DOI 10.36622/1682-7813.2025.28.1.013
УДК 003.26:681.3

РЕАЛИЗАЦИЯ РАСПРЕДЕЛЕННОГО МОНИТОРА БЕЗОПАСНОСТИ МЕДИЦИНСКИХ ИНФОРМАЦИОННЫХ СИСТЕМ КРИПТОГРАФИЧЕСКИМ МЕТОДОМ СЕМАНТИЧЕСКОГО ШИФРОВАНИЯ

В.А. Хвостов, Г.В. Сыч, В.П. Гулов, О.Н. Чопоров

Построение сетевых мониторов безопасности, реализующих единую политику распределения прав доступа в территориально распределенных медицинских информационных системах (МИС), в настоящее время не имеет нормативного решения. Традиционные модели управления доступом (дискреционная, мандатная и др.) существенно ресурсоемки при организации работы большого количества пользователей, что характерно для МИС. В этих условиях необходимости предоставления доступа большому количеству пользователей, внешних по отношению к информационной системе, предложена онтологическая модель управления доступом. В качестве критерия предоставления доступа, формирующего основную теорему безопасности, используются меры семантической близости запроса пользователя и рубрики тематического классификатора информационного ресурса. В качестве монитора безопасности распределенной онтологической модели управления доступом предлагается использовать криптографическую схему семантического шифрования. Предложенная криптографическая схема является вариацией ассиметричных алгоритмов на основе эллиптических кривых и реализует фасетный подход к построению иерархического информационного ресурса.

Ключевые слова: монитор безопасности, онтологическая модель, семантический критерий, фасетный подход.

Введение

Одной из наиболее важных функций, реализуемых системами защиты информации (СЗИ), является управление доступом. Назначением этой функции является реализация установленной политики доступа пользователей к конфиденциальным данным и защита от угроз безопасности информации (БИ), исходящих от источников – пользователей, зарегистрированных в системе, но имеющих ограничения. В качестве ограничений на доступ к конфиденциальной информации для этой категории пользователей определяются:цели и назначение обработки, уровень конфиденциальности информации, конкретные разрешенные функции (чтение,запись, выполнение отдельных команд), ограничения во времени и др. Управление доступом производитсяна основе законодательных требований, в нормативном плане регулируется стандартами, являясь основой ядра безопасности для подавляющего большинства средств защиты информации в информационных системах.

Одним из классов информационных систем, где особо остро стоит вопрос управления доступом пользователей к конфиденциальным данным, являются медицинские информационные системы (МИС), которые в рамках создания Единой государственной информационной системы в сфере здравоохранения (ЕГИСЗ) внедрены в деятельность всех медицинских организаций (МО). Основную долю конфиденциальных данных, хранящихся и обрабатываемых в МИС составляют персональных данные пациентов, относящиеся к классу специальных персональных данных и требующих повышенного уровня защиты. Следует отметить, что доступ пользователей МИС к конфиденциальным данным зависит от уровня решаемых задач. На уровне лечащего врача и среднего медицинского персонала – это доступ к персональным данным пациентов, данным о жалобах и анамнезе пациента, данным лабораторных и диагностических исследований, о лечении, к электронной медицинской карте пациента. На уровне заведующего отделением – это электронные истории болезни пациентов, информация о результатах деятельности

отдельных врачей, информация о движении больных и состоянии коечного фонда. На уровне главного врача медицинской организации – информация о деятельности медицинского персонала и отдельных структурных подразделений организации, сводные аналитические и статистические отчеты. На региональном уровне – информация о заболеваемости, деятельности и ресурсном обеспечения медицинских организаций региона. На федеральном уровне – вся совокупность информации, включая аналитическую и статистическую информацию на федеральном уровне. То есть, пользователи медицинских информационных систем в рамках ЕГИСЗ имеют доступ к иерархически структурированной информации с учетом их функционала и решаемых задач.

