УДК 621.396

05.00.00 Технические науки

МЕТОДИКА ДЕЦЕНТРАЛИЗОВАННОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕВОЙ ИНФОРМАЦИИ В СИСТЕМАХ СКРЫТОЙ СВЯЗИ ДЛЯ ФЕДЕРАЛЬНЫХ КРИТИЧЕСКИ–ВАЖНЫХ ОБЪЕКТОВ РОССИЙСКОЙ ФЕДЕРАЦИИ

Хисамов Франгиз Гильфанетдинович
Доктор технических наук, профессор

Пшеничный Игорь Сергеевич
Краснодарское высшее военное училище, Краснодар, Россия

Методика относится к области распределения ключевой информации в системах криптографической связи. Целью работы явилось решение задачи повышения оперативности распределения ключевой информации для специальных органов федеральных критически-важных объектов в условиях сетецентрического управления и создание вариантов распределения ключевой информации при компрометации ключевых документов к специальной аппаратуре. Применением методики достигается решение данной задачи путем применения способа распределения ключей на основе ассиметричной криптографии с использование симметрических многочленов

Ключевые слова: КРИТИЧЕСКИ ВАЖНЫЙ ОБЪЕКТ, КЛЮЧЕВЫЕ ДОКУМЕНТЫ, КЛЮЧЕВАЯ ИНФОРМАЦИЯ

UDC 621.396

Technical sciences

METHODOLOGY OF DECENTRALIZED DISTRIBUTION OF KEY INFORMATION IN THE SYSTEMS OF HIDDEN COMMUNICATION FOR FEDERAL CRITICAL IMPORTANT OBJECTS OF THE RUSSIAN FEDERATION

Khisamov Frangiz Gilfanetdinovich
Dr.Sci.Tech., professor

Pshenichniy Igor Sergeevich
Krasnodar high military academy, Krasnodar, Russia

The technique relates to the area of distribution of key information in cryptographic communication systems. The purpose of the work was to solve the problem of increasing the speed of distribution of key information for special bodies of federal bodies of critical facilities in the conditions of network-centric management and creating alternative options for the distribution of key information when key documents are compromised to special equipment. By applying the methodology, a solution to this problem is achieved by applying a key distribution method based on asymmetric cryptography using symmetric polynomials

Keywords: CRITICAL IMPORTANT OBJECT, KEY DOCUMENTS, KEY INFORMATION

Doi: 10.21515/1990-4665-132-029

Область применения методики. Методика относится к области распределения ключевой информации, и может быть использована центральными органами обработки документированной информации территориально распределенных организаций (далее ООДИ ТРО), имеющих подчиненные подразделения, при распределении ключевой информации.

Использование для обеспечения должностных лиц органов управления ТРО связью ключевых документов (далее КД) приводит к необходимости оперативного и конфиденциального распределения ключевой информации.

В настоящее время в целях децентрализованного ключевого обеспечения, в условиях повсеместно внедряющихся принципов сетецентрического управления, [1, 2, 3, 4] разработана аппаратура децентрализованного изготовления ключей Е-63-С (АО ПНИЭИ), которая обеспечивает децентрализованное формирование ключевых документов для аппаратуры Е-11Н [5].

Недостатком известных подходов к распределению ключей для ООДИ ТРО является:

при использовании аппаратуры Е-63-С задача распределения ключей остается открытой в связи с тем, что при компрометации КД к аппаратуре Е-11Н у взаимодействующего абонента, передача КД становится возможной только при использовании традиционного распределения с низкой оперативностью доставки ключевой информации.

Низкая оперативность доставки ключевой информации при компрометации КД при известных подходах к распределению ключей в ООДИ ТРО обусловлена:

большими временными и ресурсными затратами, необходимыми для распределения ключевой информации большому количеству корреспондентов;

фактическое отсутствие вариантов распределения ключевой информации.

Назначение методики. Целью методики является решение задачи повышения оперативности и создания вариантов распределения ключевой информации для ООДИ ТРО в условиях сетецентрического управления при компрометации ключевой информации.

