Игорь Ю. Жуков, Олег Н. Мурашов
ООО «Национальный мобильный портал»,
Волгоградский пр., 2, офис 36, Москва, 109316, Россия
e-mail: i.zhukov@inbox.ru, http://orcid.org/0000-0002-4429-8799
e-mail: olegxozbox@yandex.ru, http://orcid.org/0000-0002-4467-2170

ЗАЩИЩЕННЫЕ ПРОЦЕДУРЫ ВЗАИМНОЙ АУТЕНТИФИКАЦИИ, ФОРМИРОВАНИЯ КЛЮЧА ФИСКАЛЬНОГО ПРИЗНАКА И ЗАЩИТЫ ФИСКАЛЬНЫХ ДАННЫХ

DOI: http://dx.doi.org/10.26583/bit.2018.2.05

Аннотация. В статье дается описание криптографических механизмов взаимной аутентификации и формирования ключа фискального признака. Эти механизмы основаны на использовании блочного шифра «Кузнечик», определенного национальным стандартом Российской Федерации ГОСТ Р 34.12–2015 и реализованного в режиме гаммирования в соответствии ГОСТ Р 34.13–2015. Функции выработки имитовставки (кода аутентификации) заданы рекомендациями по стандартизации Р 50.1.113–2016.

Предлагаемое в данной работе решение направлено на обеспечение аутентификации и контроля целостности фискальных данных, передаваемых по каналам связи между фискальными накопителями и операторами фискальных данных, а также между операторами фискальных данных и уполномоченным органом. Форматы передаваемых фискальных данных, способы передачи фискальных данных и механизмы обеспечения конфиденциальности передаваемых фискальных данных определяются уполномоченным органом федеральной исполнительной власти.

В статье дано краткое описание модели протокола, проведен формальный анализ пассивных атак в предположении, что криптографическая стойкость исследуемого протокола зависит от стойкости используемых в нем криптографических преобразований, являющихся отечественными стандартизированными решениями, регламентируемыми либо национальными стандартами, либо национальными рекомендациями по стандартизации. Так как указанные криптографические преобразования не могут быть скомпрометированы нарушителем, можно сделать вывод, что нарушителем также не может быть скомпрометирован и исследуемый протокол.

Ключевые слова: взаимная аутентификация, криптографические преобразования, мастер-ключ, фискальный признак, защита фискальных данных.

Для цитирования. ЖУКОВ, Игорь Ю.; МУРАШОВ, Олег Н.. ЗАЩИЩЕННЫЕ ПРОЦЕДУРЫ ВЗАИМНОЙ АУТЕНТИФИКАЦИИ, ФОРМИРОВАНИЯ КЛЮЧА ФИСКАЛЬНОГО ПРИЗНАКА И ЗАЩИТЫ ФИСКАЛЬНЫХ ДАННЫХ. Безопасность информационных технологий, [S.l.], n. 2, p. 63-70, 2018. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1110>. Дата доступа: 26 apr. 2018. doi:http://dx.doi.org/10.26583/bit.2018.2.05.

Igor Y. Zhukov, Oleg N. Murashov
Ltd «The National Mobile Portal»,
Volgogradskiy pr.,2 off.36, Moscow, 109316, Russia
e-mail: i.zhukov@inbox.ru, http://orcid.org/0000-0002-4429-8799
e-mail: olegxozbox@yandex.ru, http://orcid.org/0000-0002-4467-2170

A secure mutual authentication procedure, generate the key fiscal basis, and fiscal data protection

DOI: http://dx.doi.org/10.26583/bit.2018.2.05

Abstract. The paper describes cryptographic transformation for mutual authentication and creation of the fiscal sign key. This transformation based on using block encryption cipher named «Kuznetchik», described in the national standard of the Russian Federation GOST R 34.12-2015 and realized in gamma generation mode as it is described in the another national standard of the Russian Federation