Нормативные документы и стандарты по защите информации в основном требуют применения дискреционных, мандатных, ролевых и тематически-иерархических моделей управления доступа. Перечисленные модели управления доступом разработаны в 70-х 80-х годах прошлого века и в основном ориентированы на применение в локальных средствах вычислительной техники (СВТ). Все проблемы взаимного доверия отдельных СВТ (кластеров СВТ), реализующих распределенные модели обработки данных, решаются подсистемой идентификации и аутентификации. При этом, в расчет не берется иерархия уровней доверия к результатам идентификации и аутентификации, сформированная стандартами. В результате при распределенной обработке информации, что характерно для медицинских информационных систем, невозможно реализовать единую общесистемную политику безопасности и требуется найти подходы к формированию распределенного монитора безопасности. Основной функцией распределенного монитора безопасности будет решение проблемы доверия верхнего уровня. Доверительные отношения между сегментами системы формируют политики удаленных доступов сегментов относительно друг друга. При этом требуется решение внутрисистемной проблемы доверия. Доверительные отношения между двумя сегментами системы $Л1$ и $Л2$ определяются не подсистемой идентификации и аутентификации, а в виде элемента доверия распределенного монитора безопасности. Элементы доверия выступают как основа для формирования доверительных прав субъектов одного сегмента к объектам другого. Перспективным для распределенных мониторов безопасности авторам статьи видится логическое иерархическое построение модели информационного ресурса как вложение одного локального сегмента в другой локальный сегмент. Обособленная совокупность субъектов и объектов нижнего уровня иерархии должна являться подмножеством совокупности субъектов и объектов верхнего уровня иерархии. При этом возникает проблема неравноправных отношений взаимного доверия локальных сегментов и требование регламентации доверительных отношений субъектов верхнего уровня иерархии к объектам нижнего уровня иерархии, не решаемые подсистемой идентификации и аутентификации сегмента нижнего уровня иерархии.

Решение этой проблемы видится в использовании онтологической модели управления доступом, предложенной авторами [1]. Представленная модель построена в виде иерархической структуры, а для формирования доверительных прав на доступ используется семантический критерий. При этом, в качестве ядра распределенной СЗИ требуется использование специализированного криптографического алгоритма, позволяющего реализовывать взаимную аутентификацию и обеспечивать конфиденциальность информационного обмена.

Использование распределенного монитора безопасности, а также решение проблемы безопасного вложения подмножеств локальных низкоуровневых прав на доступ в высокоуровневые сегменты системы и решение проблемы неравноправных отношений взаимного доверия локальных сегментов рассмотрены в ряде работ [1-3]. В основе построения

распределенных мониторов безопасности предлагаются иерархические методы шифрования на основе идентификации Hierarchica lIdentity Based Encryption (HIBE). Эти методы шифрования являются одной из разновидностей ассиметричных криптоалгоритмов на основе эллиптических кривых. Однако структура онтологической распределенной модели управления доступом не может использовать HIBE непосредственно без доработки под особенности модели управления доступом. С учетом необходимости в ассиметричных алгоритмах использовать данные семантики запроса, а не идентификационных данных, базовый алгоритм построения распределенного монитора безопасности можно назвать семантическим алгоритмом шифрования (Semantic Based Encryption (SBE)).

Таким образом, статья посвящена совершенствованию онтологической модели управления доступом, представленной в [1], в интересах обеспечении возможности построения распределенных мониторов безопасности и проведению анализа использования для этой цели ассиметричных алгоритмов шифрования.

Анализ проблемы обеспечения безопасности в распределенных информационных системах

Как объект, на котором требуется решение проблемы обеспечения информационной безопасности, распределенные информационные системы требуют проведения анализа по трем следующим направлениям.

1. Модульный принцип реализации программных комплексов. В том числе модульный принцип реализации мониторов безопасности позволяющий отдельный функционал монитора безопасности реализовывать в различных модулях.

2. Распределенная структура информационного объекта, ассоциированного с монитором безопасности, содержащего правила формирования прав на доступ субъектов, ролей, атрибутов и т.п.

3. Особенности реализации современных информационных систем в виде распределенных.

Сопряжение основных процессов, реализуемых монитором безопасности (управление памятью, инициализация ассоциированных с пользователем субъектов, применение прав на доступ к объектам, регистрация и учет, идентификация и аутентификация) является проблематичной при использовании модульного принципа его построения.

