ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

DOI 10.21672/2074-1707.2019.48.4.121-127
УДК 004.056

ИССЛЕДОВАНИЕ РЕАЛИЗАЦИИ МЕХАНИЗМОВ ИНКАПСУЛЯЦИИ КЛЮЧЕЙ ПОСТКВАНТОВЫХ КРИПТОГРАФИЧЕСКИХ МЕТОДОВ

Статья поступила в редакцию 18.11.2019, в окончательном варианте – 25.11.2019.

Власенко Александра Владимировна, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
кандидат технических наук, доцент, заведующая кафедрой компьютерных технологий и информационной безопасности Института информационных технологий и безопасности, e-mail: Vlasenko@kubstu.ru

Евсюков Михаил Витальевич, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
студент, e-mail: michael.evsyukov@gmail.com

Путято Михаил Михайлович, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
кандидат технических наук, доцент, e-mail: putyato.m@gmail.com

Макарян Александр Самвелович, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
кандидат технических наук, доцент, e-mail: msanya@yandex.ru

Стремительный прогресс в исследовании и построении квантовых компьютеров приводит к необходимости замены уже в ближайшем будущем используемых алгоритмов асимметричной криптографии на те, которые способны обеспечить устойчивость к квантовому криптоанализу. Учитывая, что внедрение таких алгоритмов обещает занять продолжительное время, неотложным становится вопрос утверждения постквантовых стандартов. Однако задача выбора алгоритмов на их роль значительно осложняется неоднородностью математической природы постквантовых криптосистем. Нередко сравнение двух алгоритмов по разным критериям может приводить к противоположным результатам оценки. В связи с этим в статье предлагается единая система критериев оценки постквантовых механизмов инкапсуляции симметричного ключа. Её задача – привести известные свойства каждой криптосистемы, связанные с безопасностью, производительностью и гибкостью к такой форме, которая позволяет провести объективное сравнение алгоритмов между собой. Указанная система критериев была применена для анализа алгоритмов-кандидатов на роль постквантового стандарта механизма инкапсуляции ключей, прошедших во второй тур конкурса NIST. В ходе анализа удалось не только выделить алгоритмы, использование которых на данный момент представляется наиболее предпочтительным, но также сформулировать некоторые рекомендации, направленные на повышение эффективности дальнейшего анализа алгоритмов. В частности, перечислены наборы алгоритмов, которые, может быть, целесообразно объединить. Кроме того, на основе проведённого анализа раскрыт характер взаимных зависимостей между группами критериев оценки алгоритмов. Использованный набор критериев и подход к сравнению методов инкапсуляции ключей могут быть легко адаптированы для проведения аналогичного анализа кандидатов на роль постквантового стандарта электронной цифровой подписи или алгоритма шифрования.

Ключевые слова: квантовый компьютер, шифрование, защита информации, асимметричная криптография, криптоанализ, анализ, кибербезопасность, гибридные криптосистемы

RESEARCH OF KEY ENCAPSULATION MECHANISMS BASED ON POSTQUANTUM CRYPTOGRAPHIC ALGORITHMS

The article was received by the editorial board on 18.11.2019, in the final version 25.11.2019.

Vlasenko Alexandra V., Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,
Cand. Sci. (Engineering), Associate Professor, Head of the Department of Computer Technologies and Information Security of the Institute of Information Technology and Security, e-mail: Vlasenko@kubstu.ru

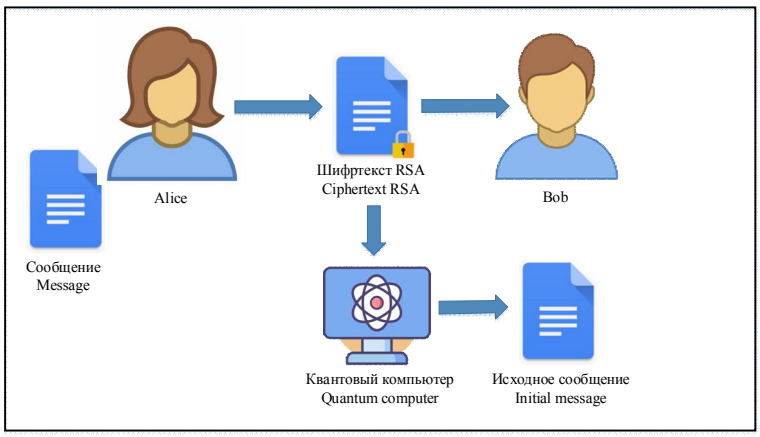
Evsyukov Michael V., Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,
student, e-mail: michael.evsyukov@gmail.com

