів безпеки інформації та культури безпеки серед персоналу є важливим елементом. Люди можуть бути слабким ланцюгом у захисті інформації, тому навчання їх впізнавати загрози та дотримуватися політик безпеки є важливим;

– резервне копіювання та відновлення: регулярне створення резервних копій даних та розробка планів відновлення допомагає уникнути втрати важливої інформації у випадку інцидентів чи катастроф;

– моніторинг та аудит: систематичний моніторинг діяльності систем та проведення аудитів допомагають вчасно виявляти можливі загрози та слабкі місця в системах захисту.

Ці заходи можуть використовуватися як частина комплексного підходу до захисту інформації в організації чи особистому користуванні.

1.2 Шифрування інформації

Шифрування – це перетворення даних у формат, незрозумілий без дешифрування, таким чином, що доступ до інформації може отримати лише авторизований користувач. Процес шифрування стає можливим завдяки криптографічним ключам в поєднанні з різними математичними алгоритмами. Розглянемо два основні типи шифрування - симетричне і асиметричне.

Метод симетричного шифрування, як випливає з назви, використовує один криптографічний ключ для шифрування та дешифрування даних. Використання одного ключа для обох операцій робить процес простим. Щоб захистити повідомлення, воно шифрується таким чином, щоб кожна літера замінювалась літерою на сім позицій вниз по алфавіту. Замість того, щоб писати «Apple», пишуть «hwwsl» (A -> H, P -> W, L -> S, E -> L). Для розшифрування повідомлення потрібно замінити кожну літеру на сім позицій в алфавітному порядку назад. Такий метод шифрування вже давно використовував римський імператор і військовий стратег Гай Юлій Цезар, і відомий як «шифр Цезаря» [4].

Найвидатнішою особливістю симетричного шифрування є простота процесу, оскільки використовується один ключ як для шифрування, так і для дешифрування. Коли необхідно зашифрувати великий обсяг даних, симетричне шифрування є відмінним варіантом. В результаті алгоритми симетричного шифрування:

– значно швидше, ніж їх аналоги асиметричного шифрування;

– вимагає менше обчислювальної потужності;

– не зменшується швидкість передачі.

Існують сотні алгоритмів симетричного типу. Найбільш поширеними серед них є AES, RC4, DES, 3DES, RC5, RC6 і т. д.

Асиметричне шифрування, на відміну від симетричного, включає кілька ключів для шифрування та дешифрування даних, які математично пов'язані один з одним. Один з цих ключів відомий як «відкритий ключ», а інший – як «закритий ключ». Асиметричний метод шифрування також відомий як «криптографія з відкритим ключем» [4].

Симетричне шифрування працює ідеально, коли треба обмінюватися інформацією між двома співрозмовника. Але що, якщо треба безпечно спілкуватися із сотнями співрозмовників? Використовувати різні ключі для кожного співрозмовника непрактично і незручно. Щоб вирішити цю проблему, використовується шифрування з відкритим ключем, тобто нажається відкритий ключ кожному, хто надсилає інформацію, а секретний ключ зберігається при собі. Пропонується зашифрувати інформацію за допомогою відкритого ключа, щоб дані можна було розшифрувати лише за допомогою особистого ключа. Це виключає ризик компрометації ключа, оскільки дані можуть бути розшифровані лише за допомогою закритого ключа, який не розголошується.

Перша перевага цього типу шифрування – безпека, яку він забезпечує. У цьому методі відкритий ключ – який є загальнодоступним – використовується для шифрування даних, тоді як розшифрування даних виконується за допомогою закритого ключа, який слід надійно зберігати. Це гарантує, що дані залишаються захищеними від атак. Інший ключовий момент полягає в тому, що криптографія з відкритим ключем дозволяє створювати зашифроване з'єднання без необхідності зустрічатися в автономному режимі, щоб спочатку обмінятися ключами.

Друга важлива особливість, яку пропонує асиметричне шифрування, – це аутентифікація. Як ми бачили, дані, зашифровані за допомогою відкритого ключа, можуть бути розшифровані лише за допомогою закритого ключа, що пов'язаний з ним. Таким чином, воно гарантує, що дані бачить та розшифровує лише той об'єкт, який повинен їх отримати.

Також існує гібридне шифрування, але гібридне шифрування не є «окремим методом», як симетричне чи асиметричне, в ньому використовуються всі переваги обох методів і створюється синергія надійних систем шифрування.

Кожен з алгоритмів шифрування має свої недоліки. Наприклад, метод симетричного шифрування ідеально підходить для швидкого шифрування великих обсягів даних. Але він не забезпечує перевірку особистості, що є необхідним, коли йдеться про безпеку в Інтернеті. Однак ця перевірка робить процес шифрування значно повільнішим.

Ідея гібридного шифрування виникла, коли стало критично важливим шифрувати дані з високою швидкістю, забезпечуючи при цьому перевірку особистості.