Ассоциированные с монитором безопасности объект (информация о разграничении доступа) должны отражать как логическую, так и физическую распределенность информационной системы. Как пример, распределенная дискреционная модель управления доступом является совокупностью локальных списков доступов с уровнями доверия к аутентификации.

Распределенный принцип реализаций информационной системы приводит к определяет физическую распределенность ассоциированных с монитором безопасности объектов. Проблему организации единой политики управления доступом в этом случае реализовать достаточно трудно. В рассмотрение приходится брать подсистему идентификации и аутентификации и учитывать достигаемый этой системой уровень доверия.

Основные положения онтологической модели разграничения доступа

Онтологическая модель разграничения доступа в МИС предложена в работе [1]. Предполагается, что защищаемый ресурс сформирован в виде иерархического тематического классификатора (рубрикатора), состоящего изконечногомножестваразнообразных тематических рубрик $T_{\text{и}} = \{t_1, t_2, \ldots t_M\}$. В рамках такой структурыклассификаторадолжна быть отражена вся информационная структура используемой медицинской информационной системы.

Структура доверительных правдля всех субъектов доступа к информационным ресурсам формализована в виде корневого дерева, позволяющегочастично упорядочить

их права.

В рамках представленной модели множество объектов (O) и субъектов (S)медицинской информационной системы ($S \cup O$) формализуется в рамках структуры корневого дерева иерархического рубрикатораT^{M}. С целью обеспечения возможности идентификации прав доступа применительно к каждому объекту и субъекту в рамках медицинской информационной системы в мультирубрику, которая соответствует объекту, для каждого момента времени добавляется функция тематического окрашивания f_M.Данная функция включается в структуру мультирубрицированного отображения объектов и субъектов на иерархический классификатор$F_{и2}$[x]и формализуетсяв следующем виде:

$$f_M[\mathrm{x}] = t^M, \quad (1)$$

где $\mathrm{x} \in S \cup O$, $t_i^M \in T^M$.

Такая модель разграничения доступа учитывается в процессе описания переходов системы из состояний в различные моменты времени τ_kиτ_{k+1}.

В процессе работы подсистемы разграничения доступом появляются новые информационные потоки (отношения доступа), которые возникают между имеющимися сущностями медицинской информационной системы$X = S \cup O$. Это, в свою очередь, приводит к появлению новых объектов и субъектов доступа.

В качестве одного из ключевых моментов в работе подсистемы разграничения доступом следует выделить принятие решения оправомочности доступа пользователей (ассоциированных с пользователем объектов) к объектам доступа. Принятые решения должны обеспечить транзитивность информационных потоков безопасных по определенному критерию.

Установленными политиками безопасности определяется формирование доверительно-тематических полномочий пользователей

$$F_{\mathrm{LTH}}(s) = \{L_S, T_S^M\}.$$

Таким образом, вводятся отношения порядка и тематический классификатор дополняется наложенной решеткой безопасности [4].

При использовании онтологического принципа разграничения доступом для назначения доверительных прав назначаются учитывается семантическая близостьтематической рубрике классификатора к запросу пользователя [1].

Для формализованного представления близости онтологических термов по семантическому критерию используется функцией вида:

$$S(x, y) \in [1,0], \quad (2)$$

где $x, y -$ онтологические термы.

В качестве меры близости в процессе формализации доверительных прав доступа используется длина кратчайшего пути между тематической рубрикой рубрикатора информационного ресурса медицинской информационной системы и таксономией запроса, которая рассчитывается как количество вершин (ребер) между вершинами графа, формализующего структуру иерархического ресурса [1]:

$$S(c_1, c_2) = \log \frac{2N}{d(c_1, c_2)}, \quad (3)$$

где N – глубина дерева тематического рубрикатора информационного ресурса;

c_1 и c_2 – таксономия запроса пользователя и тематической рубрики (соответственно);

$d(c_1, c_2)$ – метрика, определяющая длину кратчайшего пути между вершинами графа, соответствующего структуре иерархического ресурса.

На рис. 1 представлено описание правил формализации прав доступа к иерархическим информационным ресурсам в рамках предложенной модели [1].

Построение распределенного монитора безопасности онтологической модели разграничения доступа.

