УДК 621.396.9
doi:10.15217/issn1684-8853.2016.1.74

ОБЕСПЕЧЕНИЕ СЕЛЕКТИВНОГО ДОСТУПА ПРИ ШИРОКОВЕЩАТЕЛЬНОЙ ПЕРЕДАЧЕ ИНФОРМАЦИИ

С. В. Штанько[a], *канд. техн. наук, доцент*
Д. А. Лесняк[a], *канд. техн. наук, старший преподаватель*
[a]*Военно-космическая академия им. А. Ф. Можайского, Санкт-Петербург, РФ*

Постановка проблемы: *одним из основных условий эффективного функционирования любой системы передачи информации является ее информационная безопасность. Объективным свойством защищенности информационных систем является ее постепенное снижение при неизменном составе средств защиты или при фиксированных их параметрах. Для поддержания информационной безопасности и предотвращения несанкционированного доступа осуществляется периодическая замена устаревших ключей в криптосистеме. В широковещательных системах передачи информации с селективным доступом имеются особенности обеспечения информационной безопасности, связанные с отсутствием обратного канала передачи информации. Это приводит к необходимости разработки специальных методов криптографической защиты для широковещательных систем информации.* ***Цель:*** *усовершенствование существующей криптографической системы защиты данных для повышения защищенности каналов широковещательных систем передачи информации с селективным доступом от несанкционированного доступа.* ***Результаты:*** *предложена модификация методов защиты информации в целях предотвращения возможности несанкционированного доступа к системе в конфликтных условиях взаимодействия с нарушителем, основанная на асимметричных криптографических системах с использованием математического аппарата эллиптических кривых. На базе предложенных криптографических методов защиты построена криптографическая система защиты данных, передаваемых по каналам широковещательной системы передачи информации с селективным доступом. Представлен пример генерации общего сеансового ключа при передаче информации в закрытом режиме работы.* ***Практическая значимость:*** *предложенные пути повышения защищенности каналов широковещательных систем передачи информации с селективным доступом от несанкционированного доступа позволяют повысить информационную безопасность системы на основе использования комбинированных криптосистем и математического аппарата эллиптических кривых.*

Ключевые слова *— широковещательные системы передачи информации с селективным доступом, несанкционированный доступ, криптоалгоритм, протокол управления ключами.*

Введение

Одним из элементов современной глобальной информационной инфраструктуры являются широковещательные системы передачи информации, которые активно внедряются и используются в области телекоммуникаций. Широковещательные системы передачи информации отличают такие особенности, как сплошное покрытие обслуживаемых территорий, а также ограниченное число передающих и значительно превосходящее их число приемных пунктов (абонентов) при отсутствии обратного канала передачи информации. Если в такой системе предусматривается селективный доступ, то в ней необходимо использовать криптографические методы обеспечения информационной безопасности. При этом обеспечение информационной безопасности в широковещательных системах передачи информации с селективным доступом (ШСПИ с СД) связано с отсутствием обратного канала передачи информации.

Постепенное снижение защищенности информационных систем при неизменном составе средств защиты или при их фиксированных параметрах, а также пространственная электромагнитная доступность, являющаяся свойством любых радиоканалов, создает условия для реализации угроз несанкционированного доступа (НСД) к радиоканалам передачи информации [1].

Для предотвращения возможности несанкционированного использования ШСПИ с СД в условиях конфликтного взаимодействия с нарушителем необходимо применять криптографические методы защиты информации. Для этого надо построить полноценную криптографическую систему защиты данных, передаваемых по радиоканалу ШСПИ с СД. Кроме того, в некоторых ШСПИ, помимо требований по криптостойкости (информационной скрытности), предъявляются требования по имитостойкости, и при осуществлении передачи конфиденциальной информации по каналам ШСПИ с СД принципиально необходимо выполнять процедуру аутентификации — подтверждения подлинности абонента [2, 3]. Дополнительная сложность реализации полноценной криптографической системы защиты данных в ШСПИ с СД заключается в отсутствии обратного канала, в то время как для построения необходимо реализовать эффективные процедуры смены ключевой информации.

Перечисленные проблемы защиты информации в ШСПИ с СД успешно решаются с использованием асимметричных криптосистем.

