УДК 621.396.9
doi:10.31799/1684-8853-2018-5-57-65

Научные статьи
Articles

# Ограничение несанкционированного доступа в радиотехнических системах с широковещательной передачей информации

***С. В. Штанько***[a], *канд. техн. наук, доцент, orcid 0000-0002-8391-8911, craft2001@mail.ru*
[a]*Военно-космическая академия им. А. Ф. Можайского, Ждановская наб., 13, Санкт-Петербург, 197198, РФ*

***Введение:*** *использование радиотехнических систем с широковещательной передачей информации связано с возможностью организации сплошных зон радиодоступа при ограниченном числе передающих пунктов и достаточно большом количестве абонентов (потребителей информации). Однако в системах с широковещательной передачей информации имеются особенности реализации ограничения несанкционированного доступа, обусловленные пространственной электромагнитной доступностью радиоканалов и отсутствием обратного канала передачи информации.* ***Цель:*** *разработка принципов распространения ключевой информации и управления селективным доступом абонентов к информации, передаваемой в широковещательных радиотехнических системах различного назначения, с учетом ограничений, накладываемых широковещательным режимом передачи.* ***Метод:*** *модификация используемых в радиотехнических системах с широковещательной передачей информации методов ограничения несанкционированного доступа на основе комбинации симметричных и асимметричных криптоалгоритмов.* ***Результаты:*** *анализ существующих подходов к ограничению несанкционированного доступа в системах с широковещательной передачей информации показал, что ограничения, накладываемые характером функционирования радиотехнических систем с широковещательной передачей информации, в значительной степени затрудняют или делают невозможным использование различных сетевых протоколов защищенного информационного обмена, широко распространенных в компьютерных сетях. Обоснованы принципы (наличие двух или более уровней ключевой информации, возможность замены всей ключевой информации, возможность управления доступом к системе) и способ ограничения несанкционированного доступа к радиоканалам широковещательных систем передачи информации на основе комбинированного использования симметричных и асимметричных криптоалгоритмов. В качестве симметричной части возможно использование блочных или поточных криптоалгоритмов. В качестве криптоалгоритмов асимметричной части рекомендуется использовать математический аппарат эллиптических кривых, как обладающий наилучшими криптографическими и скоростными характеристиками по сравнению с другими типами асимметричных криптоалгоритмов.* ***Практическая значимость:*** *предложенный способ ограничения несанкционированного доступа может быть использован для организации защищенного информационного обмена и управления селективным доступом к информации, передаваемой в широковещательных радиотехнических системах различного назначения.*

***Ключевые слова*** *— широковещательная передача информации, несанкционированный доступ, ключевая информация, симметричные криптоалгоритмы, асимметричные криптоалгоритмы.*

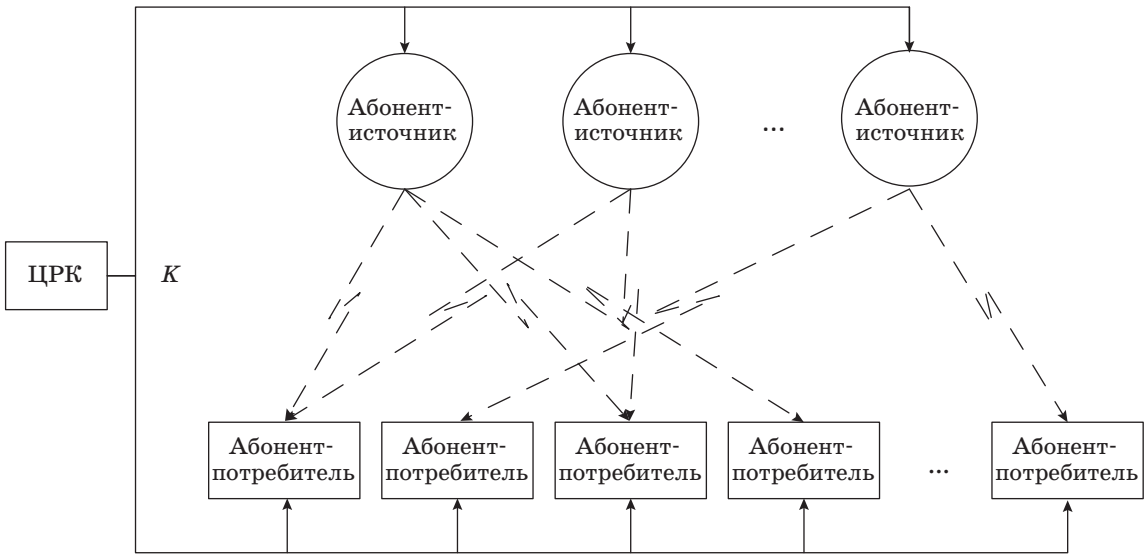
**Цитирование:** Штанько С. В. Ограничение несанкционированного доступа в радиотехнических системах с широковещательной передачей информации. *Информационно-управляющие системы*, 2018, № 5, с. 57–65. doi:10.31799/1684-8853-2018-5-57-65
**Citation:** Shtanko S. V. Restriction of unauthorized access in radio systems with broadcast data transmission. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2018, no. 5, pp. 57–65 (In Russian). doi:10.31799/1684-8853-2018-5-57-65

## Введение

Широкое использование радиотехнических систем с широковещательной передачей информации и расширение областей их применения [1–4] приводит к тому, что возникает задача ограничения доступа к информации, передаваемой (транслируемой) такими системами. Пространственная электромагнитная доступность, являющаяся свойством любых радиоканалов, создает условия для несанкционированного доступа (НСД) к информации, передаваемой широковещательными радиотехническими системами [5–8]. При этом особенности таких систем в ряде случаев не позволяют эффективно применять в них существующие криптографические алгоритмы и протоколы защищенного информационного обмена, аутентификации абонентов и распределения ключевой информации [6, 9–13], обеспечивающие селективный доступ и предотвращение НСД к передаваемой информации.

