УДК 004.056 + 004.451.36 Вестник УрФО № 3(33) / 2019, с. 20–26

Танана Д. Д.

DOI: 10.14529/secur190303

ПРОТИВОДЕЙСТВИЕ ПРОГРАММАМ-ВЫМОГАТЕЛЯМ ПРИ ПОМОЩИ СПЕЦИАЛЬНОГО КОДИРОВАНИЯ

Обсуждаются вопросы противодействия программам-вымогателям. Даны краткие сведения, относящиеся к методам распространения, вымогательства, а также управления программ-вымогателей. Рассмотрен общий принцип действия программ-вымогателей, использующих блочные шифры. На примере программы-вымогателя, использующей для шифрования файлов режим электронной кодовой книги, предложен новый метод противодействия программам-вымогателям, основанный на предварительном кодировании файлов, который был успешно апробирован в лабораторных условиях.

Ключевые слова: *программы-вымогатели, киберпреступность, блочные шифры, кодирование, режим электронной кодовой книги.*

Tanana D. D.

RANSOMWARE COUNTERACTION USING SPECIAL ENCODING

The article considers questions of counteraction to ransomware. Brief information related to methods of distribution, extortion, as well as management of ransomware is given. Considered general principle of action of ransomware using block ciphers. Using the example of ransomware which uses electronic codebook mode to encrypt files, a new method to counter ransomware, based on pre-coding of files was proposed, which was successfully tested in laboratory condition.

Keywords*: ransomware, cybercrime, block ciphers, encoding, electronic codebook mode.*

Введение.

На смену многим традиционным ресурсам, которыми пользовалось человечество, приходит новый ресурс — информация. Его особенностью, в отличие от предшественников, является возрастание, а не убывание с течением времени. Любая деятельность — научная, исследовательская, производственная, предпринимательская — тесно связана с получением, накоплением, хранением, обработкой и использованием разнообразной информации. И как любой ресурс, информация в современном мире имеет определенную цену, которую иногда не просто выразить в денежном исчислении.

В современном мире возрастает роль ин-

формации, хранящейся в цифровом виде, которая является притягательным объектом для преступников. Традиционно защите подлежит ее конфиденциальность, целостность и доступность. Применение сложных систем шифрования в первую очередь нацелено на поддержание конфиденциальности и целостности информации. Однако интеллектуальные преступники нашли иное применение криптографии, а именно нарушение доступности информации для ее собственника или владельца. Они могут попытаться нарушить ее целостность, конфиденциальность или доступность. Одним из наиболее распространенных методов кибератак в наши дни является нарушение доступности информации при помощи криптографических программ-вымогателей. Так, в первом квартале 2017 года 60% всех зафиксированных компьютерных атак были произведены программами-вымогателями [1].

Согласно исследованию сайта ZDnet, киберпреступники, использующие программы-вымогатели, получили около 27 миллионов долларов от своих жертв [2]. В течение второго квартала 2013 года было обнаружено 350000 образцов программ-вымогателей [3] и 14 новых типов программ-вымогателей было выявлено с января 2014 по сентябрь 2015 года [4]. В третьем квартале 2017 года пользователи подвергались атаке программ-вымогателей каждые 10 секунд, а предприятия – каждые 40 секунд [1].

В данной статье предложен новый метод борьбы с криптографическими программами-вымогателями, использующими блочные шифры, основанный на кодировании файлов, с последующим раскрытием ключа шифрования.

Определение.

Вредоносная программа это программа, созданная злоумышленником для выполнения нежелательных действий на компьютере жертвы. Программы-вымогатели являются подтипом вредоносных программ, которые предотвращают доступ пользователей к их данным и требуют выкуп в обмен на возврат доступа. Существует множество различных форм программ-вымогателей, однако наиболее успешной и распространенной являются криптографические программы-вымогатели, в ходе их работы часть данных пользователей подвергается шифрованию и выкуп требуется за ключ для расшифровки.

Пользователи обычно не хотят платить киберпреступникам, однако у них не остается иного выбора, поскольку они не имеют доступа к необходимым файлам, среди которых может быть информация необходимая для текущей работы или же сведения составляющие коммерческую тайну [5].

Размер выкупа зависит от уровня образования пользователя, сложности программы-вымогателя и срочности восстановления доступа к файлам [5].

