УДК 004.056.53

В.Л. Зінченко, В.О. Лифар

ІНТЕЛЕКТУАЛЬНИЙ АНАЛІЗ ІНФОРМАЦІЙНИХ ПОТОКІВ У КВАНТОВИХ СИСТЕМАХ ПЕРЕДАЧІ ІНФОРМАЦІЇ

Зінченко Володимир Леонідович

Інститут телекомунікацій і глобального інформаційного простору НАН України, м. Київ,
orcid: 0000-0001-6081-4848

zinchenko@outlook.com

Лифар Володимир Олексійович

Східноукраїнський національний університет імені Володимира Даля, м. Київ,
orcid: 0000-0002-7860-9663

lifar@snu.edu.ua

Розглянуто деякі можливості та проблеми систем передачі інформації, заснованої на квантово-механічних принципах. Незважаючи на уявно високу надійність оптоелектронних систем, що використовують когерентні фотони для захищених ліній передачі та обробки інформації, теоретично можливі методи і засоби здійснення несанкціонованого доступу до квантової інформації, що передається. Раніше передбачалося, що методи та алгоритми криптографії забезпечують дуже високий рівень надійності та безпеки інформаційних потоків. Однак з виникненням більш продуктивних обчислювальних систем, особливо квантових комп'ютерів, з'явилася можливість реалізації складних алгоритмів атак і методів викрадення ключів та потокової інформації. Крім цього, відомі протоколи криптографії були вивчені та випробувані з використанням «пробоїв» та алгоритмів дешифрування, що зробило раніше надійні системи практично непрацездатними. У статті розглянуто деякі види атак, які найбільш ймовірно можуть застосовуватися кіберзлочинцями. Окремі властивості квантових оптичних систем дозволяють використовувати деякі фізичні принципи для виявлення стану фотонних потоків і аналізу зміни цих станів з метою визначення надійності та достовірності інформації, що передається. Водночас припускається, що гібридне поєднання аналізу фізичних характеристик квантів, які передаються в q-бітному поданні, та надійних криптографічних протоколів, можливо, істотно посилить атрибути надійності та захищеності інформації. За таких умов ставиться завдання дослідити можливість застосування у надійних квантових системах деяких методів та систем інтелектуального аналізу даних для реалізації системи підтримки прийняття рішень (СППР) щодо надійності квантових засобів передачі в OLTP-режимі. Пропонується використовувати засоби підготовки та обробки інформації на базі нейронних мереж, що навчаються. Необхідно з'ясувати можливості нейронних мереж працювати у реальному часі з повною синхронізацією інформаційних потоків, а також можливості аналізу їхніх станів. Проаналізовано деякі види атак з поділом фотонів, «квантових троянів» та ін. Незважаючи на безпеку, існує безліч можливостей пробоїв у структурі самого каналу передачі квантів, що не гарантує стовідсотковий захист інформації від атак кіберзлочинців.

Ключові слова: криптографія, квантова інформація, інтелектуальний аналіз, нейронна мережа, захист інформації, підтримка рішень, атака каналу.

Вступ

Використання інформаційних технологій у сфері системи підтримки прийняття рішень (СППР) призводить до швидкого зростання кількості завдань кібернетичної безпеки. За таких умов найбільш перспективним напрямом є застосування криптографічних систем, що базуються на квантовому передаванні інформації. Математичною основою «квантової інформатики», що стрімко розвивається, є абстрактні механізми отримання, зберігання, передавання та перетворення інформаційних потоків у системах, які відповідають законам квантової механіки. Квантова інформатика базується на математичному апараті матричного та оперативного аналізу з використанням ймовірнісного аналізу систем нечіткої логіки.

Особливий інтерес становлять квантово-механічні ефекти, що проявляються в оптоелектронних системах, на рівні фотонного обміну інформацією для когерентних джерел оптичних квантових генераторів. Сучасні лазерні технології, що застосовуються в оптоелектронних системах, дозволяють створювати потоки фотонів строгого когерентного випромінювання однакових частот з певними фізичними властивостями (заданий спін або квантово заплутаний стан). Водночас на фізичному рівні з'являється можливість адаптивно контролювати стан інформаційного середовища, що своєю чергою може забезпечити абсолютний контроль керування інформаційними потоками та захист даних від несанкціонованого доступу. Вирішити в таких умовах завдання надійності та захищеності інформаційних систем можна шляхом удосконалення криптозахисту паралельно з інтелектуальним аналізом стану інформаційного середовища на основі якісних систем діагностування інформаційних перетворень.

