УДК 003.26 DOI:10.31854/1813-324X-2021-7-4-78-84

Система поддержки принятия решений для выбора оптимального постквантового механизма инкапсуляции ключей. Часть 2. Оценка прототипа

А.В. Власенко[1], **М.В. Евсюков**[1], **М.М. Путято**[1]*, **А.С. Макарян**[1]

[1]Кубанский государственный технологический университет,
Краснодар, 350072, Российская Федерация
*Адрес для переписки: putyato.m@gmail.com

Информация о статье
Поступила в редакцию 16.05.2021
Поступила после рецензирования 15.11.2021
Принята к публикации 30.11.2021

Ссылка для цитирования: Власенко А.В., Евсюков М.В., Путято М.М., Макарян А.С. Система поддержки принятия решений для выбора оптимального постквантового механизма инкапсуляции ключей. Часть 2. Оценка прототипа // Труды учебных заведений связи. 2021. Т. 7. № 4. С. 78–84. DOI:10.31854/1813-324X-2021-7-4-78-84

Аннотация: *В заключительной части цикла статей, посвященного разработке системы поддержки принятия решений для выбора оптимального постквантового механизма инкапсуляции ключей, произведено обоснование и оценка эффективности предложенной методики выбора оптимальной реализации постквантового криптографического алгоритма. Показана экономическая целесообразность предложенного подхода и продемонстрировано его положительное влияние на качество функционирования подсистемы криптографической защиты информации. Проведено сравнение эффективности разработанного прототипа системы поддержки принятия решений с существующими программными продуктами, направленными на поддержку принятия решений в области информационной безопасности. Выполнена проверка согласованности результатов работы прототипа системы поддержки принятия решений с выводами аналитических исследований в области постквантовой криптографии.*

Ключевые слова: *квантовый компьютер, информационная безопасность, постквантовая криптография, механизм инкапсуляции ключей, принятие решений, оценка эффективности, веб-приложение.*

Введение

В настоящее время усилия ведущих мировых исследовательских институтов и крупнейших технических корпораций направлены на изучение квантовых вычислений и создание полноценного квантового компьютера, способного решать прикладные задачи. Ожидается, что вычислительные возможности квантового компьютера позволят совершить прорыв в изучении искусственного интеллекта, физике, химии и многих других областях науки [1]. Тем не менее, с точки зрения информационной безопасности, важнейшей особенностью квантового компьютера является его исключительная эффективность как инструмента криптоанализа современных криптографических алгоритмов с открытым ключом, которая обусловлена квантовым алгоритмом Шора, разработанным в 1994 г. Данный алгоритм позволяет с полиномиальной сложностью решать задачи факторизации и дискретного логарифмирования (в том числе в группе точек эллиптической кривой) [2], на субэкспоненциальной сложности которых основана надежность современных асимметричных криптографических алгоритмов [3].

Таким образом, квантовый компьютер делает небезопасными все широко применяемые сегодня криптосистемы с открытым ключом. Данный факт поставил перед научным сообществом задачу поиска новых, постквантовых асимметричных криптографических алгоритмов, способных противостоять квантовому криптоанализу. В результате такие алгоритмы были разработаны и следующим шагом на пути внедрения постквантовой криптографии стал процесс принятия соответствующих стандартов. Данный процесс был инициирован

NIST и проводится в форме открытого для заявок и комментариев конкурса [4].

В момент написания данной статьи проходит 3-й этап конкурса, к началу которого был определен перечень алгоритмов-фаворитов, которые в наиболее полной мере отвечают требованиям, предъявляемым к постквантовому стандарту [5].

По сравнению с такими классическими асимметричными алгоритмами как, например, RSA или Elgamal, постквантовые криптосистемы характеризуются использованием сложных и ресурсоемких математических структур. Вследствие этого постквантовые алгоритмы уступают классическим при сравнении по различным метрикам производительности. Данный факт усложняет процесс внедрения новых алгоритмов, поскольку существенное повышение нагрузки на защищаемые информационные системы крайне нежелательно.

На конкурсе NIST представлено широкое разнообразие конкурирующих подходов к обеспечению безопасности. Конструкция и характеристики постквантовых алгоритмов существенно отличаются от заявки к заявке, что не позволяет выделить среди них безусловно лучшее решение, являющееся оптимальным для всех возможных сценариев применения [6].