Сетевой монитор безопасности выполняет роль специального системного субъекта, реализующего единую

(согласованную) политику управления в сети. Сетевая политика управления доступом имеет смысловое содержание внешней политики системы безопасности.

Теоретические подходы к созданию сетевого монитора безопасности предложены в ряде работ [5, 6]. При этом рассматриваются исключительно дискреционная, мандатная и ролевая модели управления доступа. Сетевые мониторы безопасности, реализующие распределенную онтологическую MLTHS модель не предложены.

Естественным путем реализации сетевого монитора безопасности при реализации MLTHS модели является иерархического шифрование на основе идентификации (HIBE).

Иерархическое шифрование является одним из вариантов асимметричных криптоалгоритмов, основанных на эллиптических кривых. Как представлено в исследовании [7], теоретическая стойкость таких алгоритмов определяется вычислительной сложностью дискретного логарифмирования на эллиптической кривой.

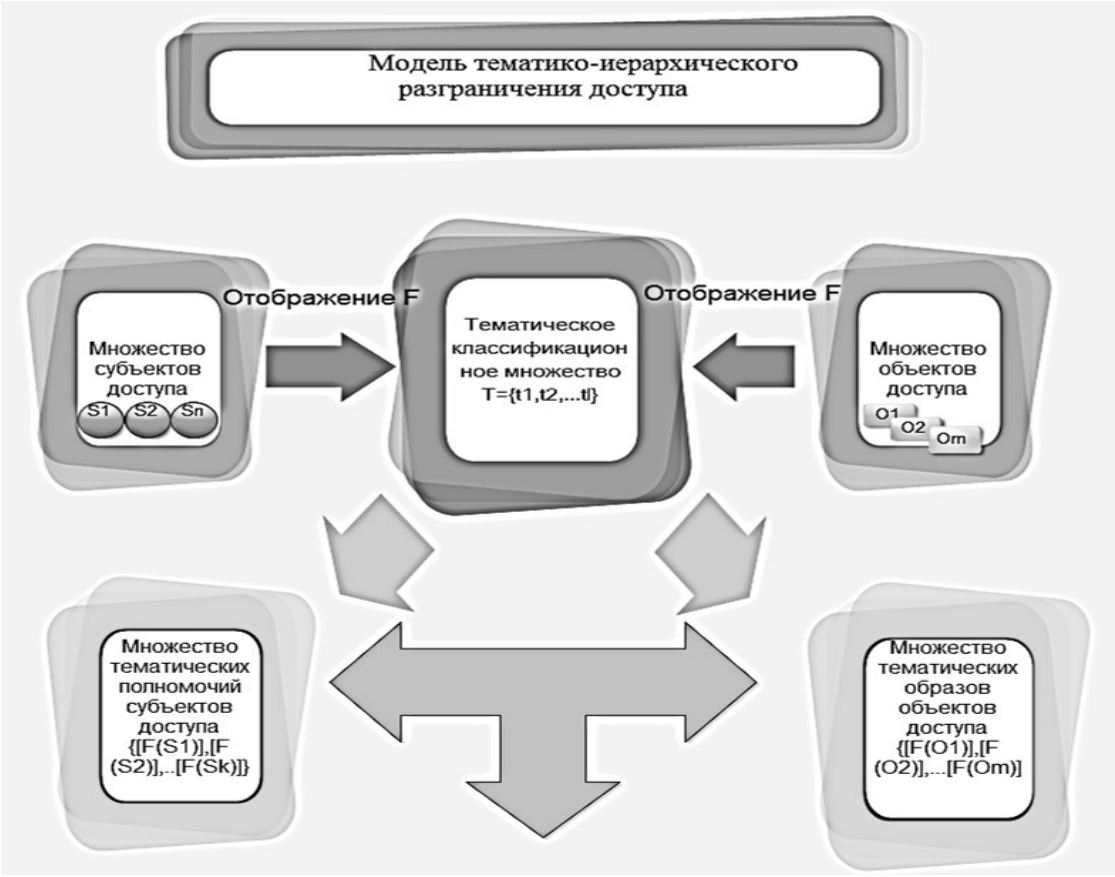

Рис. 1. Тематически иерархическая модель управления доступом

В настоящее время получили широкое распространение криптографические алгоритмы, основанные на использовании билинейных групп [8]. На базе этих алгоритмов шифрования предлагается схема семантического шифрования для реализации онтологической MLTHS модели управления доступом (Semantic Based Encryption (SBE) system).

