

ISSN 2518-1483 (Online),
ISSN 2224-5227 (Print)

2017 • 6

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫНЫҢ

БАЯНДАМАЛАРЫ

ДОКЛАДЫ

НАЦИОНАЛЬНОЙ АКАДЕМИИ НАУК
РЕСПУБЛИКИ КАЗАХСТАН

REPORTS

OF THE NATIONAL ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN

ЖУРНАЛ 1944 ЖЫЛДАН ШЫҒА БАСТАҒАН

ЖУРНАЛ ИЗДАЕТСЯ С 1944 г.

PUBLISHED SINCE 1944



Б а с р е д а к т о р ы
х.ғ.д., проф., ҚР ҰҒА академигі **М.Ж. Жұрынов**

Р е д а к ц и я а л қ а с ы:

Адекенов С.М. проф., академик (Қазақстан) (бас ред. орынбасары)
Величкин В.И. проф., корр.-мүшесі (Ресей)
Вольдемар Вуйчик проф. (Польша)
Гончарук В.В. проф., академик (Украина)
Гордиенко А.И. проф., академик (Белорус)
Дука Г. проф., академик (Молдова)
Илолов М.И. проф., академик (Тәжікстан),
Леска Богуслава проф. (Польша),
Локшин В.Н. проф. чл.-корр. (Қазақстан)
Нараев В.Н. проф. (Ресей)
Неклюдов И.М. проф., академик (Украина)
Нур Изура Удзир проф. (Малайзия)
Перни Стефано проф. (Ұлыбритания)
Потапов В.А. проф. (Украина)
Прокопович Полина проф. (Ұлыбритания)
Омбаев А.М. проф., корр.-мүшесі (Қазақстан)
Өтелбаев М.О. проф., академик (Қазақстан)
Садыбеков М.А. проф., корр.-мүшесі (Қазақстан)
Сатаев М.И. проф., корр.-мүшесі (Қазақстан)
Северский И.В. проф., академик (Қазақстан)
Сикорски Марек проф. (Польша)
Рамазанов Т.С. проф., академик (Қазақстан)
Такибаев Н.Ж. проф., академик (Қазақстан), бас ред. орынбасары
Харин С.Н. проф., академик (Қазақстан)
Чечин Л.М. проф., корр.-мүшесі (Қазақстан)
Харун Парлар проф. (Германия)
Энджун Гао проф. (Қытай)
Эркебаев А.Э. проф., академик (Қырғыстан)

«Қазақстан Республикасы Ұлттық ғылым академиясының баяндамалары»

ISSN 2518-1483 (Online),

ISSN 2224-5227 (Print)

Меншіктенуші: «Қазақстан Республикасының Ұлттық ғылым академиясы» Республикалық қоғамдық бірлестігі (Алматы қ.)
Қазақстан республикасының Мәдениет пен ақпарат министрлігінің Ақпарат және мұрағат комитетінде 01.06.2006 ж.
берілген №5540-Ж мерзімдік басылым тіркеуіне қойылу туралы куәлік

Мерзімділігі: жылына 6 рет.

Тиражы: 2000 дана.

Редакцияның мекенжайы: 050010, Алматы қ., Шевченко көш., 28, 219 бөл., 220, тел.: 272-13-19, 272-13-18,
<http://nauka-nanrk.kz>, reports-science.kz

© Қазақстан Республикасының Ұлттық ғылым академиясы, 2017

Типографияның мекенжайы: «Аруна» ЖК, Алматы қ., Муратбаева көш., 75.

Главный редактор
д.х.н., проф., академик НАН РК **М. Ж. Журинов**

Редакционная коллегия:

Адекенов С.М. проф., академик (Казахстан) (зам. гл. ред.)
Величкин В.И. проф., чл.-корр. (Россия)
Вольдемар Вуйчик проф. (Польша)
Гончарук В.В. проф., академик (Украина)
Гордиенко А.И. проф., академик (Беларусь)
Дука Г. проф., академик (Молдова)
Илолов М.И. проф., академик (Таджикистан),
Леска Богуслава проф. (Польша),
Локшин В.Н. проф. чл.-корр. (Казахстан)
Нараев В.Н. проф. (Россия)
Неклюдов И.М. проф., академик (Украина)
Нур Изура Удзир проф. (Малайзия)
Перни Стефано проф. (Великобритания)
Потапов В.А. проф. (Украина)
Прокопович Полина проф. (Великобритания)
Омбаев А.М. проф., чл.-корр. (Казахстан)
Отелбаев М.О. проф., академик (Казахстан)
Садыбеков М.А. проф., чл.-корр. (Казахстан)
Сатаев М.И. проф., чл.-корр. (Казахстан)
Северский И.В. проф., академик (Казахстан)
Сикорски Марек проф., (Польша)
Рамазанов Т.С. проф., академик (Казахстан)
Такибаев Н.Ж. проф., академик (Казахстан), зам. гл. ред.
Харин С.Н. проф., академик (Казахстан)
Чечин Л.М. проф., чл.-корр. (Казахстан)
Харун Парлар проф. (Германия)
Энджун Гао проф. (Китай)
Эркебаев А.Э. проф., академик (Кыргызстан)

Доклады Национальной академии наук Республики Казахстан»

ISSN 2518-1483 (Online),

ISSN 2224-5227 (Print)

Собственник: Республиканское общественное объединение «Национальная академия наук Республики Казахстан» (г. Алматы)

Свидетельство о постановке на учет периодического печатного издания в Комитете информации и архивов Министерства культуры и информации Республики Казахстан №5540-Ж, выданное 01.06.2006 г.

Периодичность: 6 раз в год.

Тираж: 2000 экземпляров

Адрес редакции: 050010, г.Алматы, ул.Шевченко, 28, ком.218-220, тел. 272-13-19, 272-13-18

<http://nauka-nanrk.kz> reports-science.kz

©Национальная академия наук Республики Казахстан, 2017 г.

Адрес типографии: ИП «Аруна», г.Алматы, ул.Муратбаева, 75

E d i t o r i n c h i e fdoctor of chemistry, professor, academician of NAS RK **M.Zh. Zhurinov****E d i t o r i a l b o a r d :****Adekenov S.M.** prof., academician (Kazakhstan) (deputy editor in chief)**Velichkin V.I.** prof., corr. member (Russia)**Voitsik Valdemar** prof. (Poland)**Goncharuk V.V.** prof., academician (Ukraine)**Gordiyenko A.I.** prof., academician (Belarus)**Duka G.** prof., academician (Moldova)**Ilolov M.I.** prof., academician (Tadjikistan),**Leska Boguslava** prof. (Poland),**Lokshin V.N.** prof., corr. member. (Kazakhstan)**Narayev V.N.** prof. (Russia)**Nekludov I.M.** prof., academician (Ukraine)**Nur Izura Udzir** prof. (Malaysia)**Perni Stephano** prof. (Great Britain)**Potapov V.A.** prof. (Ukraine)**Prokopovich Polina** prof. (Great Britain)**Ombayev A.M.** prof., corr. member. (Kazakhstan)**Otelbayv M.O.** prof., academician (Kazakhstan)**Sadybekov M.A.** prof., corr. member. (Kazakhstan)**Satayev M.I.** prof., corr. member. (Kazakhstan)**Severskyi I.V.** prof., academician (Kazakhstan)**Sikorski Marek** prof., (Poland)**Ramazanov T.S.** prof., academician (Kazakhstan)**Takibayev N.Zh.** prof., academician (Kazakhstan), deputy editor in chief**Kharin S.N.** prof., academician (Kazakhstan)**Chechin L.M.** prof., corr. member. (Kazakhstan)**Kharun Parlar** prof. (Germany)**Endzhun Gao** prof. (China)**Erkebayev A.Ye.** prof., academician (Kyrgyzstan)**Reports of the National Academy of Sciences of the Republic of Kazakhstan.****ISSN 2224-5227****ISSN 2518-1483 (Online),****ISSN 2224-5227 (Print)**

Owner: RPA "National Academy of Sciences of the Republic of Kazakhstan" (Almaty)

The certificate of registration of a periodic printed publication in the Committee of Information and Archives of the Ministry of Culture and Information of the Republic of Kazakhstan N 5540-Ж, issued 01.06.2006

Periodicity: 6 times a year

Circulation: 2000 copies

Editorial address: 28, Shevchenko str., of.219-220, Almaty, 050010, tel. 272-13-19, 272-13-18,

<http://nauka-nanrk.kz / reports-science.kz>

© National Academy of Sciences of the Republic of Kazakhstan, 2017

Address of printing house: ST "Aruna", 75, Muratbayev str, Almaty

A.E. Abdrakhmanov

Granit Technology, Almaty, Kazakhstan
E-mail: alzhan17@mail.ru

MODELS OF VIOLATORS OF CRYPTOGRAPHIC PROTECTION AND STANDARD ST RK 1073-2007

Abstract. This article considers the construction of models of violators of cryptographic protection of information. The constructed models take into account the motivation, knowledge, financial and technical capabilities of violators. Safe thresholds for the computational complexity of known cryptographic protection breaking algorithms are determined. A comparative analysis of violators' models and the state standard of the Republic of Kazakhstan ST RK 1073-2007 "Means of cryptographic protection of information. General technical requirements" is done. Based on the results of the analysis, specific recommendations on the unconditional processing of this standard in 2017 are given.