Putyato Michael M., Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,
Cand. Sci. (Engineering), Associate Professor, e-mail: putyato.m@gmail.com
Makaryan Alexander S., Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,
Cand. Sci. (Engineering), Associate Professor, e-mail: msanya@yandex.ru

Rapid progress in the study and construction of quantum computers leads to the need of quick replacement of the current asymmetric cryptography algorithms with those that are capable of providing resistance to quantum cryptanalysis. Since their implementation is certain to take a long time, the approval of post-quantum standards becomes an urgent issue. However, the task of choosing algorithms to serve as standards is significantly complicated by heterogeneity of the mathematical nature of post-quantum cryptosystems. A comparison of two algorithms by different criteria can often lead to opposing evaluation results. In this regard, the article proposes a unified system of criteria for evaluating the post-quantum key encapsulation mechanisms. Its purpose is to bring each cryptosystem's properties related to security, performance and flexibility to a form that allows an objective comparison of algorithms. The specified system of criteria was used to analyze candidate algorithms for the role of the post-quantum key encapsulation mechanism standard that have passed to the second round of the NIST contest. During the analysis, it was possible not only to identify the algorithms, the use of which, at the moment, seems to be the most preferable, but also to formulate some recommendations aimed at improving the efficiency of further analysis of the algorithms. In particular, sets of algorithms that may be appropriate to combine into one were listed. In addition, based on the analysis, the nature of the mutual dependencies between the groups of criteria for evaluating the algorithms is revealed. The set of criteria used and the approach to comparing key encapsulation methods can be easily adapted for a similar analysis of candidates for the role of a post-quantum standard for digital signature or encryption algorithm.

Key words: quantum computer, encryption, information security, asymmetric quantum-resistant cryptography, cryptoanalysis, analysis, cyber security

Графическая аннотация (Graphical annotation)



Введение. В последние годы всё заметнее становятся успехи в области исследования и производства квантовых компьютеров – вычислительных устройств, использующих квантовые явления «запутанности» и неопределённости для повышения эффективности обработки данных. Благодаря реализации принципиально новых вычислительных механизмов, при решении определённых типов задач они демонстрируют экспоненциально более высокую производительность по сравнению с классическими компьютерами.

Одним из важнейших примеров превосходства квантового компьютера является алгоритм Шора, позволяющий решать такие математические задачи, как дискретное логарифмирование, факторизация и дискретное логарифмирование в группе точек эллиптической кривой с полиномиальной сложностью [6], в то время как их расчёт на классическом компьютере, при правильно подобранных параметрах, может занимать десятилетия. Поскольку именно вычислительная сложность этих задач обеспечивает безопасность современных криптосистем с открытым ключом, с практической точки зрения это означает их абсолютную неспособность противостоять криптоаналитическим атакам, которые задействуют квантовый компьютер.

Появление данной угрозы привело к необходимости разработки новых криптографических систем с открытым ключом. Оценивается, что полноценный квантовый компьютер будет создан в течение ближайших 20 лет [3]. Это означает, что внедрение криптографии нового поколения – более срочная задача, чем перевод асимметричных криптосистем на ключи большей длины, который должен

периодически происходить ввиду эволюционного развития классических вычислительных устройств. Данный факт, а также предполагаемая длительность перехода на постквантовую криптографию и возможность записи трафика злоумышленником для последующего расшифрования делают разработку и использование новых стандартов и технологий еще более актуальными, чем раньше.