2 ОПИС СТЕНДУ ОПТИЧНОЇ КРИПТОГРАФІЇ

2.1 Принцип роботи

Криптографія, шифрування повідомлень та даних завжди були фундаментальною темою в галузі зв'язку. Протягом століть було розроблено безліч різних методів для запобігання розшифруванню третіми особами. Однак у всіх методів шифрування є слабкі місця; жоден метод не вважається повністю безпечним. Були запропоновані методи шифрування з використанням квантової фізики, які можуть гарантувати безпеку від перехоплення. У цьому комплекті розглядається протокол BB84, який поєднує в собі метод одноразового шифрування з методом квантового розподілу ключів.

Метод одноразового блокнота використовує випадкову двійкову послідовність 0 і 1, яка представляє собою ідеальний ключ передачі даних. Додавання цього ключа до припущеної двійкової інформації також перетворює зашифроване повідомлення в випадкову послідовність нулів і одиниць. Використання ключа для декодування зашифрованого повідомлення повертає вихідне повідомлення до розшифрування. Тільки якщо відправник («Аліса») та отримувач («Боб») знають ключ, зашифроване повідомлення може бути безпечно передано публічно. Перехоплення не має сенсу без наявності ключа, оскільки в основі ключа нема жоднаї методології чи шаблону.

Основна проблема цього методу шифрування полягає в тому, що ключ шифрування повинні знати лише «Аліса» і «Боб». Протокол шифрування BB84 був розроблений виключно для цієї мети. Цей протокол описує, як можна згенерувати ключ шифрування, відомий лише «Алісі» та «Бобу». Однією з основних переваг цього методу є те, що протокол BB84, по суті, дозволяє виявляти атаку перехоплення третьою стороною, яку називають «Єва» (для підслуховування).

Протокол BB84 діє шляхом визначення двох баз, кожна з яких містить дві поляризації світла: базис + складається з поляризацій 0° та 90°, а базис *x* складається з поляризацій –45° та 45°. У цій схемі будь-який базис може використовуватися для представлення двійкового 0 (0 ° або –45 °) і двійкової 1 (90° або 45°). «Аліса» відправляє випадковий біт випадковим чином, а «Боб» проводить вимірювання випадковим чином. Потім вони обмінюються базою через публічний канал. Якщо кожен з них використовував різні бази, вимірювання відкидається; якщо база однакова, обидва тепер згенерували ключовий біт. Оскільки публічний обмін містить лише базу, інший біт невідомий. Якщо «Єва» спробує втрутитися між «Алісою» та «Бобом», вона також зможе лише вгадати базу кожного біта. Оскільки припущення про базу є випадковим, неправильна база буде вибрана в 50 % випадків.

Аспект цього протоколу, пов'язаний з квантовою фізикою, ґрунтується на використанні однофотонного джерела світла для передачі інформації, так що один інформаційний біт переносять лише один фотон у певному стані і, отже, не може бути скопійований. Квантово-оптичні процеси також можна використовувати для генерації випадкових чисел. Оскільки квантова фізика відіграє роль «лише» у генерації ключів, термін «квантова криптографія» використовується рідше, ніж «квантове розподіл ключів (QKD)».

Цей навчальний експеримент моделює ключові принципи, використовувані в квантовій криптографії. Також виконується атака перехоплення з демонстрацією можливості її виявлення. Спочатку експеримент розпочинається з «Аліси» та «Боба», які обирають випадкові бази, а потім шляхом порівняння баз генерують секретний ключ. «Аліса» кодує і відправляє повідомлення, «Боб» отримує і декодує його. Потім до установки додається «Єва» і проводиться експеримент.

«Аліса» відправляє біт, «Єва» намагається його перехопити, а потім Єва відправляє біт «Бобу» в базисі, який вона обрала для свого вимірювання. Під час завершення експерименту «Аліса» і «Боб» порівнюють свої бази через публічний обмін, а також кількох тестових бітів. Якщо вони виявлять,

що приблизно 25 % тестових бітів тепер невірні (викликані помилками в бітах, відправлених Євою), вони зрозуміють, що присутній підслуховувач.

Замість окремих фотонів у цьому експерименті використовується імпульсний лазер. Відповідно, всі результати можна описати виключно класичною фізикою. Установка квантової фізики працює з окремими фотонами, але її функціонування є абсолютно ідентичним. Таким чином, ця установка дуже добре підходить для аналогічного експерименту.

2.2 Одноразовий блокнот

Одноразовий блокнот, також відомий як одноразовий ключ, являє собою метод шифрування, який в принцип 100 % безпечний за умови повного дотримання всіх вимог. Квантова фізика лише допомагає задовольнити ці вимоги, тоді як сам метод є класичною технікою шифрування.

Це ключ шифрування, який повністю складається з випадкової послідовності нулів та одиниць [5], званих «бітами». У свій час, повідомлення також складається з «0» та «1». Двійкове додавання повідомлення та ключа шифрування може бути виконано для отримання іншого ланцюжка з «0» і «1», який також є цілком випадковим. В результаті виходить зашифроване повідомлення.