Повышение оперативности и создание вариантов распределения ключевой информации для ООДИ ТРО при компрометации ключевой информации осуществляется применением способа [6] распределения ключей на основе ассиметричной криптографии. Способ распределения

ключа [6], заключается в формировании конфиденциального ключа центром распределения ключей как коэффициентов симметричного многочлена над заданным конечным полем, присвоении идентификаторов Y_A, Y_B пользователям (A и B номера пользователей в системе обмена, $A \neq B$), выработки личных конфиденциальных ключей пользователей как коэффициентов многочленов над заданным полем и получение сеансовых ключей для любой пары корреспондентов как значения многочленов [7].

Физическая (содержательная) постановка задачи. Аппаратура децентрализованного изготовления ключей Е-63-С решает задачу децентрализованного изготовления и хранения ключевой информации для аппаратуры Е-11Н [5], при этом в дальнейшем возникает задача оперативного и конфиденциального распределения ключевой информации, между центральным ООДИ ТРО и подчиненными ООДИ подразделений ТРО для организации непрерывного обеспечения должностных лиц органов управления ТРО связью.

Таким образом, возникают противоречия:

между потребностью ТРО в оперативном распределении ключевой информации в условиях ограниченных временных ресурсов и значительному территориальному распределению подчиненных подразделений ТРО при компрометации КД;

между потребностью ТРО в конфиденциальном распределении ключевой информации при компрометации КД и отсутствием вариантов организации необходимого уровня криптографической защиты при компрометации всех видов КД у взаимодействующего корреспондента.

На устранение указанных противоречий и направлена методика.

Показатели и критерии. Пусть показателем стойкости сформированных полиномов и соответственно сеансовых ключей является случайно выбранный образующий неприводимый полином поля Галуа $GF(2^r)$ и коэффициенты a_i, выбранные случайным образом из конечного

поля GF(2^r). В качестве критериев стойкости сформированных полиномов и сеансовых ключей для передачи КИ выступают степень образующего неприводимого полинома поля Галуа и максимальная степень, рассматриваемого полинома по каждой переменной.

Порядок вычисления значений показателей, частные критерии и их вклад в итоговый результат изложены по тексту.

Теоретической основой методики являются такие разделы теории чисел, как теория конечных полей, теория многочленов, а так же разделы математической статистики и теории моделирования систем [8, 9,10].

Исходные данные. В качестве основных исходных данных в методике выступают:

генератор построения двоичной псевдослучайной последовательности, формирующий значение образующего неприводимого полинома поля Галуа GF(2^r);

требования к значению *r*;

групповые идентификаторы ООДИ (присваиваются каждому центральному и подчиненному ООДИ ТРО), размещенные в открытом доступе;

требования к необходимому количеству индивидуальных идентификаторов ООДИ ТРО и соответственно сеансовых ключей на заданный промежуток времени;

индивидуальные идентификаторы ООДИ (присваиваются каждому отдельному ООДИ ТРО), размещенные в открытом доступе;

наличие связи между взаимодействующими ООДИ ТРО;

наличие у каждого взаимодействующего подчиненного ООДИ ТРО сформированного значения функции f_i над заданным полем Галуа вида:

$$f_i(w,x,y,z) = \sum_{b,c,d,e=0}^{t} a_{b,c,d,e} w^b x^c y^d z^e, \quad (1)$$

где a – коэффициент выбранный случайным образом из конечного поля GF(2^r); t – максимальная степень рассматриваемого полинома по каждой переменой; b, c, d, e – индексы суммирования; при этом функция f_i удовлетворяет условию:

$$f_i(w,x,y,z) = f_i(x,w,y,z) \text{ и } f_i(w,x,y,z) = f_i(w,x,z,y), \quad (2)$$

где w, x – переменные, обозначающие индивидуальные идентификаторы ООДИ ТРО; y, z – переменные, обозначающие групповые идентификаторы ООДИ ТРО. Значение коэффициента a формируется датчиком построения двоичной псевдослучайной последовательности, на основе исходной двоичной последовательности;

требования к значению t.

