СИЛАБУС ВИБІРКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ОСНОВИ КВАНТОВОЇ ТА ПОСТКВАНТОВОЇ КРИПТОГРАФІЇ

Факультет	Інформаційних технологій та кібербезпеки
Кафедра	Кібербезпеки та технічного захисту інформації
Статус навчальної дисципліни	Вибіркова компонента освітніх програм першого (бакалаврський) рівня вищої освіти
Рекомендовано для спеціальностей	Для всіх ОПП запроваджених ДУІТЗ
Форма навчання	Денна, заочна

Викладачі

Лімарь Ігор Валерійович
quantum.biology@outlook.com

Старший викладач кафедри Кібербезпеки та технічного захисту інформації, кандидат технічних наук

Загальна інформація про дисципліну

Анотація до дисципліни	Дисципліна «Основи квантової та постквантової криптографії» базується на сучасних уявленнях о нерелятивістській квантовій механіки, квантової теорії інформації а також на положеннях постквантової криптографії. Вона інтегрує, відповідно до свого предмету, знання з таких освітніх і наукових галузей: математика, фізика, теорія інформації, оптика, квантова оптика.
Мета дисципліни	формування основ знань, необхідних майбутнім фахівцям в галузі інформаційної безпеки щодо квантової та постквантової криптографії.
Компетентності,	Здатність застосовувати знання у практичних ситуаціях.

формуванню яких сприяє дисципліна	Знання та розуміння предметної області та розуміння професії. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.
Результати навчання	Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.
Обсяг дисципліни	Загальний обсяг дисципліни 6 кредитів ЄКТС (180 академічних годин)
Форма підсумкового контролю	Залік
Терміни викладання дисципліни	Відповідно до розкладу занять вибіркових компонент освітньої програми

Програма дисципліни

Тема 1.	***Вступна лекція. Розвиток методів та засобів квантової криптографії*** Кодування Віснера. Теорема Холево. Експерименти по перевірці порушень нерівностей Белла. Теорема про заборону клонування. Запропонування принципів квантової криптографії. Перша експериментальна реалізація квантової криптографії. Протокол квантової криптографії з використанням заплутаних станів.
Тема 2.	***Математичний апарат нерелятивістської квантової механіки*** Властивості комплексних векторів та матриць. Тензорний добуток. «Бра- кет» нотація. Внутрішній добуток, ортогональність та норма. Зовнішній добуток та проектори. Базиси, стандартний (обчислювальний) базис. Власні вектори, власні значення та діагоналізація. Нормальні, ермітові та унітарні матриці.
Тема 3.	***Основи нерелятивістської квантової механіки*** Матриці Паулі. Матриця Адамара. Значення глобальної та відносної фази. Існування заплутаних станів. Розрізнення ортогональних і неортогональних станів. Точно розрізняти неортогональні стани, але з імовірністю менше одиниці. Принцип відсутності сигналів. Принцип заборони клонування. Принцип заборони на видалення.
Тема 4.	***Поляризація фотонів. Принципи квантових вимірювань*** Поляризація фотону. Оптичне поле. Квантово-оптичний розгляд. Моди поля, фотони, однофотонні оптичні імпульси. Проективні вимірювання. Неточні вимірювання. Узагальнені вимірювання.
Тема 5.	***Протокол BB84. Протокол с 6-ма станами. Протокол Екерта*** Діагональна та перпендикулярна поляризація фотонів. Просіяний ключ. Правоциркулярний та лівоциркулярний напрями поляризації для переданого фотона. Протокол квантового розподілу ключів з використанням стану квантових частинок поляризації заплутаних фотонів (ЕПР-пари).
Тема 6.	***Стек протоколів квантового розподілу ключів шифрування. Основні види атак на системи квантової криптографії*** Протокол квантового передавання (передавання одиночних фотонів по оптичному волокну). Протокол просіювання ключа. Протокол оцінювання виявлення атаки пасивного перехоплення. Протокол виправлення помилок, що виникли під час квантового передавання. Некогерентні атаки. Когерентні атаки. Атаки обумовлені недосконалістю протоколів. Квантовий хакінг.