«Правила розрахунку», застосовні для двійкового додавання, такі:

– 0 + 0 = 0;
– 1 + 0 = 1;
– 0 + 1 = 1;
– 1 + 1 = 0;

Коли одержувач отримає зашифроване повідомлення, він буде використовувати двійкове додавання зашифрованого повідомлення та ключа шифрування. Це призведе до створення вихідного повідомлення. Як приклад, можемо закодувати слово «TEST». Кожну літеру можна перевести в

п'ятизначний двійковий код (табл. 2.1), для кодування літер у двійковий код вікористуемо таблицю-алфавіт (табл. 2.2)

Таблиця 2.1 – Таблиця закодованого слова

Слово	T					E					S					T				
Двійкове слово	1	0	0	1	1	0	0	1	0	0	1	0	0	1	0	1	0	0	1	1
+																				
Випадковий ключ	1	1	0	1	0	1	0	0	0	1	1	0	1	0	0	1	1	1	0	1
Зашифроване слово	0	1	0	0	1	1	0	1	0	1	0	0	1	1	0	0	1	1	1	0
+																				
Випадковий ключ	1	1	0	1	0	1	0	0	0	1	1	0	1	0	0	1	1	1	0	1
Двійкове слово	1	0	0	1	1	0	0	1	0	0	1	0	0	1	0	1	0	0	1	1
Слово	T					E					S					T				

Таблиця 2.2 – Таблиця-алфавіт

A	0	0	0	0	0
B	0	0	0	0	1
C	0	0	0	1	0
D	0	0	0	1	1
E	0	0	1	0	0
F	0	0	1	0	1
G	0	0	1	1	0
H	0	0	1	1	1
I	0	1	0	0	0
J	0	1	0	0	1
K	0	1	0	1	0
L	0	1	0	1	1
M	0	1	1	0	0
N	0	1	1	0	1
O	0	1	1	1	0
P	0	1	1	1	1
Q	1	0	0	0	0
R	1	0	0	0	1
S	1	0	0	1	0
T	1	0	0	1	1

Продовження таблиці 2.2

U	1	0	1	0	0
V	1	0	1	0	1
W	1	0	1	1	0
X	1	0	1	1	1
Y	1	1	0	0	0
Z	1	1	0	0	1

Якщо зашифроване повідомлення перехоплене, перехоплювачу буде потрібен ключ для його декодування. Без ключа випадкова послідовність нулів та одиниць при перетворенні на слово дає немаючий сенсу набір літер. Це робить повідомлення повністю захищеним від перехоплення.

Підсумки основних вимог.

1. Ключ повинен бути не менше довжини повідомлення.
2. Ключ можна використовувати лише один раз.
3. Ключ має бути абсолютно випадковим.
4. Ключ повинен бути відомий лише відправнику та одержувачу.

Вимога 1 легко виконати відправнику, який може зашифрувати лише кількість бітів, менше або дорівнює кількості доступних ключових бітів.

Вимога 2 є обов'язком відправника та одержувача і також легко реалізовано.

Вимогу 3 важко виконати при найближчому розгляді, оскільки кожен генератор випадкових чисел зрештою заснований на алгоритмі. Це означає, що випадкові числа, що генеруються комп'ютером завжди є просто «псевдовипадковими». Однак квантова фізика може бути використана для вирішення цієї проблеми, оскільки вона уможливлює справжню випадковість.

Вимога 4 також проблематична, оскільки класична передача ключа відкриває можливість його перехоплення. Цю проблему також можна вирішити за допомогою квантової фізики.

2.3 Передача даних з однією основою

Цей підрозділ коротко описує процес передачі даних з однією основою, з використанням експериментальної установки.

Фотон буде використовуватися для передачі «0» або «1». У цьому прикладі напрям поляризації використовується як біт: фотон із горизонтальною поляризацією інтерпретується як «0», а фотон із вертикальною поляризацією як «1».

Експериментальна установка, яка може передавати дані таким чином представлена на рис. 2.1.

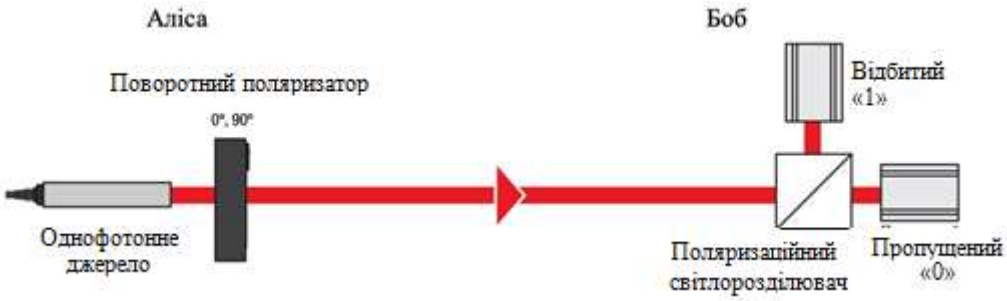

Рисунок 2.1 – Передача даних з одним базисом поляризації

Відправник «Аліса» складається з однофотонного джерела світла, яке поляризоване горизонтально, та пластини $\lambda/2$.