Для широкого успеха программа-вымогатель должна обладать следующими свойствами [6]:

1. Вредоносный код не должен содержать никаких секретов (например, ключей расшифрования). Или хотя бы не содержать секретов в легкодоступной форме [7].

2. Только организатор атаки должен иметь возможность расшифровать пораженные файлы.

3. Расшифрование одного пораженного устройства не должно давать никакой полезной информации для расшифрования других пораженных устройств, в частности ключ шифрования не должен быть общим для всех пораженных устройств.

Распространение.

Чаще всего программы-вымогатели распространяются через электронную почту, скомпрометированное программное обеспечение и посещение зараженных сайтов. Альтернативные пути распространения включают в себя социальную инженерию, прямой взлом компьютера жертвы или же загрузку другой вредоносной программой [8, 9].

Методы платежей злоумышленникам.

Конечной целью программы-вымогателя является получение денежных средств [10]. Первые программы-вымогатели использовали банковские переводы или подарочные карты (такие как Amazon или Apple). В редких случаях встречались также SMS или звонки на платные номера. Эти методы получения денежных средств могут быть достаточно легко отслежены силами правопорядка, поэтому масштабное распространение программ-вымогателей было ограничено – злоумышленники не могли привлекать к себе внимание. Именно поэтому новое поколение программ-вымогателей практически полностью полагается на Биткоин и иные криптовалюты. Появление Биткоина несомненно спровоцировало взрывной рост программ-вымогателей, т.к. Биткоин обладает следующими привлекательными для злоумышленников

свойствами: конфиденциальностью, высокой скоростью переводов и отсутствием регуляторов, таким образом являясь идеальным средством для требования выкупа. В 2014 году протокол Биткоин был расширен и может быть использован для хранения 80 байт, не относящихся непосредственно к транзакции. Новый вариант CTB-Locker использует это поле как канал для передачи ключа расшифрования после того как выкуп был уплачен [11].

Управление и контроль.

Для реализации второго свойства у успешной программы-вымогателя должна быть связь со злоумышленником. Она обычно осуществляется через сервер управления и контроля, чей минимальный функционал состоит в предоставлении жертве ключа расшифрования после выплаты выкупа. Для реализации третьего свойства, ключ расшифрования должен быть уникален для каждой жертвы, таким образом сервер должен генерировать ключи самостоятельно. Различные типы программ вымогателей используют сервер управления и контроля по-разному – некоторым нужно лишь одно соединение для получения ключей, другим требуется просто проверить доступность сервера. Статичный сервер может быть легко закрыт правоохранительными органами, поэтому авторы программ-вымогателей используют различные альтернативные схемы, такие как применение алгоритма генерации доменов. Тем не менее довольно часто попадаются программы-вымогатели, которые не могут связаться с сервером управления и контроля, а соответственно и зашифровать файлы.

Шифрование файлов.

Злоумышленникам доступно множество криптографических библиотек, находящихся в свободном доступе, таких как OpenSSL, mbed TSL, libsodium. Новейшие программы-вымогатели используют криптографию на эллиптических кривых для генерации индивидуальных ключей каждой жертвы [12]. Однако, пока что большая часть пораженных файлов шифруется протоколом Advanced Encryption Standart (AES), разница между различными видами программ-вымогателей заключается лишь в режимах использования. Авторы программ вымогателей могут использовать как встроенные библиотеки шифрования, такие как CryptoAPI, так и сторонние, описанные выше. Как правило, файлы шифруются лишь поверхностно, целью злоумышленника является прежде всего сделать их недоступными, а не провести шифрование по всем канонам криптографической науки.

Режимы работы блочных шифров.

Блочный шифр шифрует данные блоками длиной строго в n байт. Если файл превышает эту длину, то он разбивается на несколько блоков длиной в n байт. Если размер файла не делится нацело на n, то последний блок дополняется до n. Программы-вымогатели используют 2 классических режима работы – режим электронной кодовой книги и режим сцепления блоков. В данной статье F – алгоритм шифрования, T- исходный текст, C – зашифрованный текст и K – ключ шифрования. Исходный текст разбит на блоки Bi длиной n.

Режим электронной кодовой книги.

В этом режиме данные делятся на блоки и каждый блок шифруется независимо от других: $C_i=F(B_i, K_i)$, как представлено на рис.1.