Key words: information security, cryptography, model of violator, state standard, security level.

УДК 004.056.5

А.Е. Абдрахманов

ТОО "Granit Technology", Алматы, Казахстан

МОДЕЛИ НАРУШИТЕЛЕЙ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ И СТАНДАРТ СТ РК 1073-2007

Аннотация. Данная статья рассматривает вопросы построения моделей нарушителей криптографической защиты информации. Построенные модели учитывают мотивацию, знания, финансовые и технические возможности нарушителей. Определены безопасные пороги для вычислительной сложности известных алгоритмов вскрытия криптографической защиты. Выполнен сравнительный анализ моделей нарушителей и государственного стандарта Республики Казахстан СТ РК 1073-2007 "Средства криптографической защиты информации. Общие технические требования". По результатам анализа даны конкретные рекомендации по безусловной переработке этого стандарта в 2017 году.

Ключевые слова: защита информации, криптография, модель нарушителя, государственный стандарт, уровень безопасности.

1. Введение

Государственный стандарт Республики Казахстан СТ РК 1073-2007 "Средства криптографической защиты информации. Общие технические требования" (далее – Стандарт) был принят 10 лет назад и за эти годы стал основным казахстанским стандартом для оценки качества средств криптографической защиты информации (далее – СКЗИ) [1, 2].

Вместе с тем, в течение этих лет продолжалось развитие теоретической криптографии, а также рост квалификации и вычислительных возможностей потенциальных нарушителей. Так, за 5 лет с июня 2007 года по июнь 2012 года лидерство в списке 500 наиболее мощных электронно-вычислительных машин TOP500 постепенно перешло от IBM Blue Gene/L с 65536 2-ядерными процессорами и производительностью 280 TFLOPS к IBM Sequoia – Blue Gene/Q с 98304 16-ядерными процессорами и производительностью 16,3 PFLOPS. Следовательно, производи-

тельность лидера выросла почти в 60 раз или в 2,25 раза в год. Суммарная вычислительная мощность ЭВМ всего списка за тот же период выросла в 25 раз с 4,9 до 123,4 PFLOPS или в 1,9 раза в год.

За последние 5 лет с июня 2012 года по июнь 2017 года лидерство постепенно перешло к Sunway TaihuLight с 40960 260-ядерными процессорами и производительностью 93,0 PFLOPS. Следовательно, производительность лидера выросла еще в 5,7 раз или в 1,4 раза в год. Суммарная вычислительная мощность ЭВМ всего списка за тот же период выросла еще в 5,4 раза до 672 PFLOPS или тоже в 1,4 раза в год [3].

Это, как подтверждает закон Мура о тенденции 2-кратного роста производительности вычислительной техники каждые 2 года, так и показывает возможность более существенного прогресса вычислительной техники с 2-кратным ежегодным ростом производительности, что соответствует периодам наиболее бурного развития вычислительной техники.

Указанные изменения делают актуальным построение современных моделей нарушителей и соответствующего пересмотра уровней безопасности и других положений стандарта СТ РК 1073-2007 [4].

2. В отношении модели нарушителя "Обыватель"

В первые годы массовой компьютеризации в качестве возможных нарушителей было целесообразным рассматривать категорию "обыватель", к которой относилось подавляющее большинство населения даже экономически развитых стран. Считалось, что обыватель практически не имеет знаний в области криптографии, может иметь в своем распоряжении персональную ЭВМ незначительной производительности, достаточной для работы текстовых редакторов, электронных таблиц и простейших игр, для которой сам обыватель или его знакомые могут разработать прикладное программное обеспечение, реализовав криптографический алгоритм из случайно попавшей к ним книги по криптографии. Также считалось, что обывателем движет, в основном, спортивный интерес прочесть чужую переписку, попавшую к нему, как правило, случайно.

Практически любая криптографическая защита, даже многие ручные шифры и, тем более, подавляющее большинство механических шифров, электронных шифров и средств аутентификации являлись достаточной защитой от такого обывателя [5, 6].

Однако тенденцией является повсеместное повышение компьютерной и криптографической грамотности, доступность персональных ЭВМ с существенно возросшей вычислительной мощностью, появление в широком доступе в Интернете значительного количества программ и методик для вскрытия криптографической защиты, а также иного вредоносного программного обеспечения. Изменилась и мотивация нарушителей из-за повсеместной коммерциализации и, как следствие, криминализации общества.

В таких условиях нарушитель-обыватель, как правило, становится специалистом и утрачивается потребность в рассмотрении модели нарушителя "Обыватель".

3. Модель нарушителя "Специалист"

К категории "специалист" будем относить специалистов в информационных технологиях, индивидуальных предпринимателей, преступников и иных физических лиц, для вскрытия криптографической защиты конкретной системы располагающих материальными и финансовыми средствами в объеме до 1000 МРП (около 2 млн. тенге, 6 тыс. евро или 5 тройских унций золота, в 2017 году 1 МРП = 2269 тенге $\approx$ 6 евро $\approx$ 7 USD).

В эту категорию попадает подавляющее большинство населения Казахстана, так как 1000 МРП – это более 90 минимальных размеров заработной платы (в 2017 году МРЗП = 24459 тенге), около 16 среднемесячных заработных плат (в 2016 году СЗП = 142351 тенге), более 11 среднемесячных заработных плат по виду деятельности "Информация и связь" (в 2016 году – 202019 тенге) [7]. Так как по ВВП на душу населения Казахстан соответствует среднемировому уровню (в 2016 году – 7453 и 10038 USD соответственно, 74 место из 186 стран), то в эту же категорию попадает и подавляющее большинство населения Земли [8]. То есть большинству специалистов и других физических лиц придется накапливать финансовые средства в течение

нескольких лет, чтобы собрать указанную сумму. Таким образом, верхняя оценка в 1000 МРП для модели нарушителя "Специалист" является оправданной.

В отношении нарушителя-специалиста будем полагать следующее:

1. Основными мотивами нарушителя являются получение прибыли или удовлетворение профессиональных амбиций, как правило, в краткосрочной перспективе.

2. Нарушитель имеет глубокие знания в области информационных технологий и базовые знания в области криптографии. В частности, может запрограммировать самостоятельно или найти в Интернете программы и методики вскрытия криптографической защиты.

3. До 50% имеющихся финансовых средств нарушитель израсходует на приобретение средств вычислительной техники – персональных ЭВМ, которые будут работать 24 часа в сутки, 7 дней в неделю, с полным износом за 4 года, а остальные финансовые средства уйдут на оплату электроэнергии. Стоимость процессоров может достигать половины от стоимости персональной ЭВМ, то есть до $1000 \times 0,5 \times 0,5 = 250$ МРП. Согласно данным основных производителей процессоров для персональных ЭВМ, часть из которых приведены в таблице 1, условная стоимость одного ядра большинства процессоров, кроме малобюджетных и уцененных, составит 8-10 МРП при нормировании на производительность в 4 миллиарда 64-разрядных операций в секунду [9, 10]. При использовании таких процессоров нарушитель может эксплуатировать в течение 4 лет несколько ЭВМ с общим количеством ядер до 25-32, на которых решать задачи с вычислительной сложностью до 32 (ядер) $\times 4 \times 10^9$ (операций/с/ядро) $\times 3600$ (с/час) $\times 24$ (час/сутки) $\times 365,25$ (сутки/год) $\times 4$ (года) $\approx 2^5 \times 2^{32} \times 2^{25} \times 2^2 = 2^{64}$.

Таблица 1 - Характеристики современных процессоров персональных ЭВМ

Произ- води-тель	Модель	Год выпу- ска	Кол-во ядер	Частота (ГГц)	Турбо частота (ГГц)	Цена (USD)	Цена ядра (МРП)
AMD	Athlon X4 845	2016	4	3,5	3,8	60	2,1
AMD	Athlon X4 870K	2015	4	3,9	4,1	70	2,5
AMD	Athlon X4 880K	2016	4	4,0	4,2	80	2,9
AMD	Ryzen 5 1400	2017	4	3,2	3,4	170	6,1
AMD	Ryzen 5 1500X	2017	4	3,5	3,7	190	6,8
AMD	Ryzen 5 1600	2017	6	3,2	3,6	220	5,2
AMD	Ryzen 5 1600X	2017	6	3,2	4,0	250	6,0
AMD	Ryzen 7 1700	2017	8	3,0	3,7	320	5,7
AMD	Ryzen 7 1700X	2017	8	3,4	3,8	380	6,8
AMD	Ryzen 7 1800X	2017	8	3,6	4,0	470	8,4
Intel	Celeron G3930	2017	2	2,9	–	42	3,0
Intel	Celeron G3950	2017	2	3,0	–	52	3,7
Intel	Core i3 7100	2017	2	3,9	–	117	8,4
Intel	Core i3 7300	2017	2	4,0	–	138	9,9
Intel	Core i3 7320	2017	2	4,1	–	149	10,6
Intel	Core i5 7400	2017	4	3,0	3,5	182	6,5
Intel	Core i5 7500	2017	4	3,4	3,8	192	6,9
Intel	Core i5 7600	2017	4	3,5	4,1	213	7,6
Intel	Core i7 7700	2017	4	3,6	4,2	303	10,8
Intel	Core i7 7700K	2017	4	4,2	4,5	339	12,1

4. Нарушитель имеет информацию об используемых криптографических алгоритмах. Так, многие производители СКЗИ не скрывают используемые алгоритмы и большинство современных СКЗИ используют ограниченный набор криптографических алгоритмов, например, алгоритмы шифрования ГОСТ 28147-89, TripleDES или AES.