## Общий подход к реализации ограничения доступа в системах с широковещательной передачей информации

Рассмотрим типовую радиотехническую систему с широковещательной передачей информации (широковещательную сеть) для большого количества абонентов (рис. 1). Такая система представляет собой ограниченное количество абонентов-источников и достаточно большое количество абонентов-приемников, или потреби-




■ ***Рис. 1.*** Схема радиотехнической системы с широковещательной передачей информации: ЦРК — центр распределения ключей

■ ***Fig. 1.*** Broadcast radio system scheme: ЦРК — rey distribution center

телей информации. При этом накладывается ограничение на отсутствие обратного канала от абонента-приемника (потребителя системы с широковещательной передачей информации) к абоненту-источнику.

При реализации ограничения доступа к информации, передаваемой в широковещательных радиотехнических системах, возникает необходимость защиты таких ресурсов от НСД. Основным техническим методом защиты информации, передаваемой по радиоканалам, от НСД является криптографическая защита информации [14, 15]. Условием ее реализации является распространение ключевой информации между абонентами. Генерацию и распространение ключевой информации $K$ осуществляет ЦРК.

В основу принципа защиты информации от НСД в широковещательных сетях с учетом ограничений, накладываемых широковещательным режимом передачи, может быть положено совместное использование симметричных (одноключевых) и асимметричных (двухключевых) криптоалгоритмов [7, 16]. При этом непосредственно для шифрования передаваемых данных целесообразно использовать симметричные криптоалгоритмы, которые обладают бóльшим быстродействием при аппаратной и программной реализации, чем асимметричные [9, 14, 15], а для процедур распределения ключей, аутентификации абонентов и сообщений и управления доступом целесообразно использовать асимметричные криптоалгоритмы, которые обладают большими возможностями и гибкостью для решения таких задач [17–19].

Опишем систему ограничения НСД к радиотехнической системе с широковещательной передачей информации следующим выражением:

$$S = <\{\mathbf{A}\}, \{KC\}>, \quad (1)$$

где $\mathbf{A}$ — используемые в системе ограничения несанкционированного доступа криптоалгоритма; $KC$ — функция, описывающая процедуру замены ключевой информации криптоалгоритмов.

Теоретико-множественное описание симметричного криптоалгоритма $\mathbf{A}$ определяется четверкой [9, 15]

$$\mathbf{A}_c = <X, K, Y, f>, \quad (2)$$

где $X = \{x_1, x_2, ..., x_n\}$ — множество открытых сообщений; $K = \{k_1, k_2, ..., k_l\}$ — множество ключей; $Y = \{y_1, y_2, ..., y_m\}$ — множество криптограмм; $f$: $X \times K \to Y$ — функция, однозначно определяющая отображение $X$ на $Y$; $f(x, k) = y$, $x \in X$, $k \in K$, $y \in Y$.

В выражении (2) функция $f$ определяет семейство отображений $f_k$: $x \to y$, $k \in K$. Тогда преобразование зашифровывания характеризует функция $E_k(x) = f_k(x) = f(x, k)$, а преобразование расшифровывания характеризует функция $D_k(y) = f^{-1}(y, k) = x$. В симметричном криптоалгоритме для процессов зашифровывания и расшифровывания используется один и тот же ключ $k$ (либо различные ключи, но такие, что один легко вычислить из другого). Для реализации абонентского шифрования посредством симметричных криптоалгоритмов необходимо, чтобы либо

все абоненты обладали одним и тем же ключом $k$, либо каждая пара абонентов обладала своим ключом $k$, что достаточно трудно реализовать при большом количестве абонентов.

Процедура замены ключевой информации с использованием симметричных криптоалгоритмов сводится к двум возможным вариантам: либо рекурсивная генерация нового ключа с использованием предыдущего ключа, либо выбор нового ключа из заранее сформированного (сгенерированного) множества [17]. При этом к первому из указанных вариантов замены ключевой информации можно отнести как непосредственно схемы формирования нового ключа на основе некоторой циклической функции от старого ключа, так и передачу нового сгенерированного ключа по открытым каналам, шифруя его старым ключом.

Рекурсивную генерацию нового ключа с использованием предыдущего ключа можно описать следующим образом:

$$k_i = KC(k_{i-1}, r_i), \qquad (3)$$

где $r_i$ — некоторая дополнительная информация, используемая на текущем шаге формирования ключа.

Выбор нового ключа из заранее сформированного множества может быть описан следующим образом:

$$k_i = KC(\{k_l, l = 1..n\}, \varphi), \qquad (4)$$

где $\varphi$ — правило выбора очередного ключа из множества $\{k_l, l = 1..n\}$; $n$ — мощность ключевого множества.