Тема 7.	***Теорема Цизара – Кернера. Методи підсилення стійкості протоколів квантової криптографії*** Твердження Цизара-Кернера. Геш-функція. Інформація в сенсі Реньї.
Тема 8.	***Квантовий прямий безпечний зв'язок. Пінг-понг протокол*** Переваги та недоліки квантового прямого безпечного зв'язку. Пінг-понг протокол зі станами Бела пар кубітів. Атака пасивного перехоплення з використанням переплутування.
Тема 9.	***Вразливість криптографічних протоколів до атак з використанням квантового комп'ютера. Алгоритм Шора*** Квантове перетворення Фур'є. Квантова оцінка фази. Алгоритм факторизації Шора. ведення факторизації до пошуку порядку.
Тема 10.	***Розвиток протоколів постквантової криптографії. Основи криптографічної системи NTRUEncrypt*** Основні протоколи постквантової криптографії. Протоколи постквантової криптографії, що перемогли у конкурсі NIST у 2022 році. Основи криптографічної системи NTRUEncrypt.

Список рекомендованих джерел

1. The Physics of Quantum Information: Quantum Cryptography, Quantum Teleportation, Quantum Computation / Bouwmeester D., Ekert A. K., Zeilinger A. Berlin: Springer, 2000. 326 p.
2. Nielsen M.A., Chuang I.L. Quantum Computation and Quantum Information. Cambridge University Press, 2001. 674 p.
3. Вакарчук І.О. Квантова механіка : підручник. Львів : ЛНУ імені Івана Франка, 2012. 872 с.
4. Quantum information science [електронний ресурс]/Режим доступу: https://en.wikipedia.org/wiki/Category:Quantum_information_science
5. Quantum information theory [електронний ресурс]/Режим доступу: https://en.wikipedia.org/wiki/Category:Quantum_information_theory

Інформація про консультації

Індивідуальні та колективні консультації проводяться в час, визначений за попередньою домовленістю з викладачем через засоби зв'язку.

Загальна схема оцінювання

<table>
<tr><td rowspan="2">Сума балів за всі види навчальної діяльності</td><td rowspan="2">Шкала ЄКТС</td><td colspan="2">Оцінка за національною шкалою</td><td rowspan="2">Нарахування балів</td><td>Бали нараховуються таким чином:</td></tr>
<tr><td>для іспиту</td><td>для заліку</td><td rowspan="6">Оцінювання знань здобувачів вищої освіти здійснюється за 100-бальною шкалою і становить: за поточну до 60 балів, за результати індивідуального завдання – до 40 балів.
При оформленні документів за екзаменаційну сесію використовується таблиця відповідності оцінювання знань здобувачів вищої освіти за</td></tr>
<tr><td>90-100</td><td>A</td><td>Відмінно</td><td rowspan="5">зараховано</td></tr>
<tr><td>82-89</td><td>B</td><td rowspan="2">Добре</td></tr>
<tr><td>74-81</td><td>C</td></tr>
<tr><td>64-73</td><td>D</td><td rowspan="2">Задовільно</td></tr>
<tr><td>60-63</td><td>E</td></tr>
</table>

35-59	FX	Незадовільно з можливістю повторного складання	Не зараховано з можливістю повторного складання		різними системами
0-34	F	Незадовільно з обов’язковим повторним вивченням дисципліни	Не зараховано з обов’язковим повторним вивченням дисципліни		

Політика опанування дисципліни

Відвідування:
Відвідування та відпрацювання пропущених занять є обов’язковим. Допускаються пропуски занять з поважних причин, які підтверджується документально. За такої умови навчання може відбуватися в режимі он-лайн за погодженням із деканатом.
Дотримання принципів академічної доброчесності:
Політика щодо академічної доброчесності побудована на основі «Положення про академічну доброчесність» в університеті. Списування під час виконання письмових контрольних видів робіт заборонено. Користуватися мобільними пристроями, під час проведення різних видів контролю успішності, дозволяється лише з дозволу викладача.
Умови зарахування пропущених занять:
Відпрацювання пропущених занять проходять в дні згідно графіку консультацій викладачів кафедри.