5. Нарушитель имеет значительный объем защищенной переписки, то есть наборы шифртекстов, текстов с имитовставками и/или текстов с ЭЦП.

6. Нарушитель имеет некоторое количество пар открытый-шифрованный текст. Так, многие информационные системы обмениваются стандартными сообщениями.

7. Нарушитель не имеет информации о ключах.

Таким образом, для защиты от нарушителя-специалиста вычислительная сложность существующих и широко известных алгоритмов вскрытия криптографической защиты должна составлять не менее 2^{64} . Если ущерб законного владельца информации от такого вскрытия и, соответственно, потенциальный выигрыш нарушителя не превышают 100 МРП, то есть 10-кратно меньше затраченных им средств, то это сделает заведомо экономически невыгодным вскрытие криптографической защиты даже в условиях, когда нарушитель располагает существенно большими материальными и финансовыми средствами, объединяет свои усилия с другими нарушителями-специалистами, использует малобюджетные или уцененные средства вычислительной техники или приступает к вскрытию криптографической защиты через 5 лет с учетом роста производительности средств вычислительной техники.

4. Модель нарушителя "Предприятие"

К категории "предприятие" будем относить группы специалистов в информационных технологиях и криптографии, предприятия, организованные преступные группы и иных физических и юридических лиц, для вскрытия криптографической защиты конкретной системы располагающих материальными и финансовыми средствами в объеме до 1 млн. МРП (около 2 млрд. тенге, 6 млн. евро или 5 тыс. тройских унций золота).

Например, в эту категорию попадают практически все казахстанские субъекты малого и среднего предпринимательства, то есть предприятия со среднегодовой численностью до 100 и 250 работников и со среднегодовым доходом до 300 тыс. и 3 млн. МРП соответственно. В противном случае им придется израсходовать для вскрытия криптографической защиты весь свой доход за более чем 3 года и более чем 4 месяца работы соответственно.

В отношении нарушителя-предприятия будем полагать следующее:

1. Основным мотивом нарушителя является получение прибыли в краткосрочной или среднесрочной перспективе 5-10 лет.

2. Нарушитель имеет глубокие знания в области информационных технологий и криптографии. В частности, может разработать и запрограммировать параллельные алгоритмы вскрытия криптографической защиты до 1000 раз более эффективные, чем общеизвестные.

3. До 90% имеющихся финансовых средств нарушитель израсходует на приобретение средств вычислительной техники – серверных ЭВМ, которые будут работать 24 часа в сутки, 7 дней в неделю, с полным износом за 8 лет, а остальные финансовые средства уйдут на зарплату работников, приобретение или аренду помещений, оплату электроэнергии и других коммунальных услуг. Стоимость процессоров, в том числе сопроцессоров, может составлять до 90% от стоимости многопроцессорных серверных ЭВМ, то есть до $1 \text{ млн.} \times 0,9 \times 0,9 = 810 \text{ тыс. МРП}$. Согласно данным основных производителей процессоров для серверных ЭВМ, часть из которых приведены в таблице 2, условная стоимость одного ядра большинства процессоров составит 8-10 МРП при нормировании на производительность в 4 миллиарда 64-разрядных операций в секунду [9, 10]. Однако более эффективную категорию серверных сопроцессоров составляют многоядерные вычислительные ускорители типа Tesla, для которых условная стоимость одного ядра составит 0,15-0,30 МРП, а при аналогичном нормировании всего 0,5-1,0 МРП [11]. При использовании таких ускорителей нарушитель может эксплуатировать в течение 8 лет несколько ЭВМ с общим количеством ядер до 810 тыс. : $0,15 = 5,4 \text{ млн.}$, на которых решать задачи с вычислительной сложностью до $5,4 \times 10^6 \text{ (ядер)} \times 1,4 \times 10^9 \text{ (операций/с/ядро)} \times 3600 \text{ (с/час)} \times 24 \text{ (час/сутки)} \times 365,25 \text{ (сутки/год)} \times 8 \text{ (лет)} \approx 2^{22,5} \times 2^{30,5} \times 2^{25} \times 2^3 = 2^{81}$.

4. Нарушитель имеет информацию об используемых криптографических алгоритмах и протоколах. Даже в случае усилий сохранить эту информацию в секрете будем предполагать, что специалисты нарушителя в состоянии идентифицировать используемые СКЗИ, приобрести аналогичные и провести их обратный инжиниринг.

5. Нарушитель имеет весь объем переписки, то есть все шифртексты, тексты с имитовставками и/или тексты с ЭЦП.

6. Нарушитель имеет значительное количество пар открытый-шифрованный текст, в том числе может разово инициировать посылку сообщений с известным ему открытым текстом, который будет далее зашифрован СКЗИ

7. Нарушитель не имеет информации о ключах.
8. Нарушитель может разово инициировать случайные искажения ключей на этапе их распределения и загрузки в СКЗИ.
9. Нарушитель может разово инициировать случайные искажения переписки, включая зашифрованные тексты.

Таблица 2 - Характеристики современных процессоров серверных ЭВМ

Произ- води-тель	Модель	Год выпу- ска	Кол-во ядер	Частота (ГГц)	Турбо частота (ГГц)	Цена (USD)	Цена ядра (МРП)
AMD	Opteron 6338P	2014	12	3,2	3,6	220	5,2
AMD	Opteron 6370P	2014	16	2,0	2,2	600	5,4
Intel	Xeon E5 4660v4	2016	16	2,2	3,0	4727	42,2
Intel	Xeon E7 4850v4	2016	16	2,1	2,8	3003	26,8
Intel	Xeon E7 8880v4	2016	22	2,2	3,3	5895	38,3
Intel	Xeon E7 8890v4	2016	24	2,2	3,4	7174	42,7
Intel	Xeon E7 8894v4	2017	24	2,4	3,4	8894	53,0
Intel	Xeon Phi 7210	2016	64	1,3	1,5	2438	5,4
Intel	Xeon Phi 7230	2016	64	1,3	1,5	3710	8,2
Intel	Xeon Phi 7250	2016	68	1,4	1,6	4876	10,2
Intel	Xeon Phi 7290	2016	72	1,5	1,7	6254	12,4
NVIDIA	Tesla K40	2015	2880	0,745	0,875	4100	0,20
NVIDIA	Tesla K80	2015	4992	0,560	0,875	5400	0,15
NVIDIA	Tesla M40	2015	3072	0,950	1,100	5500	0,26
NVIDIA	Tesla M60	2015	4096	0,900	1,180	5500	0,19
NVIDIA	Tesla P40	2016	3840	1,300	1,530	7500	0,28
NVIDIA	Tesla P100	2016	3584	1,325	1,480	7500	0,30

Таким образом, для защиты от нарушителя-предприятия, в том числе в случае попытки вскрытия им криптографической защиты через 5-10 лет, вычислительная сложность существующих и широко известных алгоритмов вскрытия криптографической защиты должна составлять не менее $2^{81} \times 2^{10:2} \times 1000 \approx 2^{96}$. Если ущерб законного владельца информации от такого вскрытия и, соответственно, потенциальный выигрыш нарушителя не превышают 50 тыс. МРП, то есть 20-кратно меньше затраченных им средств, то это сделает заведомо экономически невыгодным вскрытие криптографической защиты даже в условиях, когда нарушитель располагает существенно большими материальными и финансовыми средствами, объединяет свои усилия с другими нарушителями-предприятиями, использует малобюджетные средства вычислительной техники.

5. Модель нарушителя "Корпорация"

К категории "корпорация" будем относить транснациональные корпорации, специальные службы, преступные сообщества и иных физических и юридических лиц, для вскрытия криптографической защиты конкретной системы располагающих материальными и финансовыми средствами в объеме до 1 млрд. МРП (около 2 трлн. тенге, 6 млрд. евро или 5 млн. тройских унций золота).

В эту категорию попадают практически все транснациональные корпорации. Так, если для мировых лидеров по прибыли в 2016 году среди публичных компаний Apple (53,7 млрд. USD прибыли), ICBC (44,2 млрд.) и China Construction Bank (36,4 млрд.) указанный объем соответствует их прибыли за 1-2 месяца, то для лидеров в области электроники, вычислительной техники и программного обеспечения Alphabet (17,0 млрд.), Samsung Electronics (16,5 млрд.), IBM (12,9 млрд.), Intel (11,5 млрд.) и Microsoft (10,2 млрд.) этот объем соответствует их прибыли уже за 5-8 месяцев [12].