Пластина $\lambda/2$ обертає поляризацію падаючого світла на подвійний фізичний кут обертання хвильової пластини. Наприклад, коли хвильова пластина фізично обертається на 45° відносно напрямку падіння поляризації, поляризація світла фактично обертається на 90°. Тому пластину $\lambda/2$ також відомо синонімічно як «обертач поляризації».

Приймальний блок «Боб» складається з поляризаційного світлодільника та двох детекторів. Куб поляризаційного світлодільника, виконаний у вигляді двох ідентичних діелектричних призм, суміщених гіпотенузами, який являє собою «товсту» плоскопаралельну пластину [6]. Він

відбиває вертикально поляризовану (90°) складову падаючого світла, пропускаючи при цьому горизонтально поляризовану (0°) складову.

Якщо стан поляризації світла, надісланого Алісою, встановлено на 0°, фотон пройде через світлодільник (позначається як подія «0»). Якщо хвильова пластина налаштована на поворот поляризації на 90°, фотон відбиватиметься світлодільником (позначається як подія «1»).

2.4 Розподіл ключів

Хоча метод з однією основою (0° або 90°) достатній для передачі даних від Аліси до Боба, він не здатний гарантувати безпеку від перехоплення. Для досягнення цієї мети використовується друга основа. Крім основи з 0° і 90°, яку ми тепер називатимемо «основа +», використовується друга основа з –45° і 45°. Назвемо її «основою *x*».

Тепер установка виглядає так (рис. 2.2)

Рисунок 2.2 – Передача даних з основами + (0° и 90°) та *x* (–45° и 45°)

Тепер «Аліса» має прийняти два випадкових рішення для генерації ключа:

– «Аліса» має вибрати свою основу навмання, + або *x*;

– «Аліса» має вибрати випадковий біт, 0 або 1:

- вибір 0 із основою + означає налаштування 0°;
- вибір 1 із основою + означає налаштування 90°;

– вибір 0 із основою x означає налаштування -45°;
– вибір 1 із основою x означає налаштування 45°.

Боб встановлює свій поляризаційний ротатор, щоб розрізняти основи + і *x*. Відповідно «Бобу» потрібні лише налаштування 0° і 45°. Якщо Боб вибрав основу +, а «Аліса» надсилає основу +, «Боб» отримує однозначне значення результат; це стосується відповідно, якщо обидва обирають основу *x*. Але що, якщо «Боб» вибере а інша основа, ніж «Аліса»? Результатом вибору іншої основи, ніж Аліса, є 45° поляризоване світло надсилатиметься до світлорозподілювача. Для безперервного променя пропускається половина а половина відбивається. Однак, якщо припустити, що відправляється лише один фотон, лише один із двох детекторів може зреагувати. Детектор, який реагує, надається на волю випадку. Якщо дві бази не збігаються, Боб все одно виміряє сигнал на одному з двох детекторів. Ймовірність виявлення фотона на одному з двох детекторів становить 50 % відповідно (табл. 2.3).

Таблиця 2.3 – Таблиця можливих випадків

«Аліса»			«Боб»				Співадіння основ
Основа	Біт	Кут	Основа	Кут	Детектор «0»	Детектор «1»	
+	0	0	+	0	100%	0%	так
+	1	90	+	0	0%	100%	так
x	1	45	+	0	50%	50%	ні
x	0	-45	+	0	50%	50%	ні
+	1	0	x	45	50%	50%	ні
+	1	90	x	45	50%	50%	ні
x	0	45	x	45	0%	100%	так
x	0	-45	x	45	100%	0%	так

Якщо «Аліса» відправить сигнал, що складається з випадкових бітів у випадковій основі, а «Боб» проаналізує сигнал, використовуючи випадкову основу, як це стане ключем для передачі даних? Відповідь полягає в тому, що і «Аліса», і «Боб» пізніше розкажуть один одному, яка основа використовується у передачі кожного біта. В останніх трьох стовпцях таблиці

результат однозначний (100 %) лише за однакових основах. На практиці «Аліса» та «Боб» пройдуть кожен вимір і повідомлять лише «+» чи «*x*». Якщо вони різні, обидва відкидають вимір. Але якщо обидві бази однакові, то обидва знають, який біт було передано, на підставі результату, отриманого детекторами Боба. Основи, але не біті, завжди публікуються публічно. Таким чином, ключ шифрування виходить на основі вимірів, в яких Аліса та «Боб» обрали однакові основи.

Як тільки «Аліса» та «Боб» проведуть таким чином усі виміри, обидва отримають (випадковий) ключ. Тепер Аліса може зашифрувати повідомлення і відправити його з основою «+». «Боб» отримує повідомлення з основою «+» і може його розшифрувати.