Построение системы защиты широковещательной системы связи на основе комбинированных криптосистем

В простейшем случае в ШСПИ с СД используется единый несменяемый ключ симметричного алгоритма, что делает такую систему уязвимой. Посредством этого ключа авторизованным пользователем расшифровывается получаемая им информация. Для повышения защищенности системы необходимо предусмотреть возможность смены ключей как в передающих (ПРД), так и в приемных (ПРМ) пунктах [4].

Для разработки полноценной криптосистемы следует обеспечить процедуру смены единого ключа для системы, а в лучшем случае — процедуру формирования рабочих ключей, защищаемых долговременным мастер-ключом, а также процедуру смены мастер-ключа [5].

Предпочтительным представляется применение комбинированных криптосистем, использующих преимущество симметричных по скорости и асимметричных по широким возможностям построения схем аутентификации и доставки ключей. В качестве алгоритмов асимметричной части комбинированной схемы рекомендуется прибегнуть к математическому аппарату эллиптических кривых как обладающий наилучшими криптографическими и скоростными характеристиками по сравнению с другими типами асимметричных алгоритмов [6]. Непосредственно шифрование защищаемых данных в этом случае осуществляется симметричным способом методом гаммирования, а для генерации сеансовых ключей и проведения процедуры аутентификации применяются асимметричные методы [7, 8].

Алгоритм шифрования и генерация ключа с использованием асимметричного алгоритма можно представить в следующем формализованном виде:

$$c = E_{k_o}(m); \quad (1)$$

$$m = D_{k_з}(c), \quad (2)$$

где E — шифрующее преобразование асимметричного алгоритма; D — расшифровывающее преобразование асимметричного алгоритма; m — исходный информационный массив; c — зашифрованный массив на ключе $k_з$; $k_з$ — закрытый ключ, сгенерированный случайным образом; k_o — открытый ключ, полученный путем одностороннего преобразования [9]:

$$k_o = f(k_з). \quad (3)$$

Сеансовые ключи симметричной системы для шифрования и асимметричной для аутентификации (в случае необходимости) генерируются на основе алгоритма Диффи — Хеллмана с использованием долговременных ключей асимметричной системы и случайного числа либо меток времени (либо того и другого) для того, чтобы сеансовые ключи отличались друг от друга [3]. В случае однонаправленных каналов ШСПИ с СД алгоритм Диффи — Хеллмана является упрощенным в том смысле, что у всех абонентов долговременные ключи одинаковы и алгоритм не зависит от того, какому абоненту передается информация, и не требует передачи информации от наземного абонента [10].

Эллиптическую кривую над конечным полем Галуа GF_p можно представить в виде

$$E_p(a, b): y^2 = x^3 + ax + b(\mathrm{mod}\ p). \quad (4)$$

Здесь $E_p(a, b)$ — эллиптическая группа по модулю p, элементами которой (x, y) являются пары неотрицательных чисел, меньших p и удовлетворяющих уравнению кривой, а также точка в бесконечности O.

Групповой закон сложения точек $P_1 \oplus P_2$ имеет вид $P_1 \oplus P_2 = (x_3, y_3)$, где

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_2 - x_1; \quad (5)$$

$$y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1. \quad (6)$$

При $P_1 = P_2 = (x_1, y_1)$ получаем $2P_1 = (x_2, y_2)$:

$$x_2 = \frac{(3x_1^2 + a)^2}{4y_1^2} - 2x_1; \quad (7)$$

$$y_2 = \frac{(3x_1^2 + a)}{2y_1}(x_1 - x_2) - y_1. \quad (8)$$

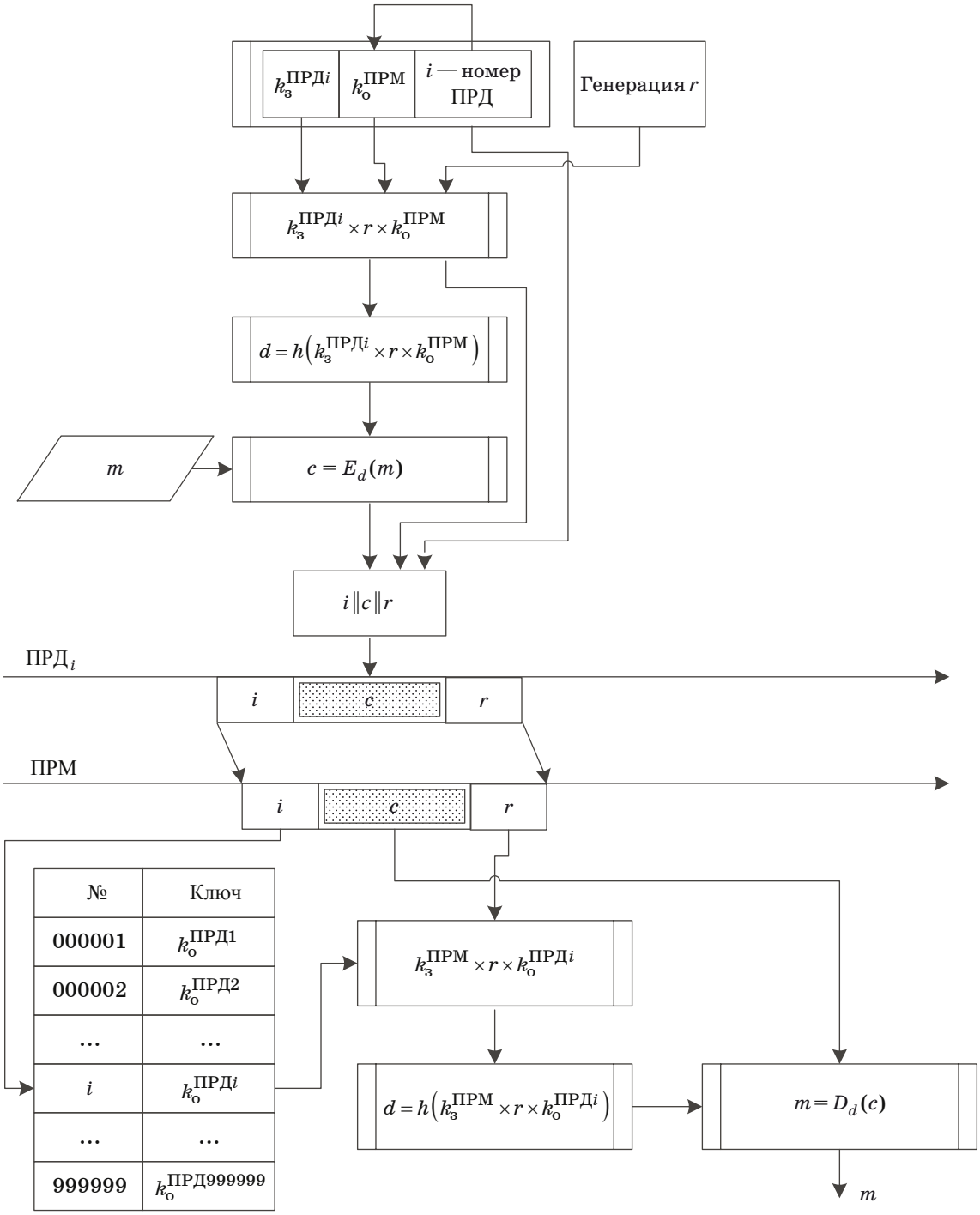
Для организации обмена ключевой информацией на основе асимметричных криптосистем необходима односторонняя функция. В качестве такой функции в математическом аппарате эллиптических кривых выступает умножение точки на число. Пусть p — простое число, G — генератор аддитивной циклической подгруппы группы точек эллиптических кривых, а P — произвольная точка, принадлежащая данной кривой.

Тогда любую точку P кривой $E(GF_p)$ можно представить как кратную генератору подгруппы в виде

$$P = n * G = \underbrace{G \oplus G \oplus \ldots \oplus G}_{n\ \text{раз}}, \quad (9)$$

где n — кратность данной точки генератору подгруппы; «$\oplus$» — знак групповой операции в группе точек кривой.

Алгоритм передачи информации по радиоканалу ШСПИ с СД с осуществлением криптографической защиты представлен на рисунке.



