показателям) эффективности фактографического поиска в АСОИБ. Проведено исследование полученных оценок и выявлены их свойства. В процессе выполненной работы и проведенных исследований были успешно получены необходимые охранные документы Федеральной службы по интеллектуальной собственности (Роспатент).

СПИСОК ЛИТЕРАТУРЫ:

1. *Кулик С. Д.* Информационная безопасность АФИПС // Известия Южного федерального университета. Технические науки. 2003. Т. 33. № 4. С. 238.
2. *Salton G.* Automatic information organization and Retrieval. New York: McGraw-Hill, 1968. — 514 р.
3. *Fukunaga K.* Introduction to Statistical Pattern Recognition. Elsevier Academic Press. San Diego, San Francisco, New York, Boston, London, Sydney, Tokyo, 1990. — 592 p.
4. *Вентцель Е. С.* Теория вероятностей. М.: Высшая школа, 2001. — 575 с.
5. *Колмогоров А. Н.* Основные понятия теории вероятностей. М.: ФАЗИС, 1998. — 144 с.
6. *Feller W.* An introduction to probability theory and its applications. Vol. 1. 3rd ed. John Wiley & Sons. New York, 1968. — 509 p.
7. *Галушкин А. И.* Теория нейронных сетей: Учебное пособие для вузов. Кн. 1. М.: ИПРЖР, 2000. — 416 с.
8. *Haykin S.* Neural Networks — A Comprehensive Foundation. Second Edition. Pearson Education, Inc., 1999. Reprint: 2005.

REFERENCES:

1. *Kulik S. D.* Informatsionnaya bezopasnost' AFIPS // Izvestiya Yuzhnogo federal'nogo universiteta. Tekhnicheskiye nauki. 2003. T. 33. № 4. P. 238.
2. *Salton G.* Automatic information organization and Retrieval. New York: McGraw-Hill, 1968. — 514 p.
3. *Fukunaga K.* Introduction to Statistical Pattern Recognition. Elsevier Academic Press. San Diego, San Francisco, New York, Boston, London, Sydney, Tokyo, 1990. — 592 p.
4. *Wentzel E. S.* Teoriya veroyatnostey. M.: Vysshaya shkola, 2001. — 575 p.
5. *Kolmogorov A. N.* Osnovnyye ponyatiya teorii veroyatnostey. M.: FAZIS, 1998. —144 p.
6. *Feller W.* An introduction to probability theory and its applications. Vol. 1. 3rd ed. John Wiley & Sons. New York, 1968. — 509 p.
7. *Galushkin A. I.* Teoriya neyronnykh setey: Uchebnoye posobiye dlya vuzov. Kn. 1. M.: IPRZHR, 2000. — 416 p.
8. *Haykin S.* Neural Networks — A Comprehensive Foundation. Second Edition. Pearson Education, Inc., 1999. Reprint: 2005.

M. A. Kupriyashin, G. I. Borzunov

Evolution of Knapsack Ciphersystems

Key words: knapsack problem, knapsack ciphersystems

The knapsack problem is known to be used in numerous public key ciphersystems designs. These ciphersystems have been receiving increased attention from analytics, resulting in many being compromised. Therefore, modern systems incorporate new algorithms making them at least partially immune to known attacks. In this paper, three types of knapsack ciphersystems are introduced. The difference between types is how the keys are generated and used. Classical systems, being the first type, use superincreasing sequences and low-density knapsacks and are therefore vulnerable. Modern cryptosystems are based on high-density knapsacks. That makes them difficult to analyze. Hybrid cryptosystems incorporate several security mechanisms (not only trapdoor knapsacks) that makes analysis, as well as implementation, even more complicated.

М. А. Куприяшин, Г. И. Борзунов

ЭВОЛЮЦИЯ РЮКЗАЧНЫХ СИСТЕМ ШИФРОВАНИЯ

Задача о рюкзаке — NP-полная задача, представляющая большой интерес в области создания асимметричных систем шифрования. История развития рюкзачных систем шифрования началась вскоре после зарождения асимметричной криптографии, в 1978 году. Несмотря на то что многие рюкзачные шифрсистемы оказались нестойкими и непригодными для практического применения [1], интерес к ним сохраняется и сегодня [2]. Это связано с таким достоинством этого класса систем, как высокая скорость шифрования. Кроме того, рюкзачные шифрсистемы актуальны в постквантовой криптографии: вследствие реализации алгоритма Шора системы, основанные на проблеме дискретного логарифмирования, станут уязвимыми, а часть рюкзачных систем останется в строю [3, 4].