3 РОЗРОБКА ВІРТУАЛЬНОГО СТЕНДУ

3.1 Використані технології

При розробці віртуального стенду квантової криптографії для інформаційно-вимірювальних технологій, як середовище розробки та подальшої роботи додатку, була обрана WEB-платформа. Як одна з найпоширініших, та непотребуючих інших специальніх середовищ для запуску окрім браузера, який входить у стандартний пакет програм будь-якої операційної системі. Що у свою чергу додає гнучкості та відкриває великі можливості для вікористання як на комп'ютерах, так і на мобільних девайсах, без значних доробок зі сторони розробки.

У додатку вікористано такі основні мови программування:

– HTML 5 (HyperText Markup Language – «мова гіпертекстової розмітки») – базовий будівельний блок веб-сторінок та веб-додатків. Він визначає зміст та структуру веб-контенту [7–8];

– CSS 3 (Cascading Style Sheets) – це мова ієрархічних правил (таблиць стилів), що використовується для представлення зовнішнього вигляду документа, написаного на HTML або XML (включаючи різні мови XML, такі як SVG і XHTML. CSS описує, яким чином елемент повинен відображатися на екрані, на папері або з використанням інших засобів виводу інформації [9–10];

– JavaScript – мова програмування, яка дозволяє створювати динамічно оновлюваний контент, керувати мультимедіа, анімувати зображення, виконувати математичні та логічні обчислювання та багато іншого [11–12].

З метою покращення продуктивністі, додаток розроблений з використанням бібліотеки ReactJS. Це JavaScript-бібліотека з відкритим вихідним кодом для розробки інтерфейсів користувача [13]. React розробляється та підтримується Facebook, Instagram та спільнотою окремих розробників та корпорацій. Використовується для розробки односторінкових та мобільних додатків. Його мета – надати високу швидкість розробки, простоту та масштабованість при розробці інтерфейсів користувача.

3.2 Алгоритм роботи та структура

Як основу алгоритма віртуального стенду було взято принцип роботи демонстраційного стенду квантової криптографії EDU-QCRY1, за схемою передачі даних з однією основою. Також використовується принцип «одноразового блокноту» для генерування публічного секретного ключа, який відомий як відправнику, так і отримувачу.

Одиничний фотон представлений як бінарна однобітна змінна, тобто являє собою «0» або «1». Кодування та декодування літер у двійковий код виконано за бопомогою об’єкта-алфавіта, де кожній літері англійського алфавіту відповідає п’яти-бітовий двійковий код. Приклад алфавіту розглянутий у розділі «2.2 Одноразовий блокнот».

Архітектурно додаток поділено на чотири частини.

1. Блок «Аліса». Виступає відправником, являє собою контекст-сервис для зберігання введених даних, методів операцій над ними та інтерфейс користувача для відображення введиних, розрахованих даних та елементів керування.

2. Блок «Боб». Виступає отримувачем, як і «Аліса» складається з контекст-сервису та інтерфейсу користувача з елементами керування.

3. Блок «Публічне сховище». Представляє собою інтерфейс для відображення публічних даних, які «пересилаються» від «Аліси» до «Боба».

4. Спільний сервіс. Зберігає загальні методи для операцій над даними, такі як: кодування тексту в двійковий код та обратне декодування двійкового коду у текст. Також зберігає дані для відображення у блоку «Публічне сховище».

У той же час існує інкапсуляція логіки та деякий зв’язок між компонентами. Аліса інкапсулює в собі логіку відправника, має метод для кодування повідомлення, може приймати значення текстового повідомлення від користувача, та зберігати його. «Знає» про компонент спільного сервісу, має доступ до його методів і може записувати в нього дані. «Не знає» про існування Боба.

Боб инкапсулює логіку отримувача, має методи декодування повідомлення. Також «знає» про спільний сервіс і може брати з нього дані та використовувати методи спільних операцій. «Не знає» про існування Аліси.

Спільний сервіс «не знає» ні про Алісу, ні про Боба, надає лише можливість використовувати його методи, записувати та считувати публічні дані.

Загальний алгоритм роботи додатку (рис. 3.1) покроково виглядає так:

1) користувач вводить тескстове повідомлення, латнськими літерами без пропусків. Повідомлення записується до сервісу Аліси;

2) обирається основа кодування для Аліси «0» або «45» градусів. За замовчуванням виставлено «0»;

3) запускається конвертація тексту повідомлення у бінарний код;

4) генерує секретний ключ;

5) бінарне повідомлення бінарно сумується з обраною основою;

6) повідомлення з основою бінарно сумується з секретним ключом;

7) зашифроване повідомлення разом з секретним ключом передається та записується у спільний сервіс;

8) обирається основа кодування для «Боба» «0» або «45». За замовчуванням виставлено «0»;

9) «Боб» считує зашифроване повідомлення та секретний ключ з спільного сервісу;

10) зашифроване повідомлення бінарно сумується з обраною Бобом основою;

11) повідомлення бінарно сумується з секрентним ключом;

12) запускається конвертація бінарного коду тексту повідомлення у текстове повідомлення.