К постквантовым криптосистемам предъявляется большой набор сложно выполнимых требований. Они должны не только надёжно защищать информацию от всевозможных методов классического и квантового криптоанализа, но и быть совместимыми с существующими протоколами и приложениями, поскольку необходимость их основательного перестроения, деградация скорости работы или повышение ресурсоёмкости как следствие внедрения новых криптосистем крайне нежелательны.

В связи с этим NIST (Национальный институт стандартов и технологий США) инициализировал процесс выбора алгоритмов на роль постквантовых криптографических стандартов электронно-цифровой подписи, алгоритма асимметричного шифрования (ААШ) и механизма инкапсуляции ключей (МИК). Для каждого из этих механизмов планируется выбрать как минимум по одному алгоритму [7].

Стандарты NIST имеют определяющее значение для криптографии во всём мире, поскольку многие зарубежные и международные организации, включая крупные банки и удостоверяющие центры, используют криптографические алгоритмы, стандартизованные NIST.

Тем не менее существует ряд причин, усложняющих процесс стандартизации:

1) требования к асимметричным криптосистемам и цифровым подписям сложнее, чем к симметричным алгоритмам и алгоритмам хеширования;

2) недостаток научного понимания ожидаемой мощности квантового компьютера;

3) математическое обеспечение и принципы работы некоторых алгоритмов задают разные свойства и параметры их функционирования, в связи с этим отсутствует возможность их прямого сравнения.

Вследствие этого NIST активно использует поддержку научного сообщества в процессе разработки критериев и оценке алгоритмов. В результате на конкурс потенциальных постквантовых стандартов было подано 82 заявки, из которых 69 удовлетворили основным требованиям NIST и были допущены в первый тур. В это же время на конкурс AES было подано 15 заявок, а на конкурс SHA-3 – 51.

В ходе первого тура 5 заявок были отозваны заявителями, 16 – взломаны или успешно атакованы, 13 – не смогли предоставить достаточно убедительного доказательства безопасности, некоторые похожие заявки были объединены. В итоге 26 кандидатов, 17 из которых – алгоритмы асимметричного шифрования и инкапсуляции ключей, а 9 – схемы цифровой подписи, успешно прошли во второй тур [4].

Во втором туре NIST уделяет больше внимания производительности программных и аппаратных реализаций, а также тому, как алгоритмы проявляют себя при работе в ограниченных устройствах. Эти сведения необходимы для определения кандидатов, которые лучше всего пригодны для использования в существующих приложениях и протоколах.

NIST рассчитывает получить черновой вариант стандарта в 2022 г., но оставляет за собой право на перенос строка. Вероятно, потребуется проведение третьего тура [4].

Определение критериев оценки механизмов инкапсуляции ключей. Для всестороннего и объективного анализа криптографических алгоритмов необходимо выделить набор критериев и определить их важность по сравнению друг с другом.

NIST объединяет требования, предъявляемые к алгоритмам, в три группы критериев [7]:

1. Безопасность.

1a. Изученность – изученность математической задачи, вычислительная сложность решения которой обеспечивает надёжность криптосистемы. Характеристика отражает временной срок, на протяжении которого математический аппарат, используемый криптосистемой, изучается в качестве механизма обеспечения криптографической стойкости: задача, предложенная более 20 лет назад; задача, предложенная более 10 лет назад; задачи, предложенные менее 10 лет назад.

1b. Доказательство – убедительность теоретического обоснования надёжности схемы. Качество доказательства криптографической стойкости алгоритма вносит не меньший вклад в обеспечение уверенности в безопасности криптосистемы, чем выбор математического аппарата: одно из наиболее убедительных доказательств; доказательство не содержит суждений, которые оцениваются экспертами NIST как сомнительные; доказательство содержит суждения, истинность которых не вызывает у экспертов NIST полной уверенности.

1c. Устойчивость МИК – тип криптоаналитических атак, к которым устойчив МИК: устойчивость к атакам на основе подобранного шифртекста (CCA); устойчивость к атакам на основе подобранного открытого текста (CPA).

