масштабируемые сети, в том числе в существующую телекоммуникационную сеть.

Технология QKD находит своё применение в различных сферах. В первую очередь там, где важна высокая степень защиты информации. Например, банковский сектор, используя QKD для передачи финансовой информации гарантирует безопасность транзакций и предотвращение мошенничества, государственные органы применяя технологию квантового распределения ключей повышают защищённость передачи конфиденциальных данных, в телекоммуникации организуются защищённые линий связи, исключающие возможность несанкционированного прослушивания. Концепция квантового распределения ключей открывает новые горизонты в области информационной безопасности, предлагая надежный механизм защиты данных, не зависящий от вычислительных мощностей противника.

Список использованных источников

1.Zapatero V., Zhang Q., Weinfurter H. Advances in device-independent quantum key distribution //npj Quantum Inf. 2023. Vol. 9(10). pp. 105-117. DOI:10.1038/s41534-023-00684-x.

2.Колыхалов Г.А., Кравченко Е.Г. Интерпретация квантов энергии и массы фотона с позиций закона всемирного тяготения //Учёные записки КнАГТУ. 2025. №7(87). С. 109 – 114.

3.Кунуспаев Д.С., Шойынбек А. Роль квантовой криптографии в развитии цифровой экономики: исследование стойкости протоколов распределения ключей // Вестник науки. 2026. №2(95) том 1. С. 745 – 769.

5.Pittuluga M., Brzosko A., Long-distance coherent quantum communications in deployed telecom networks // Nature. 2025. Vol. 640. pp. 911-917. DOI:10.1038/s41586-025-08801-w.

Обласов Андрей Александрович, к.э.н., доцент, и. о. зав. каф. «Информационная безопасность автоматизированных систем», oblasov_andrei@mail.ru.
Воропаев Даниил Валерьевич, студ. каф. «Информационная безопасность автоматизированных систем», danvoron481@gmail.com.

УДК 519.7; 004.2; 004.3

О ВЫЧИСЛИТЕЛЬНЫХ УСТРОЙСТВАХ, ИСПОЛЬЗУЮЩИХ СХЕМУ QAM-OFDM МОДУЛЯЦИИ

В.П. Цветов
«Самарский национальный исследовательский университет имени академика С.П. Королёва», г. Самара

Ключевые слова: гибридные детерминированно-стохастические вычислительные системы, радио биты.

В докладе описывается модель вычислительных устройств, использующих в качестве элементной базы источники многочастотного электромагнитного излучения.

Обычно, под вычислительным устройством понимается специальным образом подобранная система взаимосвязанных материальных объектов и их контролируемо изменяемых и измеряемых характеристик, которые изоморфно отображаются на некоторую числовую алгебру или алгебраическую систему. Измеряемые характеристики играют роль элементов числовых множеств, а объекты роль алгебраических операций и отношений. Подобные системы предназначены для выполнения детерминированной последовательности преобразований начальных измеряемых характеристик в конечные, значения которых интерпретируются как входные данные и решение некоторой задачи (выходные данные), а сама последовательность как алгоритм этого решения. В более общем понимании алгоритма по Маркову [1] числовые множества могут быть заменены на множества слов над некоторым алфавитом, а операции набором формул подстановок. Различия между аналоговыми и цифровыми вычислительными устройствами определяются способами управления последовательностью преобразований, а их эффективность при решении конкретных задач – временем получения результата и объемом требуемых для этого материальных и энергетических ресурсов. Сами алгоритмы решения задач, которые реализуют вычислительные устройства, условно можно разбить на два класса – детерминированные и рандомизированные. К первому относятся те, при выполнении которых все измеряемые характеристики вычислительной системы однозначно определяются их начальными значениями. Ко второму – те, при выполнении которых часть измеряемых характеристик может изменяться случайным образом. Вообще говоря, только алгоритмы первого класса являются алгоритмами в классическом понимании. Конечность и корректность алгоритмов второго класса может быть оценена только с некоторой долей вероятности. Рандомизированные алгоритмы используются как альтернатива детерминированным тогда, когда они оказываются более эффективными при решении той или иной задачи [2-6]. В частности, при атаках на системы защиты информации, которые опираются на сложность решения задач факторизации целых чисел или дискретного логарифмирования, время получения результата является критически важным параметром. Рандомизированные алгоритмы могут быть реализованы, например, как с помощью случайного/псевдослучайного изменения измеряемых характеристик – модель вероятностной машины Тьюринга, так и за счет использования элементной базы измерение характеристик, которой возможно лишь с некоторой долей неопределенности и поэтому носит случайный характер – модель квантовой машины Тьюринга.

Модели вычислительных устройств принято описывать в терминах обработки слов над двухбуквенным алфавитом, общий элемент которого в зависимости от физической реализации принято называть битом (двоичной цифрой), *p*-битом (вероятностным битом), *q*-битом (квантовым битом).