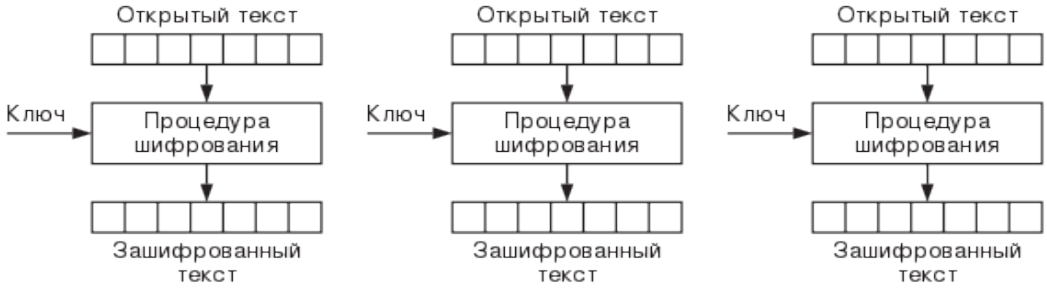

Рис. 1. Иллюстрация работы блочного шифра в режиме электронной кодовой книги

Режим сцепления блоков.

В режиме сцепления блоков каждый блок исходного текста проходит операцию сложения по модулю 2 с предыдущим блоком зашифрованного текста перед процедурой шифрования. Вектор инициализации (IV) складывается по модулю 2 с первым блоком B0 , как представлено на рис.2.

$$\begin{cases} C_0=F(B_0 \oplus IV, K_0) \\ C_{i+1}=F(B_{i+1} \oplus C_i, K_i) \end{cases}$$

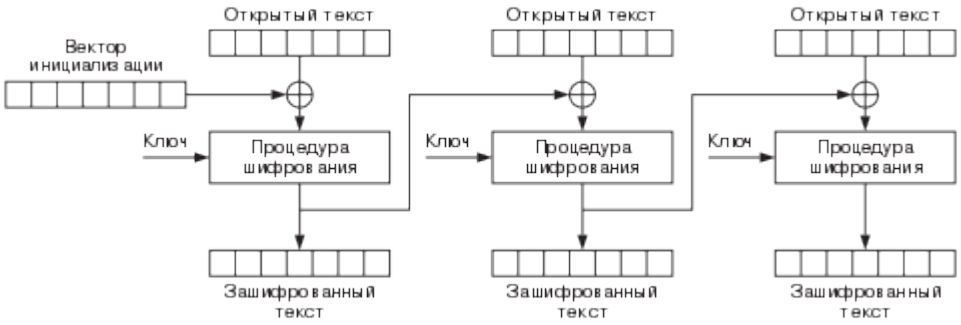

Рис. 2. Иллюстрация работы блочного шифра в режиме сцепления блоков

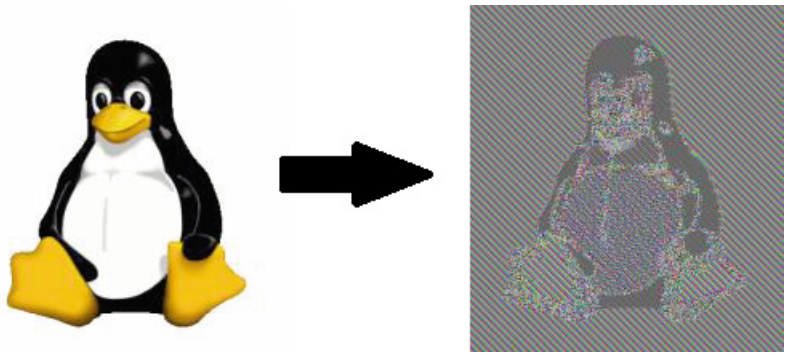

Рис. 3. Пример работы блочного шифра в режиме электронной кодовой книги на изображении

Традиционные антивирусы чаще всего обнаруживают и излечивают вредоносные программы, основываясь на их сигнатурах, что делает практически невозможным обнаружение новых вредоносных программ или же обнаружение полиморфных вредоносных программ. Более того, результат действия программ-вымогателей особенно трудно исправить, так как даже после устранения самой программы-вымогателя, файлы остаются зашифрованными [13]. Наиболее перспективные методы борьбы с программами-вымогателями основаны не на их внешних характеристиках, а на их функционале. Особенно актуальным представляется проведение атак на программы-вымогатели, так как зачастую те используют устаревшие шифры, чьи уязвимости исследованы и изучены.