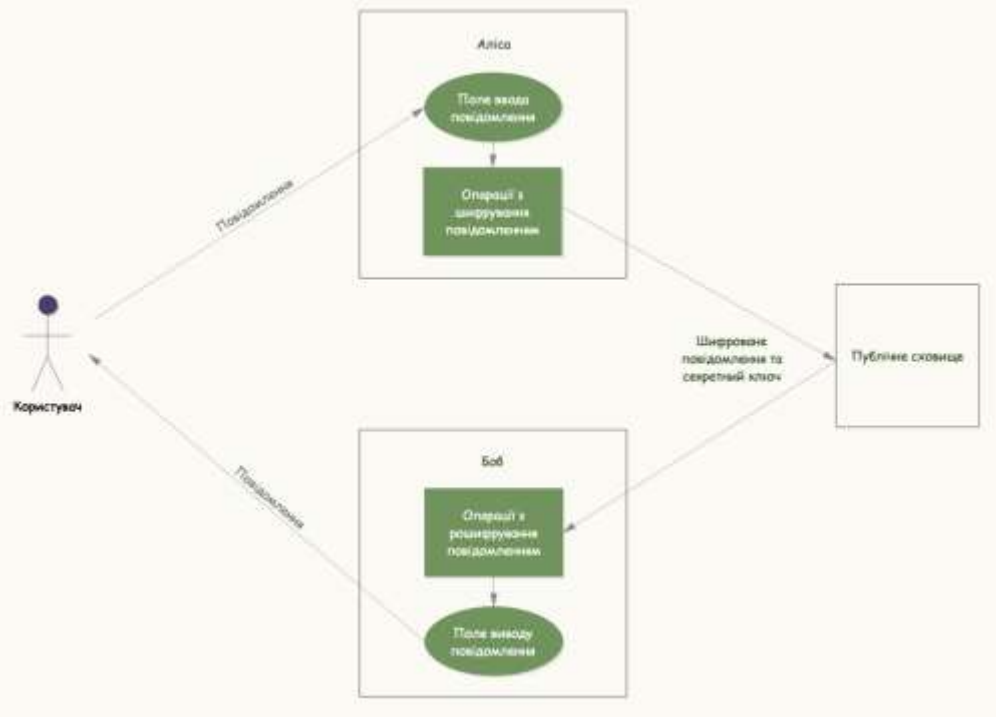

Рисунок 3.1 – Загальний алгоритм роботи додатку

Якщо обрані «Алісою» та «Бобом» основи однакові, Боб отримує вірно розшифроване текстове повідомлення «Аліси». У іншому віпадку текствое повідомлення являє собою не маючий сенсу набір літер. Алгоритм може бути повторено за тими ж крокамі необхідну кількість разів.

3.3 Дизайн та робота з додатком

Дизайн додатку можно умовно поділити на три частини (рис. 3.2).

1. Блок відображення «Аліси».
2. Блок відображення «Боба».
3. Публичне сховище.

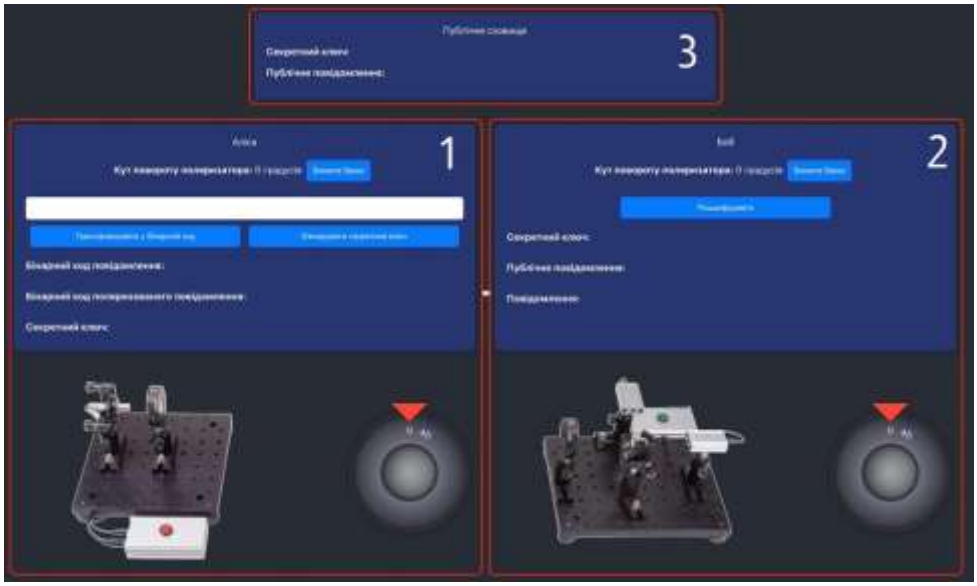

Рисунок 3.2 – Загальний вигляд додатку

Розглянемо кожну частину та їх контент більш детально.