Квантові лінії зв'язку надійно захищають інформаційні системи від атак, в яких робляться спроби викрадення за допомогою посередницьких операцій зчитування інформації. Тобто спроба несанкціонованого доступу до інформаційного потоку не може відбуватися без зчитування окремих фотонів, що є фізичною подією, і неминуче змінює фізичні параметри квантового середовища [1, 2]. Для того щоб обійти такі фізичні явища і залишитися непоміченими, кібершпигунам потрібно не тільки перехопити фотонні потоки, а й згенерувати їхній абсолютно однаковий за станом параметрів клон для його передачі наступному офіційному приймачу. Сама по собі ця задача викликає суттєві складнощі. Раніше вважалося, що це неможливо, але нещодавно було розроблено деякі методи і засоби створення клонів. Однак створити абсолютно співпадаючі за характеристиками прийнятий і переданий потоки в середовищі криптографічної інформації неможливо. Отже, для теоретично високонадійної схеми генерації передачі та обробки інформації, повністю захищеної від несанкціонованого доступу і випадково виникаючих помилок, можна застосовувати гібридні методи використання квантово-механічних явищ у поєднанні з інтелектуальною системою криптографічного захисту. Далі розглянуто кілька прикладів атак на криптографічні структури і методів протидії їм. Очевидно, що надійну роботу такої системи можна забезпечити тільки шляхом поєднання методів інтелектуального аналізу даних в інформаційних технологіях СППР. Для організації СППР у квантово-механічних системах передачі інформації пропонується використовувати уніфіковану нейронну мережу, яка могла б забезпечити автоматичний інтелектуальний режим аналізу стану системи. Такий аналіз дозволяє класифікувати сукупності поточних параметрів системи до рівня діагностики стану інформаційних потоків і висновків на основі такої діагностики з підтримкою прийняття рішення про якість та надійність переданої інформації. Подібна система в режимі OLAP (Online Analytical Processing) могла б забезпечити автоматичне керування процесом генерації та передачі інформації, без втручання людини реагуючи на критичні помилки або спроби несанкці-

онованого доступу шляхом злому системи. Ефект спостерігача [3] призводить до того, що спроба виміряти стан фотона неминуче викликає практично миттєву зміну цього стану. Спроба розпаралелювання фотона має такі самі наслідки. Це не може бути непоміченим при подальшому санкціонованому прийманні інформації.

Постановка задачі

Найчастіше відбуваються когерентні атаки. Зловмисник перехоплює потік фотонів, зчитує дані у випадковому базисі та застосовує перебір порівняння інформації. Якщо базис побітного порівняння вгадано, зловмисник генерує відповідний клоновий потік фотонів, надсилаючи його офіційному приймачу. Когерентність забезпечується збігом фаз перехоплених та згенерованих і відправлених офіційному приймачу фотонів. Розмір ключа, який використовується для шифрування, впливає на ефективність захисту, зменшуючи ймовірність злому коду зі збільшенням розміру ключа *N*. Якщо проводити побітне порівняння відправлених та прийнятих фотонів для *n*-бітів, то ймовірність виявлення зловмисника, який міг перехопити частину цих бітів, дорівнює $1-0,75^N$ [4]. Зазвичай з такими завданнями справляється протокол BB84. Під час колективних атак кожен фотон, отриманий від передавача, переплутується з фотонами, отриманими з квантових зразків. Внаслідок квантової заплутаності та побітного порівняння інформації зловмисник може визначити повний базис відправника. Якщо атака не є когерентною, то хакеру потрібно порівнювати кожен отриманий фотон в режимі перехоплення інформації та її відправлення клону.

Квантова заплутаність фотонів може бути забезпечена несепарабельним станом системи. Якщо 2-кубітна квантова система (для кубітів *A* і *B*) представлена вектором $|\phi\rangle \in C^4 = C^2 \otimes C^2$, то цей стан називається сепарабельним (не заплутаним) при виконанні рівності $|\phi\rangle = |\phi_1\rangle \otimes |\phi_2\rangle$ для існуючих станів $|\phi_1\rangle \in C^2$ кубіта *A* та $|\phi_2\rangle \in C^2$ кубіта *B*. У іншому разі цей стан є несепарабельним (заплутаним) [5, 6]. Властивість заплутаності (несепарабельності) фотонів у лініях передачі інформації може допомогти вирішити задачу непрозорих атак у разі перехоплення фотонів зловмисниками та відправки далі на приймач клонів таких заплутаних фотонів.