■ Алгоритм передачи информации в широковещательных системах с селективным доступом по радиоканалу ПРД — ПРМ с осуществлением криптографической защиты

Параметры алгоритма:

E — шифрующее преобразование симметричного алгоритма;

D — расшифровывающее преобразование симметричного алгоритма;

GF_p — конечное поле простой характеристики p;

$E_p(a, b)$ — эллиптическая кривая над полем GF_p в форме Вейрштрасса (кривая может быть задана на простом GF_p или расширенном GF_{qn} поле в аффинных либо проективных координатах);

$\#E(GF_p)$ — порядок группы точек кривой;

G — базовая точка — генератор подгруппы;

q — порядок циклической подгруппы;

h — односторонняя хеш-функция, принимающая значения в множестве двоичных векторов

длины 256, определенная стандартом Р 34.11-2012 [11];

i — номер передающего пункта;

$k_{з}^{ПРДi}$ — закрытый долговременный ключ передающего пункта (число);

$k_{о}^{ПРДi}$ — открытый долговременный ключ передающего пункта (точка эллиптической кривой), где $k_{о}^{ПРДi} = k_{з}^{ПРДi} \times G$;

$k_{з}^{ПРМ}$ — закрытый долговременный ключ абонентов приемного пункта (число);

$k_{о}^{ПРМ}$ — открытый долговременный ключ абонентов приемного пункта (точка эллиптической кривой), где $k_{о}^{ПРМ} = k_{з}^{ПРМ} \times G$;

d — секретный сеансовый ключ шифрования данных (число);

r — случайное число.

Алгоритм передачи информации по каналу связи осуществляется следующим образом.

1. Передающий пункт формирует информационный массив m.

2. Передающий пункт генерирует случайное число r.

3. Передающий пункт вычисляет сеансовый ключ:

$$d = h\left(k_{з}^{ПРДi} \times r \times k_{о}^{ПРМ}\right) = h\left(k_{з}^{ПРДi} \times r \times k_{з}^{ПРМ} \times G\right).$$

4. Передающий пункт шифрует кадр m на ключе d:

$$c = E_d(m).$$

5. Передающий пункт передает комбинацию $i\|c\|r$.

6. Приемный пункт, получив комбинацию $i\|c\|r$, в матрице доступности находит открытый ключ передающего пункта: i — $k_{о}^{ПРДi}$.

7. Приемный пункт вычисляет сеансовый ключ d:

$$d = h\left(k_{з}^{ПРМ} \times r \times k_{о}^{ПРДi}\right) = h\left(k_{з}^{ПРМ} \times r \times k_{з}^{ПРДi} \times G\right).$$

8. Приемный пункт расшифровывает полученный кадр:

$$m = D_d(c).$$

В качестве r может быть использовано как собственно случайное число, так и временная метка τ и их совокупность $R = r \times \tau$.

Пример генерации общего сеансового ключа при передаче информации по каналу с осуществлением криптографической защиты (без использования хеш-функции)

Начальные условия:

Параметры эллиптической кривой:

модуль p = 56*eefdd*4*da*5*da*8*de*9*c*6*e*7*d*42*cd*2406*c*58*d*71*cb*82*ee*7*af*4*bc*4121d57$_{16}$;

коэффициенты:

a = 420507356*e*57*e*70*f*37*fb*2108*f*63*bb*3*b*32815*e*46*d*237*e*396*ec*3*dbf*74$_{16}$;

b = 5*f*5*f*3*cca*03*cf*28*a*09*cac*8*f*15*bb*72*cccf*2*dccb*4*a*8*ac*45*ca*0*bdc*9*d*45$_{16}$;

порядок циклической подгруппы

q = 27*bdb*5*dda*5*a*728*a*04782*f*76*efeb*04676*dc*5*c*338*eb*26*c*48*d*9*b*7819*d*$_{16}$;

базовая точка G:

x = 9*ff*29581*d*0*e*93626157*f*777*c*31*c*6*c*2654661*b*7*c*4109*a*94*c*86*d*3*b*7*d*$_{16}$;

y = 4*c*5*f*6*c*882*bce*511*fedf*257*cbf*11*d*06*a*43*dcf*8*d*2754*ec*020*d*7*c*3190*d*$_{16}$.

Ключи передающего пункта:

$k_{з}^{ПРДi}$ = 1759783648*d*84246*da*7*a*202*c*170*e*6*bbff*320924*a*65543153*c*10*bb*$_{16}$;

$k_{о}^{ПРМi}$:

x = 4*b*805969*bc*68*df*959*ffd*0534*ad*27468*d*87*af*03*cc*613661591d*ad*9*eb*$_{16}$;

y = 45397*a*89*d*17*ffe*0913*d*73*fff*194*c*55*f*98*f*8*fc*3*ddaf*8*e*2265*b*69582*d*$_{16}$.