Более того, каждый из заявленных алгоритмов имеет несколько различных реализаций, каждая из которых нацелена на определенный сценарий применения и задает собственный баланс между метриками безопасности и производительности.

Перечисленные выше особенности текущего состояния постквантовой криптографии делают актуальной задачу выбора оптимальной реализации постквантового криптографического алгоритма для защиты конкретной информационной системы. Данный тезис подтверждается отчетами NIST, в которых подчеркивается полезность дифференцированного подхода к выбору используемой криптосистемы. В зависимости от особенностей защищаемого канала связи, предпочтительным может быть применение алгоритма, отличного от того, который закреплен в стандарте [4].

Оценивается, что полноценный квантовый компьютер будет создан в течение ближайших 10 лет. За это время необходимо успеть не только принять постквантовые стандарты, но и внедрить новые алгоритмы в практическое использование. Например, внедрение симметричного алгоритма AES заняло более 5 лет, однако переход на новые асимметричные алгоритмы, электронные подписи и механизмы инкапсуляции ключей обещает быть более сложной задачей. В то же время, важно учитывать, что квантовый компьютер уже сейчас представляет угрозу для критически важной информации. Это связано с тем, что злоумышленник имеет возможность записать интересующие его данные и дешифровать их после появления полноценного квантового компьютера.

В связи с этим, задача внедрения постквантовых криптографических алгоритмов станет актуальной в ближайшем будущем. Именно поэтому цель предыдущей части цикла статей состояла в том, чтобы предложить алгоритм автоматизированного выбора оптимальной для конкретной информационной системы реализации постквантового криптографического алгоритма и разработать прототип системы поддержки принятия решений (СППР), использование которой позволило бы упростить внедрение постквантовых средств криптографической защиты информации в работу организации [7].

В результате, в предыдущей статье цикла был произведен выбор алгоритмов принятия решения для разрабатываемой системы, а также выполнена адаптация метода последовательных уступок в соответствии с особенностями рассматриваемой задачи. В качестве частных критериев для метода последовательных уступок предложено использовать метрики канала связи, которые затем выражены через характеристики методов инкапсуляции ключей. Сформирована база данных характеристик существующих реализаций механизмов инкапсуляции ключей. Выполнена практическая реализация прототипа поддержки принятия решения в форме веб-приложения [7].

Однако конкурентоспособность предложенного подхода требует обоснования. Для этого требуется провести оценку эффективности разработанной СППР с учетом существующих аналитических исследований в области постквантовой криптографии.

Для оценки эффективности предложенного подхода предполагается использовать следующие критерии:

– экономическая эффективность;

– повышение качества работы защищаемого сервиса;

– эффективность по сравнению с аналогичными системами;

– согласованность предлагаемых решений с результатами аналитических исследований в области постквантовой криптографии.

Экономическая эффективность

Предложенное решение позволяет оптимизировать сроки исполнения задач, связанных с разработкой программного продукта, использующего реализации криптографических алгоритмов, или сроки создания комплексной системы защиты информации для конкретного объекта информатизации.

В свою очередь, это приводит к следующим позитивным последствиям:

– получение конкурентного преимущества от максимально быстрого выпуска продукта, что позволяет избежать потери доли рынка из-за более

раннего выпуска аналогичного продукта конкурентами;

– более ранний выпуск продукта позволяет избежать упущенной за время простоя (невозможности выполнения критических функций) выгоды;

– снижение вероятности нарушения сроков выполнения проекта и, следовательно, потери доверия со стороны заказчиков;

– своевременное достижение целей позволяет избежать нарушения сроков выполнения зависимых задач.

С точки зрения бизнеса, более быстрый выпуск продукта позволяет уменьшить такие показатели эффективности как «Time to Market» и «Cost of Delay» [8]. Концепция показателя «Cost of Delay» проиллюстрирована на рисунке 1.