Следовательно, при использовании только симметричных криптоалгоритмов способа получения нового ключа без передачи дополнительной закрытой информации не существует. Кроме того, симметричные криптоалгоритмы обладают рядом ограничений: они не позволяют реализовывать эффективные процедуры $KC$ замены ключевой информации $K$ и процедуры аутентификации (в случае необходимости подтверждения подлинности абонентов или данных) [17–20].

Данные задачи более эффективно решаются с использованием асимметричных криптоалгоритмов. Теоретико-множественное описание асимметричного криптоалгоритма определяется пятеркой [9, 15]

$$\mathbf{A}_{\text{ac}} = <X, K, Y, E, D>, \qquad (5)$$

где $X = \{x_1, x_2, ..., x_n\}$ — множество открытых сообщений; $K = \{k_1, k_2, ..., k_l\}$ — множество ключей, включающее в себя два подмножества: $K = \{K_E, K_D\}$, $K_E$ — подмножество ключей зашифровывания, $K_D$ — подмножество ключей расшифровывания; $Y = \{y_1, y_2, ..., y_m\}$ — множество криптограмм; $E$: $X \times K_E \to Y$ — алгоритм зашифровывания; $D$: $Y \times K_D \to X$ — алгоритм расшифровывания.

В асимметричном алгоритме для процессов зашифровывания и расшифровывания используются различные ключи $k^{\text{о}}$ и $k^{\text{з}}$ такие, что вычисление закрытого ключа $k^{\text{з}}$ по открытому $k^{\text{о}}$ является вычислительно сложной задачей.

Для асимметричных алгоритмов функция замены ключа может быть описана следующим образом:

$$k_i = KC(k_1^{\text{о}}(k_1^{\text{з}}), k_2^{\text{о}}(k_2^{\text{з}}), r_i), \qquad (6)$$

где $k_1^{\text{о}}$, $k_2^{\text{о}}$ — открытые ключи 1-го и 2-го абонентов соответственно; $k_1^{\text{з}}$, $k_2^{\text{з}}$ — закрытые ключи 1-го и 2-го абонентов соответственно.

Выражение (6) в общем случае описывает как непосредственно шифрование информации открытыми ключами абонентов, так и использование открытых ключей для передачи закрытых ключей симметричного криптоалгоритма либо для формирования ключа симметричного криптоалгоритма.

Следовательно, асимметричные криптоалгоритмы позволяют сформировать новый закрытый ключ без передачи закрытой информации. Тем не менее применение асимметричных криптоалгоритмов в системах с широковещательной передачей информации также ограничено, так как отсутствует возможность проведения диалоговых процедур. Абоненты-потребители информации в общем случае являются пассивными участниками информационного обмена и не могут передавать свою ключевую информацию для осуществления процедур формирования сеансовых ключей и аутентификации.

Ограничения, накладываемые характером функционирования радиотехнических систем с широковещательной передачей информации, в значительной степени затрудняют или делают невозможным использование различных сетевых протоколов защищенного информационного обмена, широко распространенных в компьютерных сетях [18, 19]. Существующие в настоящее время подходы к организации защищенного информационного обмена в широковещательных радиотехнических системах в основном сводятся к использованию единственного ключа (фиксированного множества ключей) или к передаче текущих (рабочих) ключей абонентам-потребителям, зашифрованных на долговременных ключах (индивидуальных ключах, мастер-ключах), как это сделано, например, в протоколах защищенного информационного обмена в спутниковом телевидении (протоколы Viaccess, DRECrypt, «Роскрипт» и др.) [3, 4, 7, 8, 21, 22]. Однако всегда

существует ненулевая вероятность компрометации любой ключевой информации: единственного ключа, множества ключей, долговременных ключей, в том числе индивидуальных, — поэтому необходимо иметь возможность замены любой ключевой информации [23].

Для разработки полноценной системы ограничения НСД в спутниковых системах с широковещательной передачей информации необходимо обеспечить реализацию процедуры смены единого ключа, а в лучшем случае — процедуры формирования рабочих ключей, защищаемых долговременным ключом, а также процедуры смены долговременного ключа [24, 25]. Принципиальное значение при предотвращении НСД с использованием симметричных криптоалгоритмов состоит в том, что в соответствии с формулами (3) и (4) они не позволяют осуществлять замену всей ключевой информации без передачи дополнительных закрытых данных. В существующих радиотехнических системах с широковещательной передачей информации с использованием симметричных криптоалгоритмов используются различные многоуровневые схемы, имеющие целью снизить вероятность компрометации всей системы. В таких схемах ключи первого уровня используются только для шифрования ключей второго уровня, а ключи второго уровня используются непосредственно для шифрования передаваемой информации. Рассмотрим существующие способы реализации двухуровневых схем распространения ключевой информации.

Первый способ заключается в использовании единого несменяемого мастер-ключа (долговременного ключа, ключа первого уровня) для шифрования рабочих ключей (ключей второго уровня). Функция замены ключа в этом случае выглядит следующим образом:

$$k_i = KC(k_m, <k_i>), \qquad (7)$$

где $k_m$ — мастер-ключ.