Ключи приемного пункта:

$k_{з}^{ПРМi}$ = 2249*d*446910301796*b*96*e*840*d*82*b*7460*f*010*b*2*be*78*be*8755*cc*9*d*52$_{16}$;

$k_{о}^{ПРМi}$:

x = 12*fea*6*bc*3*f*5047*b*4*c*098806*c*386*dbacb*12*a*767*dcde*8592911175*b*81$_{16}$;

y = 45*e*07*d*359*a*5*b*34904193580*de*8519*b*4226679*c*7*bbf*07*dbbddcce*86*f*$_{16}$.

1. Передающий пункт генерирует случайное число:

r = *cc*7*d*574*f*7*c*697502*baf*9*cbfb*83*d*04*e*29*fbd*3*efd*5*b*018*bc*347*f*$_{16}$.

2. Передающий пункт вычисляет сеансовый ключ: $d = k_{з}^{ПРДi} \times r \times k_{о}^{ПРМ}$ = 1759783648*d*84246*da*7*a*202*c*170*e*6*bbff*320924*a*65543153*c*10*bb*$_{16}$× ×*cc*7*d*574*f*7*c*697502*baf*9*cbfb*83*d*04*e*29*fbd*3*efd*5*b*018*bc*347*f*$_{16}$×(12*fea*6*bc*3*f*5047*b*4*c*098806*c*386*dbacb*12*a*767*dcde*8592911175*b*81$_{16}$, 45*e*07*d*359*a*5*b*34904193580*de*8519*b*4226679*c*7*bbf*07*dbbddcce*86*f*$_{16}$) = = 15*e*3*c*4*b*397*db*60794*e*42*a*6*d*84*e*8*c*590629*c*8*d*6*d*4*d*928676*b*9*f*18493255*b*792*a*2*fbfff*731*beb*290*a*13*de*2*cec*1*a*48*fc*31*d*74*f*39*c*27*c*3*f*302$_{16}$.

3. Приемный пункт, получив r, вычисляет сеансовый ключ $d = k_{з}^{ПРМ} \times r \times k_{о}^{ПРДi}$ = 2249*d*446910301796*b*96*e*840*d*82*b*7460*f*010*b*2*be*78*be*8755*cc*9*d*52$_{16}$×*cc*7*d*574*f*7*c*697502*baf*9*cbfb*83*d*04*e*29*fbd*3*efd*5*b*018*bc*347*f*$_{16}$×(4*b*805969*bc*68*df*959*ffd*0534*ad*27468*d*87*af*03*cc*613661591*dad*9*eb*$_{16}$, 45397*a*89*d*17*ffe*0913*d*73*fff*194*c*55*f*98*f*8*fc*3*ddaf*8*e*2265*b*69582*d*$_{16}$) = 15*e*3*c*4*b*397*db*60794*e*42*a*6*d*84*e*8*c*590629*c*8*d*6*d*4*d*928676*b*9*f*18493255*b*792*a*2*fbfff*731*beb*290*a*13*de*2*cec*1*a*48*fc*31*d*74*f*39*c*27*c*3*f*302$_{16}$.

Таким образом, оба абонента обладают одним и тем же секретным ключом d. Очевидно, что если в алгоритм добавить хеш-функцию, как описано выше, результат вычислений также у обоих абонентов будет одинаков, так как аргументы хеш-функции у абонентов равны. В ходе дальнейшей передачи по каналу связи информация может быть зашифрована на полученном ключе.

В случае необходимости абонент на передающем пункте может сформировать аутентифицирующие блоки (аналог электронной цифровой подписи), используя свой закрытый ключ, а на приемных пунктах абоненты осуществляют верификацию аутентифицирующих блоков с использованием открытого ключа передающего пункта [12].

Долговременные ключи передающего и приемного пунктов ($k_з^{ПРМ}$ и $k_з^{ПРМi}$) также требуют замены. При этом закрытые ключи передающего пункта могут генерировать самостоятельно, поскольку каждый передающий пункт обладает личным закрытым ключом, а также вычислять соответствующие открытые ключи с последующей передачей их на приемный пункт. Замена же пары долговременных ключей приемным пунктом представляет большую проблему, так как приемный пункт не осуществляет передачу.

Одним из таких способов является периодическая (раз в месяц) замена на основе проведения циклической операции со старыми ключами. Смена может производиться как в жесткой привязке ко времени, так и по команде центра [13]. Для реализации циклической смены ключей необходим криптографически стойкий генератор псевдослучайной последовательности. В качестве аппарата, осуществляющего циклическую операцию, может быть также использован математический аппарат эллиптических кривых. Примером может служить генератор, основанный на умножении точки на число в группе точек эллиптической кривой.