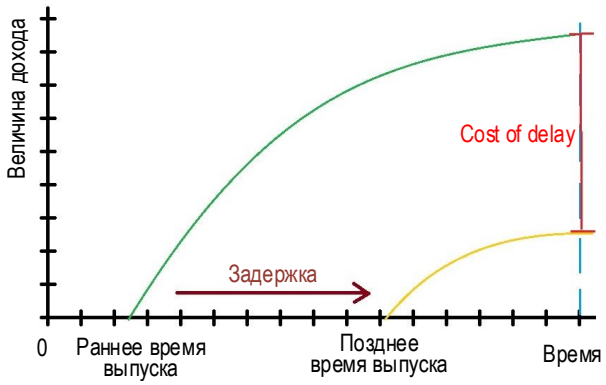

Рис. 1. Иллюстрация концепции показателя «Cost of Delay»

Fig. 1. Illustration of the "Cost of delay" Metric Concept

Однако коммерческая выгода от использования предложенной СППР не исчерпывается оптимизацией сроков исполнения задач. Другая важная составляющая экономического эффекта – экономия времени специалистов, задействованных в проектировании системы, использующей реализации постквантовых криптографических алгоритмов.

Задача разработанного прототипа СППР – предложить оптимальную реализацию постквантового механизма инкапсуляции ключей для использования в информационной системе, обладающей указанными пользователем набором характеристик. Таким образом, с экономической точки зрения, эффективность разработанной программы можно выразить как экономию ресурсов и времени специалистов, которое расходуется на принятие решения при неавтоматизированном выборе реализации постквантового алгоритма.

Для того, чтобы сделать обоснованный выбор, специалистам необходимо детально изучить свойства и особенности каждой реализации алгоритма и принять решение о том, какая из них наиболее полно соответствует требованиям системы. Однако разработанное приложение использует указываемые пользователем характеристики защищаемой системы для того, чтобы предложить оптимальную реализацию постквантового алгоритма, что существенно снижает издержки на принятие решения.

Реализованный в прошлой части цикла статей подход к решению задачи выбора оптимального средства защиты заключается в формализованном представлении характеристик криптографических алгоритмов и свойств защищаемых разновидностей информационных систем. Далее эти сведения используются для того, чтобы для указанной информационной системы предложить рейтинг оптимальных реализаций постквантовых механизмов инкапсуляции ключей [7].

Таким образом, можно сказать, что работа специалистов, занимающихся развитием конкретной информационной системы, направленная на анализ реализаций постквантовых алгоритмов, заменяется работой создателей СППР, направленной на имплементацию алгоритма принятия решений и настройку параметров системы. Преимущество такого подхода заключается в том, что СППР разрабатывается в форме веб-приложения, что позволяет многократно использовать ее неограниченно большому кругу пользователей. Кроме того, при изменении предметной области, а именно набора алгоритмов или характеристик реализаций, параметры системы могут быть актуализированы.

Повышение качества работы защищаемого сервиса

Обязательность внедрения постквантовой криптографии обусловлена необходимостью поддержания безопасности информационных систем на должном уровне после появления угрозы нового поколения – квантового компьютера. Для достижения этой цели неизбежен переход к использованию более сложных и ресурсоемких алгоритмов, ввиду чего становится актуальной задача сохранения производительности работы сервисов на максимально возможном уровне.

Неоптимальный, с точки зрения производительности, выбор криптографического алгоритма способен привести к возникновению следующих нежелательных технических проблем в работе сервиса:

– чрезмерное расходование вычислительных ресурсов вплоть до прихода сервиса в состояние «отказ в обслуживании»;

– повышение частоты сбоев из-за повышенной нагрузки, т. е. уменьшение средней доступности;

– увеличение времени отклика сервиса;

– уменьшение полезной пропускной способности (увеличение количества служебного трафика).

Перечисленные выше проблемы, в свою очередь, способны привести к следующим последствиям для владельца сервиса:

– потеря пользователей;

– необходимость материальных затрат на увеличение доступной вычислительной мощности;

– наступление последствий нарушения штатного режима работы объектов критической информационной инфраструктуры;

– нарушение утвержденного соглашения об уровне услуг.