«Аліса» (рис. 3.3). Складається з заголовку, рядка з відображенням поточного кута повороту поляризатора. Правіше є кнопка для перемикання кута повороту. Нижче розташовано текстове поле вводу тексту повідомлення та дві кнопки керування. «Трансформувати у бінарний код» – запускає алгоритм перетворення тестку у його двійковий код. Кнопка «Знегерувати секретний ключ» – вікликає генерування секретного ключа відповідно до довжини бінарного коду повідомлення. Нижче, за для наочності та прозорості роботи алгоритмів, розташовано виведення рядків трансформованого бінарного коду повідомлення, результату підсумовування бінарного коду повідомлення з бінарним кодом поляризації та згенерований віпадковий секретний ключ. У нижній частині розташовано фотографію «Аліси» з реального демонтраційного комплексу та графічний перемикач куту повороту поляризатора.

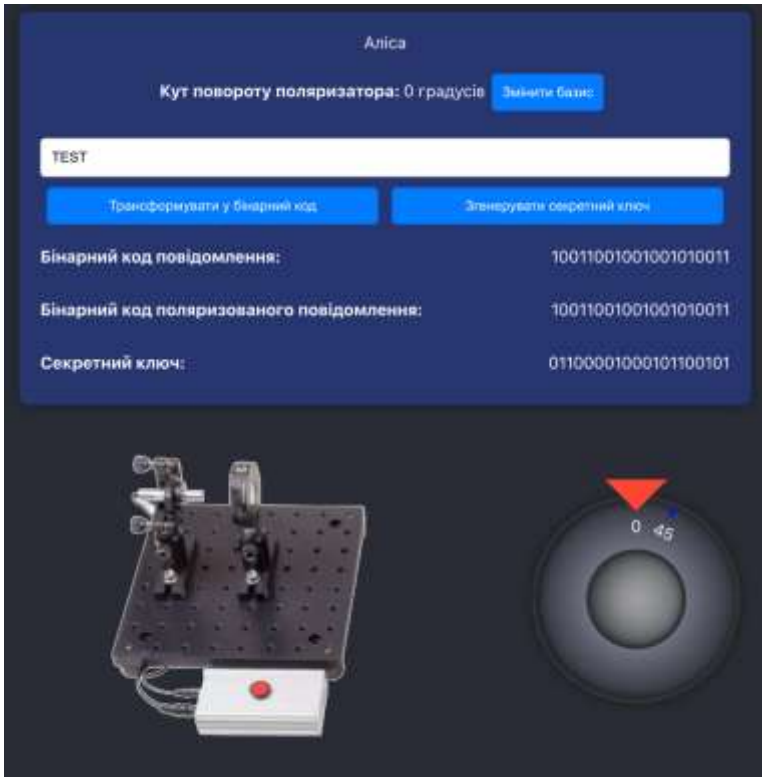

Рисунок 3.3 – «Аліса»

«Боб» (рис. 3.4). Має схожий вігляд з «Алісою», але має лише одну кнопку керування. Це кнопка «Розшифрувати», яка запускає алгоритм розшифрування повідомлення, переданого «Алісою». За для наочності, має рядки виводу отриманого секретного ключа, публічного повідомлення та результуючуго розшифрованого повідомлення.

Рисунок 3.4 – Боб

Публічне сховище (рис. 3.5). Складається з заголовку та рядків відображаючих данні, що були передані від «Аліси» «Бобу» публічно. А саме видображае секретний ключ та зашифроване публічне повідомлення.

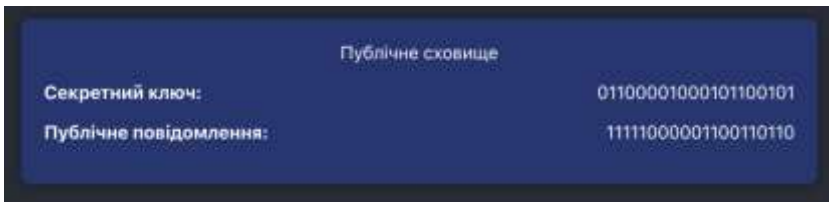

Рисунок 3.5 – Публічне сховище

Робота з додатком є доволі простою, та завдяки логічному послідовному розташуванню єлементів інтерфейсу, інтуїтивно зрозуміла.

Покрокова інструкція з використання виглядає так:

1) запустити додатку у браузері. Точка входу index.html;
2) ввести текстове повідомлення. Латинськими літерами без пробілів;

3) виставити для «Аліси» потрібний кут повороту поляризатора через кнопку «Змінити базис» або клікнувши по графічному перемикачу куту повороту поляризатора;

4) натиснути кнопку «Трансформувати у бінарний код»;

5) переконтись, що з’явилось значення бінарного кода повідомлення.

6) натиснути «Згенерувати секретний ключ»;

7) переконатись, що з’явилось значення секретного ключа;

8) виставити для «Боба» потрібний кут повороту поляризатора через кнопку «Змінити базис» або клікнувши по графічному перемикачу куту повороту поляризатора;

9) натиснути кнопку «Розшифрувати»;

10) отримати результат у рядку «Повідомлення».