Защита от программ-вымогателей с использованием специального кодирования.

Предлагается метод борьбы с криптографическими программами-вымогателями, использующими блочные шифры путем специального кодирования файлов. Режим электронной кодовой книги особенно уязвим, тогда как противодействие режиму сцепления блоков требует большей обработки и плохого знания криптографии злоумышленником.

Защита в режиме электронной кодовой книги.

В криптографии у режима электронной кодовой книги есть большой недостаток. Идентичные блоки исходного текста превращаются в идентичные блоки зашифрованного текста, таким образом он некорректно скрывает форму данных, как представлено на рис.3.

В данном режиме возможно провести атаку повторного воспроизведения [14] на программу-вымогателя.

Главная идея представленной в этой статье системы защиты заключается в использовании недостатков режима электронной кодовой книги для защиты данных от программ-вымогателей. Защита, в свою очередь, состоит из специального кодирования данных.

Первый шаг – расширение данных. Каждый байт данных дополняется нулевыми байтами до получения блока размера n. В случае шифра AES, n=16. Таким образом, файл T размером m байт: $T = B_0, B_1, \ldots B_m$, превращается в расширенный файл: $eT = B_0,0\ldots0, B_1,0\ldots0, \ldots B_m,0\ldots0$ (1), где между ненулевыми символами располагается n-1 нулей. Дополнительно создается словарь: dic = 0,0…0,1,0…0,…,255,0…0, где между ненулевыми символами располагается n-1 нулей.

Если программа-вымогатель использует один и тот же ключ для шифрования всех файлов, она также шифрует файл словаря. Пользователь может восстановить все файлы путем соотнесения зашифрованных блоков из файлов с зашифрованными блоками из словаря, для которых известно незашифрованное значение.

Если программа-вымогатель использует индивидуальный ключ для каждого файла, то словарь может быть создан в начале каждого файла. Таким образом файл T расширяется в dic+eT: dic+eT=0,0…0,1,0…0,…,255,0…0, B_0,0…0, B_1,0…0, … B_m,0…0 , где между ненулевыми символами располагается n-1 нулей.

Альтернативным решением является использование частотного анализа. Если T – текст, то можно предположить, что пользователь знает язык, на котором тот был написан. В этом случае в словаре нет необходимости, текст просто расширяется как в (1) и для восстановления данных используется классический частотный анализ.

Защита в режиме сцепления блоков.

Если программа-вымогатель использует блочный шифр в режиме сцепления блоков, то меры, описанные в предыдущем разделе, оказываются неэффективны из-за сложения по модулю 2 в начале шифрования каждого нового блока. Предлагается более сложное решение, основанное на предположении, что программа-вымогатель шифрует вновь созданный файл тем же самым ключом, что и файл который мы хотим восстановить. Файлы расширяются точно так же, как в (1), но словарь создается другим способом. Пользователь создает не один файл словаря, а 256 файлов dic_b^0, по одному для каждого возможного значения байта $b \in [0, 255]$, например dic_b^0 = b,0…0, где всего n-1 нулей.

Программа-вымогатель шифрует все файлы и 256 файлов словаря dic_b^0. На этом этапе пользователь может восстановить только первый байт B0 для каждого зашифрованного файла.

Затем пользователь создает новые словари – по одному для каждого зашифрованного файла и каждого возможного значения байта $b \in [0, 255]$: $dic_b^1 = (b,0\ldots0) \oplus C_0$.

Далее программа-вымогатель шифрует вновь созданные словари. На этом этапе пользователь может восстановить все вторые байты B_1 для каждого зашифрованного файла. Повторяя шаг данного алгоритма пользователь может в итоге восстановить все байты B_i для каждого зашифрованного файла: $dic_b^i = (b,0\ldots0) \oplus C_i$.

Ограничения.

Главным недостатком данного метода противодействия является сильно увеличивающийся размер защищаемых файлов – он возрастает в n раз. В нашем описании размер элементов словаря зафиксирован одним байтом, в реальности он может быть любым. Чем больше элемент словаря, тем больше сам словарь и тем больше размеры файлов. В будущих работах возможно будет оптимизировать эти размеры.

Важно заметить, что противодействие блочному шифру в режиме сцепления блоков возможно только для программ-вымогателей, удовлетворяющих следующим условиям:

1) программа всегда использует один и тот же ключ и один и тот же вектор инициализации;

2) шифрует все вновь созданные файлы.