Например, для провайдеров информационных услуг критически важно поддержание показателей уровня обслуживания (SLI, *аббр. от англ.* Service Level Indicator) в соответствии с обозначенным целевым уровнем обслуживания (SLO, *аббр. от англ.* Service Level Objectives) [9]. Обычно допускается, что реальные SLI могут отклоняться от SLO не более, чем на некоторую допустимую величину (*от англ.* Error Budget). Выход данных показателей за установленный предел может привести к нарушению критических функций бизнеса, потере клиентов и утрате конкурентного преимущества. Также это способно повлечь за собой нарушение договорных обязательств перед клиентами, а именно соглашения об уровне оказываемых услуг (SLA, *аббр. от англ.* Service Level Agreement) и, следовательно, юридические последствия и штрафы.

Таким образом, правильный выбор криптографического алгоритма способен упростить переход на постквантовую криптографию, минимизировать риски, избежать лишних материальных затрат и обеспечить максимально качественный пользовательский опыт. Дополнительным преимуществом оптимизации использования располагаемых вычислительных ресурсов компании является минимизация расходов на модернизацию информационной системы, потребность в которой может возникнуть в результате перехода на новые криптографические алгоритмы.

Эффективность по сравнению с аналогичными системами

Проблема выбора набора средств защиты информации, соответствующего требованиям конкретного объекта информатизации и обеспечивающего достаточную защиту, в условиях ограниченности ресурсов – важная задача в сфере информационной безопасности, которая является предметом большого числа исследований. Например, в [10] на основе модели целочисленного программирования разрабатывается прототип инструмента поддержки принятия решения, нацеленный на оптимизацию портфеля средств управления безопасностью организации, в который входят элементы управления оборудованием, ПО, политиками, процедурами и учебными мероприятиями. В [11] разрабатывается компьютерная СППР, а также ее методическое обеспечение выбора вариантов систем информационной безопасности коммерческих организаций на основе предложенных критериев (и шкал их измерений), не сводимых к одному критерию. При этом, в качестве теоретической базы используются исследования работы ведущих отечественных и зарубежных специалистов в области многокритериального принятия решений. В [12] с целью повышения эффективности системы обеспечения информационной безопасности разрабатываются механизмы интеллектуализации процессов защиты информации. В качестве теоретического базиса выступают методы системного анализа, математического моделирования, нечеткой логики и теории принятия решений.

Как было показано ранее, проблема выбора оптимального средства защиты особенно актуальна для постквантовой криптографии, но на данный момент отсутствуют программные средства, осуществляющие поддержку решения данной задачи. К настоящему моменту созданы программные библиотеки, предлагающие разработчикам ПО широкое разнообразие реализаций постквантовых криптографических алгоритмов, например, OpenSSL [13]. Однако пользователю зачастую неясно, какая конкретная реализация способна наилучшим образом удовлетворить его требования. Таким образом, присутствует потребность в дополнении имеющегося разнообразия криптосистем руководством или информационным ресурсом, облегчающим выбор наиболее подходящего.

В контексте сравнения с другими системами поддержки принятия решений в области информационной безопасности разработанный подход обладает следующими преимуществами:

– ориентированность на задачу (пользователю достаточно указать характеристики системы и целевой уровень защиты, чтобы получить рейтинг наиболее подходящих реализаций);

– возможность актуализации сведений о реализациях постквантовых алгоритмов с учетом актуальных исследований;

– легкость «доставки» веб-приложения до пользователей;

– интерактивность;

– фокус на решении конкретной задачи.

Согласованность предлагаемых решений с результатами аналитических исследований

Важнейшим критерием корректности работы любой СППР является согласованность с результатами актуальных исследований в соответствующей предметной области. Сравнительный анализ результатов работы СППР и результатов аналитических исследований в сфере постквантовой криптографии [14–18] представлена в таблице 1. Здесь видно, что наиболее оптимальные для конкретных сценариев применения, согласно аналитических исследований, постквантовые механизмы инкапсуляции ключей находятся на первых местах в рейтинге, составленном СППР. Это свидетельствует о том, что результаты работы СППР согласуются с выводами аналитических исследований в области постквантовой криптографии.