В открытом доступе достоверные сведения о бюджетах спецслужб и преступных сообществ, как правило, отсутствуют. Опираясь на отрывочные сведения из Интернета, Агентство национальной безопасности США (годовой бюджет от 5 до 50 млрд. USD), Министерство

государственной безопасности КНР (4-5 млрд. USD), Штаб-квартира правительственной связи Великобритании (около 1 млрд. фунтов стерлингов), Федеральная служба безопасности России (около 60 млрд. рублей), БНД ФРГ (552 млн. евро) и другие специальные службы для вскрытия криптографической защиты конкретной системы не располагают средствами свыше 1 млрд. МРП, что примерно соответствует их квартальному (только АНБ США), годовому (МГБ КНР, ШКПС Великобритании, ФСБ России) или даже десятилетнему бюджету (БНД ФРГ и др.). Аналогичными средствами располагают наиболее сильные транснациональные преступные сообщества, в частности, сицилийская Коза Ностра, неапольская Каморра и другие преступные организации итальянской мафии (суммарный годовой доход всех организаций итальянской мафии около 200 млрд. евро).

В категорию "корпорация" заведомо попадают около 50 стран мира, имевшие в 2016 году ВВП не более 1 млрд. МРП, в том числе Таджикистан (6,9 млрд. USD, 143 место из 191 оцененной страны), Молдова (6,8 млрд., 144 место), Косово (6,7 млрд., 145 место), Киргизстан (6,6 млрд., 146 место). Кроме того, представляется маловероятным, что даже в военное время страна на вскрытие криптографической защиты системы противника в состоянии потратить более 10% своего ВВП. Поэтому к этой же категории нарушителей целесообразно отнести более широкий перечень стран, включая Кению (68,9 млрд. USD, 70 место), Гватемалу (68,2 млрд., 71 место), Узбекистан (66,5 млрд., 72 место) и многие другие [13].

В отношении нарушителя-корпорации будем полагать следующее:

1. Основным мотивом нарушителя является получение не только непосредственно финансовых, но военных и политических дивидендов, в том числе в долгосрочной перспективе 10-20 лет.

2. Нарушитель имеет уникальные знания в области информационных технологий и криптографии. В частности, может разработать и запрограммировать параллельные алгоритмы вскрытия криптографической защиты до 10^6 раз более эффективные, чем общеизвестные.

3. До 90% имеющихся финансовых средств нарушитель израсходует на приобретение средств вычислительной техники – супер-ЭВМ, в том числе из списка TOP500, которые будут работать 24 часа в сутки, 7 дней в неделю, с полным износом за 8 лет, а остальные финансовые средства уйдут на зарплату работников, приобретение или аренду помещений, оплату электроэнергии и других коммунальных услуг. Стоимость процессоров, в том числе сопроцессоров, может составлять до 90% от стоимости многопроцессорных супер-ЭВМ, то есть до $1 \text{ млрд.} \times 0,9 \times 0,9 = 810 \text{ млн. МРП}$. При использовании многоядерных вычислительных ускорителей, ранее рассмотренных в модели нарушителя "Предприятие", нарушитель-корпорация может эксплуатировать в течение 8 лет несколько ЭВМ с общим количеством ядер до 810 млн. : $0,15 = 5,4 \text{ млрд.}$, на которых решать задачи с вычислительной сложностью до $5,4 \times 10^9$ (ядер) $\times 1,4 \times 10^9$ (операций/с/ядро) $\times 3600$ (с/час) $\times 24$ (час/сутки) $\times 365,25$ (сутки/год) $\times 8$ (лет) $\approx 2^{32,5} \times 2^{30,5} \times 2^{25} \times 2^3 = 2^{91}$. Для сравнения, согласно тестам Linpack при аналогичном использовании супер-ЭВМ Sunway TaihuLight стоимостью 270 млн. USD возможно решать задачи сложностью до $93,0$ (PFLOPS) $\times 3600$ (с/час) $\times 24$ (час/сутки) $\times 365,25$ (сутки/год) $\times 8$ (лет) $\approx 2^{56,5} \times 2^{25} \times 2^3 = 2^{84,5}$ операций с плавающей точкой [3]. На 25-32 таких супер-ЭВМ общей стоимостью около 1 млрд. МРП станет возможным выполнение до $2^{84,5} \times 32 = 2^{89,5}$ операций.

4. Нарушитель имеет исчерпывающую информацию об используемых криптографических алгоритмах и протоколах. Даже в случае усилий сохранить эту информацию в секрете будем предполагать, что специалисты нарушителя в состоянии идентифицировать используемые СКЗИ, приобрести аналогичные и провести их обратный инжиниринг, а также получить доступ к используемым СКЗИ, к их технической документации и даже похитить некоторые экземпляры, в том числе через инсайдеров.

5. Нарушитель имеет весь объем переписки, то есть все шифртексты, тексты с имитовставками и/или тексты с ЭЦП.

6. Нарушитель имеет значительное количество пар открытый-шифрованный текст, а также может инициировать создание таких пар, в том числе путем послышки через инсайдеров сообщений с известным ему открытым текстом, который будет далее зашифрован СКЗИ. Также для создания таких пар могут быть использованы похищенные СКЗИ.

7. Нарушитель может регулярно получать доступ к ключам на этапе их распределения и загрузки в СКЗИ.

8. Нарушитель может регулярно искажать ключи на этапе их распределения и загрузки в СКЗИ.

9. Нарушитель может регулярно искажать переписку, включая зашифрованные тексты.

Таким образом, для защиты от нарушителя-корпорации, в том числе в случае попытки вскрытия криптографической защиты через 10-20 лет и со 100-кратным резервированием, вычислительная сложность существующих и широко известных алгоритмов вскрытия криптографической защиты должна составлять не менее $2^{91} \times 2^{20,2} \times 10^6 \times 100 \approx 2^{128}$. Если ущерб законного владельца информации от такого вскрытия и, соответственно, потенциальный выигрыш нарушителя не превышают 25 млн. МРП, то есть 40-кратно меньше затраченных им средств, то это сделает заведомо экономически и политически невыгодным вскрытие криптографической защиты даже в условиях, когда нарушитель располагает существенно большими материальными и финансовыми средствами, объединяет свои усилия с другими нарушителями-корпорациями, использует малобюджетные средства вычислительной техники.

6. Модель нарушителя "Империя"

К категории "империя" будем относить ведущие страны мира и иных физических и юридических лиц, для вскрытия криптографической защиты конкретной системы располагающих материальными и финансовыми средствами в объеме до 1 трлн. МРП (около 2 квдрлн. тенге, 6 трлн. евро или 5 млрд. тройских унций золота).

Например, в эту категорию попадают США (18,6 трлн. USD ВВП в 2016 году, 1 место в мире), КНР (11,2 трлн., 2 место), Япония (4,9 трлн., 3 место), ФРГ (3,5 трлн., 4 место), Великобритания (2,6 трлн., 5 место) и другие ведущие страны, а также НАТО (892 млрд. USD бюджет 2016 года) [13].

В отношении нарушителя-империи будем полагать следующее (пункты 4-9 совпадают с соответствующими пунктами для нарушителя-корпорации):

1. Основным мотивом нарушителя является получение не столько непосредственно финансовых, сколько военных и политических дивидендов, в том числе в долгосрочной перспективе 15-30 лет.

2. Нарушитель имеет уникальные знания во всех областях науки и техники. В частности, может разработать и запрограммировать параллельные алгоритмы вскрытия криптографической защиты до 10^9 раз более эффективные, чем общеизвестные.

3. Практически все имеющиеся финансовые средства нарушитель израсходует на разработку, производство или приобретение средств вычислительной техники – супер-ЭВМ с доминантой передовых процессоров и сопроцессоров, которые будут работать 24 часа в сутки, 7 дней в неделю, с полным износом за 8 лет. При государственном подходе издержки на производство гигантской партии вычислительной техники и, в частности, вычислительных ускорителей нарушитель сможет снизить до 0,01 МРП на ядро, то есть в 15-25 раз по сравнению с ценами вычислительных ускорителей, ранее рассмотренных в модели нарушителя "Предприятие", а производительность каждого ядра повысится до 5 GFLOPS. В результате, нарушитель-империя может эксплуатировать в течение 8 лет значительное количество ЭВМ с общим количеством ядер до 1 трлн. : $0,01 = 100$ трлн., на которых решать задачи с вычислительной сложностью до 100×10^{12} (ядер) $\times 5 \times 10^9$ (операций/с/ядро) $\times 3600$ (с/час) $\times 24$ (час/сутки) $\times 365,25$ (сутки/год) $\times 8$ (лет) $\approx 2^{46,5} \times 2^{32,5} \times 2^{25} \times 2^3 = 2^{107}$.

4. Нарушитель имеет исчерпывающую информацию об используемых криптографических алгоритмах и протоколах.

5. Нарушитель имеет весь объем переписки, то есть все шифртексты, тексты с имитовставками и/или тексты с ЭЦП.

6. Нарушитель имеет значительное количество пар открытый-шифрованный текст, а также может инициировать создание таких пар.

7. Нарушитель может регулярно получать доступ к ключам на этапе их распределения и загрузки в СКЗИ.

8. Нарушитель может регулярно искажать ключи на этапе их распределения и загрузки в СКЗИ.

9. Нарушитель может регулярно искажать переписку, включая зашифрованные тексты.