Результаты.

16 наиболее распространенных программ-вымогателей, принадлежащих к 5 различным семействам, были протестированы в лабораторных условиях. В виду сложности реализации атаки на режим сцепления блоков, применялась только атака с использованием режима электронной кодовой книги для шифра AES. В тех случаях, когда программа-вымогатель использует шифр AES в режиме электронной кодовой книги была достигнута 100% эффективность восстановления файлов. Общая эффективность предложенного метода противодействия составила 37,5%, как показано в табл. 1.

Таблица 1.

Результаты испытания программы-защитника, использующей описанный выше метод противодействия программам-вымогателям

Семейство	Число образцов	Число успешных атак
Gpcode	5	5
Cryptolocker	2	0
CTB-Locker	4	0
Teslacrypt	3	1
Petya	2	0

Несмотря на кажущуюся узконаправленность предложенного метода противодействия, он эффективен в отношении большого числа программ-вымогателей, все еще использующих блочные шифры в режиме элек-

тронной кодовой книги и может быть использован в рамках комплексной защиты от программ-вымогателей. Также предложен метод восстановления файлов, подвергшихся атаке программы-вымогателя, использующей блочный шифр в режиме сцепления блоков с определенными ограничениями. Даже учитывая ограничения, он все же может быть использован для восстановления файлов большой важности.

Литература.

1. Crowe J. Must-know ransomware statistics 2017 // Endpoint Protection | Barkly: сайт. — 2017. — URL: https://blog.barkly.com/ransomware-statistics-2017 (дата обращения: 11.10.2018).

2. Violet B. CryptoLocker's crimeware: a trail of millions in laundered Bitcoin // ZDNet: сайт. — 2013. — URL: http://www.zdnet.com/article/cryptolockers-crimewave-a-trail-of-millions-in-laundered-bitcoin/ (дата обращения: 11.10.2018).

3. Смирнов Д.В. Исследование особенностей поведения вредоносного программного обеспечения класса крипторов-вымогателей / Д.В. Смирнов, И.А. Лубкин // Решетневские чтения / Сибирский государственный аэрокосмический университет. —Красноярск, 2016. — С. 271-273.

4. Дроботун Е.Б. Исследование и анализ кода наиболее популярных вредоносных программ типа «блокиратор-шифровальщик файлов» / Е.Б. Дроботун // Программные продукты, системы и алгоритмы. — Тверь, 2016. — №1. — С. 2.

5. Upadhyaya R. Cyber ethics and cyber crime: A deep dwelved study into legality, ransomware, underground web and bitcoin wallet / R. Upadhyaya, A. Jain // Proceeding - IEEE International Conference on Computing, Communication and Automation / International Conference on Computing, Communication and Automation. — Greater Noida, 2016. — P. 143-148.

6. Gazet A. Comparative analysis of various ransomware virii / A. Gazet // Journal Computer Virology. — 2008. — No 6. — P. 77-90.

7. Josse, S. White-box attack context cryptovirology / S. Josse // Journal Computer Virology. — 2009. — No 5. — P. 321-334.

8. Wyke, J. The Current State of Ransomware // Sophos: сайт. — 2015. — URL: https://www.sophos.com/en-us/medialibrary/PDFs/technical%20papers/sophos-current-state-of-ransomware.pdf (дата обращения: 11.10.2018).

9. Kotov, V. Understanding Crypto-Ransomware // Bromium: сайт. — 2014. — URL: https://www.bromium.com/sites/default/files/bromium-report-ransomware.pdf (дата обращения: 11.10.2018).

10. Young, A.L. Cryptovirology: Extortion-based security threats and countermeasures / A.L. Young, M. Yung // Proceedings of IEEE Symposium on Security and Privacy. — Oakland, 1996. — P. 129–140.

11. Sinegubko, D. How CTB-Locker Ransomware Uses Bitcoin and Blockchain // Cryptocoinsnews: сайт. — 2016. — URL: https://www.cryptocoinsnews.com/how-ctb-locker-ransomware-uses-bitcoin-andblockchain/ (дата обращения: 11.10.2018).

12. Mohan J.C. On the efficacy of android ransomware detection techniques: A survey / J.C. Mohan, R. Kumar // International Journal of Pure and Applied Mathematics. — 2017. — No 8. — P. 115-120.