GOST R 34.13-2015. The function of the integrity protection (authentication code) is defined by the recommendation for standardization R 50.1.113–2016.
The solution proposed in this paper is aimed for an authentication and integrity control of fiscal data transmitted through communication channels between fiscal storage devices and fiscal data operators, as well as between the fiscal data operators and the authorized agency. Formats of transmitted fiscal data, methods of transmission and mechanisms to ensure the confidentiality of transmitted fiscal data determined by the authorized agency of the Federal Executive power.
The article gives a short description of the protocol model, a formal analysis of passive attacks in the assumption that the cryptographic properties of the protocol depends on the feature of cryptographic transformations used, which are standardized solutions regulated by national standards, or national recommendations for standardization. Since the cryptographic transformations could not be compromised by the intruder we can conclude that the intruder also can not compromise the fiscal signs protection protocol.
Keywords: mutual authentication, cryptographic transformation, master key, fiscal sign, fiscal data protection.
For citation. ZHUKOV, Igor Y.; MURASHOV, Oleg N.. A secure mutual authentication procedure, generate the key fiscal basis, and fiscal data protection. IT Security (Russia), [S.l.], n. 2, p. 63-70, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1110>. Date accessed: 26 apr. 2018.
doi:http://dx.doi.org/10.26583/bit.2018.2.05.

Введение

Одним из важнейших направлений реализации программы «Цифровая экономика Российской Федерации» является развитие киберфизических систем, в частности, интернета вещей. При этом актуальной задачей становится обеспечение целостности и достоверности информационного обмена между элементами указанных систем. Решение этой задачи, как правило, достигается использованием защищенных процедур обмена информацией, основанных на применении симметричных криптографических преобразований и отечественных стандартов шифрования ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015.

Такая задача, в частности, возникает при реализации требований действующего законодательства по электронному обмену фискальной информацией между торговыми предприятиями и налоговыми органами [1-3]. Обязательное повсеместное использование таких процедур должно быть основано на применении стандартизованных криптографических механизмах, предложенных в [4, 7].

Настоящая работа содержит результаты исследований и обоснования криптографических качеств механизмов аутентификации и выработки ключа фискального признака для применения в средствах формирования и проверки фискальных признаков, обеспечивающих работу контрольно-кассовой техники, операторов и уполномоченных органов обработки фискальных данных в дополнение к исследованию безопасности ключевой системы фискального признака [5].

Под фискальным признаком [6] понимается достоверная информация, сформированная с использованием фискального накопителя и ключа фискального признака или с использованием средств формирования фискального признака и мастер-ключа. Последний предназначен для создания серии ключей фискального признака, а также проверки фискальных признаков, сформированных с использованием ключей фискального признака этой серии. Достоверность данных достигается в результате криптографического преобразования фискальных данных, наличие которого дает возможность выявления корректировки или фальсификации этих фискальных данных при их проверке с использованием фискального накопителя и (или) средства проверки фискального признака.

Предложенный в [4] протокол обмена представляет собой последовательность действий, в ходе которой:

- средством формирования фискальных признаков и средством проверки фискальных признаков вырабатывается разовый ключ K, однозначно зависящий от общего секретного ключа K_{FSC} и номера фискального документа *FDN*;
- выполняется аутентификация фискальных данных;
- выполняется аутентификация средства проверки фискального признака.

Следует отметить, что последовательность и размеры передаваемых сообщений жестко фиксированы соответствующими нормативными документами налоговой службы России [2, 3], что не позволяет модифицировать протокол и интегрировать в него дополнительные механизмы защиты, например, аутентификацию средства выработки фискального признака. Кроме того, следует учитывать [2, 3], что процедуры взаимной аутентификации могут выполняться в течение суток, то есть представлять собой последовательность обмена сообщениями, существенно разделенными между собой по времени.

1. Модель протокола

Для целей нашего исследования предлагаемого протокола требуется дать его схематичное описание (модель). Без ограничения общности будем считать, что общий ключ средства формирования и средства проверки фискального признака KFSC известен обоим участникам протокола заранее. Тогда, изложенный в [4] протокол может быть схематично описан следующим образом:

Средство формирования ФП		**Средство проверки ФП**
Дано: SN_{FSC}, *KFSC, FD; FDN*		Дано: K_{FSC}, SN_{FSV}
1. $K = KDF(K_{FSC}, FDN);$		
2. $FS = HMAC(K_{0...255}, FD);$		
3. $C = Enc(K_{256...511}, FS, FD);$		
	———SN_{FSC}, *FDN, FS, FD* или *C*———>	
		1. $K = KDF(K_{FSC}, FDN);$
		2. $FD = Dec(K_{256...511,} FS, C);$
		3. $FS` = Mac(K_{0...255}, FD);$
		4. *FS` != FS ——> выход с неудачей.*
		5. $M = SN_{FSV} \| SN_{FSC} \| FDN \| FS;$
		6. $FS_{FSV} = HMAC(K_{0...255}, M);$
	<——— *FDN,* $SN_{FSV,}$ FS_{FSV} ——	
4. $M = SN_{FSV} \| SN_{FSC} \| FDN \| FS;$		
5. $FS` = HMAC\ (K_{0...255}, M);$		
6. *FS` != FS ——> выход с неудачей.*		

2. Анализ пассивных атак

Учитывая, что все используемые криптографические преобразования являются отечественными стандартизированными решениями, регламентируемыми либо национальными стандартами, либо национальными рекомендациями по стандартизации, мы проведем анализ пассивных атак достаточно формально, полагая, что все используемые преобразования являются стойкими относительно атак нарушителя (в естественных предположениях о его вычислительных, финансовых и временных ресурсах) [8].

2.1. Атака на ключ фискального признака

При перехвате нарушителем фискальных данных *FD* и соответствующего им фискального признака (часть значения ключевой функции хэширования $HMAC_{256}$) *FS* возникает задача определения секретного ключа K_1, используемого в преобразовании:

$$FS = HMAC\ (K_1, FD).$$

Учитывая, что данное преобразование регламентируется рекомендациями [7], мы считаем, что эта задача является трудноразрешимой для нарушителя [9].

Здесь стоит отметить, что в силу ограниченности множества возможных значений номера фискальных данных, ключи, используемые для шифрования, принадлежат небольшому множеству мощности 2^{32}. Однако дать такое описание этому множеству, что оно может быть эффективно выписано и, как следствие опробовано, в настоящее время не представляется возможным.

Аналогично, при перехвате нарушителем зашифрованного текста *C* возникает задача определения секретного ключа K_2, используемого в преобразовании:

$$C = Enc(K_2, FD),$$

где, *Enc* – алгоритм шифрования открытого текста *FD* с помощью блочного алгоритма «Кузнечик» в режиме гаммирования, согласно ГОСТ Р 34.13-2015. При этом, величина *FD* нарушителю неизвестна[1]. Данная задача является трудноразрешимой для нарушителя.

2.2. Подделка фискального признака

Подделка фискального признака FS_{FSV} заключается в вычислении значения *FS`*, удовлетворяющего равенству:

$$FS` = HMAC(K1, FD),$$

при известном значении *FD* и неизвестном значении ключа K_1. В силу выбора преобразования HMAC, данная задача является трудноразрешимой для нарушителя [9].

2.3. Аутентификация фискальных данных

Согласно изложенной схеме легко видеть, что средство проверки фискальных данных выполняет только аутентификацию данных. Детализируем данное высказывание и рассмотрим фрагмент изложенной выше последовательности действий:

Средство формирования ФП		**Средство проверки ФП**
2. $FS = Mac(K_{0...255}, FD);$		
3. $C = Enc(K_{256...511}, FS, FD);$		
	———SN_{FSC}; FDN, FS, FD или C———>	
		2. $FD = Dec(K_{256...511,} FS;C);$
		3. $FS` = HMAC(K_{0...255}, FD);$

В данном фрагменте протокола для фискальных данных FD средством выработки сначала вычисляется часть значения ключевой функции хэширования $HMAC_{256}$, то есть значение *FS*, а после данные *FD* передаются в открытом или зашифрованном виде.

Средство проверки получает сообщение, расшифровывает данные (в случае необходимости), а после вычисляет часть значения ключевой функции хэширования $HMAC_{256}$ на своей копии ключа *K*. В этом случае аутентификация данных выполняется, когда полученное *FS* и вычисленное средством проверки FS` значения совпадают (очевидно, что совпадение произойдет, когда ключи выработки значения ключевой функции хэширования совпадают, а переданные данные не были модифицированы при передаче) [10].

Тем не менее, данный фрагмент не позволяет аутентифицировать участника, отправившего сообщение. Действительно, предположим, что нарушитель сохранил переданные ранее данные и отправляет их повторно. В этой ситуации, с формальной точки зрения, именно нарушитель является инициатором протокола. Вместе с тем, средство проверки фискальных данных совершенно корректно обработает посланное сообщение, продолжит протокол и выдаст в ответ нарушителю корректное сообщение.