Кроме того, для замены ключевой информации в приемном пункте можно хранить не один мастер-ключ, а множество, и централизованно переходить с одного на другой в случае необходимости. Чтобы исключить несанкционированный доступ к сигналу, доступ ко всем ключам в приемном пункте должен осуществляться по предъявлению пароля либо с использованием средств типа «электронных паролей», т. е. посредством ввода парольной информации с электронных носителей (специальный чип и т. д.).

Заключение

Таким образом, для разработки полноценной криптосистемы необходимо предусмотреть процедуры формирования рабочих ключей, защищаемых долговременным мастер-ключом, а также процедуру смены мастер-ключа. Предпочтительными являются комбинированные криптосистемы, использующие преимущество первых по скорости и вторых по широким возможностям построения схем аутентификации и доставки ключей. Окончательный вариант архитектуры зависит от требований, предъявляемых к криптографической системе защиты информации, наличия связных каналов, способов доставки ключей до приемных пунктов и т. д. В качестве алгоритмов асимметричной части комбинированной схемы рекомендуется применить математический аппарат эллиптических кривых как обладающий наилучшими криптографическими и скоростными характеристиками по сравнению с другими типами асимметричных алгоритмов.

Литература

1. **Малюк А. А.** Информационная безопасность: концептуальные и методологические основы защиты информации. — М.: Горячая линия–Телеком, 2004. — 280 с.
2. **Stallings W.** Cryptography and Network Security Principles and Practices. — New Jersey: Prentice Hall, 2000. — 592 p.
3. **Schneier B.** Applied Cryptography. Protocols, Algorthms and Source Code in C. — N. Y.: John Wiley, 1996. — 1027 p.
4. **Ростовцев А. Г., Маховенко Е. Б.** Введение в криптографию с открытым ключом. — СПб.: Мир и Семья, 2001. — 336 с.
5. **Иванов М. А.** Криптографические методы защиты информации в компьютерных системах и сетях. — М.: Кудиц-Образ, 2001. — 368 с.
6. **Корниенко А. А., Еремеев М. А., Ададуров С. Е.** Средства защиты информации на железнодорожном транспорте: Криптографические методы и средства. — М.: Маршрут, 2006. — 256 с.
7. **Мальцев Г. Н., Штанько С. В.** Протоколы аутентификации абонентов и защиты информации на основе асимметричных криптоалгоритмов // Проблемы информационной безопасности. Компьютерные системы. 2003. № 1. С. 51–56.
8. **Корниенко А. А., Штанько С. В.** Криптографический протокол защиты информации в радиоканалах сетевых спутниковых систем с использованием асимметричных алгоритмов // Информационно-управляющие системы. 2006. № 5(24). С. 21–26.
9. **Харин Ю. С., Берник В. И., Матвеев Г. В., Агиевич С. В.** Математические и компьютерные основы криптологии. — Мн.: Новое знание, 2003. — 382 с.
10. **Штанько С. В., Жукова Н. А.** Схемы аутентификации данных и пользователей в распределенных информационных системах // Известия СПбГЭТУ «ЛЭТИ». 2012. № 8. С. 46–51.
11. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования. — М.: Стандартинформ, 2012. — 29 с.

12. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. — М.: Стандартинформ, 2013. — 18 с.
13. **Мальцев Г. Н., Панкратов А. В., Лесняк Д. А.** Исследование вероятностных характеристик изменения защищенности информационной системы от несанкционированного доступа нарушителей // Информационно-управляющие системы. 2015. № 1(74). С. 50–59. doi:10.15217/issn1684-8853.2015.1.50

UDC 621.396.9
doi:10.15217/issn1684-8853.2016.1.74

Providing Selective Access for Broadcasting Information Transfer

Shtanko S. V.[a], PhD., Tech., Associate Professor, craft2001@mail.ru
Lesniak D. A.[a], PhD., Tech., Lecturer, denislesnyk@mail.ru
[a]A. F. Mozhaiskiy Military Space Academy, 13, Zhdanovskaia St., 197082, Saint-Petersburg, Russian Federation.