В этом случае новый рабочий ключ не зависит от предыдущего, и схема позволяет в любой момент сформировать новый ключ и распространить его, зашифровав на мастер-ключе. Рабочий ключ заменяется ЦРК с заданной периодичностью либо при необходимости. Малый объем шифруемой на мастер-ключе информации (только периодически распространяемый рабочий ключ) не позволяет нарушителю проводить его эффективный криптоанализ. Тем не менее данный способ ограничения НСД также не позволяет реализовывать механизм замены мастер-ключа.

Второй способ заключается в использовании несменяемых индивидуальных ключей абонентов (ключей первого уровня) и множества рабочих ключей (ключей второго уровня), зашифрованного предварительно на индивидуальных ключах. Расшифровать любой рабочий ключ из данного множества может только тот абонент, на чьем индивидуальном ключе данное множество зашифровано. ЦРК распространяет очередной ключ $k_i$ (периодически либо по необходимости) в зашифрованном виде $<k_i>$ индивидуально для каждого абонента. Каждый абонент расшифровывает очередной рабочий ключ на своем индивидуальном ключе, получая один и тот же ключ. Функция замены ключа в этом случае выглядит следующим образом:

$$k_i = KC(k^{и},\{<k_l>, l = 1..n\}), \qquad (8)$$

где $k^{и}$ — индивидуальный ключ абонента; $\{<k_l>, l = 1..n\}$ — множество зашифрованных на индивидуальном ключе абонента рабочих ключей мощностью $n$.

Данный способ позволяет заменять рабочие ключи, передавая их абонентам в зашифрованном виде на их индивидуальных ключах, однако так же, как и в первом способе, отсутствует возможность замены долговременных индивидуальных ключей. Кроме того, в случае если индивидуальные ключи известны только самим абонентам, отсутствует возможность изменять сформированное множество ключей.

## Способ ограничения НСД в радиотехнических системах с широковещательной передачей информации с комбинированным использованием асимметричных криптоалгоритмов

Существующие способы распространения ключевой информации на основе симметричных криптоалгоритмов не обладают возможностью обновления всей ключевой информации без передачи дополнительных закрытых данных, а все возможные варианты сводятся либо к рекурсивной функции (3), либо к выбору ключа из заранее сформированного множества (4). При использовании двухуровневых ключевых схем (с индивидуальными ключами, мастер-ключами) существует возможность передавать ключи второго уровня (новые рабочие ключи) в соответствии с формулами (7) и (8), однако в этом случае проблема замены ключей просто переносится на ключи первого уровня (долговременные ключи). При этом рассмотренные способы и функции замены ключей (3), (4), (7) и (8) для радиотехнических систем с широковещательной передачей информации охватывают практически все возможные варианты с использованием только симметричных криптоалгоритмов, а другие возможные варианты

являются их комбинацией в том или ином виде. Поэтому для принципиального решения вопроса замены всей ключевой информации необходимо использовать асимметричные криптоалгоритмы.

Таким образом, существуют задача разработки способа ограничения НСД, позволяющего осуществлять распространение ключевой информации в радиотехнических системах с широковещательной передачей информации с учетом их особенностей и ограничений, и задача управления доступом к системе с широковещательной передачей информации, для чего также необходимо осуществлять замену ключевой информации, в том числе индивидуальных ключей с тем, чтобы исключать при необходимости абонентов из числа допущенных к системе. Симметричные криптоалгоритмы обладают рядом ограничений, не позволяющих осуществлять замену всей ключевой информации без передачи дополнительных закрытых данных (таким образом, чтобы текущие ключи не были аргументом функции *КС* для генерации новой ключевой информации). Для решения данной проблемы необходимо модифицировать существующие схемы посредством введения асимметричных криптоалгоритмов и создания комбинированных систем ограничения НСД к радиотехническим системам с широковещательной передачей информации с учетом их особенностей и ограничений.

Для устранения недостатков существующих способов ограничения НСД в радиотехнических системах с широковещательной передачей информации необходимо разработать способ с комбинированным использованием симметричных и асимметричных криптоалгоритмов, позволяющий осуществлять замену всей ключевой информации — ключей первого и второго уровня (рабочих и долговременных), а также осуществлять управление доступом, исключая абонентов в случае их компрометации из числа авторизованных абонентов.

Для реализации такого способа ограничения НСД для шифрования и передачи рабочих ключей $\{k_i\}$ необходимо использовать асимметричный криптоалгоритм. Схема реализации способа ограничения НСД в радиотехнических системах с широковещательной передачей информации с использованием асимметричных криптоалгоритмов представлена на рис. 2. В аппаратуре шифрования *АШ* каждого абонента формируется пара ключей асимметричного криптоалгоритма (открытый и закрытый) $[k_j^{\text{о}}, k_j^{\text{з}}]$, при этом открытые ключи остаются в базе данных (матрице доступности) ЦРК, а закрытые известны только абонентам, для которых они сформированы (рис. 2, *а*). Затем каждый ключ $k_i$ может быть зашифрован открытыми ключами абонентов и передан каждому абоненту индивидуально (рис. 2, *б*):

$$<k_i^j> = E_{Kj}^{\text{о}}(k_i), \qquad (9)$$

где $<k_i^j>$ — зашифрованный новый рабочий ключ на открытом ключе $k_j^{\text{о}}$ абонента $j$; $E_{Kj}^{\text{о}}$ — процесс зашифровывания на открытом ключе $k_j^{\text{о}}$ абонента $j$.