1d. Устойчивость ААШ – тип криптоаналитических атак, к которым устойчив ААШ, связанный с МИК: устойчивость к атакам на основе подобранного шифртекста (CCA); устойчивость к атакам на основе подобранного открытого текста (CCA); не обозначена возможность применения алгоритма в качестве ААШ.

2. Ресурсоёмкость.

2a. Размер открытого ключа: менее 550 байт; от 550 до 1600 байт; от 1600 байт до 10000 байт; более 10000 байт.

2b. Размер шифртекста: менее 550 байт; от 550 до 1600 байт; от 1600 байт до 5000 байт; более 5000 байт.

2c. Производительность инкапсуляции – вычислительная эффективность операции зашифрования передаваемого симметричного ключа в циклах работы процессора: менее 400 тысяч циклов работы процессора; от 400 до 1600 тысяч циклов работы процессора; от 1600 до 10000 тысяч циклов работы процессора; более 10000 тысяч циклов работы процессора.

2d. Производительность декапсуляции – вычислительная эффективность операции расшифрования передаваемого симметричного ключа в циклах работы процессора: менее 400 тысяч циклов работы процессора; от 400 до 1600 тысяч циклов работы процессора; от 1600 до 10000 тысяч циклов работы процессора; более 10000 тысяч циклов работы процессора.

2e. Производительность генерации пары ключей – вычислительная эффективность операции расшифрования передаваемого симметричного ключа в циклах работы процессора: менее 600 тысяч циклов работы процессора; от 600 до 2500 тысяч циклов работы процессора; от 2500 до 10000 тысяч циклов работы процессора; более 10000 тысяч циклов работы процессора.

2f. Возможность некорректной декапсуляции – способность алгоритма при правильном применении производить шифртексты, которые не могут быть декапсулированы: отсутствует; присутствует.

3. Гибкость.

3a. Гибкость МИК – возможность использования МИК в различных сценариях применения: предусмотрены CPA- и CCA-устойчивые версии МИК; предусмотрена только CCA-устойчивая версия МИК.

3b. Гибкость ААШ – возможность использования ААШ, связанной с МИК, в различных сценариях применения: предусмотрены CPA- и CCA-устойчивые версии ААШ; предусмотрена CCA-устойчивая версия ААШ; не предусмотрена возможность использования алгоритма в качестве CCA-устойчивой ААШ.

3c. Особенности алгоритма – гибкой называют криптосистему, которая предоставляет пользователю возможность достижения оптимального компромисса между показателями ресурсоёмкости и безопасности путём настройки параметров.

Анализ механизмов инкапсуляции ключей второго тура конкурса NIST. Кандидаты рассмотрены по состоянию на момент предоставления в NIST первых корректив, которые NIST и научное сообщество предлагали им внести в заявки по результатам первого тура (крайний срок для их подачи был 31 мая 2019 г.).

На основании приведённого списка критериев оценки МИК представим анализ МИК, прошедших во второй тур конкурса NIST в форме таблицы.

В результате сравнения можно сделать вывод о том, что криптосистемы с высокой итоговой оценкой в одной группе критериев могут находиться близко к нижней границе оценочной шкалы в другой группе.

Например, МИК Classic McEllice и NTS-KEM основаны на криптосистеме Мак-Элиса, разработанной в 1978 г., поэтому они более качественно изучены, чем остальные кандидаты [1]. Тем не менее большая длина открытого ключа этих алгоритмов ставит под сомнение возможность их эффективного использования в современных приложениях и протоколах.

В то же время при поиске способов обеспечения более сбалансированных показателей производительности создателям криптосистемы неизбежно приходится модифицировать её математический аппарат. Внесение изменений способно привести к существенному упрощению задачи, вычислительная сложность решения которой обеспечивает безопасность алгоритма. На примере двух МИК, основанных на решётках: FrodoKEM и LAC, из анализа видно, что LAC имеет более высокую итоговую оценку производительности по сравнению с FrodoKEM. Это обусловлено тем, что LAC использует менее консервативный математический аппарат, чем FrodoKEM, а именно структурированные решётки. В то время как FrodoKEM оценивается экспертами NIST как один из са-

мых безопасных кандидатов [1], недавние исследования выявили уязвимость в параметрах LAC уровня безопасности 5, предоставленных во второй тур конкурса. В итоге эти параметры были отозваны заявителями [4].