Таким образом, для защиты от нарушителя-империи, в том числе в случае попытки вскрытия криптографической защиты через 15-30 лет и со 250-кратным резервированием, вычислительная сложность существующих и широко известных алгоритмов вскрытия криптографической защиты должна составлять не менее $2^{107} \times 2^{30:2} \times 10^9 \times 250 \approx 2^{160}$. Если ущерб законного владельца информации от такого вскрытия и, соответственно, потенциальный выигрыш нарушителя не превышают 10 млрд. МРП, то есть 100-кратно меньше затраченных им средств, то это сделает заведомо экономически невыгодным вскрытие криптографической защиты даже в условиях, когда нарушитель располагает существенно большими материальными и финансовыми средствами, объединяет свои усилия с другими нарушителями-империями, использует малобюджетные средства вычислительной техники.

7. Сравнительный анализ стандарта СТ РК 1073-2007

Стандарт предусматривает 4 уровня безопасности, которые в порядке возрастания в определенной мере соответствуют построенным моделям нарушителей "Специалист", "Предприятие", "Корпорация" и "Империя". В результате их сравнительного анализа получаем следующее:

1. Согласно Стандарту СКЗИ первого уровня безопасности предназначены для защиты информации, ущерб от разглашения, навязывания или несанкционированного изменения которой в объеме, защищенном с использованием одного и того же ключа, не превышает 100 МРП; а вычислительная сложность существующих алгоритмов вскрытия криптографической защиты должна составлять не менее 2^{50} [1]. Сравнение этих характеристик с моделью нарушителя "Специалист" показывает, что требование Стандарта о вычислительной сложности алгоритмов вскрытия уже недостаточно, так как для защиты от нарушителя с бюджетом до 1000 МРП вычислительная сложность существующих и широко известных алгоритмов вскрытия криптографической защиты должна составлять не менее 2^{64} . То есть, нарушитель-специалист за 4 года сможет вскрыть до $2^{64} : 2^{50} = 2^{14} = 16384$ криптографических систем первого уровня безопасности или по одной системе каждые 2 часа, нанеся ущерб законным владельцам информации и получив потенциальный выигрыш до 1,6 млн. МРП, что многократно окупит бюджет, израсходованный нарушителем. Кроме того, многие требования первого уровня безопасности, например, длина ключа симметричных алгоритмов не менее 60 бит, длина ключа асимметричных алгоритмов не менее 120 бит и длина хеш-кода не менее 120 бит, теоретически недостаточны, так как в случае граничных значений дают возможность применения алгоритмов вскрытия криптографической защиты с вычислительной сложностью всего 2^{60} операций шифрования, формирования и проверки ЭЦП или вычисления хеша [4]. При реализации этих операций за одну операцию процессора, нарушитель-специалист за 4 года сможет вскрыть до $2^{64} : 2^{60} = 2^4 = 16$ криптографических систем с указанными характеристиками или по одной системе каждые 3 месяца, нанеся ущерб законным владельцам информации и получив потенциальный выигрыш до 1600 МРП, что, возможно, окупит бюджет, израсходованный нарушителем.

2. Согласно Стандарту СКЗИ второго уровня безопасности предназначены для защиты информации, ущерб от вскрытия криптографической защиты которой не превышает 10 тыс. МРП; а вычислительная сложность существующих алгоритмов вскрытия криптографической защиты должна составлять не менее 2^{80} [1]. Сравнение этих характеристик с моделью нарушителя "Предприятие" показывает, что требование Стандарта о вычислительной сложности алгоритмов вскрытия уже теоретически недостаточно, так как для защиты от нарушителя с бюджетом до 1 млн. МРП вычислительная сложность существующих и широко известных алгоритмов вскрытия криптографической защиты должна составлять не менее 2^{91} при использовании современной вычислительной техники и не менее 2^{96} в случае попытки вскрытия криптографической защиты через 5-10 лет. То есть, нарушитель-предприятие за 8 лет после начала вычислений сможет вскрыть до $2^{91} : 2^{80} = 2^{11} = 2048$ и $2^{96} : 2^{80} = 2^{16} = 65536$ криптографических систем второго уровня безопасности или по одной системе каждые 35 часов и каждый час, нанеся ущерб законным

владельцам информации и получив потенциальный выигрыш около 20 млн. и 600 млн. МРП соответственно, что многократно окупит бюджет, израсходованный нарушителем. Кроме того, некоторые требования второго уровня безопасности, например, длина ключа асимметричных алгоритмов не менее 160 бит и длина хеш-кода не менее 160 бит, также теоретически недостаточны, так как в случае граничных значений влекут наличие алгоритмов вскрытия криптографической защиты с вычислительной сложностью 2^{80} операций шифрования, формирования и проверки ЭЦП или вычисления хеша [4].

3. Согласно Стандарту СКЗИ третьего уровня безопасности предназначены для защиты информации, ущерб от вскрытия криптографической защиты которой не превышает 1 млн. МРП; а вычислительная сложность существующих алгоритмов вскрытия криптографической защиты должна составлять не менее 2^{120} [1]. Сравнение этих характеристик с моделью нарушителя "Корпорация" показывает, что требование Стандарта о вычислительной сложности алгоритмов вскрытия финансово достаточно, так как для защиты от нарушителя с бюджетом до 1 млрд. МРП вычислительная сложность существующих и широко известных алгоритмов вскрытия криптографической защиты должна составлять не менее 2^{121} в случае попытки вскрытия криптографической защиты через 10-20 лет и без резервирования. То есть, нарушитель-корпорация за 8 лет после начала вычислений сможет вскрыть до $2^{121} : 2^{120} = 2$ криптографических систем третьего уровня безопасности или по одной системе каждые 4 года, нанеся ущерб законным владельцам информации и получив потенциальный выигрыш не более 2 млн. МРП, что финансово, да и политически, не окупит бюджет, израсходованный нарушителем.

4. Согласно Стандарту СКЗИ четвертого уровня безопасности предназначены для защиты информации, ущерб от вскрытия криптографической защиты которой не превышает 100 млн. МРП; а вычислительная сложность существующих алгоритмов вскрытия криптографической защиты должна составлять не менее 2^{160} [1]. Сравнение этих характеристик с моделью нарушителя "Империя" показывает, что требование Стандарта о вычислительной сложности алгоритмов вскрытия вполне достаточно, так как для защиты от нарушителя с бюджетом до 1 трлн. МРП вычислительная сложность существующих и широко известных алгоритмов вскрытия криптографической защиты должна составлять не менее тех же 2^{160} в случае попытки вскрытия криптографической защиты через 15-30 лет и с 250-кратным резервированием. И даже вскрыв эту криптографическую защиту, несмотря на заложенный резерв, нарушитель-империя нанесет ущерб законным владельцам информации и получит потенциальный выигрыш не более 100 млн. МРП, что никак не окупит бюджет, израсходованный нарушителем.

Заключение

Построенные модели нарушителей криптографической защиты информации доказывают то, что ряд положений стандарта СТ РК 1073-2007, особенно касающиеся первого и второго уровня безопасности, устарели, а сам стандарт подлежит безусловной переработке. В частности, в новой редакции стандарта СТ РК 1073-2017 для 1, 2, 3 и 4 уровней безопасности целесообразно указать:

- СКЗИ предназначены для защиты информации стоимостью не более 100, 50 тыс., 25 млн. и 10 млрд. МРП от потенциальных нарушителей с бюджетом не более 1000, 1 млн., 1 млрд. и 1 трлн. МРП соответственно;

- вычислительная сложность известных алгоритмов вскрытия криптографической защиты должна быть не менее 2^{64} , 2^{96} , 2^{128} и 2^{160} с учетом поправки на вероятность успешного применения этих алгоритмов;

- длина ключа используемых симметричных алгоритмов криптографического преобразования должна быть не менее 80, 120, 160 и 200 бит соответственно.

ЛИТЕРАТУРА

[1] СТ РК 1073-2007. Средства криптографической защиты информации. Общие технические требования. – Астана: Госстандарт, 2008. – 30 с.

[2] Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности: Постановление Правительства РК от 20.12.2016г. № 832 // САПП РК. – 2016. – № 65. – С.428.

[3] TOP500 List. – Waibstadt: Prometheus, 2017. – Доступно: <https://www.top500.org/lists>.