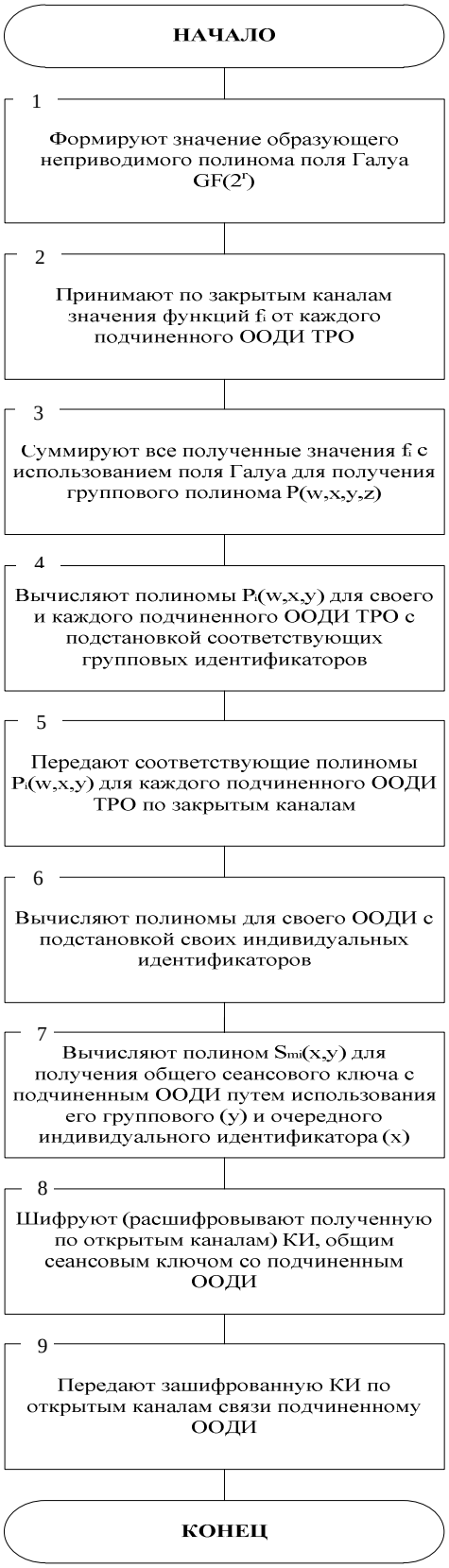
Для достижения цели методики осуществляют следующую последовательность действий. Задают исходные данные:

в центральном ООДИ используется генератор построения двоичной псевдослучайной последовательности, формирующий значение образующего неприводимого полинома поля Галуа GF(2^r), на основе исходной двоичной последовательности;

требования к значению r;

групповые идентификаторы ООДИ ТРО, сформированные центральным ООДИ ТРО для своего ООДИ и подчиненных ООДИ, размещенные в открытом доступе;

требования к необходимому количеству индивидуальных идентификаторов у ООДИ ТРО и соответствующих сеансовых ключей на заданный временной промежуток;



$$P_i(w,x,y) = \sum_{k=1}^{n} f_k(w,x,y,i)$$

где k – переменная суммирования, перебирающая возможные f_i; i – групповой идентификатор ООДИ; n – максимальное количество ООДИ ТРО.

$$S_{mi}(x,y) = P_i(ID,x,y)$$

где ID – индивидуальный идентификатор

Рис. 1 Блок-схема распределения ключевой информации для центрального ООДИ ТРО

индивидуальные идентификаторы ООДИ ТРО, сформированные центральным ООДИ ТРО для своего ООДИ и подчиненных ООДИ ТРО, размещенные в открытом доступе;

наличие связи между взаимодействующими ООДИ ТРО;

наличие у каждого подчиненного ООДИ ТРО сформированного значения функции f_i над заданным полем Галуа;

требования к значению t.

Далее ООДИ ТРО выполняется порядок действий, показанный на рис. 1.

В блок-схеме, показанной на рис. 1, центральный ООДИ ТРО формирует значение образующего неприводимого полинома поля Галуа $GF(2^r)$, на основе исходной двоичной последовательности. В дальнейшем центральный ООДИ ТРО принимает по закрытым каналам значения функции f_i от каждого подчиненного ООДИ ТРО. Центральный ООДИ ТРО суммирует все полученные значения f_i с использованием поля Галуа для получения группового полинома P(w,x,y,z), таким образом, каждый подчиненный ООДИ ТРО принимает участие в построении группового полинома.