Каждый абонент расшифровывает рабочий ключ на своем закрытом ключе, получая один и тот же ключ:

$$k_i = D_{Kj}^{\text{з}}(<k_i^j>), \qquad (10)$$

где $D_{Kj}^{\text{з}}$ — процесс расшифровывания на закрытом ключе $k_j^{\text{з}}$ абонента $j$.

Процедуру замены ключей можно описать следующей функцией:

$$k_i = KC(k^{\text{о}}, \{<k_l>, l = 1..n\}). \qquad (11)$$

Затем абонент-источник широковещательной передачи информации передает информацию, шифруя ее на рабочем ключе:

$$c = E_{Ki}(m), \qquad (12)$$

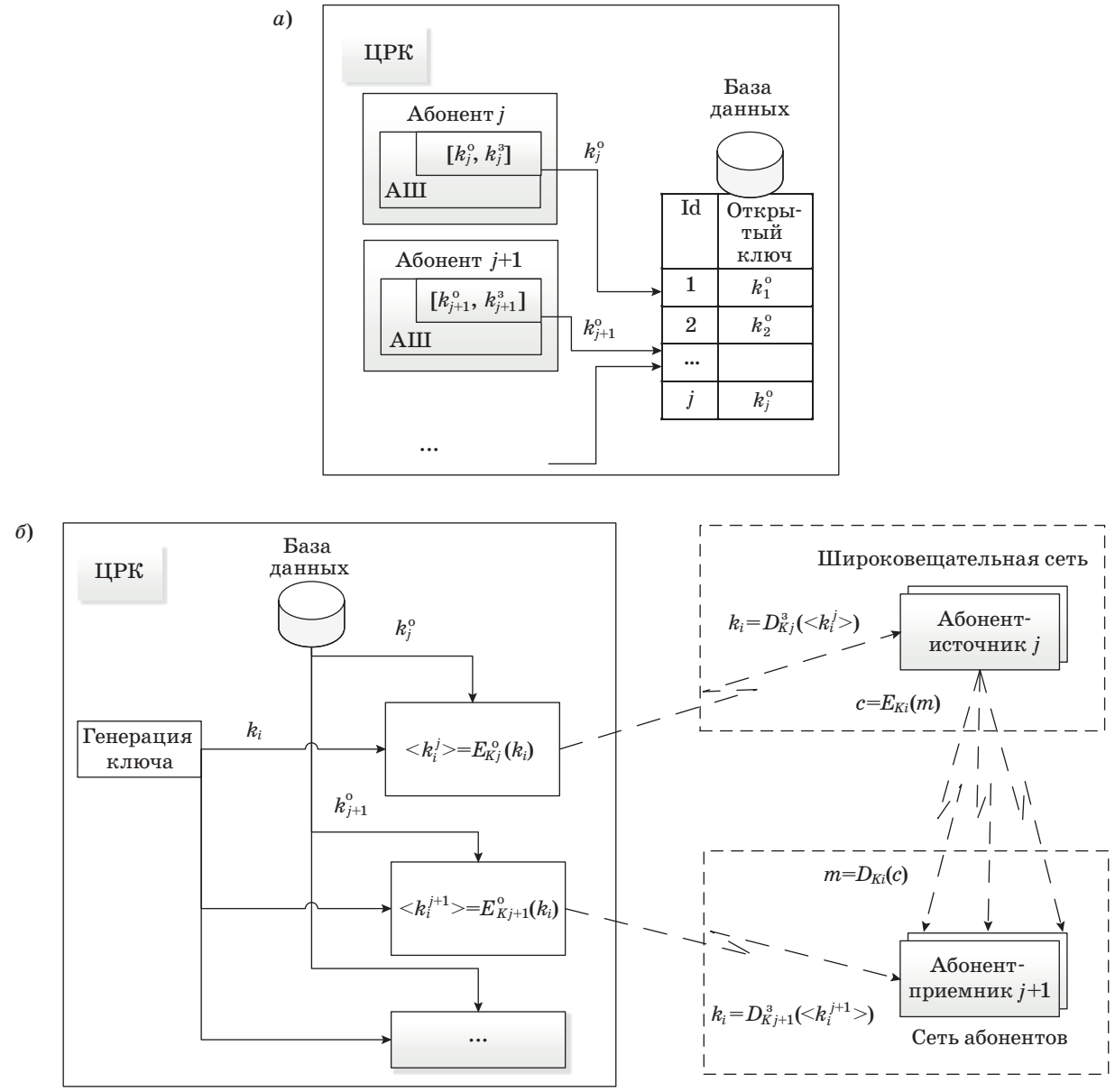
где $c$ — зашифрованные данные; $m$ — исходные открытые данные; $E_{Ki}$ — процедура шифрования на ключе $k_i$.

Абонент-получатель расшифровывает информацию

$$m = D_{Ki}(c), \qquad (13)$$

где $D_{Ki}$ — процедура расшифровывания на ключе $k_i$.