- [4] Абдрахманов А.Е., Байбатчаева Д.А. Криптографические основания разработки стандарта СТ РК 1073-2007 // XI Международная научно-практическая конференция "Безопасность информации в информационно-телекоммуникационных системах". Тезисы докладов. – К.: ЕКМО, ТЕЗИС, КПИ, 2008. – С.20-21.
- [5] Бабаш А.В., Шанкин Г.П. Криптография / Под ред. В.П.Шерстюка, Э.А.Применко. – М.: СОЛОН-Р, 2002. 512 с.
- [6] A.Menezes, P.Oorschot, S.Vanstone. Handbook of Applied Cryptography. – Boca Raton, New York, London, Tokyo: CRC Press, 1997. – 780 p.
- [7] Оплата труда в Республике Казахстан. 2012-2016. Статистический сборник. – Астана: Керемет Баспа Уйі, 2017. – 126 с. – Доступно: <http://www.stat.gov.kz>.
- [8] Gross domestic product per capita, current prices. 2016 // Word Economic Outlook Database. – Washington: IMF, 2017, April. – Доступно: <http://www.imf.org>, [https://ru.wikipedia.org/wiki/Список_стран_по_ВВП_\(номинал\)_на_душу_населения](https://ru.wikipedia.org/wiki/Список_стран_по_ВВП_(номинал)_на_душу_населения).
- [9] Desktop Processors. Server Processors. – Sunnyvale: AMD, 2017. – Доступно: <http://shop.amd.com/en-us/components/processors>.
- [10] Процессоры. – Санта-Клара: Intel, 2017. – Доступно: <https://ark.intel.com/ru>.
- [11] Tesla Server Solutions. – Санта-Клара: NVIDIA, 2017. – Доступно: <http://www.nvidia.com/object/tesla-servers.html>.
- [12] The World's Biggest Public Companies. – Jersey City: Forbes, 2017. – Доступно: <https://www.forbes.com/global2000/list>.
- [13] Gross domestic product, current prices. 2016 // Word Economic Outlook Database. – Washington: IMF, 2017, April. – Доступно: <http://www.imf.org>, [https://ru.wikipedia.org/wiki/Список_стран_по_ВВП_\(номинал\)](https://ru.wikipedia.org/wiki/Список_стран_по_ВВП_(номинал)).

REFERENCES

- [1] ST RK 1073-2007. Means of cryptographic protection of information. General technical requirements. Astana: Gosstandart, 2008. 30 p. (in Russ.)
- [2] On the approval of unified requirements in the field of information and communication technologies and information security: Decree of the Government of the Republic of Kazakhstan of 20.12.2016 № 832. *SAPP RK*. 2016. № 65. P.428. (in Russ.)
- [3] TOP500 List. Waibstadt: Prometheus, 2017. Available at <https://www.top500.org/lists>. (in Eng.)
- [4] Abdrakhmanov A.E., Baibatchaeva D.A. Cryptographic grounds for the development of standard ST RK 1073-2007. *XI International Scientific and Practical Conference "Information Security in Information and Telecommunication Systems"*. K.: EKMO, TEZIS, KPI, 2008. P.20-21. (in Russ.)
- [5] Babash A.V., Shankin G.P. Cryptography. M.: SOLON-R, 2002. 512 p. (in Russ.)
- [6] A.Menezes, P.Oorschot, S.Vanstone. Handbook of Applied Cryptography. Boca Raton, New York, London, Tokyo: CRC Press, 1997. 780 p. (in Eng.)
7. Remuneration of labor in the Republic of Kazakhstan. 2012-2016. Statistical compilation. Astana: Keremet Baspa Uii, 2017. 126 p. (in Russ.) Available at <http://www.stat.gov.kz>.
8. Gross domestic product per capita, current prices. 2016. *Word Economic Outlook Database*. Washington: IMF, 2017, April. (in Eng.) Available at <http://www.imf.org>, [https://en.wikipedia.org/wiki/List_of_countries_by_GDP_\(nominal\)_per_capita](https://en.wikipedia.org/wiki/List_of_countries_by_GDP_(nominal)_per_capita).
9. Desktop Processors. Server Processors. Sunnyvale: AMD, 2017. (in Eng.) Available at <http://shop.amd.com/en-us/components/processors>.
10. Processors. Santa Clara: Intel, 2017. (in Eng.) Available at <https://ark.intel.com/en>.
11. Tesla Server Solutions. – Santa Clara: NVIDIA, 2017. (in Eng.) Available at <http://www.nvidia.com/object/tesla-servers.html>.
12. The World's Biggest Public Companies. Jersey City: Forbes, 2017. (in Eng.) Available at <https://www.forbes.com/global2000/list>.
13. Gross domestic product, current prices. 2016. *Word Economic Outlook Database*. Washington: IMF, 2017, April. (in Eng.) Available at <http://www.imf.org>, [https://en.wikipedia.org/wiki/List_of_countries_by_GDP_\(nominal\)](https://en.wikipedia.org/wiki/List_of_countries_by_GDP_(nominal)).

А.Е.Абдрахманов

ЖШС "Granit Technology", Алматы, Қазақстан

КРИПТОГРАФИЯЛЫҚ ҚОРҒАУ БҰЗУШЫЛАР МОДЕЛДЕР
ЖӘНЕ ҚР СТ 1073-2007 СТАНДАРТЫ

Аннотация. Бұл мақалада ақпараттың криптографиялық қорғауын бұзушылар моделдері мәселесі қарастырылған. Құрастырылған моделдерде бұзушылар мотивациясы, білімі, қаржы және техникалық мүмкіншіліктері ескерілді. Криптографиялық қорғанысты ашуда есептеуі қиын болатын белгілі алгоритмдердің қауіпсіздік шегі анықталды. Бұзушылар моделдері және ҚР СТ 1073-2007 "Ақпаратты криптографиялық қорғау құралдары. Жалпы техникалық талаптар" Қазақстан Республикасының мемлекеттік стандартына салыстырмалы талдау жасалды. Талдау нәтижесі бойынша осы стандартты 2017 жылы сөзсіз қайта өндеуге нақты ұсынымдар берілген.

Тірек сөздер: ақпаратты қорғау, криптография, бұзушы моделі, мемлекеттік стандарт, қауіпсіздік деңгейі.

Сведения об авторе:

Абдрахманов Альжан Есиркепович – кандидат физ.-мат. наук, советник директора по криптографической защите информации ТОО "Granit Technology", СЭЗ ПИТ "Алатау", Алматы, Казахстан.

МАЗМҰНЫ

<i>Генбач А.А., Джаманкулова Н.О.</i> Жоғарғы үдемелі капиллярлық-кеуектік жылуалмастырғышты зерттеу және есептеу.....	5
<i>Ламбекова А.Н.</i> Ішкі аудит тиімділігі: ауқымды мәліметтерді талдау.....	11
<i>Мынбаева Д.Е., Нургалиева А.М.</i> Екінші деңгейдегі банктердің басқару есебінде трансферттік бағалау белгілеудің қалыптасуы.....	15
<i>Сунакбаева Д.К.</i> Болашақ эколог мамандарды кәсіби даярлауда мобильді технологияларды пайдалану.....	19

Химия

<i>Стацюк В.Н., Айт С., Журинов М. Ж., Фогель Л.А., Абрашов А. А.</i> Гетероциклді аминдердің сынаптағы адсорбциялық сипаттамалары мен темірдегі ингибиторлық қабілеті арасындағы өзара байланыс.....	23
<i>Ермагамбет Б.Т., Қазанқапова М.Қ., Нургалиев Н.У., Касенова Ж.М., Сайранбек А., Абылгазина Л.Д.</i> «Кендірлік» кенішінен алынған тақтатаст негізінде кеуекті-көміртекті материалдарды алу.....	30
<i>Шамбилова Г. Қ., Абдықадыров Б. К., Ажғалиев М. Н., Аманов Н.К.</i> Целлюлоза мен синтетикалық полимерлердің N-метилморфолин-N-оксидіндегі аралас ерітінділерінің фазалық ауысулары мен реологиялық қасиеттері.....	38

Техникалық ғылымдар

<i>Жәрменов Ә.А., Шалғымбаев С.Т., Ниязов А.А., Ли Э.М., Болотова Л.С., Агибаева Д.Н., Тюгай О.М., Шегай О.Г.</i> «Қажықонған» кенішінің тотықтырылған мыс кендерін қайта өңдеу құрамдастырылған флотациялық-гидрометаллургиялық технологиясын әзірлеу.....	46
---	----

Ақпараттық технологиялар

<i>Абдрахманов А.Е.</i> Криптографиялық қорғау бұзушылар моделдер және ҚР СТ 1073-2007 стандарты.....	62
---	----

Медицина

<i>Филиппова А.А., Рахимов Қ.Д., Абуова Ж.Б.</i> Ауруханада антибиотиктерді тиімді пайдалану қағидалары.....	72
<i>Сапаров Қ.А., Әсіл Ж.С.</i> Әр түрлі дозадағы темекі түтінінің әсеріне өкпенің құрылымдық-функциональдік өзгерістерін зерттеу.....	77

Биология

<i>Аширбеков Е.Е., Ботбаев Д.М., Белкожаев А.М., Абайлдаев А.О., Неупокоева А.С., Мухатаев Ж.Е., Алжанұлы Б., Шарафутдинова Д.А., Мукушкина Д.Д., Рахымгожин М.Б., Хансеитова А.К., Лимборская С.А., Айтхожина Н.А.</i> Оңтүстік-қазақстан, жамбыл және алматы облысы қазақтарының Y-хромосома гаплотоптарының таралуы.....	85
<i>Мустафин К.Г., Ахметсадыков Н.Н., Нармуратова Ж.Б., Жакипбекова А.С.</i> <i>Ganoderma Lucidum</i> және <i>Trametes Versicolor</i> саңырауқұлақтары биомассасының биологиялық белсенділігін зерттеу.....	96
<i>Мухтубаева С.К., Нелина Н.В., Ситпаева Г.Т., Құдабаева Г.М., Веселова П.В., Билибаева Б.К., Жумадилова А.</i> Солтүстік Тянь-Шанның (Күнгей және Қырғыз Алатауы) сирек, эндемді, реликті және жойылып бара жатқан өсімдік түрлері	103
<i>Лаханова К.М., Кедельбаев Б.Ш.</i> Сыра үгіндісі гидролитикалық гидролиз және гидрлеу арқылы ксилит алу процесін зерттеу.....	111