Нижче наведено приклад спроби застосування прозорої атаки для заплутаних фотонів.

Відправник	Випадковий біт	0	1	0	0
	Базис	+	×	×	×
	Поляризація	↑	↘	↗	↗
Хакер	Базис	+	+	+	×
	Поляризація	↑	→	→	↗
Отримувач	Базис	+	×	×	×
	Поляризація	↑	↗	↗	↗
Ключ	Спотворення	–	+	–	–
	Витік	+	–	–	+

Крім того, можливі атаки з осліпленням однофотонного детектора, під час яких кіберзлочинець зчитує інформацію передавача та відправляє її далі за допомогою дуже потужного імпульсу лазера. Такий прийом може призвести до того, що неідеальний детектор приймача сприйматиме імпульс без урахування ефекту

спостерігача. В цьому разі зчитування інформації доступне без санкції. Якщо перед детекторами встановлене випадкове джерело одиничних фотонів, то виникає можливість переконатися, що детектор не зчитує світлові сигнали, а працює в квантовому режимі, тобто завдяки виявленню квантових ефектів можливе виявлення кіберзлому [7, 8].

Цікавим є метод атаки з розділенням фотонів. За один такт передачі інформації може бути згенеровано кілька фотонів. Зазвичай генеруються лазерні світлодіоди малої потужності. Якщо виявиться, що фотонів більше двох, хакер зможе спробувати їх розділити, і виникне заплутаність з пробним фотоном. Незмінна частина даних передається отримувачу, а зловмисник має можливість отримати правильне значення переданого біта, не вносячи додаткових похибок у ключі при фільтрації. Це дозволяє йому залишатися непоміченим і перехоплювати інформацію [9, 10].

Вирішити проблеми, пов'язані з такою атакою, можна різними методами. Сьогодні успішно розробляються ідеальні джерела квантів з точно заданою кількістю генерацій на один такт і абсолютно схожими характеристиками фотонів необхідної потужності. До того ж удосконалюються протоколи, такі як BB84 або SARG04 [11–14].

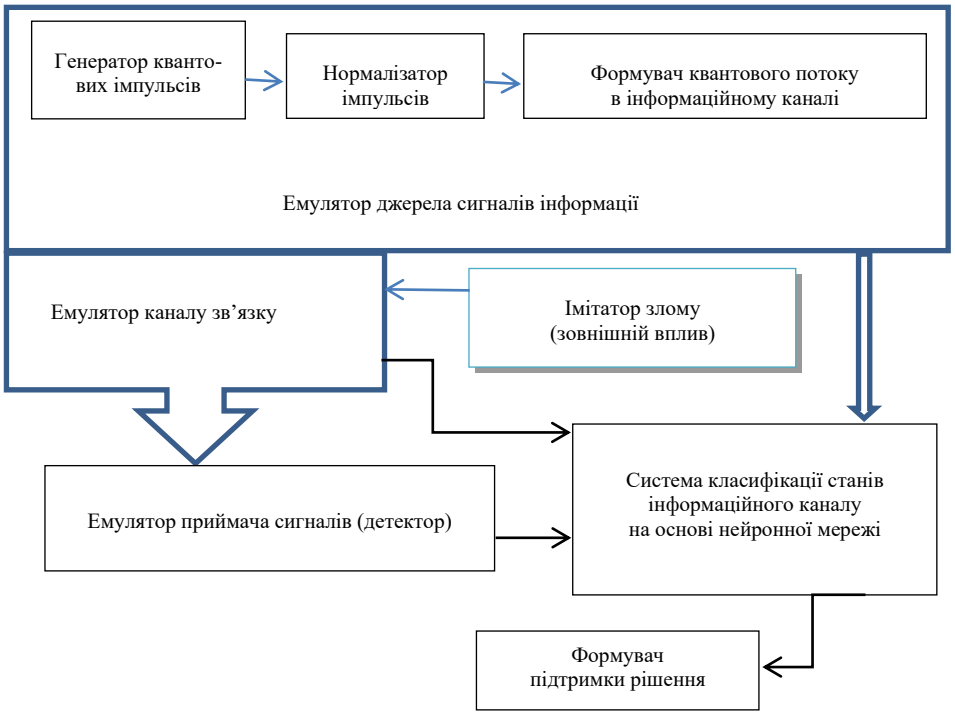
Крім описаних, існує багато інших випадків унікальних атак і процесів перетворення інформації [15]. Також необхідно враховувати, що можуть бути розроблені нові методи кіберзлому. Наразі відомо близько 20 типів таких атак, і кожного року їх кількість зростає приблизно на 20 %. Для квантової передачі інформації використовуються складні електронно-оптичні пристрої. Приховані та явні недоліки таких пристроїв також можуть представляти суттєву проблему для гарантування надійної та безпечної роботи квантових систем передачі інформації. У зв'язку з цим виникає необхідність розробити та впровадити методи детектування перетворення інформації або несанкціонованого доступу до неї, ідентифікації та класифікації в квантових лініях зв'язку і створення інформаційних технологій якісної підтримки прийняття рішень в автоматичному режимі щодо процесів передачі інформації. Одним із шляхів вирішення цих проблем може бути розробка технології інтелектуального аналізу даних на основі нейронних мереж, які могли б у режимі OLAP впоратися з класифікацією станів квантових потоків у реальному часі та забезпечити надійність і конфіденційність передачі цифрової інформації в квантовому режимі.