При реализации рассмотренного способа, в отличие от способов ограничения НСД на основе симметричных криптоалгоритмов, множество рабочих ключей $\{k_i\}$ не является неизменяемым и может быть в любой момент дополнено или изменено, поскольку в ЦРК имеются открытые ключи всех абонентов, в том числе абонентов-источников, и в любой момент существует возможность сгенерировать новый ключ, зашифровать его на открытых ключах абонентов и передать им. Ключи могут быть переданы абонентам-потребителям как через широковещательную сеть через абонентов-источников, так и по другим каналам. Кроме того, существует возможность смены и самих ключей $[k_j^{\text{о}}, k_j^{\text{з}}]$ абонентов. Ключи могут быть сформированы самими абонентами, и они могут передать открытые ключи $k_j^{\text{о}}$ в ЦРК, оставив закрытые ключи $k_j^{\text{з}}$ у себя. Такая схема позволит управлять доступом абонентов-потребителей информационных ресурсов к сети. В случае необ-




■ ***Рис. 2***. Схема реализации способа ограничения НСД с использованием асимметричных криптоалгоритмов: *а* — первый этап — подготовительный; *б* — второй этап — рабочий

■ ***Fig. 2***. The unauthorized access restriction method scheme with asymmetric crypto algorithms using: *а* — the first stage — the preparatory phase; *б* — the second stage — the worker

ходимости исключения абонента-потребителя из числа авторизованных новый рабочий ключ $k_i$ не шифруется на его открытом ключе $k_j^o$ и не передается по сети, в результате чего абонент-потребитель теряет доступ к ресурсам сети.

При реализации предложенного способа ограничения несанкционированного доступа на основе комбинированного использования симметричных и асимметричных криптоалгоритмов в качестве симметричной части возможно использование блочных или поточных криптоалгоритмов, например, отечественных криптоалгоритмов шифрования, определяемых ГОСТ Р 34.12-2015 (например, шифр «Магма», ранее определяемый ГОСТ 28147-89). Данный шифр имеет три режима шифрования (режим простой замены, режим гаммирования, режим гаммирования с обратной связью) и режим выработки имитовставки. В качестве криптоалгоритмов асимметричной части рекомендуется использовать математический аппарат эллиптических кривых как обладающий наилучшими криптографическими и скоростными характеристиками по сравнению с другими типами асимметричных криптоалгоритмов.

## Заключение

Предложенный способ ограничения несанкционированного доступа к радиоканалам широковещательных систем передачи информации на основе комбинированного использования симметричных и асимметричных криптоалгоритмов позволяет решать поставленную задачу замены всей ключевой информации — как рабочих ключей, так и индивидуальных (ключей первого и второго уровня), а также управлять доступом абонентов-получателей к системе. Кроме того, используя асимметричные криптоалгоритмы, можно осуществлять дальнейшее развитие предложенного способа, реализовывать более гибкие схемы и различные сервисы, в том числе сервисы аутентификации. Данный способ может быть применен для организации защищенного информационного обмена и управления доступом к радиотехническим системам с широковещательной передачей информации различного назначения.

## Литература


1. **Сакалема Д. Ж.** Подвижная радиосвязь. — М.: Горячая линия–Телеком, 2012. — 512 с.
2. **Карташевский В. Г., Семенов С. Н., Фирстова Т. В.** Сети подвижной связи. — М.: Эко-Трендз, 2001. — 296 с.
3. **Кукк К. И.** Спутниковая связь: прошлое, настоящее, будущее. — М.: Горячая линия–Телеком, 2016. — 256 с.
4. **Костин М. В.** Системы условного доступа//Телеспутник. 2004. № 11(109). С. 62–64.
5. **Нелюб С. А.** Защита речевой информации в радиосетях связи // Инженерный вестник. 2012. № 9. http://ainjournal.ru/doc/501059.html (дата обращения: 15.07.2018).
6. **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.
7. **Штанько С. В., Лесняк Д. А.** Алгоритмы защищенного информационного обмена в радиоканалах космической навигационной системы // Известия высших учебных заведений России. Радиоэлектроника. 2015. № 5. С. 47–51.
8. **Гладченков А.** Спутниковые технологии VSAT и информационная безопасность сети // Журнал сетевых решений/LAN. 2007. № 09. https://www.osp.ru/lan/2007/09/4374549/ (дата обращения: 06.05.2018).
9. **Stallings W.** Cryptography and Network Security Principles and Practices. Fourth Ed. — New Jersey: Prentice Hall, 2005. — 592 p.
10. **Yevpak S. A.** The Special Broadcast Security Scheme based on RM-codes and the Protection from Some Linear Algebraic Attacks// Numerical Algebra with Applications: Proc. of Fourth China-Russia Conf., Rostov-on-Don, SFedU, 2015. P. 183.
11. **Деундяк В. М., Косолапов Ю. В.** Криптосистема на индуцированных групповых кодах // Моделирование и анализ информационных систем. 2016. № 23(2). С. 137–152. https://doi.org/10.18255/1818-1015-2016-2-137-152 (дата обращения: 06.05.2018).
12. **Деундяк В. М., Таран А. А.** О применении кодов Хэмминга в системе распределения ключей для конференций в многопользовательских системах связи // Вестник ВГУ. Серия: Системный анализ и информационные технологии. 2015. № 3. С. 43–50.
13. **Щеглов К. А., Щеглов А. Ю.** Новый подход к защите данных в информационной системе // Изв. вузов. Приборостроение. 2015. Т. 58. № 3. С. 157–166. doi:10.17586/0021-3454-2015-58-3-157-166/issn0021-3454
14. **Шаньгин В. Ф.** Защита информации в компьютерных системах и сетях. — М.: ДМК, 2012. — 592 с.
15. **Schneier B.** Applied Cryptography. Protocols, Algorthms and Source Code in C. — New York: John Wiley & Sons, 2015. — 784 p.
16. **Корниенко А. А., Штанько С. В.** Криптографический протокол защиты информации в радиоканалах сетевых спутниковых систем с использованием асимметричных алгоритмов // Информационно-управляющие системы. 2006. № 5. С. 21–26.
17. **Остроумов О. А., Синюк А. Д.** Протокол открытого формирования трехстороннего ключа // Наукоемкие технологии в космических исследованиях Земли. 2014. Т. 6. Вып. 2. С. 48–52.
18. **Штанько С. В., Жукова Н. А.** Схемы аутентификации данных и пользователей в распределенных информационных системах // Изв. СПбГЭТУ «ЛЭТИ». 2012. № 8. С. 46–51.
19. **Штанько С. В., Лесняк Д. А.** Обеспечение селективного доступа при широковещательной передаче информации // Информационно-управляющие системы. 2016. № 1. С. 74–79. doi:10.15217/issn1684-8853.2016.1.74
20. **Osipov D. S., Frolov A. A., Zyablov V. V.** Multiple Access System for a Vector Disjunctive Channel//Problems of Information Transmission. 2012. Vol. 48. N 3. P. 243–249.
21. **Frolov A. A., Zyablov V. V.** A New Coding Method for a Multiple-Access System with a Large Number of Active users// Proc. IEEE Information Theory Workshop (ITW), 2015, April 26 –May 1, Jerusalem, Israel. 2015. P. 1–5.
22. **Анисимов Д. В., Дмитриев С. В.** Управление доступом к среде передачи данных в беспроводных сетях стандарта IEEE 802.11 с учетом ненасыщенного со-