Отметим, что аутентификация данных, а не их источника (средства формирования фискальных данных), является достаточной для функционирования системы передачи

[1] В классической постановке задачи нарушителю известен открытый и зашифрованный тексты, которые используется для нахождения секретного ключа. Вместе с тем, в нашей ситуации один ключ используется для шифрования одного сообщения, следовательно, если нарушителю известен открытый текст *FD*, то определение секретного ключа на котором он зашифрован является бесполезной задачей.

фискальных данных, поскольку сами данные содержит в себе информацию о том, кто их выработал.

Вместе с тем, описанная нами ситуация должна рассматриваться как атака на средство проверки фискальных данных. Ситуация, в которой нарушитель может повторно послать данные, которые будут корректно обработаны средством проверки фискальных данных, должна рассматриваться как успешная атака на навязывание сообщений, приводящая к компрометации протокола.

Стоит отметить, что успех данной атаки связан с отсутствием каких-либо механизмов аутентификации серийного номера средства формирования фискальных данных. Кроме того, при аутентификации данных, выработанных средством формирования фискальных данных, не используется возможность учета реального время выработки значения фискального признака, а также возможность выработки ключа в момент выработки фискального признака (формально, все ключи средства формирования фискального признака могут быть выработаны заранее, для каждого из возможных значений номера фискального документа).

Учитывая жестко фиксированную в [8, 9] последовательность передачи сообщений, а также форматов передаваемых сообщений, криптографическими методами решить указанную проблему не представляется возможным. В связи с этим, в средстве проверки фискального признака должен быть реализован механизм контроля уникальности поступающих значений *FDN* – номеров фискальных документов, привязанный к конкретному серийному номеру средства формирования фискальных документов. Это может быть достигнуто, например, использованием в качестве последовательности *FDN* монотонно возрастающей последовательности целых чисел от 0 до $2^{32} - 1$.

2.4. Аутентификация средства проверки фискального признака

Рассматриваемый протокол осуществляет аутентификацию средства проверки фискального признака – средство формирования фискального признака доказуемо подтверждает, что оно отправило фискальный признак именно тому средству проверки фискальных признаков, которому оно предназначалось (то есть оно имеет такой же секретный ключ KFSC, что и средство формирования). Для иллюстрации этого рассмотрим фрагмент исследуемого протокола:

Средство формирования ФП		**Средство проверки ФП**
	———SN_{FSC}, *FDN, FS, FD* или *C*———>	
		5. $M = SN_{FSV} \mid\mid SN_{FSC} \mid\mid FDN \mid\mid FS;$
		6. $FS_{FSV} = HMAC(K_{0...255}, M);$
	<——— *FDN*, SN_{FSV}, FS_{FSV} ——	

Таким образом, для подтверждения факта владения ключом K_{FSC} средство формирования фискального признака направляет средству проверки фискального признака, характеризуемому заданным значением SN_{FSV} случайное значение (в качестве которого выступает значение ключевой функции хэширования *FS*). В ответ средство формирования получает значение ключевой функции хэширования FS_{FSV} под отправленным значением *FS*, вычисленное с использованием общего ключа K_{FSC}.

При этом, средство проверки фискального признака вычисляет свой ответ в процессе выполнения протокола, то есть аутентифицируется в реальном времени. Стоит также отметить, что данный протокол аутентификации является модификацией протокола аутентификации из ISO/IEC 9798-2, [10], с заменой функции шифрования на функцию вычисления ключевой функции хэширования.

Также как и в случае аутентификации фискальных данных, здесь есть некоторые особенности, влияющие на корректность работы протокола. Предположим, что программная или аппаратная реализация исследуемого протокола вычисляет ключ проверки части значения ключевой функции хэширования FS_{FSV} исходя из тех данных, что получены в ответном

сообщении от средства проверки фискальных данных. В этом случае, нарушитель может навязать ложное значение FS_{FSV} , перехваченное им ранее в другом сеансе передачи данных (с другим средством проверки фискальных данных и другим номером фискального документа). Из этого следует, что средство формирования фискального признака сначала должно проверять полученные значения SN_{FSC}, SN_{FSV} и FDN на совпадение с теми, что были использованы им при выработке фискального признака, и только потом переходить к проверке значения FS_{FSV}.