Вирішення поставленої задачі

Для розробки надійної системи класифікації стану лінії квантового передавання інформації пропонується створити емулятор, який зміг би віртуально уявити універсальну абстрактну систему генерації квантових сигналів, імітувати передачу квантової інформації у різних режимах і типові процеси спроб злому лінії передачі квантової інформації, а також розробити структуру нейронної мережі та математичний апарат обробки квантової інформації, яка змогла б підключатися до емулятора за допомогою універсального відкритого протоколу і виконувати обробку віртуальної інформації в активному OLAP-режимі. Необхідно також розробити інформаційну модель та методи навчання і експлуатації нейронної мережі для чіткої та достовірної класифікації стану ліній передачі інформації з метою вироблення рекомендацій у СППР щодо забезпечення надійності та конфіденційності даних. Водночас важливою задачею дослідження є визначення меж і характеристик роботи нейронної мережі та її можливостей обробки інформації в реальному часі й навчання на прикладах реальних ситуацій під час обробки інформації. На рисунку представлено структуру такої інформаційної СППР.

Емулятор джерела сигналів інформації забезпечує вхідний стан системи квантової передачі даних. Генератор квантових імпульсів імітує потоки фотонів, необхідних для формування *q*-бітів. Нормалізатор сигналів забезпечує заповнення множин вхідних станів, що відповідають процесу формування черги бітів за регістрами каналу зв'язку. Формувач квантового потоку в інформаційному каналі відповідає процесу модуляції або заповнення бітами цінної інформації, необхідної для передачі та формування ключів. Унаслідок цього емулятор джерела формує блок вхідної інформації каналу зв'язку та створює множини, що відображають атрибути *q*-бітів системи.

Емулятор каналу зв'язку переміщає потік бітів інформації між вхідними та вихідними регістрами, імітуючи процес проходження фотонів через оптоелектронні пристрої. Водночас програмні модулі блоку імітаторів злому або зовнішнього впливу та емулятора каналу зв'язку взаємодіють між собою, імітуючи зміну інформації у разі несанкціонованого доступу або небажаного зовнішнього впливу. Такі впливи формуються в програмному модулі імітації злому за алгоритмами, що відповідають описаним вище стратегіям несанкціонованого доступу або атак. Програмне забезпечення цієї частини системи передбачає наявність стандартного протоколу представлення та введення даних за зовнішніми алгоритмами, створеними експертами в галузі кібербезпеки. Чим більше стратегій атаки буде розглянуто, тим більш досконалою буде розроблювана СППР.