Далее центральный ООДИ ТРО вычисляет полиномы $P_i(w,x,y)$ для своего и каждого подчиненного ООДИ ТРО с подстановкой соответствующих групповых идентификаторов вместо z в групповой полином P(w,x,y,z), вычисления проводятся в поле Галуа $GF(2^r)$ с образующим полиномом $F_n(x)$. Полиномы $P_i(w,x,y)$ для каждого подчиненного ООДИ ТРО передаются центральным ООДИ ТРО по защищенным каналам, при этом групповой полином храниться в секрете. Центральный ООДИ ТРО в дальнейшем вычисляет полиномы $S_{mi}(x,y)=P_i(ID,x,y)$ путем подстановки вместо ID значения своих индивидуальных идентификаторов, вычисления проводятся в поле Галуа $GF(2^r)$ с образующим полиномом $F_n(x)$, при этом для получения первого

полинома $S_{mi}(x,y)$ подставляется первый индивидуальный идентификатор, для получения второго полинома $S_{mi}(x,y)$ подставляется второй индивидуальный идентификатор и т. д. После этого, для получения общего сеансового ключа с подчиненным ООДИ, центральный ООДИ подставляет в очередной, неиспользуемый ранее, полином $S_{mi}(x,y)$ вместо значения *x* очередной, неиспользуемый ранее, индивидуальный идентификатор подчиненного ООДИ, а вместо значения *y* групповой идентификатор подчиненного ООДИ. При следующем сеансе передачи ключевой информации, центральный ООДИ ТРО будет использовать очередной полином $S_{mi}(x,y)$ с подстановкой вместо *x* значения очередного индивидуального идентификатора подчиненного ООДИ. На общем сеансовом ключе центральный ООДИ ТРО шифрует ключевую информацию и передает ее по открытым каналам связи подчиненному ООДИ. Подчиненный ООДИ ТРО приняв криптограмму от центрального ООДИ вычисляет такой же сеансовый ключ, путем подстановки в очередной полином $S_{mi}(x,y)$ группового и очередного, неиспользуемого ранее, индивидуального идентификатора центрального ООДИ и расшифровывает на данном ключе криптограмму.

Таким образом, применением методики достигается решение задачи повышения оперативности и создания вариантов распределения ключевой информации для центрального ООДИ ТРО в условиях сетецентрического управления при компрометации ключевой информации.

Научная новизна методики заключается в применении способа распределения ключей на основе ассиметричной криптографии с использованием симметричных многочленов [6, 7] в предметной области распределения ключевой информации для центральных ООДИ ТРО.

Практическая значимость заключается в обосновании возможности применения данного подхода в центральном ООДИ ТРО.

Литература

1. Затуливетер Ю. С., Фищенко Е. А. Подход к формированию универсального алгоритмического пространства распределенных и параллельных вычислений для задач сетецентрического управления // 6-я Международная конференция «Управление развитием крупномасштабных систем» (MLSD-2012), Москва : сборник материалов – М. : ИПУ РАН, – 2012. – Т. 2. – С. 307–313.

2. Затуливетер Ю. С. Компьютерный базис сетецентрического управления // Российская конференция с международным участием «Технические и программные средства в системе управления, контроля и измерения» (УКИ'10), Москва : труды конференции – М. : ИПУ РАН, – 2010. – С. 17–37.

3. Легков К.Е. Управление ресурсами информационных систем специального назначения при построении сетецентрической системы управления на основе радиосетей нового поколения // T-Comm: Телекоммуникации и транспорт : сб. науч. труд. – М. : Издательский дом Медиа Паблишер, – 2012. – Т. 6. – № 10. – С. 60–63.

4. Галактионов Н. С., Галактионова Ю. О., Стенькин Н. Н. Мобильный автономный комплекс сетецентрического управления в кризисной ситуации // Современные тенденции развития науки и технологий : сб. науч. труд. – Белгород : Ткачева Е.П., – 2016. – № 10-3. – С. 143–147.

5. URL: http://xn--h1aanh6e.xn--p1ai/activity/production/e-63.htm

6. Заявка на изобретение № 2017110214 от 27.03.2017 года. Способ формирования ключа шифрования-дешифрования. Хисамов Ф.Г. и др.

7. Способ формирования ключа шифрования/дешифрования : пат. 2090006 Рос. Федерация / заявитель, патентообладатель Военная академия связи, Военная академия связи. – № 94027301/09 ; заявл. 18.07.94. ; опубл. 10.09.97, Бюл. № 25. – 3 с.