ВИСНОВКИ

В ході виконання кваліфікаційної роботи було розглянуто види та методи захисту інформації, проведено дослідження фізичних основ оптичної криптографії, вивчено конструкцію комплексу оптичної криптографії та проаналізовано алгоритми оптичного шифрування.

Основною метою було створення віртуального стенду квантової криптографії, який емулює функціонал демонстраційного комплексу та дозволяє вивчати принципи оптичної криптографії в інтерактивному режимі. Використані для досягення цієї мети технології та засоби є сучасними, гнучкими, продуктивними, не потребуючими великих потужностей від користувача, не займають багато пам’яті та доступні на багатьох пристроях. У парі з прогресивною архітектурою можуть показувати відмінні показники швидкості роботи, надійності та мають гарний потенціал для масштабованості.

Додаток віртуальний стенду квантової криптографії розроблений на WEB-платформі, та являє собою SPA (single page application). За для написання коду було викристано мови программування такі як: HTML 5 – відповідає за розмітку та структуру веб-контенту, JavaScript – основна логіка та алгоритми обчислень, CSS 3 – позиціонування елементів інтерфейсу та їх стилістичне відображення згідно з дизайну, бібліотека ReactJS – незалежне динамічне оновлення та перерисовка елементів у реальному часі. Сбірка, мініфікування, запуск у режимі розробки та фінальне компілювання додатку здійснюється за допомогою інструменту Create React App, що має у собі збиральник пакетів WebPack.

Отримані результати вказують на важливість подальших досліджень у сфері квантової криптографії та оптичного шифрування. Розроблений віртуальний стенд є ефективним інструментом для навчання та дослідження в галузі інформаційно-вимірювальних технологій. Він також сприяє розвитку

систем оптичної криптографії, бо може служити сучасною та стабільною базою для подальшої розробки та покращення функціональності.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Sivni, V. B., & Hnatenko, O. S. (2018). Use of femtosecond lasers to encode information. *Фізика, електроніка, електротехніка: матеріали та програма науково-технічної конференції*, 23-26.

2. Hnatenko O. Quantum computing. Quantum information technologies as the basis for future learning platforms / O. Hnatenko // The 19 th INTERNATIONAL CONFERENCE INFORMATION TECHNOLOGIES AND MANAGEMENT 2021 April 22-23, 2021, ISMA University of Applied Science, Riga, Latvia - P. 87-89.

3. Друга квантова революція URL: https://habr.com/ru/companies/online patent/articles/736810/ (дата звернення 10.09.2023).

4. Шифрування: типи і алгоритми. Що це, чим відрізняються і де використовуються? URL: https://hostpro.ua/wiki/ua/security/encryption-types-algorithms (дата звернення 11.10.2023).

5. Щур Н.О., Покотило О.А. Основи криптології: навч. посібник. Житомир: Житомирська політехніка, 2021. 120 с. URL: https://learn.ztu.edu.ua/pluginfile.php/264055/mod_resource/content/1/ (дата звернення 15.10.2023).

6. Gnatenko, A. S., & Machechin, Y. P. (2015). Vasko K.O Providing control of the polarization inside the resonator fiber ring laser. *Вісник Київського національного університету імені Тараса Шевченка. Радіофізика та електроніка. Київ*, 20-23. С. 34.

7. HTML. URL: https://developer.mozilla.org/ru/docs/Web/HTML (дата звернення 01.11.2023).

8. Gnatenko, A. S., & McHekhin, Y. P. (2015). Generation mode stability of a fiber ring laser. Telecommunications and Radio Engineering, 74(7), 641-647.

9. Cascading Style Sheets **(**CSS**)** URL:https://developer.mozilla.org/ru/docs /Web/CSS (дата звернення 10.11.2023).

10. Afanasieva, I., Golian, N., Hnatenko, O., Daniiel, Y., & Onyshchenko, K. (2019). Data exchange model in the internet of things concept. Telecommunications and Radio Engineering, 78(10), 869-878.

11. What is JavaScript URL: https://developer.mozilla.org/ru/docs/Learn/JavaScript/First_steps/What_is_JavaScript (дата звернення 15.11.2023).

12. React JS URL: https://react.dev (дата звернення 11.11.2023).

13. Лазерні, оптико-електронні прилади та системи. Ч. 3. Фемтосекундні лазери для інформаційно-вимірювальних технологій / О. С. Гнатенко ; Харків : Факт, 2023 - 130 с. ISBN 978-966-617-8072-88-9.

14. Методичні рекомендації та вимоги щодо оформлення пояснювальної записки атестаційної роботи магістрантів денної форми навчання спеціальності 152 «Метрологія та інформаційно-вимірювальна техніка» спеціалізацій «Лазерна і оптоелектронна техніка» та «Фотоніка та оптоінформатика» / Упоряд.: Гнатенко О.С, Крючков А.І., Чернишова Н.М. Харків: ХНУРЕ, 2017. 48 с.