Среди оставшихся в процессе стандартизации кандидатов присутствуют 2 родственных криптосистемы, которые сочетают в себе высокие показатели безопасности и производительности. Из анализа видно, что алгоритмы NTRU и NTRUPrime имеют максимальное значение итогового параметра безопасности и близкие к максимальным итоговые значения параметра ресурсоёмкости, что означает безусловное преобладание этих криптосистем над соперниками по двум наиболее приоритетным группам критериев.

Таблица – Анализ МИК, прошедших во второй тур конкурса NIST

	Заявки	Classic McEliece	NTS-KEM	Rollo	RQC	BIKE	HQC	LEDAcrypt	ThreeBears	FrodoKEM	Round5	CRYSTALS-Kyber	Saber	LAC	NewHope	NTRU Prime	NTRU	SIKE
Безопасность [1, 4]	Изученность	3	3	1	1	2	2	2	1	3	2	2	2	2	2	3	3	1
	Доказательство	3	3	1	1	1	1	1	2	3	1	2	1	1	3	3	3	2
	Устойчивость МИК	2	2	1	2	2	2	2	2	2	1	2	2	2	2	2	2	2
	Устойчивость ААШ	1	1	2	1	0	1	2	1	1	2	1	1	2	2	1	1	1
	Итог	**9**	**9**	**5**	**5**	**5**	**6**	**7**	**6**	**9**	**6**	**7**	**6**	**7**	**9**	**9**	**9**	**6**
Ресурсоёмкость [5]	Производительность инкапсуляции	4	4	3	2	3	3	2	4	2	2	3	3	4	3	4	4	1
	Производительность декапсуляции	3	3	2	2	2	3	1	4	2	4	3	3	4	3	4	4	1
	Производительность генерации ключей	1	1	2	3	4	4	1	4	3	3	3	1	1	1	2	3	1
	Размер открытого ключа	1	1	3	3	2	2	2	4	2	2	3	3	4	3	3	3	4
	Размер шифртекста	4	4	3	3	2	2	2	3	1	2	3	3	3	3	3	3	4
	Возможность некоректной декапсуляции	1	0	0	1	0	0	0	0	0	0	0	0	0	0	1	1	1
	Итого	**14**	**13**	**13**	**14**	**13**	**14**	**8**	**19**	**10**	**13**	**15**	**13**	**16**	**13**	**17**	**18**	**12**
Гибкость [1,4]	Гибкость МИК	0	0	0	0	1	0	1	1	0	0	0	1	1	1	0	0	0
	Гибкость ААШ	0	0	1	0	0	0	1	0	0	1	0	0	2	2	0	0	0
	Особенности алгоритма	0	1	0	0	0	0	0	1	1	3	1	0	0	–1	0	0	2
	Итого	**0**	**1**	**1**	**0**	**1**	**0**	**2**	**2**	**1**	**4**	**1**	**1**	**3**	**2**	**0**	**0**	**2**

Продолжая рассмотрение существующих между группами критериев зависимостей, стоит отдельно остановиться на гибкости. Гибкость позволяет в некоторой степени нивелировать ограничения производительности криптосистемы путём настройки её параметров. Однако главное преимущество более гибких алгоритмов по сравнению с менее гибкими состоит в возможности их адаптации под особенности конкретного объекта защиты. Например, алгоритм Round5 способен не только предоставлять возможность регулирования показателей производительности и безопасности, но также обеспечивать необходимый баланс между расходом CPU и пропускной способностью [2]. Поэтому, несмотря на не очень высокую общую производительность Round5, отражённую в анализе, он обладает потенциалом для использования в ситуациях, предъявляющих специфичные требования криптосистеме, которые не могут быть покрыты другими алгоритмами.