2.5. Об алгоритмах выработки фискального признака

Согласно [4] используется четыре типа фискального признака:

1) фискальный признак документа размером 48 бит;
2) фискальный признак архива размером 256 бит;
3) фискальный признак сообщения размером 64 бита;
4) фискальный признак оператора размером 128 бит.

Размеры фискальных признаков жестко фиксированы соответствующими нормативными документами ФНС России [2, 3].

В связи с вышесказанным, для вычисления фискальных признаков различных длин был выбран алгоритм $HMAC_{256}$, регламентируемый рекомендациями по стандартизации [7].

Данный алгоритм является криптографически обоснованным и позволяет выработать значение ключевой функции хэширования любой необходимой нем длины, методом взятия нужного значения значащих бит от начала вектора – результата преобразования.

При выработке фискальных признаков используются криптографические механизмы, регламентируемые национальными стандартами Российской Федерации или рекомендациями по стандартизации Технического комитета № 26 Росстандарта России «Криптографическая защита информации».

2.6. О сроке действия ключа фискального признака при работе в автономном режиме

Согласно нормативным требованиям налоговой службы срок действия ключа фискального признака при работе в автономном режиме должен составлять не менее 36 месяцев.

За время действия ключа средство выработки фискального признака может использовать данный ключ для выработки фискальных признаков, а также для обеспечения конфиденциальности данных, передаваемых совместно с фискальными признаками.

С точки зрения криптографической защиты информации накопление нарушителем передаваемой информации в течение столь длительного времени может привести к возможности определения секретного ключа и, как следствие, к нарушению конфиденциальности передаваемой информации.

Однако, исходя из условий эксплуатации средств выработки фискальных признаков работа контрольно-кассовой техники в автономном режиме, можно предположить либо отсутствие каналов связи, по которым может передаваться зашифрованная информация, либо отсутствие необходимости передачи зашифрованной информации. Тем самым не возникают предпосылок к накоплению нарушителем передаваемой информации и нарушению ее конфиденциальности.

Поскольку при проведении анализа нельзя в точности заявить, что в автономном режиме использования контрольно-кассовой техники зашифрованная информация не может передаваться вообще, было бы корректным определение границы максимально возможного объема передаваемой информации в автономном режиме, исходя из криптографических свойств алгоритма ключевой функции хэширования, а также модельных эксплуатационных характеристик работы контрольно-кассовой техники в автономном режиме. На наш взгляд, точное значение данной величины должно устанавливаться в ходе проведения тематических исследований конкретного типа аппаратуры, реализующей процедуры взаимной

аутентификации, формирования ключа фискального признака, а также защиты фискальных данных.

Заключение

Из приведенных выше результатов обоснования достаточности мер криптографической защиты, принятых в ходе выполнения криптографических механизмов протокола аутентификации и выработки ключа фискального признака [4], можно сделать следующие выводы.

- Исследуемый протокол допускает возможность повторного навязывания средству проверки фискального признака переданных ему ранее сообщений. Учитывая фиксированную в [2, 3] последовательность передачи сообщений, а также форматов передаваемых сообщений, защита от повторного навязывания должна быть реализована организационными методами, основанными на отслеживании уникальности обрабатываемых номеров фискальных документов.
- Криптографическая стойкость исследуемого протокола зависит от стойкости используемых в нем криптографических преобразований, являющихся отечественными стандартизированными решениями, регламентируемыми либо национальными стандартами, либо национальными рекомендациями по стандартизации. В предположении, что указанные криптографические преобразования не могут быть скомпрометированы нарушителем, можно сделать вывод, что нарушителем также не может быть скомпрометирован и исследуемый протокол.