ТАБЛИЦА 1. Сравнительный анализ результатов работы СППР и результатов аналитических исследований

TABLE 1. Comparative Analysis of the Results of the Work of the Decision Support System and the Results of Analytical Studies in the Field

Способ управления ключами	Характеристики				Уровень безопасности	Лучший алгоритм на основе исследований	Место в рейтинге, составленном СППР
	клиента		сервера				
	Тип	Канал связи	Тип	Количество подключений			
Эфемерный	Ноутбук	Узкий	ПК	Высокое	AES-512	NTRU	1
Эфемерный	ПК	Узкий	Промышленный	Среднее	AES-128	SIKE	2
Эфемерный	Смартфон	Узкий	Микрокомпьютер	Среднее	AES-128	Round5	1
Повторная отправка	Смартфон	Средний	ПК	Высокое	AES-256	Saber	1
Кеширование на стороне клиента	ПК	Широкий	Промышленный	Низкое	AES-256	FrodoKEM	2

Также из таблицы 1 видно, что лучший, согласно исследованиям, алгоритм не всегда находится на первом месте. Это связано с тем, что, как было обозначено в предыдущей части цикла статей, разрабатываемая СППР способна учесть только формализуемые параметры криптосистем, в частности, их количественные метрики, связанные с безопасностью и производительностью. В то же время, в аналитических исследованиях принимаются во внимание более тонкие особенности каждого алгоритма, которые не всегда возможно учесть при автоматизированном принятии решения.

Именно поэтому пользователю системы предлагается не единственный «лучший» алгоритм, а рейтинг альтернатив, составленный по убыванию характеристик алгоритмов, связанных с безопасностью и производительностью. Информация о неформализованных свойствах алгоритмов предоставляется в форме справочной информации [7].

Заключение

Предложенный в [7] подход продемонстрировал свою эффективность в обеспечении информационной поддержки задачи внедрения постквантовых средств криптографической защиты в рамках организации, которая является одной из наиболее актуальных проблем современной информационной безопасности.

К недостаткам представленного подхода можно отнести необходимость корректной настройки параметров системы экспертами, а также потребность в постоянной актуализации сведений о реализациях криптографических алгоритмов. Также, в работе системы используется ряд допущений, в частности, все многообразие реальных вычислительных машин представлено набором абстрактных устройств. Кроме того, при составлении рейтинга альтернатив принимаются во внимание только формализованные характеристики алгоритмов.

Список используемых источников

1. Гринштейн Д., Зайонц А. Квантовый вызов. Современные исследования оснований квантовой механики. М.: Изд-во Интеллект, 2012. 432 с.
2. Shor P. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer // SIAM Journal on Scienticand Statistical Computing. 1997. Vol. 26. Iss. 5. PP. 1484–1509. DOI:10.1137/S0097539795293172
3. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Изд-во Триумф, 2002. 815 с.
4. NIST Report. Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standartization Process. Gaithersburg: NIST, 2016. 25 p.
5. Alagic G., Alperin-Sheriff J., Apon D., et al. Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process. Gaithersburg: NIST, 2020. 39 p.
6. Alagic G., Alperin-Sheriff J., Apon D., et al. Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process. Gaithersburg: NIST, 2019. 27 p.
7. Власенко А.В., Евсюков М.В., Путято М.М., Макарян А.С. Система поддержки принятия решений для выбора оптимального постквантового механизма инкапсуляции ключей. Часть 1. Алгоритм принятия решений // Труды учебных заведений связи. 2020. Т. 6. № 4. С. 70–79. DOI:10.31854/1813-324X-2020-6-4-70-79
8. Larson E., Gray C. Project Management: The Managerial Process. NY: McGraw-Hill Education, 2017. 688 p.
9. Wetzstein B., Karastoyanova D., Leymann F. Towards Management of SLA-Aware Business Processes Based on Key Performance Indicators // Proceedings of the 9th Workshop on Business Process Modeling Development and Support (BPMDS'08 Montpellier, France, 16–17 June 2008). URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.623.3105&rep=rep1&type=pdf (дата обращения 14.05.2021)
10. Almeida L., Respicio A. Decision support for selecting information security controls // Journal of Decision Systems. 2018. Vol. 27. No. S1. PP. 173–180. DOI:10.1080/12460125.2018.1468177
11. Рагозин Ю.Н. Система поддержки принятия управленческих решений при выборе вариантов информационной безопасности. М.: ГОУ МГИУ, 2011. 23 с.