Как известно, во втором туре конкурса NIST присутствует несколько пар идентичных алгоритмов, реализующих общие принципы функционирования:

- Classic McEllice и NTS-KEM, основанные на кодах Гоппы;
- Rollo и RQC, основанные на низкоранговых кодах;
- HQC и LEDAcrypt, основанные на кодах Хемминга;
- NTRU и NTRUPrime, основанные на проблеме NTRU (усечённом кольце полиномов N-й степени).

Проведённый анализ подтверждает, что эти пары алгоритмов обладают не только схожими принципами функционирования, но также аналогичными достоинствами и ограничениями. Таким образом, слияние каждой из них в один алгоритм или выбор одного лучшего алгоритма из пары при переходе на следующий этап конкурса NIST представляется разумным способом упрощения процесса выбора постквантовых стандартов.

Выводы. Конкурс NIST для постквантовых криптосистем является динамическим процессом. Теоретические и практические аспекты новых криптосистем постоянно дорабатываются заявителями. Даже если новым алгоритмам не удастся занять роли стандартов в результате текущего процесса стандартизации, они могут значительно укрепить свои позиции вследствие будущих исследований. Сам факт того, что подобные заявки прошли во 2-й тур соревнования NIST свидетельствует о том, что они вызывают заинтересованность, а их доказательство внушает некоторую уверенность.

В ходе данного исследования были достигнуты следующие результаты:

- на основе существующих количественных и качественных характеристик постквантовых криптосистем, в частности МИК, предложена система критериев, позволяющих провести всесторонний анализ и сравнение алгоритмов;
- проведена формализованная оценка по этим критериям и анализ постквантовых МИК, которые прошли во второй тур конкурса NIST;
- определены 2 МИК, которые представляются оптимальными с точки зрения значимости критериев, заявленной NIST;
- выделены наборы алгоритмов, слияние которых может упростить процедуру выбора стандарта;
- раскрыт характер взаимных зависимостей между группами критериев оценки алгоритмов.

Использованный набор критериев и подход к сравнению МИК могут быть легко адаптированы для проведения аналогичного анализа кандидатов на роль постквантового стандарта ЭЦП.

Кроме того, результаты анализа могут быть использованы для более глубоко исследования соответствия криптографических алгоритмов требованиям конкретных протоколов, приложений и других предполагаемых сценариев использования будущих стандартов.

Библиографический список

1. Alagic J. Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process / J. Alagic, J. Alperin-Sheriff, D. Apon, D. Cooper, Q. Dang, Yi-Kai Liu., C. Miller, D. Moody, R. Peralta, R. Perlner, A. Robinson, D. Smith-Tone // National Institute of Standards and Technology. – Режим доступа: http://dx.doi.org/10.6028/NIST.IR.8240, свободный. – Заглавие с экрана. – Яз. англ.

2. Baan H. Round5: KEM and PKE based on (Ring) Learning with Rounding / H. Baan, S. Bhattacharya, S. Fluhrer, O. Garcia-Morchon1, T. Laarhoven, R. Player, R. Rietman1, M.-J. O. Saarinen, L. Tolhuizen1, J. L. Torre-Arce, Z. Zhang. – Режим доступа: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-2-Submissions, свободный. – Заглавие с экрана. – Яз. англ.

3. Chen L. Report on Post-Quantum Cryptography / L. Chen, S. Jordan, Y. K. Liu, D. Moody, R. Peralta, R. Perlner, D. Smith-tone // National Institute of Standards and Technology. – Режим доступа: https://doi.org/10.6028/NIST.IR.8105, свободный. – Заглавие с экрана. – Яз. англ.

4. Moody D. Round2 of the NIST PQC “Competition” what was NIST thinking? / D. Moody // National Institute of Standards and Technology. – Режим доступа: https://csrc.nist.gov/CSRC/media/Presentations/Round-2-of-the-NIST-PQC-Competition-What-was-NIST/images-media/pqcrypto-may2019-moody.pdf, свободный. – Заглавие с экрана. – Яз. англ.