СПИСОК ЛИТЕРАТУРЫ:

1. Федеральный закон «О применении контрольно-кассовой техники при осуществлении наличных денежных расчетов и (или) расчетов с использованием электронных средств платежа» от 22.05.2003 N 54-ФЗ (последняя редакция). http://www.consultant.ru/document/cons_doc_LAW_42359. Дата обращения 28.02.2018.
2. Контрольно-кассовая техника. Описание интерфейса фискального накопителя. Версия 1.2 от 06.07.2016. Вводится в действие 01.07.2016. Отладочная версия ФН 1.32_1. https://pkfn.ru/files/opisanie.pdf. Дата обращения 28.02.2018.
3. Приказ ФНС России от 21 марта 2017 г., №ММВ-7-20/229. https://www.nalog.ru/rn77/about_fts/docs/6719054. Дата обращения 28.02.2018.
4. Росстандарт. Информационная технология. Криптографическая защита информации. Рекомендации по стандартизации. Криптографические механизмы аутентификации и выработки ключа фискального признака для применения в средствах формирования и проверки фискальных признаков, обеспечивающих работу контрольно-кассовой техники, операторов и уполномоченных органов обработки фискальных данных (Проект). — 2018. — 28 стр. http://www.ramec.ru/services/soprovogdenie/standart/. Дата обращения 28.02.2018.
5. Горбатов, Виктор С; Жуков, Игорь Ю; Мурашов, Олег Н. Безопасность ключевой системы фискального признака. Проблемы информационной безопасности. Компьютерные системы. СПбПУ, № 1. 2018.
6. Словарь финансовых и юридических терминов. http://www.consultant.ru/law/ref/ju_dict/word/fiskalnyj_priznak_dokumenta/ Дата обращения 28.02.2018.
7. Р 50.1-113.2016. Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования. — Стандартинформ, Москва, 2016.
8. Черемушкин А.В. Криптографические протоколы. Основные свойства и уязвимости. — М.: Академия. — 2009. — 272 с.
9. Preneel B. Analysis and Design of Cryptographic Hash Functions. — Doctoral dissertation. — Katholieke Universiteit Leuven. — January 1993. 321p.
10. Menezes A.V., van Oorschot P. C., Vanstone S. A. Handbook of applied cryptography.— CRC Press. — 1996. — 816p.

REFERENCES:

[1] Federal law «About application of cash registers with cash calculations and (or) calculations with use of electronic tools of payment» of 05/22/2003 N54-FZ (latest edition). http://www.consultant.ru/document/cons_doc_LAW_42359. Check date 02/28/2018. (in Russian).

[2] Cash register equipment. The Fiscal storage interface description. Version 1.2 of 07/06/2016. Enforced 07/01/2016. The debug version of FN 1.32_1. https://pkfn.ru/files/opisanie.pdf. Check date 02/28/2018. (in Russian).
[3] Order of the Federal tax service of 21 March 2017, №ММВ-7-20/229. https://www.nalog.ru/rn77/about_fts/docs/6719054 Check date 02/28/2018. (in Russian).
[4] Rosstandart. Information technology. Cryptographic protection of information. Recommendations for standardization. Cryptographic authentication mechanisms and development of key fiscal signs to use in means of generating and verifying fiscal characteristics, providing the operation with fiscal data of cash registers, operators and authorities (Draft).— 2018. — 28 p. (in Russian).
[5] Gorbatov, Victor S.; Zhukov, Igor Y.; Murashov, Oleg N. The security of the fiscal sign key system. The problems of the information security. Computer systems. SpbPU, № 1, 2018. (in Russian).
[6] Dictionary of financial and legal terms. http://www.consultant.ru/law/ref/ju_dict/word/fiskalnyj_priznak_dokumenta/. Check date 02/28/2018. (in Russian).
[7] R 50.1-113.2016. Information technology. Cryptographic protection of information. Cryptographic algorithms associated with the use of electronic digital signature algorithms and hashing functions. - Standartinform, Moscow, 2016. (in Russian).
[8] Cheremushkin A. V. Cryptographic protocol. The main characteristics and vulnerabilities. — Moscow.: Academia. — 2009. — 272 p. (in Russian).
[9] Preneel B. Analysis and Design of Cryptographic Hash Functions. — Doctoral dissertation. — Katholieke Universiteit Leuven. — January 1993. 321 p.
[10] Menezes A.V., van Oorschot P. C., Vanstone S. A. Handbook of applied cryptography.— CRC Press. — 1996. — 816 p.

Поступила в редакцию – 10 марта 2018 г. Окончательный вариант – 27 апреля 2018 г.
Received – March 10, 2017. The final version – April 27, 2018.