Аграрлық ғылым

<i>Айдарханова Г.С., Тілеуберді А.Н.</i> Ағаш емес орман ресурстарының қолдану мәселелері мен келешегі.....	117
---	-----

Қоғамдық ғылымдар

<i>Азатбек Т., Тлесова Э., Бочарова А.</i> Беларусь республикасының экономикасындағы шетелдік инвестициялардың рөлін бағалау.....	128
<i>Асаинов А.Ж., Сәкенов Н.А., Сарыбаева И.Е.</i> Қазақстанның экономикалық қауіпсіздігі заманауи шарттары.....	138
<i>Аюпова З.К., Құсайынов Д.Ө.</i> Құқықтың эволюциялық даму кезеңдері туралы.....	142
<i>Бекенова Л.М.</i> Алматыдағы инновациялық дамуды стратегиялық басқару.....	147
<i>Буткенова А. Қ.</i> (Мысалы Қазақмыс корпорациясы ЖШС) адам капиталын басқарудың өнеркәсіптік кәсіпорындар зерттеу саясаты.....	154
<i>Калиева Г.Т.</i> Агроөнеркәсіптердің инновациялық даму бағалау әдістері.....	158
<i>Құлбекова А.Ж.</i> Кәсіпкерлік мәні және бағалау, кәсіпкерлік тәуекелді қабылдау кезінде инвестициялық жобасының мұнай-газ саласы.....	165
<i>Молдашева А. К.</i> Атырау облысы бойынша шағын және орта бизнестің даму ерекшеліктері.....	176
<i>Насимов М. Ө.</i> Бәсекелік қабілет ұғымының негізгі белгілері мен ерекшеліктері.....	182

<i>Нурлихина Г.Б., Кольбаев М.К., Маткаримова Л.К.</i> Қазақстандағы шағын кәсіпкерліктің инновациялық инфрақұрылымының қазіргі жағдайы.....	190
<i>Хуаныш Л.</i> Заманауи шарттардағы қр кәсіпорындарында ішкі бақылау.....	205
<i>Серикова М.А.</i> Қазақстан республикасындағы салық аудитінің даму жағдайы мен перспективалары.....	211
<i>Темирова А.Б., Амирова Г., Юсупова С.А. Баймунинова Н.Х.</i> Халықаралық интеграция жағдайында ұлттық экономиканың бәсекеге қабілеттілігін арттыру.....	218
<i>Уахитжанова А.М.</i> Экономика аграрлық секторының бәсекеге қабілеттілігінің кепілі ретіндегі Қазақстан агроөнеркәсіптік кешені дамуын қаржыландыру	226
<i>Жанбырбаева С.М., Зурбаева А.Б.</i> Фасилити менеджмент кәсіпорын инфрақұрылымын басқарудың заманауи бағыты ретінде.....	236
<i>Саткалиева Т.С.</i> Қазақстандағы еңбекақы төлеу және қызметкерлерді ынталандыру жүйесі.....	245
<i>Ниеталина Г.К.</i> Қазақстандағы агроөнеркәсіп кешенінің бүгінгі жағдайы.....	252
<i>Әбжет Б.С., Шайхыстамова М.Б.</i> Түркі халықтарында қисса жанрының дамуы және оның архаикалық эпос жанрына тигізген әсері.....	260
<i>Шойбеков Р., Картаева Т.</i> Кимешек атрибуциясы.....	267
<i>Сабирова Р.К., Джумаева А.К., Тепова Г.Б., Масалимова А.К.</i> Қазақстан мен Қытай темір жол саласын дамытудың өзекті мәселелері.....	277

СОДЕРЖАНИЕ

Генбач А.А., Джаманкулова Н.О. Исследование и расчет высокофорсированного капиллярно-пористого теплообменника.....	5
Ламбекова А.Н. Эффективность внутреннего аудита: анализ большими данными.....	11
Мынбаева Д.Е., Нургалиева А.М. Формирование трансфертного ценообразования в системе управленческого учета в банках второго уровня.....	15
Сунакбаева Д.К. Использование мобильных технологий в формировании профессиональной компетенции будущих экологов.....	19

Химия

Стацюк В.Н., Айт С., Журинов М. Ж., Фогель Л.А., Абрашов А. А. Взаимосвязь между адсорбционными характеристиками гетероциклических аминов на ртути и их ингибирующей способностью на железе.....	23
Ермагамбет Б.Т., Казанкапова М.К., Нургалиев Н.У., Касенова Ж.М., Сайранбек А., Абылгазина Л.Д. Получение пористо-углеродных материалов на основе сланца месторождения «Кендырлык».....	30
Шамбилова Г. К., Абдыкадыров Б. К., Ажгалиев М. Н., Аманов Н.К. Фазовые переходы и реологические свойства смешанных растворов целлюлозы и синтетических полимеров в N-метилморфолин-N-оксиде.....	38

Технические науки

Жарменов А.А., Шалгымбаев С.Т., Ниязов А.А., Ли Э.М., Болотова Л.С., Агибаева Д.Н., Тюгай О.М., Шегай О.Г. Разработка комбинированной флотационно - гидрометаллургической технологии переработки окисленной медной руды месторождения «Хаджиконган».....	46
--	----

Информационные технологии

Абдрахманов А.Е. Модели нарушителей криптографической защиты и стандарт СТ РК 1073-2007.....	62
--	----

Медицина

Филиппова А.А., Рахимов К.Д., Абуова Ж.Б. Принципы рационального применения антибиотиков в стационаре.....	72
Сапаров К.А., Асил Ж.С. Структурно-функциональное исследование легких на воздействия различных доз сигаретного дыма.....	77

Биология

Аширбеков Е.Е., Ботбаев Д.М., Белкожаев А.М., Абайлдаев А.О., Неупокоева А.С., Мухатаев Ж.Е., Алжанулы Б., Шарафутдинова Д.А., Мукушкина Д.Д., Рахымгожин М.Б., Хансеитова А.К., Лимборская С.А., Айтхожина Н.А. Распределение гаплогрупп Y-хромосомы казахов южно-казахстанской, Жамбылской и Алматинской областей.....	85
Мустафин К.Г., Ахметсадыков Н.Н., Нармуратова Ж.Б., Жакипбекова А.С. Изучение биологической активности биомассы грибов <i>Ganoderma Lucidum</i> и <i>Trametes Versicolor</i>	96
Мухтубаева С.К., Нелина Н.В., Ситпаева Г.Т., Кудаббаева Г.М., Веселова П.В., Билибаева Б.К., Жумадилова А. Редкие, эндемичные, реликтовые и исчезающие виды растений северного Тянь-Шаня (Кунгей и Киргизский Алатау).....	103
Лаханова К.М., Кедельбаев Б.Ш. Гидролитическое гидрирование целлюлозы гуза-паи с целью получения сорбита.....	111

Аграрные науки

Айдарханова Г.С., Тілеуберді А.Н. Проблемы и перспективы развития использования недревесных лесных ресурсов.....	117
--	-----

Общественные науки

Азатбек Т.А., Тлесова Э.Б., Бочарова А. Оценка роли иностранных инвестиций в экономике республики Беларусь.....	128
Асаинов А.Ж., Сакенов Н.А., Сарыбаева И.Е. Состояния экономической безопасности Казахстана в современных условиях.....	138
Аюпова З.К., Кусаинов Д.У. Об этапах эволюционного развития права.....	142
Бекенова Л.М. Стратегическое управление инновационным развитием Алматы.....	147
Буткенова А.К. Исследование политики промышленных предприятий в области управления человеческим капиталом (на примере ТОО корпорация Казахмыс).....	154
Калиева Г.Т. Методы оценки инновационного развития предприятий агропромышленного комплекса.....	158
Кулубекова А.Ж. Оценка предпринимательских рисков при принятии инвестиционного проекта в нефтегазовой отрасли.....	165

<i>Молдашева А.К.</i> Особенности развития малого и среднего бизнеса по Атырауской области.....	176
<i>Насимов М. О.</i> Основные признаки и особенности понятия конкурентоспособность	182
<i>Нурлихина Г.Б., Кольбаев М.К., Маткаримова Л.К.</i> Современное состояние инновационной инфраструктуры малого предпринимательства в Казахстане.....	190
<i>Хуаныш Л.</i> Внутренний контроль на предприятиях РК в современных условиях.....	205
<i>Серикова М.А.</i> Состояние и перспективы развития налогового аудита в республике Казахстан.....	211
<i>Темирова А.Б., Амирова Г., Юсупова С.А., Баймуминова Н.Х.</i> Повышение конкурентоспособности национальной экономики в условиях международной интеграции.....	218
<i>Уахитжанова А.М.</i> Финансирование развития агропромышленного комплекса Казахстана, как залог конкурентоспособности аграрного сектора экономики.....	226
<i>Жанбырбаева С.М., Зурбаева А.Б.</i> Фасилити менеджмент как современное направление управления объектами инфраструктуры предприятия.....	236
<i>Саткалиева Т.С.</i> Система оплаты труда и стимулирования персонала в Казахстане.....	246
<i>Ниеталина Г.К.</i> Современное состояние АПК в Казахстане.....	252
<i>Абжет Б.С., Шайхыстамова М.Б.</i> Развитие жанра саги в тюркском народе и его влияние на жанр архаического эпоса	260
<i>Шойбеков Р., Картаева Т.</i> Атрибуция кимешека.....	267
<i>Сабирова Р.К., Джумаева А.К., Тепова Г.Б., Масалимова А.К.</i> Современные проблемы развития железнодорожной отрасли Казахстана и Китая	277