12. Рахимов Е.А. Модели и методы поддержки принятия решений в интеллектуальной системе защиты информации. Уфа: УГАТУ, 2006. 21 с.
13. OpenSSL. Cryptography and SSL/TLS Toolkit. URL: https://www.openssl.org (дата обращения 14.11.2021)
14. Луценко М.С., Киян А.С., Кузнецова Т.Ю., Кузнецов А.А. Анализ и сравнительные исследования кодовых схем инкапсуляции ключей, представленные на конкурсе NIST PQC // Всеукраинский межведомственный научно-технический сборник «Радиотехника». 2018. № 193. URL: https://nure.ua/wp-content/uploads/2018/Scientific_editions/rvmnts_2018_193_8.pdf (дата обращения 14.11.2021)
15. Moody D. Round2 of the NIST PQC "Competition" what was NIST thinking? // The 10th International Conference on Post-Quantum Cryptography (PQCrypto 2019), Chongqing, China, 8–10 May 2019. URL: https://csrc.nist.gov/CSRC/media/Presentations/Round-2-of-the-NIST-PQC-Competition-What-was-NIST/images-media/pqcrypto-may2019-moody.pdf (дата обращения 03.11.2020)
16. Baan H., Bhattacharya S., Fluhrer S., et al. Round5: KEM and PKE based on (Ring) Learning with Rounding // Round 5. URL: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-2-Submissions (дата обращения 14.11.2021)
17. Власенко А.В., Евсюков М.В., Путято М.М., Макарян А.С. Исследование реализации механизмов инкапсуляции ключей постквантовых криптографических методов // Прикаспийский журнал: управление и высокие технологии. 2019. № 4. С. 121–127. DOI:10.21672/2074-1707.2019.48.4.121-127
18. Nist software perfomance tests // SAFEcrypto. URL: https://www.safecrypto.eu/pqclounge (дата обращения 14.11.2021)

* * *

Decision Support System for Finding an Optimal Postquantum Key Encapsulation Mechanism. Part 2. Prototype Evaluation

A. Vlasenko[1], **M. Evsyukov**[1], **M. Putyato**[1], **A. Makaryan**[1]

[1]Kuban State Technological University,
Krasnodar, 350072, Russian Federation

Article info
DOI:10.31854/1813-324X-2021-7-4-78-84
Received 16th May 2021
Revised 15th November 2021
Accepted 30th November 2021

For citation: Vlasenko A., Evsyukov M., Putyato M., Makaryan A. Decision Support System for Finding an Optimal Postquantum Key Encapsulation Mechanism. Part 2. Prototype Evaluation. *Proc. of Telecom. Universities.* 2021;7(4): 78–84. (in Russ.) DOI:10.31854/1813-324X-2021-7-4-78-84

Abstract: *This is the final part of the series of articles devoted to the development of a decision support system for choosing the optimal post-quantum key encapsulation mechanism. Efficiency of the methodology proposed for choosing the optimal implementation of the post-quantum cryptographic algorithm is evaluated and substantiated. The economic feasibility of approach is shown and its positive impact on the quality of the cryptographic information protection subsystem is demonstrated. Efficiency comparison of the prototype of the decision support system with existing software products aimed at supporting decision-making in the field of information security is carried out. The consistency of prototype's recommendations with the conclusions of analytical studies in the field of post-quantum cryptography is checked.*

Keywords: *quantum computer, information security, postquantum cryptography, key encapsulation mechanism, decision making, efficiency estimation, web-application.*

References

1. Grinshteyn D., Zayonz A. *Quantum Challenge. Modern Research of Quantum Mechanic's Basics*. Moscow: Intellect Publ.; 2012. 432 p. (in Russ.)
2. Shor P. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Scienticand Statistical Computing*. 1997;5(26):1484–1509. DOI:10.1137/S0097539795293172
3. Schneier B. *Applied Cryptography. Protocols, Algorthms, and Source Code*. Moscow: Triumph Publ.; 2002. 815 p. (in Russ.)