5. Nist software perfomance tests. – Режим доступа: https://www.safecrypto.eu/pqclounge/round-1-candidates/software-analysis-kem/, свободный. – Заглавие с экрана. – Яз. англ.

6. Shor P. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer / P. Shor // SIAM Journal on Computing. – 1997. – Vol. 26, № 5. – С.1484–1509.

7. Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standartization Process // National Institute of Standards and Technology. – Режим доступа: https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf , свободный. – Заглавие с экрана. – Яз. англ.

References

1. Alagic J., Alperin-Sheriff J., Apon D., Cooper D., Dang Q., Yi-Kai Liu., Miller C., Moody D., Peralta R., Perlner R., Robinson A., Smith-Tone D. Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process. *National Institute of Standards and Technology.* Available at: http://dx.doi.org/10.6028/NIST.IR.8240.

2. Baan H., Bhattacharya S., Fluhrer S., Garcia-Morchon1 O., Laarhoven T., Player R., Rietman1 R., Saarinen M.-J. O., Tolhuizen1 L., Torre-Arce J. L., Zhang Z. Round5: KEM and PKE based on (Ring) Learning with Rounding. *National Institute of Standards and Technology.* Available at: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-2-Submissions.

3. Chen L., Jordan S., Liu Y.K., Moody D., Peralta R., Perlner R., Smith-tone D. Report on Post-Quantum Cryptography. *National Institute of Standards and Technology.* Available at: https://doi.org/10.6028/NIST.IR.8105.

4. Moody D. Round2 of the NIST PQC "Competition" what was NIST thinking. *National Institute of Standards and Technology.* Available at: https://csrc.nist.gov/CSRC/media/Presentations/Round-2-of-the-NIST-PQC-Competition-What-was-NIST/images-media/pqcrypto-may2019-moody.pdf.

5. *Nist software perfomance tests.* Available at: https://www.safecrypto.eu/pqclounge/round-1-candidates/software-analysis-kem/.

6. Shor P. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing*, 1997, vol. 26, no. 5, pp 1484–1509.

7. Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standartization Process. Available at: https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf.

DOI 10.21672/2074-1707.2019.48.4.127-135
УДК 004.01

РАЗРАБОТКА МОДЕЛИ УГРОЗ ДЛЯ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ С УЧЕТОМ МЕТОДОВ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Статья поступила в редакцию 13.11.2019, в окончательном варианте – 25 11.2019.

Новикова Елизавета Федоровна, Кубанский государственный университет, 350072, Российская федерация, г. Краснодар, ул. Московская, д. 2,
аспирант, e-mail: lizanovicova@mail.ru

Хализев Вячеслав Николаевич, Кубанский государственный университет, 350072, Российская федерация, г. Краснодар, ул. Московская, д. 2,
кандидат технических наук, профессор e-mail: ha53@mail.ru

Рассмотрен новый подход к разработке модели угроз безопасности информации объектов критической информационной инфраструктуры (КИИ). Значимость настоящей работы обуславливается увеличением компьютеризации населения, что повышает вероятность возникновения угроз от использования методов социальной инженерии. Вследствие отсутствия до конца проработанной нормативной и методической базы в области безопасности объектов КИИ в работе используется как основа обязательная к реализации «классическая» методика ФСТЭК формирования модели угроз безопасности информации. Данная модель расширяется компонентами, учитывающими человеческий фактор, который отсутствует в «классической» методике. В статье выделены виды нарушителей, которые могут использовать методы социальной инженерии, а также непосредственно сопоставлены нарушители и реализуемые ими методы. Приводятся возможные деревья угроз и атак. Результаты данного исследования являются основой для программной реализации системы моделирования угроз и выработки мер противодействия.

Ключевые слова: критическая информационная инфраструктура, категорирование, объект критической информационной инфраструктуры, модель потенциального нарушителя, модель угроз безопасности информации, человеческий фактор, социальная инженерия