8. Прасолов, В.В. Многочлены, издание второе, стереотипное / В.В. Прасолов. – М., МЦНМО, 2001. – 336 с.

9. Винберг, Э.Б. Симметрия многочленов / Э.Б. Винберг. – М., МЦНМО, 2001. – 24 с.

10. Шеннон Р. Имитационное моделирование систем – искусство и наука – М. : Мир, 1978. – 418 с.

References

1. Zatuliveter Ju. S., Fishhenko E. A. Podhod k formirovaniju universal'nogo algoritmicheskogo prostranstva raspredelennyh i parallel'nyh vychislenij dlja zadach setecentricheskogo upravlenija // 6-ja Mezhdunarodnaja konferencija «Upravlenie razvitiem krupnomasshtabnyh sistem» (MLSD-2012), Moskva : sbornik materialov □ M. : IPU RAN, □ 2012. □ T. 2. □ S. 307□313.

2. Zatuliveter Ju. S. Komp'juternyj bazis setecentricheskogo upravlenija // Rossijskaja konferencija s mezhdunarodnym uchastiem «Tehnicheskie i programmnye sredstva v sisteme upravlenija, kontrolja i izmerenija» (UKI'10), Moskva : trudy konferencii □ M. : IPU RAN, – 2010. □ S. 17□37.

3. Legkov K.E. Upravlenie resursami informacionnyh sistem special'nogo naznachenija pri postroenii setecentricheskoj sistemy upravlenija na osnove radiosetej novogo pokolenija // T-Comm: Telekommunikacii i transport : sb. nauch. trud. □ M. : Izdatel'skij dom Media Pablisher, □ 2012. □ T. 6. □ № 10. □ S. 60□63.

4. Galaktionov N. S., Galaktionova Ju. O., Sten'kin N. N. Mobil'nyj avtonomnyj kompleks setecentricheskogo upravlenija v krizisnoj situacii // Sovremennye tendencii

razvitija nauki i tehnologij : sb. nauch. trud. Belgorod : Tkacheva E.P., 2016. № 10-3. S. 143147.

5. URL: http://xn--h1aanh6e.xn--p1ai/activity/production/e-63.htm

6. Zajavka na izobretenie № 2017110214 ot 27.03.2017
goda. Sposob formirovanija kljucha shifrovanija-deshifrovanija.
Hisamov F.G. i dr.

7. Sposob formirovanija kljucha shifrovanija/deshifrovanija : pat. 2090006 Ros. Federacija / zajavitel', patentoobladatel' Voennaja akademija svjazi, Voennaja akademija svjazi. – № 94027301/09 ; zajavl. 18.07.94. ; opubl. 10.09.97, Bjul. № 25. – 3 s.

8. Prasolov, V.V. Mnogochleny, izdanie vtoroe, stereotipnoe / V.V. Prasolov. – M., MCNMO, 2001. – 336 s.

9. Vinberg, Je.B. Simmetrija mnogochlenov / Je.B. Vinberg. – M., MCNMO, 2001. – 24 s.

10. Shennon R. Imitacionnoe modelirovanie sistem – iskusstvo i nauka – M. : Mir, 1978. – 418 s.

Примечение: В ранее опубликованной статье в научной электронном журнале КубГАУ: Лойко В.И. Квантовые системы распределения ключей: физические основы, протоколы, перспективы применения / В.И. Лойко, Ф.Г. Хисамов, М.В. Бобылев, К.Е. Власов // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета (Научный журнал КубГАУ) [Электронный ресурс]. – Краснодар: КубГАУ, 2016. – №05(119). С. 938 – 956. – IDA [article ID]: 1191605066. – Режим доступа: http://ej.kubagro.ru/2016/05/pdf/66.pdf, 1,188 у.п.л. были использованы материалы из работы коллектива авторов: д.ф.-м.н. Алиев Ф.К., к.т.н. Вассенков А.В., к.т.н. Гузенко О.Б., Матвеев Е.А., д.т.н., профессор Шеремет И.А. В связи с тем, что в опубликованной работе были использованы материалов из работы указанного авторского коллектива без ссылок на них, В.И.Лойко, Ф.Г. Хисамов, М.В. Бобылев, К.Е. Власов: приносят свои искренние извинения за допущенную грубую оплошность и подтверждают, что в опубликованной им работе были использованы материалы указанного авторского коллектива.