стояния канала // Информационные системы и технологии. 2018. № 4(108). С. 99–107. issn2072-8964

23. **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. С. 50–59. doi:10.15217/issn1684-8853.2015.1.50
24. **Gentry C., Waters B.** Adaptive Security in Broadcast Encryption Systems// Advances in Cryptology — EUROCRYPT 2009. Springer, 2009. P. 171–188.
25. **Blundo C., Mattos L. A. F., Stinson D. R.** Trade-offs between Communication and Storage in Unconditionally Secure Schemes for Broadcast Encryption and Interactive Key Distribution//Advances in Cryptology. LNCS. 1996. Vol. 1109. P. 387–400.

UDC 621.396.9
doi:10.31799/1684-8853-2018-5-57-65

**Restriction of unauthorized access in radio systems with broadcast data transmission**

S. V. Shtanko[a], PhD, Tech., Associate Professor, orcid 0000-0002-8391-8911, craft2001@mail.ru
[a]A. F. Mozhaiskii Military Space Academy, 13, Zhdanovskaia Emb., 197198, Saint-Petersburg, Russian Federation

**Introduction:** The usage of broadcast radio systems is associated with the possibility of organizing continuous radio access zones with a limited number of transmission points and a considerable number of subscribers (information consumers). However, radio broadcasting systems have specific features of unauthorized access restriction related to the spatial electromagnetic accessibility of radio channels and the absence of a reverse information channel. **Purpose:** Developing principles for key information distribution and for the control over selective access of subscribers to the data transmitted in broadcast radio systems of various purposes, taking into account the restrictions imposed by the broadcasting mode of transmission. **Method:** Modification of the unauthorized access restriction methods used in radio broadcast systems, based on a combination of symmetric and asymmetric crypto algorithms. **Results:** The analysis of the existing approaches to unauthorized access restriction in broadcast radio systems has shown that the restrictions imposed by the peculiarities of these systems often make it difficult or impossible to apply various network protocols of protected data exchange commonly used in computer networks. We substantiate the principles (presence of two or more levels of key information; possibility to replace all the key information; ways to control the access to the system) and a way to restrict unauthorized access to the radio channels of broadcast systems, based on the combined use of symmetric and asymmetric crypto algorithms. As the symmetric part, you can use block or stream ciphers. As algorithms for the asymmetric part, elliptic curves are recommended, as they have the best cryptographic and speed characteristics as compared to other types of asymmetric cryptographic algorithms. **Practical relevance:** The proposed unauthorized access restriction method can be used to organize secure data exchange and selective control over the access to data transmitted in broadcast radio systems of various purposes.

**Keywords** — broadcast data transmission, unauthorized access, key information, symmetric crypto algorithms, asymmetric crypto algorithms.