С учетом особенностей развития рюкзачных систем шифрования можно выделить несколько различных типов таких систем. Классические шифрсистемы — ряд систем, предлагавшихся на начальном этапе развития асимметричной криптографии [1]. Основная идея, лежащая в основе этих систем: создать две связанные задачи о рюкзаке, одна решается за линейное время (для расшифрования), а другая является NP-полной. Первоначально Меркль и Хеллман использовали сверхрастущий рюкзак в качестве закрытого ключа и связывали его с открытым ключом при помощи модульного умножения (шифрсистема Меркля — Хеллмана, 1978). В 1983 г. Ади Шамир нашел способ восстановления закрытого ключа по открытому ключу шифрсистемы Меркля — Хеллмана: как выяснилось, вычисляемый открытый ключ обладал характерными свойствами, связанными с быстрым ростом элементов закрытого ключа. Атака Шамира имела полиномиальную временную сложность. Благодаря работам Лагариаса, Одлыжко и других исследователей был разработан универсальный алгоритм нахождения сокращенного базиса решетки, известный как LLL-решатель. LLL-решатель имеет полиномиальную временную сложность, но является ресурсоемким, так как его сложность пропорциональна шестой степени размерности задачи [2]. Успешность применения этого алгоритма при анализе рюкзачной системы шифрования существенно зависит от плотности рюкзака. Плотность определяется соотношением между количеством элементов рюкзака и их размером в битовом представлении. При пороговом значении плотности 0,94 и ниже LLL-решатель считается эффективным [2]. В отдельных случаях удавалось эффективно применять этот метод при плотности до 1,26 [5]. Все широко известные системы классического типа оказались в той или иной степени подвержены атакам с использованием LLL-решателя. Это сделало их не применимыми на практике. Следующим шагом в развитии рюкзачных систем было использование новых принципов генерации ключей, позволяющих повысить плотность рюкзаков. Второй тип рюкзачных шифрсистем — современные системы — использует различные достижения современной математики и теории чисел для решения плотных рюкзаков [4]. Еще одно современное направление развития рюкзачных шифрсистем связано с сокрытием упаковки рюкзака при помощи дополнительных алгоритмов шифрования. Такой тип рюкзачных шифрсистем назовем гибридным. Например, текст, зашифрованный на открытом рюкзаке, впоследствии шифруется другой асимметричной системой шифрования [6]. Применяются дополнительные преобразования для сокрытия или динамической генерации открытых ключей для шифрования [7, 8]. Анализ таких систем крайне затруднен, так как требует решения нескольких вычислительно сложных проблем. Но использование дополнительных механизмов шифрования усложняет генерацию ключей и процедуры шифрования и расшифрования. Это существенные недостатки, так как быстрая процедура шифрования является одним из главных достоинств рюкзачных шифрсистем.

Таким образом, среди известных рюкзачных шифрсистем выделено три типа. Классические системы манипулировали ключами-рюкзаками низкой плотности и уязвимы к атакам с

использованием LLL-решателя. Современные системы работают с рюкзаками высокой плотности — их применимость на настоящий момент под вопросом. Наконец, гибридные шифрсистемы наиболее эффективно противостоят всем известным атакам, но оказываются более медленными.

СПИСОК ЛИТЕРАТУРЫ:

1. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: ТРИУМФ, 2013. — 816 с.
2. *Kate A., Goldberg I.* Generalizing cryptosystems based on the subset sum problem // International Journal of Information Security. 2011. Т. 10. № 3. Р. 189–199.
3. *Okamoto T.* Quantum Public-Key Cryptosystems Lecture Notes in Computer Science / Ed. M. Bellare. Springer Berlin Heidelberg, 2000. Р. 147–165.
4. *Murakami Y., Nasako T.* Knapsack Public-Key Cryptosystem Using Chinese Remainder Theorem // IACR Cryptology ePrint Archive. 2007. — 12 p.
5. *Schnorr C.-P.* Attacking the Chor-Rivest cryptosystem by improved lattice reduction. Springer, 1995. Р. 1–12.
6. *Rastaghi R.* Cryptanalysis and Improvement of Akleylek et al.'s cryptosystem. 2013.
7. *Kasahara M.* Construction of New Classes of Knapsack Type Public Key Cryptosystem Using Uniform Secret Sequence, K (II) ΣП PKC, Constructed Based on Maximum Length Code // IACR Cryptology ePrint Archive. 2012. — 8 p.
8. *Pan Y., Deng Y., Jiang Y., Tu Z.* A New Lattice-Based Cryptosystem Mixed with a Knapsack // IACR Cryptology ePrint Archive. 2009. — 12 p.

REFERENCES:

1. *Schneier B.* Applied cryptography. Protocols, Algorithms, and Source Code in C. John Wiley & Sons. Inc., 2013. — 816 p.
2. *Kate A., Goldberg I.* Generalizing cryptosystems based on the subset sum problem // International Journal of Information Security. 2011. Т. 10. № 3. Р. 189–199.
3. *Okamoto T.* Quantum Public-Key Cryptosystems Lecture Notes in Computer Science / / Ed. M. Bellare. Springer Berlin Heidelberg, 2000. Р. 147–165.
4. *Murakami Y., Nasako T.* Knapsack Public-Key Cryptosystem Using Chinese Remainder Theorem // IACR Cryptology ePrint Archive. 2007. — 12 p.
5. *Schnorr C.-P.* Attacking the Chor-Rivest cryptosystem by improved lattice reduction. Springer, 1995. Р. 1–12.
6. *Rastaghi R.* Cryptanalysis and Improvement of Akleylek et al.'s cryptosystem. 2013.
7. *Kasahara M.* Construction of New Classes of Knapsack Type Public Key Cryptosystem Using Uniform Secret Sequence, K (II) ΣП PKC, Constructed Based on Maximum Length Code // IACR Cryptology ePrint Archive. 2012. — 8 p.
8. *Pan Y., Deng Y., Jiang Y., Tu Z.* A New Lattice-Based Cryptosystem Mixed with a Knapsack // IACR Cryptology ePrint Archive. 2009. — 12 p.

V. S. Makeev, A. S. Zaytsev

Research of IT-sabotage Problem

Key words: IT-sabotage, insider, fishbone diagram

This article presents a research of the threat of IT-sabotage with the use of information resources of an organization. Based on statistical information and relevant research, a scheme and a fishbone diagram of insider were designed here.