Рассмотрим физическую реализацию бита в форме гармонического электромагнитного колебания, например, радиоволны, модель измерения характеристик которой в заданной точке пространства на временном интервале $[0,T]$ имеет вид $s(t) = r \cdot e^{\frac{i\omega t}{T}}$, где r можно трактовать как элемент двухэлементного множества $\{z_0, z_1\} \subset \mathbb{R}$ или случайные величины со значениями в этом множестве. Такой бит будем называть *r*-битом (радио битом) или *pr*-битом (вероятностным радио битом), когда r рассматривается как случайная величина. Если $r \in \{z_0, z_1\} \subset \mathbb{C}$, то подобную реализацию будем называть *r*-тетритом (двубитом). Аналогично определяются *m*-позиционные реализации $r \in \{z_0, z_1, .., z_{m-1}\} \subset \mathbb{R}$. *N*-разрядный регистр может быть реализован как сигнал, полученный с помощию технологии мультиплексирования цифровых потоков на основе ортогонального частотного разделения OFDM (Orthogonal frequency-division multiplexing) и квадратурной амплитудной модуляции QAM (Quadrature Amplitude Modulation) [7-8] в виде $s(t) = \sum_{k=0}^{N-1} z_k \cdot e^{\frac{i2\pi kt}{T}}$. Арифметические операции сложения и вычитания реализуемы измерениями в области интерференции, умножения – усилением сигнала или его поднесущих до мультиплексирования. Результирующий цифровой поток получается после регистрации значений на конечном наборе временных отсчетов $t_n = \frac{T}{N} \cdot n$, где $n \in 0..N-1$, и последующего применения той же схемы регистрации к сигналу $z(t) = \frac{1}{N} \sum_{k=0}^{N-1} s(t_k) \cdot e^{\frac{-i2\pi kt}{T}}$. Фазовые вращатели пригодны для реализации унитарных преобразований, рандомизация достигается наложением шумов.

Вопросы разработки конкретных архитектур процессоров и эффективных алгоритмов решения задач из класса NP для такого вида вычислительных устройств требуют отдельного изучения.

Список использованных источников

1.Марков, Андрей Андреевич. Теория алгорифмов, Тр. МИАН СССР, 42, Изд-во АН СССР, М.–Л., 1954, 3–375

2.Kolmogoroff, A. Zur Theorie der stetigen zuf˙alligen Prozesse // Math. Ann. 1933. Bd. 108, H. 1. S. 149-160.

3.Pollard, J. M. Theorems on factorization and primality testing. // Mathematical Proceedings of the Cambridge Philosophical Society. – 1974. – Vol. 76, no. 3. – P. 521. – doi:10.1017/S0305004100049252.

4.Solovay, Robert M. and Volker Strassen. A fast Monte-Carlo test for primality (англ.) // SIAM Journal on Computing[англ.] : journal. – 1977, submitted in 1974. – Vol. 6, no. 1. – P. 84-85. – doi:10.1137/0206006

5.Lenstra, Jr., H. W. Factoring integers with elliptic curves (англ.) // Annals of Mathematics : journal. – 1987. – Vol. 126, no. 2. – P. 649-673.

6.Shor, P. Algorithms for Quantum Computation: Discrete Logarithms and Factoring (англ.) // Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on – IEEE, 1994. – P. 124-134. – ISBN 0-8186-6580-7 – doi:10.1109/SFCS.1994.365700

7.Bahai, A., Saltzberg, B., Ergen, M. Multi-Carrier Digital Communications: Theory and Publications of OFDM // Springer, New york, 2004.

8.Hanzo, L, Webb, W., Keller, T. Single- and Multi-carrier Quadrature Amplitude Modulation // Wiley, New York, 2000.

Цветов Виктор Петрович, к.физ.-мат.наук, доцент, доцент каф. безопасности информационных систем, tsf-su@mail.ru.

УДК 004.942;004.414.23;004.056.53

МОДЕЛИРОВАНИЕ ПРОЦЕССОВ ОБЕСПЕЧЕНИЯ УСТОЙЧИВОСТИ ОБЛАЧНОЙ ИНФРАСТРУКТУРЫ ПРИ ОСУЩЕСТВЛЕНИИ КОМПЬЮТЕРНЫХ АТАК

А. В. Кулдыркаев, В. Е. Дементьев
Мордовский государственный университет имени Н. П. Огарева, г.Саранск

Ключевые слова: математическое моделирование**,** оценка защищенности, облачная инфраструктура, устойчивость инфраструктуры

Одной из важнейших особенностей современных информационных технологий является широкое применение виртуализации и облачных вычислений. Оборотной стороной этих решений является появление новых актуальных угроз безопасности, из-за чего возникает задача оценки устойчивости размещенных в облачной инфраструктуре объектов информатизации при реализации различных сценариев компьютерных атак [1]. Очевидно, что реализация критичных угроз не является единичным событием, а представляет собой многоэтапную последовательность действий злоумышленника.

В настоящей работе для оценки устойчивости размещенных в облачной инфраструктуре объектов предлагается использовать инструменты имитационного моделирования, позволяющие математически прогнозировать исходы компьютерных атак и эффективность средств защиты.