**Citation:** Shtanko S. V. Restriction of unauthorized access in radio systems with broadcast data transmission. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2018, no. 5, pp. 57–65 (In Russian). doi:10.31799/1684-8853-2018-5-57-65

**References**

1. Sakalema D. Zh. *Podvizhnaia radiosviaz'* [Mobile Radio Communication]. Moscow, Goriachaia liniia–Telecom Publ., 2012. 512 p. (In Russian).
2. Kartashevskii V. G., Semenov S. N., Firstova T. V. *Seti podvizhnoi sviazi* [Mobile Networks]. Moscow, Eko-Trendz Publ., 2001. 296 p. (In Russian).
3. Kukk K. I. *Sputnikovaia sviaz': proshloe, nastoiashchee, budushchee* [Satellite Communication: Past, Present, Future]. Goriachaia liniia–Telecom Publ., 2016. 256 p. (In Russian).
4. Kostin M. V. Conditional Access Systems. *Telesputnik*, 2004, no. 11(109), pp. 62–64 (In Russian).
5. Nelyub S. A. Speech Information Protection in Radio Networks. *Inzhenernyj vestnik*, 2012, no. 9. Available at: http://ainjournal.ru/doc/501059.html (accessed 15 July 2018) (In Russian).
6. Mal'tsev G. N., Shtan'ko S. V. Protocols of Authentication of Subscribers and Information Security on the Basis of Asymmetric Cryptoalgorithms. *Problemy informatsionnoi bezopasnosti. Komp'iuternye sistemy* [Information Security Problems. Computer Systems], 2003, no. 1, pp. 51–56 (In Russian).
7. Shtan'ko S. V., Lesniak D. A. Algorithms for Secure Information Exchange in Space Radio Navigation Systems. *Izvestiia vysshikh uchebnykh zavedenii Rossii. Radioelektronika*, 2015, no. 5, pp. 47–51 (In Russian).
8. Gladchenkov A. Satellite VSAT Technology and Information Security Network. *Zhurnal setevykh reshenii/LAN*, 2007, no. 9. Available at: https://www.osp.ru/lan/2007/09/4374549/ (accessed 06 May 2018) (In Russian).
9. Stallings W. *Cryptography and Network Security Principles and Practices*. Fourth Ed. New Jersey, Prentice Hall, 2005. 592 p.
10. Yevpak S. A. The Special Broadcast Security Scheme based on RM-codes and the Protection from Some Linear Algebraic Attacks. *Proc. of Fourth China-Russia Conference "Numerical Algebra with Applications"*, Rostov-on-Don, SFedU, 2015, pp. 183.
11. Deundyak V. M., Kosolapov Y. V. Cryptosystem Based on Induced Group Codes. *Modelirovanie i analiz informatsionnykh sistem*, 2016, no. 23(2), pp. 137–152. Available at: https://doi.org/10.18255/1818-1015-2016-2-137-152 (accessed 06 May 2018) (In Russian).
12. Deundyak V. M., Taran A. A. On the Hamming Codes Application in the Key Distribution System for Conferencing in a Multi-user Communication Systems. *Vestnik VGU. Seriya: Sistemnyj analiz i informacionnye tekhnologii*, 2015, no. 3, pp. 43–50. issn1995-5499 (In Russian).
13. Shcheglov K. A., Shcheglov A. Yu. New Approach to Data Securing in Information System. *Izvestiya vysshikh uchebnykh zavedeniy. Priborostroenie*, 2015, vol. 58, no. 3, pp. 157–166 (In Russian). doi:10.17586/0021-3454-2015-58-3-157-166/issn0021-3454
14. Shan'gin V. F. *Zashchita informacii v komp'yuternyh sistemah i setyah* [Information Security in Computer Systems and Networks]. Moscow, DMK Publ., 2012. 592 p. (In Russian).
15. Schneier B. *Applied Cryptography. Protocols, Algorthms and Source Code in C*. New York, John Wiley & Sons, 2015. 784 p.

16. 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, pp. 21–26 (In Russian).
17. Ostroumov O. A., Sinyuk A. D. Protocol of Open Formation of a Tripartite Key. *Naukoemkie tekhnologii v kosmicheskikh issledovaniyakh Zemli* [High Tech in Earth Space Research], 2014, no. 2(82), pp. 48–52 (In Russian).
18. 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).
19. Shtanko S. V., Lesniak D. A. Providing Selective Access for Broadcasting Information Transfer. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2016, no. 1, pp. 74–79 (In Russian). doi:10.15217/issn1684-8853.2016.1.74
20. Osipov D. S., Frolov A. A., Zyablov V. V. Multiple Access System for a Vector Disjunctive Channel. *Problems of Information Transmission*, 2012, vol. 48, no. 3, pp. 243–249.
21. Frolov A. A., Zyablov V. V. A New Coding Method for a Multiple-Access System with a Large Number of Active users. *Proc. IEEE Information Theory Workshop (ITW)*, 2015, April 26–May 1, Jerusalem, Israel, 2015, pp. 1–5.
22. Anisimov D. V., Dmitriev S. V. Managing Access to the Transmission Medium in Wireless Networks IEEE 802.11 Standard Taking into Account the Unsaturated State of the Channel. *Informatsionnye sistemy i tekhnologii* [Information Systems and Technologies], 2018, no. 4(108), pp. 99–107 (In Russian). issn2072-8964
23. Maltsev G. N., Pankratov A. V., Lesniak D. A. Probabilistic Characteristics of Information System Security Changes under Unauthorized Access. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2015, no. 1, pp. 50–59 (In Russian). doi:10.15217/issn1684-8853.2015.1.50
24. Gentry C., Waters B. Adaptive Security in Broadcast Encryption Systems. *Advances in Cryptology — EUROCRYPT 2009*, Springer, 2009, pp. 171–188.
25. Blundo C., Mattos L. A. F., Stinson D. R. Trade-offs between Communication and Storage in Unconditionally Secure Schemes for Broadcast Encryption and Interactive Key Distribution. *Advances in Cryptology, LNCS*, 1996, vol. 1109, pp. 387–400.