В криптосистеме SBE на основе таксономии запроса пользователя к информационному ресурсу (3) множество закрытых ключей генерируется доверенным центром. Закрытый ключ запроса генерируется на основе самого содержания запроса пользователя. При формировании запроса пользователь шифрует запрос с использованием открытого ключа и информации, содержащейся в запросе (семантическое содержание запроса пользователя). При расшифровке полученных данных проводится проверка

соответствия таксономии, запроса которые составляют закрытые ключи пользователя и параметра семантического критерия (3) онтологической модели управления доступа. Если семантическое расстояние, рассчитанное по критерию (3), меньше значения критерия то данные корректно расшифровываются. Решение задачи шифрования n запросов к T^M мультирубрикам иерархического классификатора требуют применения мультилинейных алгоритмов SBE.

Мультилинейный алгоритм SBE

По аналогии с мультилинейными алгоритмами HIBE, при применении семантического шифрования используются следующие криптографические примитивы: инициализация, получения закрытого ключа запроса, шифрация и дешифрация.

Для процедуры инициализации вводится параметр стойкости реализуемого алгоритма $k \in Z$.

Инициализация запроса пользователя

Доверенный центр (монитор безопасности) иерархического ресурса, используя параметр k генерирует группы G_1 и G_2, имеющие простой порядок q и мультилинейное отображение $\mu: G_1 \times G_1 \times \ldots G_1 \to G_2$, а также произвольный образующий элемент группы $P \in G_1$.

G_1 представляет собой аддитивную циклическую, а G_2 – мультипликативную циклическую группу.

На следующем этапе монитором безопасности осуществляется выбор случайных элементов $s_1, s_2, \ldots s_n \in Z_q$, а также определяется набор открытых ключей запроса

$$P_{\text{pab1}} = s_1 P, P_{\text{pab2}} = s_2 P, \ldots, P_{\text{pabn}} = s_n P.$$

Множества сообщений и шифротекстовSBE представляют собой множества $\vartheta = \{0,1\}^l$ и $c = G_t\{0,1\}^l$ соответственно. Мастер ключи абонентов формируются как $s_1, s_2, \ldots s_n \in Z_q$. В качестве системных параметров выступают $\langle G, G_2, \mu, l, P, P_{\text{pabi}}, H_1, H_2 \rangle$.

Криптографический алгоритм системы защиты информации, реализующий распределенный онтологический принцип управления доступом, должен использовать семантику запроса к иерархическому информационному ресурсу вместе с набором разрешенных действий с этим ресурсом. В отличии от идентификационного шифрования, семантика запроса определяет множество разрешенных действий для различных мультирубрик иерархического ресурса. При этом аутентификация пользователя может осуществляться средствами аутентификационного обмена, по паролю или токену доступа. Механизмы аутентификации пользователя могут быть не связаны с управлением доступом. Тогда подсистема управления доступом обеспечит для любого пользователя набор мультирубрик T^M с набором возможных действий. Центром ядра системы защиты становится функция отображения семантического критерия доступа на множество закрытых ключей вида:

$$\Xi_{S(c_1,c_2)}: S_{\text{kr}}(c_1, c_2) \to d_{c21}, d_{c22} \ldots d_{c2i}$$

где d_{c2i} – закрытые ключи тематических рубрик $c_{21}, c_{22}, \ldots c_{2i}$, доступ к которым разрешается доступ запросу c_1 в соответствии с критерием онтологической модели управления доступом,

i – количество рубрик классификатора доступных для запроса c_1 в соответствии с правилами (2) и (3).

Универсальная семантика запроса используется для всех ресурсов. Такая ситуация дает возможность реализации единой политики управления доступом наразных серверах или машинах или сегментах информационной системы, содержащих отдельные мультирубрики ресурса.