Емулятор приймача сигналів забезпечує формування множини станів регістрів каналу зв'язку у форматі, який дозволяє відобразити ці стани на інформаційну множину вхідних нейронів системи класифікації стану інформаційного каналу. Своєю чергою ця система програмно реалізує структуру нейронної мережі, яка має шар вхідних нейронів, проміжний шар нейронів для формування патернів типових станів та вихідний шар нейронів, який відображає класи в стані під час атак або небажаних перетворень інформації. Метою цього програмного модуля є діагностика каналу зв'язку з подальшим відображенням даних, отриманих класифікатором, на множину рекомендацій або рішень модуля формування підтримки рішень.

ISSN 2786-6491

Для формувача підтримки рішень розробляються уніфіковані протоколи керування пристроєм передачі даних. У протоколах регламентуються послідовність і критичні значення атрибутів та показників інформаційної системи, на які формується однозначна реакція.

Інформаційна ємність пропонованої СППР не перевищуватиме 100 типових алгоритмів стратегій атаки та стільки ж небажаних впливів перетворення інформації. Передбачається, що синхронізація та тривалість процесів інтелектуальної обробки інформаційних потоків не перевищуватимуть 50 мс на розряд каналу зв'язку. Таким чином, для 8-розрядного каналу реакція СППР регламентується від 400 мс до 1 с. Такі показники можуть не задовольнити багатьох потенційних користувачів, однак перспектива значного прискорення роботи нейронної мережі дуже обнадійлива і є предметом подальших досліджень.

Висновок

У зв'язку зі швидким розвитком цифрового середовища та інформатизації життєдіяльності постійно збільшується попит на гарантування кібербезпеки та захисту інформації. Практика показує, що абсолютно надійних систем не може бути в принципі. Найефективніше гарантування безпеки спостерігається в системах оптоелектронних засобів передачі та обробки інформації. Це пов'язано з унікальними можливостями фотонів як носіїв інформації. Водночас такі фізичні характеристики, як поляризація, квантова заплутаність і когерентність, дозволяють на фізичному рівні виявляти та ідентифікувати зміну властивостей носія інформації, хоча це не дає надії на абсолютний захист, оскільки хакери постійно вдосконалюють свої стратегії. Універсальне вирішення задачі гарантування кібербезпеки також неможливе.

Однак запропоновані метод та інформаційна технологія СППР у керуванні надійністю каналів квантової передачі інформації є одними з простих і ефективних рішень проблеми реагування на несанкціонований витік інформації в реальному часі. Важливо відзначити, що, використовуючи нейронну мережу для задач класифікації станів каналів зв'язку, можна необмежено навчати систему на практиці появи нових, таких що раніше не проявлялися, стратегій атаки з боку кіберзлочинців.

V. Zinchenko, V. Lyfar

INTELLIGENT ANALYSIS OF INFORMATION FLOWS IN QUANTUM INFORMATION TRANSMISSION SYSTEMS

Volodymyr Zinchenko

Institute of Telecommunications and Global Information Space of NAS of Ukraine, Kyiv,

zinchenko@outlook.com

Volodymyr Lyfar

Volodymyr Dahl East Ukrainian National University, Kyiv,

lifar@snu.edu.ua

The authors examined some possibilities and problems of information transmission systems based on quantum mechanical principles. Despite the apparent high reliability of optoelectronic systems that use coherent photons for secure transmission and information processing lines, methods and means of unauthorized access to transmitted, quantum information are theoretically possible and are constantly emerging. Previously, it was assumed that cryptography methods and algorithms provide a high level of reliability and security of information flows. However, with the emergence of more productive computing systems and especially quantum computers, it has

become possible to implement complex attack algorithms and methods for stealing keys and streaming information. In addition, known cryptography protocols were studied and subjected to «breakdowns» and decryption algorithms, which made previously reliable systems practically unworkable. The authors examined some types of attacks that are most promising for use by cybercrime. Certain properties of quantum optical systems make it possible to use certain physical principles to identify the state of photon flows and analyze changes in these states in order to determine the reliability and reliability of the transmitted information. At the same time, the authors suggest that a hybrid combination of analysis of the physical characteristics of quanta transmitted in a *q*-bit representation and reliable cryptographic protocols can significantly enhance the attributes of reliability and security of information. At the same time, the task is set to study some methods and systems of data mining on the possibility of application in reliable quantum systems to implement a decision support system on the reliability of quantum means of information transmission in OLTP mode. It is proposed to use means of preparing and processing information based on learning neural networks. It is necessary to find out the capabilities of neural networks to work in real time with complete synchronization of information flows and analysis of their states. Some types of attacks with photon separation, «quantum Trojan» and others are analyzed. Despite the security, in reality there are many possibilities for breakdowns in the structure of the quantum transmission channel itself, which does not guarantee complete confidentiality of information from cyber criminals.