13. Kharraz, A. Cutting the Gordian knot: a look under the hood of ransomware attacks / A. Kharraz, W. Robertson, D. Balzarotti, L. Bilge, E.Kirda // Proceedings of Conference on Detection of Intrusions and Malware & Vulnerability Assessment. — Milan, 2015. — P. 3–24.

14. Syverson, P. A taxonomy of replay attacks [cryptographic protocols] / P. Sylverson // Proceedings of Computer Security Foundations Workshop VII. — Franconia, 1994. — P. 187–191.

References.

1. Crowe J. Must-know ransomware statistics 2017, Available at: https://blog.barkly.com/ransomware-statistics-2017.

2. Violet B. CryptoLocker's crimeware: a trail of millions in laundered Bitcoin, Available at: http://www.zdnet.com/article/cryptolockers-crimewave-a-trail-of-millions-in-laundered-bitcoin/.

3. Smirnov D.V., Lubkin I.A. Investigation of malicious software cryptor-ransomware behavior [Issledovanie osobennostey povedeniya vredonosnogo programmnogo obespecheniya klassa kriptorov-vymogateley], Reshetnevskie chteniya [Reshetnev's Readings]. Krasnoyarsk, 2017, pp. 271-273.

4. Drobotun Ye. B. Investigation and analysis of the of the most popular malicious programs code type «file encryption blocker » [Issledovanie i analiz koda naibolee populyarnykh vredonosnykh programm tipa «blokirator-shifroval'shchik faylov »]. Programmnye produkty, sistemy i algoritmy [Program products, systems and algorythms], 2016, No. 1, pp. 2.

5. Upadhyaya R., Jain. A., Cyber ethics and cyber crime: A deep dwelved study into legality, ransomware, underground web and bitcoin wallet, IEEE International Conference on Computing, Communication and Automation, Greater Noida, 2016, pp. 143-148.

6. Gazet A. Comparative analysis of various ransomware virii, Journal Computer Virology, 2008, No 6, pp. 77-90.

7. Josse, S. White-box attack context cryptovirology, Journal Computer Virology, 2009, No 5, pp. 321-334.

8. Wyke, J. The Current State of Ransomware, Available at: https://www.sophos.com/en-us/medialibrary/PDFs/technical%20papers/sophos-current-state-of-ransomware.pdf.

9. Kotov, V. Understanding Crypto-Ransomware, Available at: https://www.bromium.com/sites/default/files/bromium-report-ransomware.pdf.

10. Young, A.L, Yung M., Cryptovirology: Extortion-based security threats and countermeasures, Proceedings of IEEE Symposium on Security and Privacy, Oakland, 1996, pp. 129–140.

11. Sinegubko, D. How CTB-Locker Ransomware Uses Bitcoin and Blockchain, Available at: https://www.cryptocoinsnews.com/how-ctb-locker-ransomware-uses-bitcoin-andblockchain/.

12. Mohan J.C., Kumar. R., On the efficacy of android ransomware detection techniques: A survey, International Journal of Pure and Applied Mathematics, 2017, No 8, pp. 115-120.

13. Kharraz, A., Robertson. W., Balzarotti D., Bilge L., Kirda E., Cutting the Gordian knot: a look under the hood of ransomware, Proceedings of Conference on Detection of Intrusions and Malware & Vulnerability Assessment, Milan, 2015, pp. 3–24.

14. Syverson, P. A taxonomy of replay attacks [cryptographic protocols], Proceedings of Computer Security Foundations Workshop VII, Franconia, 1994, pp. 187–191.

ТАНАНА Дмитрий Дмитриевич, аспирант кафедры Алгебры и фундаментальной информатики, ФГАОУ ВО «УрФУ имени первого Президента России Б.Н. Ельцина», 620002, Россия, Екатеринбург, ул. Мира, 19. E-mail: ddtanana@urfu.ru

TANANA Dmitry Dmitrievich, Postgraduate of Department of Algebra and Fundamental Informatics, Federal State Autonomous Educational Institution of Higher Education «Ural Federal University named after the first President of Russia B.N.Yeltsin», 620002, Russia, Yekaterinburg, Mira 19. E-mail: ddtanana@urfu.ru

Работа выполнена в рамках проекта № 1.3253.2017 Министерства науки и высшего образования РФ «Комбинаторные модели в компьютерных науках и их приложениях»