CONTENT

<i>Genbach A.A., Jamankulova N.O.</i> Research and calculation of high-forced capillary-porous heat exchanger.....	5
<i>Lambekova A.N.</i> Efficiency of internal audit: large data analysis.....	11
<i>Mynbayeva D.Y., Nurgaliyeva A.M.</i> Formation of pricing in the system of management accounting of second-tier banks...	15
<i>Sunakbayeva D.K.</i> Application of mobile technologies in forming the professional competence of future ecologists.....	19
Chemistry	
<i>Statsyuk V.N., Ait S., Zhurinov M.Zh., Fogel L.A., Abrashov A. A.</i> The relationship between the adsorption characteristics of heterocyclic amines on mercury and their inhibitory ability on iron.....	23
<i>Ermagambet B.T., Kazankapova M.K., Nurgaliyev N.U., Kasenova Zh.M., Sayranbek A., Abylgazina L.D.</i> The production of porous-carbon materials from based on oil shale of the Kendyrlыk deposit.....	30
<i>Shambilova G. K., Abdykadyrov B. K., Azhgaliev M. N., Amanov N. K.</i> Phase transitions and rheological properties of mixed solutions of cellulose and synthetic polymers in N-methylmorpholine-N-oxide.....	38
Technical sciences	
<i>Zharmenov A.A., Shalgymbaev S.T., Niyazov A.A., Lee E.M., Bolotova L.S., Agibaeva D.N., Tugai O.M., Shegai O.G.</i> Development of a combined flotation-hydrometallurgical technology for the processing of oxidized copper ore at the Khadjikong deposit.....	46
Information technology	
<i>Abdrakhmanov A.E.</i> Models of violators of cryptographic protection and standard ST RK 1073-2007.....	62
Medicine	
<i>Filippova A.A., Rakhimov K.D., Abuova Zh.B.</i> Principles of rational use of antibiotics in a hospital.....	72
<i>Saparov K.A., Asil Zh.A.</i> Structural and functional study of the lungs on the effects of various doses of cigarette smoke.....	77
Biology	
<i>Ashirbekov E.E., Botbaev D.M., Belkozhaev A.M., Abayldaev A.O., Neupokoeva A.S., Mukhataev J.E., Alzhanuly B., Sharafutdinova D.A., Mukushkina D.D., Rakhymgozhin M.B., Khanseitova A.K., Limborska S.A., Ayt Khozhina N.A.</i> Distribution of Y-chromosome haplogroups of the kazakh from the south Kazakhstan, Zhambyl and almaty regions.....	85
<i>Mustafin K.G., Akhmetsadykov N.N., Narmuratova Zh.B., Zhakipbekova A.S.</i> Biological activity of <i>Ganoderma Lucidum</i> and <i>Trametes Versicolor</i> biomass	96
<i>Mukhtubaeva S.K., Nelina N.V., Sitpayeva G.T., Kudabayeva G.M., Veselova P.V., Bilibayeva B.K., Jumadilova A.</i> Rare, endemic, relict and endangered plant species of the northern Tien Shan (Kungei, Kirgizskiy Alatau).....	103
<i>Lakhanova K.M., Kedelbaev B.Sh.</i> Hydrolytic hydrogenation of 291ellulose guza-paya with the aim of obtaininc sorbitol.....	111
Agricultural science	
<i>Aidarkhanova G. S., Tileuberdi A. N.</i> Problems and prospects of development of use of non-wood	117
Social Sciences	
<i>Azatbek T.A., Tlesova E.B., Bocharova A.</i> Evaluation of the role of foreign investment in the economy of the republic of Belarus.....	128
<i>Asainov A.Zh., Sakenov NA, A., Sarybaeva I.E.</i> Status of economic safety of Kazakhstan in modern conditions.....	138
<i>Ayupova Z.K., Kussainov D.U.</i> About the stages of evolutionary development of law.....	142
<i>Bekenova L.M.</i> Strategic management of innovational development in Almaty.....	147
<i>Butkenova A. K.</i> Investigation of politics of industrial enterprises in the field of management of human capital (on the example of LLP Kazakhmys corporation).....	154
<i>Kaliyeva G.T.</i> Methods of estimation of innovative development of agro industrial complex enterprises	158
<i>Kulubekova A.Zh.</i> Estimation of enterprise risks at acceptance of investment project in oil and gas industry.....	165
<i>Moldasheva A. K.</i> Features of development of small and medium business in Atyrau region.....	176
<i>Nassimov M. O.</i> Main signs and features of the concept competitiveness.....	182
<i>Nyurlikhina G.B., Kolbayev M.K., Matkarimova L.K.</i> Contemporary state of innovative infrastructure of small entrepreneurship in Kazakhstan.....	190
<i>Huanysheva L.</i> Internal control at rk enterprises in modern conditions.....	205
<i>Serikova M.A.</i> Condition and perspectives of the development of tax audit in the republic of Kazakhstan.....	211
<i>Temirova A.B., Amirova G., Yssupova S.A., Baimuminova N.H.</i> Improving the competitiveness of the National Economy in the conditions of International Integration.....	218

<i>Uakhitzhanova A.M.</i> Financing the development of the agro-industrial complex of Kazakhstan, as a guarantee of competitiveness of the agrarian sector of the economy.....	226
<i>Zhanbyrbayeva S., Zurbayeva A.</i> Facilities management as modern direction of enterprise's infrastructure management.....	236
<i>Satkaliyeva T.S.</i> System of payment and stabulation of personnel in Kazakhstan.....	245
<i>Nietalina G.K.</i> The present state of the APK in Kazakhstan.....	252
<i>Abjet B.S. Shaykhystamova M.B.</i> Development of the genre of sagi in turkish people and its impact on genre of archaic epos.....	260
<i>Shoibekov R., Kartaeva T.E.</i> Attribution of kimeshek.....	267
<i>Sabirova P.K., Zhumayeva A.K., Tlepova G.B., Masalimova A.K.</i> Modern problems of development of railway industry of Kazakhstan and China.....	277

**Publication Ethics and Publication Malpractice
in the journals of the National Academy of Sciences of the Republic of Kazakhstan**

For information on Ethics in publishing and Ethical guidelines for journal publication see <http://www.elsevier.com/publishingethics> and <http://www.elsevier.com/journal-authors/ethics>.

Submission of an article to the National Academy of Sciences of the Republic of Kazakhstan implies that the work described has not been published previously (except in the form of an abstract or as part of a published lecture or academic thesis or as an electronic preprint, see <http://www.elsevier.com/postingpolicy>), that it is not under consideration for publication elsewhere, that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out, and that, if accepted, it will not be published elsewhere in the same form, in English or in any other language, including electronically without the written consent of the copyright-holder. In particular, translations into English of papers already published in another language are not accepted.

No other forms of scientific misconduct are allowed, such as plagiarism, falsification, fraudulent data, incorrect interpretation of other works, incorrect citations, etc. The National Academy of Sciences of the Republic of Kazakhstan follows the Code of Conduct of the Committee on Publication Ethics (COPE), and follows the COPE Flowcharts for Resolving Cases of Suspected Misconduct (http://publicationethics.org/files/u2/New_Code.pdf). To verify originality, your article may be checked by the originality detection service Cross Check <http://www.elsevier.com/editors/plagdetect>.

The authors are obliged to participate in peer review process and be ready to provide corrections, clarifications, retractions and apologies when needed. All authors of a paper should have significantly contributed to the research.

The reviewers should provide objective judgments and should point out relevant published works which are not yet cited. Reviewed articles should be treated confidentially. The reviewers will be chosen in such a way that there is no conflict of interests with respect to the research, the authors and/or the research funders.

The editors have complete responsibility and authority to reject or accept a paper, and they will only accept a paper when reasonably certain. They will preserve anonymity of reviewers and promote publication of corrections, clarifications, retractions and apologies when needed. The acceptance of a paper automatically implies the copyright transfer to the National Academy of sciences of the Republic of Kazakhstan.

The Editorial Board of the National Academy of sciences of the Republic of Kazakhstan will monitor and safeguard publishing ethics.

Правила оформления статьи для публикации в журнале смотреть на сайте:

www.nauka-nanrk.kz

ISSN 2518-1483 (Online), ISSN 2224-5227 (Print)

<http://www.reports-science.kz/index.php/ru/>

Редакторы *М. С. Ахметова, Т.А. Апендиев*
Верстка на компьютере *А.М. Кульгинбаевой*

Подписано в печать 13.12.2017.
Формат 60x881/8. Бумага офсетная. Печать – ризограф.
18,3 п.л. Тираж 2000. Заказ 6.

Национальная академия наук РК
050010, Алматы, ул. Шевченко, 28, т. 272-13-18, 272-13-19