Keywords: cryptography, quantum information, intelligent analysis, neural network, information protection, decision support, channel attack.

ПОСИЛАННЯ

1. Huang D., Chen Z., Guo Y., Lee M. Quantum secure direct communication based on chaos with authentication. *Journal of the Physical Society of Japan*. 2007. Vol. 76, N 12. P. 124001.
2. TLS (Channel SSP) changes in Windows 10 and Windows Server. Microsoft. Docs. 2018. [Electronic resource]. URL: https://docs.microsoft.com/en-us/windows-server/security/tls/tls-schannel-ssp-changes-in-windows-10-and-windowsserver (date of access: 09.05.2020)
3. Квантовый троян: «абсолютно защищенная» связь оказалась дырявой. РИА Новости. 2018. [Электронный ресурс]. URL: https://ria.ru/20181122/1533223834.html?utm_ource=news.mail.ru&utm_medium=region_informer&utm_campaign=rian_partners (дата обращения: 09.05.2020)
4. Василиу Е.В. Стойкость квантовых протоколов распределения ключей типа «приготовление–измерение». *Computer Sciences and Telecommunications*. 2007. № 2 (13). С. 52–64.
5. Стиб В.-Х., Харди Й. Задачи и их решения в квантовых вычислениях и квантовой теории информации. Ижевск : НИЦ «Регулярная и хаотическая динамика», 2007. 296 с.
6. Холево А.С. Квантовые системы, каналы, информация. М. : МЦНМО, 2010. 328 с.
7. Действительно ли надежна квантовая криптография? Блог компании Toshiba. 2019. [Электронный ресурс]. URL: https://habr.com/ru/company/toshibarus/blog/444502/ (дата обращения: 09.05.2020)
8. Lydersen L., Wiechers C., Wittmann C., Elser D., Scaar J., Makarov V. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature Photonics*. 2010. N 4. P. 686–689. DOI: https://doi.org/10.48550/arXiv.1008.4593
9. Bennett C., Brassard G. Quantum cryptography: public key distribution and coin tossing. Part 1. *Theoretical Computer Science*. 2014. Vol. 560. P. 7–11. DOI: https://doi.org/10.48550/arXiv.2003.06557
10. Brassard G., Lütkenhaus N., Mor T., Sanders B.C. Security aspects of practical quantum cryptography — EUROCRYPT 2000. Advances in Cryptology. *Lecture Notes in Computer Science*. Berlin, Heidelberg : Springer, 2000. Vol. 1807. P. 289–299.
11. Intallura P.M., Ward M.B., Karimov O.Z., Yuan Z.L., See P., Shields A.J., Atkinson P., Ritchie D.A. Quantum key distribution using a triggered quantum dot source emitting near 1.3 microns. *Applied Physics Letters*. 2007. Vol. 91. P. 161103. DOI: https://doi.org/10.48550/arXiv.0710.0565
12. Череданова Е.М., Мамченко Е.А., Марчук А.М., Речкунов А.А. Математическое моделирование квантового распределения ключа протокола BB84. *Политехнический молодежный журнал.* 2018. № 5. [Электронный ресурс]. URL: http://ptsj.ru/articles/319/319.pdf (дата обращения: 09.05.2020)
13. Scanari V., Acin A., Ribordi G., Gisin N. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulses implementations. *Physical Review Letters*. 2004. Vol. 92, N 5. P. 057901. DOI: https://doi.org/10.1103/PhysRevLett.92.057901
14. Aliev F.K., Borodin A.M., Vassenkov A.V., Matveev E.A., Tzarkov A.N., Sheremet I.A. ATF-technology of communication based on using the resource of entangled states of quantum systems. *Electromagnetic Waves and Electronic Systems*. 2015. Vol. 20, N 3. P. 60–72.
15. Самарцев В.В. Коррелированные фотоны и их применение. М. : ФИЗМАТЛИТ, 2014. 168 с.

Отримано 15.01.2024