Introduction: One of the main conditions for effective functioning of any information transfer system is its information security. An objective property of information system security is its gradual decrease at an invariable structure of the protection means, or when their parameters are fixed. To maintain the information security and prevent unauthorized access, the outdated keys in the cryptosystem are periodically replaced. In broadcasting systems of information transfer with selective access, there are features of ensuring information security related to the lack of a return channel of information transfer. Therefore we need to develop special methods of cryptographic protection for broadcasting information systems. **Purpose:** The goal is to improve the existing cryptographic system of data protection in order to increase the security of information transfer broadcasting channels with selective access. **Results:** A modification of data protection methods is proposed which should prevent unauthorized access to the system under conflict conditions of interaction with the violator. The modification is based on asymmetrical cryptographic systems with the mathematics of elliptic curves. On the base of the proposed methods, a cryptographic system is built to protect the data transferred via the channels of a broadcasting information system with selective access. An example of generating a common session key is given for the closed operation mode. **Practical relevance:** The proposed ways of improving the information transfer protection from unauthorized access can increase the information security of the system on the basis of using combined cryptosystems and mathematics of elliptic curves.

Keywords — Broadcasting Systems of Information Transfer with Selective Access, Unauthorized Access, Cryptoalgorithm, Key Management Protocol.

References

1. Maliuk A. A. *Informatsionnaia bezopasnost': kontseptual'nye i metodologicheskie osnovy zashchity informatsii* [Information Security: Conceptual and Methodological Bases of Information Security]. Moscow, Goriachaia liniia–Telecom Publ., 2004. 280 p. (In Russian).
2. Stallings W. *Cryptography and Network Security Principles and Practices*. New Jersey, Prentice Hall, 2000. 592 p.
3. Schneier B. Applied *Cryptography. Protocols, Algorthms and Source Code in C*. New York, John Wiley, 1996. 1027 p.
4. Rostovtsev A. G., Makhovenko E. B. *Vvedenie v kriptografiiu s otkrytym kliuchom* [Introduction to Cryptography With an Open Key]. Saint-Petersburg, Mir i Sem'ia Publ., 2001. 336 p. (In Russian).
5. Ivanov M. A. *Kriptograficheskie metody zashchity informatsii v komp'iuternykh sistemakh i setiakh* [Cryptographic Methods of Information Security in Computer Systems and Networks]. Moscow, Kudits-Obraz Publ., 2001. 368 p. (In Russian).
6. Korniyenko A. A., Yeremeyev M. A., Adadurov S. E. *Sredstva zashchity infor-matsii na zheleznodorozhnom transporte: Kriptograficheskie metody i sredstva* [Information Means of Protection on Railway Transport: Cryptographic Methods and Means]. Moscow, Marshrut Publ., 2006. 256 p. (In Russian).
7. Maltsev G. N., Shtanko S. V. Protocols of Authentication of Subscribers and Information Security on the Basis of Asymmetric Cryptoalgorithms. *Problemy informatsionnoi bezopasnosti. Komp'iuternye sistemy,* 2003, no. 1, pp. 51–56 (In Russian).
8. Kornienko A. A., Shtanko S. V. Information Security Protocol for Network Satellite Systems Using Asymmetric Algorithms. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2006, no. 5(24), pp. 21–26 (In Russian).
9. Kharin Iu. S., Bernik V. I., Matveev G. V., Agievich S. V. *Matematicheskie i komp'iuternye osnovy kriptologii* [Mathematical and Computer Fundamentals of Cryptology]. Minsk, Novoe znanie Publ., 2003. 382 p. (In Russian).
10. Shtanko S. V., Zhukova N. A. Schemes of Authentication of Data and Users in the Distributed Information Systems. *Izvestiia SPbGETU «LETI»*, 2012, no. 8, pp. 46–51 (In Russian).
11. State Standard R 34.11-2012. Information Technology. Cryptographic Information Security. Hashing Function. Moscow, Standartinform Publ., 2012. 29 p. (In Russian).
12. State Standard R 34.10-2012. Information Technology. Cryptographic Information Security. Processes of Formation and Check of a Digital Signature. Moscow, Standartinform Publ., 2013. 18 p. (In Russian).
13. Maltsev G. N., Pankratov A. V., Lesniak D. A. A Probabilistic Characteristics of Information System Security Changes under Unauthorized Access. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2015, no. 1(74), pp. 50–59 (In Russian). doi:10.15217/issn1684-8853.2015.1.50