4. *NIST Report. Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standartization Process*. Gaithersburg: NIST; 2016. 25 p.
5. Alagic G., Alperin-Sheriff J., Apon D.et al. *Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process*. Gaithersburg: NIST; 2020. 39 p.
6. Alagic G., Alperin-Sheriff J., Apon D.et al. *Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process*. Gaithersburg: NIST; 2019. 27 p.
7. Vlasenko A., Evsyukov M., Putyato M., Makaryan A. Decision Support System for Finding an Optimal Postquantum Key Encapsulation Mechanism. Part 1. Decision Making Algorithm. Proc. of Telecom. Universities. 2020;6(4):70–79. (in Russ.) DOI:10.31854/1813-324X-2020-6-4-70-79
8. Larson E., Gray C. *Project Management: The Managerial Process.* NY: McGraw-Hill Education; 2017. 688 p.
9. Wetzstein B., Karastoyanova D., Leymann F. Towards Management of SLA-Aware Business Processes Based on Key Performance Indicators. *Proceedings of the 9th Workshop on Business Process Modeling Development and Support, BPMDS'08, 16–17 June 2008, Montpellier, France*. Available from: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.623.3105&rep=rep1&type=pdf [Accessed 14 May 2021]
10. Almeida L., Respicio A. Decision support for selecting information security controls. *Journal of Decision Systems*. 2018;27(S1):173–180. DOI:10.1080/12460125.2018.1468177
11. Ragozin Y. *Management Decision Support System for Choosing Information Security Options*. Moscow: Moscow State Industrial University Publ.; 2011. 23 p. (in Russ.)
12. Rahimov E. *Models and Methods of Decision Support in an Intelligent Information Security System*. Ufa: Ufa State Aviation Technical University Publ.; 2006. 21 p. (in Russ.)
13. OpenSSL. Cryptography and SSL/TLS Toolkit. Available from: https://www.openssl.org/ [Accessed 14th November 2021]
14. Lucenko M.S., Kiyan A.S., Kuznetsova T.U., Kuznetsov A.A. Analysis and Comparative Studies of Key Encapsulation Code Schemes Presented at the NIST PQC Competition. *All-Ukrainian Interdepartmental Scientific and Technical Collection "Radiotekhnika"*. 2018;193. (in Russ.) Available from: https://nure.ua/wp-content/uploads/2018/Scientific_editions/rvmnts_2018_193_8.pdf [Accessed 14th November 2021]
15. Moody D. Round2 of the NIST PQC "Competition" what was NIST thinking? // The 10th International Conference on Post-Quantum Cryptography (PQCrypto 2019), Chongqing, China, 8–10 May 2019. URL: https://csrc.nist.gov/CSRC/media Presentations/Round-2-of-the-NIST-PQC-Competition-What-was-NIST/images-media/pqcrypto-may2019-moody.pdf [Accessed 3rd November 2020]
16. Baan H., Bhattacharya S., Fluhrer S. et al. Round5: KEM and PKE based on (Ring) Learning with Rounding // Round 5. Available from: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-2-Submissions [Accessed 14th November 2021]
17. Vlasenko A.V., Evsyukov M.V., Putyato M.M., Makaryan A.S. Research of Key Encapsulation Mechanisms Based on Postquantum Cryptographic Algorithms. Caspian journal: Management and High Technologies. 2019;4(48):121–127. (in Russ.) DOI:10.21672/2074-1707.2019.48.4.121-127
18. Nist software perfomance tests. SAFEcrypto. Available from: https://www.safecrypto.eu/pqclounge [Accessed 14th November 2021]

Сведения об авторах:

ВЛАСЕНКО Александра Владимировна — кандидат технических наук, профессор, заведующая кафедрой «Компьютерных технологий и информационной безопасности» Кубанского государственного технологического университета, alex_vlasenko@list.ru
https://orcid.org/0000-0002-4134-4980

ЕВСЮКОВ Михаил Витальевич — аспирант кафедры «Компьютерных технологий и информационной безопасности» Кубанского государственного технологического университета, michael.evsyukov@gmail.com

ПУТЯТО Михаил Михайлович — кандидат технических наук, доцент, доцент кафедры «Компьютерных технологий и информационной безопасности» Кубанского государственного технологического университета, putyato.m@gmail.com
https://orcid.org/0000-0001-9974-7144

МАКАРЯН Александр Самвелович — кандидат технических наук, доцент, доцент кафедры «Компьютерных технологий и информационной безопасности» Кубанского государственного технологического университета, msanya@yandex.ru
https://orcid.org/0000-0002-1801-6137