На этапе генерации закрытых ключей запроса схемой SBE вычисляются $Q1_{c1} = H_1(c_1) \in G_1$, $Q2_{c1} = H_2(c_1) \in G_1 \ldots \mathrm{QI}_{c1} = H_i(c_1) \in G_1$

Центром PKG вычисляются и передаются абонентам по защищенному каналу закрытые ключи запроса:

$$d_{c21} = s_1 c_{21}, \ldots d_{c2i} = s_1 c_{2i}, (3)$$

где $s_1, s_2, \ldots s_n$ – мастер-ключи запроса.

Формирование запроса

На этапе шифрования сообщения информации M в соответствии с параметрами запроса $c_1 \in \{0,1\}$сторона, производящая запрос к защищенному ресурсу, выполняет следующие вычисления.

Вычисляется $Q1_{c1} = H_1(c_1) \in G_1$.

Выбирается случайный элемент $r \in Z_q$.

Вычисляется шифротекст:

$$\mathrm{c}_1 = \langle \mathrm{rP}, M \otimes H_2(g^r) \rangle,$$

где $g = \mu(Q1_{c1}, P_{\mathrm{pabc1}}) \in G_2$.

Обработка ответа от защищенного ресурса

При расшифровании $\mathrm{c}_{21}, \mathrm{c}_{22}, \ldots \mathrm{c}_{2i}$, полученных на запрос c_1 с помощью закрытых ключей запроса $d_{c21}, \mathrm{ds}c_{22} \ldots d_{c2i} \in G_1$ вычисляется открытый текст:

$$M = V \oplus H_2(\mu(Q1_{c1}, Q2_{c1}, \ldots \mathrm{QI}_{c1}, c_1, U, P_{\mathrm{pabC1}}, d_{c21}, \ldots d_{c2i})).$$

Реализация распределенного монитора безопасности методами SBE при использовании онтологической модели управления доступом в иерархическом информационном ресурсе МИС

Определяющее значение МИС, построенных рамках ЕГИСЗ, имеет понятие тематического классификатора в тематической классификационной системе. В настоящее время при построении распределенных мониторов безопасности можно рассмотреть следующие виды тематической классификации.

Перечислительная классификация, использующая дескрипторный подход. Данный вид классификации приводит к построению неупорядоченных классификационных схем. В классификационных схемах перечислительной классификации невозможно построить отношения старшинства, ассоциативности и частичного упорядочивания между рубриками. Тематики и рубрики при перечислительной классификации имеет произвольный характер. Пользователь имеет права работы документами для определенного набора тематических рубрик. Таким образом, для пользователей фактически так же, как и документов в произвольном порядке требуется назначать тематические рубрики. Монитор безопасности при этом должен содержать данные о всех тройках элементов безопасности субъект – объект – права доступа. Таким образом, преимущества MLTHS модель перед дискреционными моделями полностью теряются.

Иерархическая классификация

Распределенный монитор безопасности должен содержать только значения права пользователя и значения классификатора. В контексте SBE шифрования определяемых парами ключей (3). Возможность наследования право работы на документы с тематикой соответствующих подчиненных узлов приводит к снижению количества требуемых ключей. Таким образом, иерархическая классификация приемлема при построении распределенных мониторов безопасности методами SBE шифрования.

Фасетная классификация. При фасетной классификации информационный ресурс МИС формируется как блоки-фасеты. Совокупность блоков фасетов формирует логику предметной области. Каждый фасет представляет собой классификационный признак тематики (рубрики) и имеет иерархический тип.

Тематика информационного объекта конкретной предметной области включает комбинацию наборов тематических узлов для множеств фасетных рубрик. Сочетание определенных рубрик по фасетам классификатора определяет права доступа пользователя к информационному ресурсу.

Фасетная классификация наиболее приемлема при построении распределенных мониторов безопасности криптографическими методами. Данный вид классификации естественным образом формирует наборы классификационных рубрик, позволяет диверсифицировать набор доступов к разным фасетам одним набором ключей запроса. Эти особенности построения иерархических классификаторов

делают использование фасетных классификаторов наиболее приемлемыми для реализации распределенных мониторов безопасности методами **семантического шифрования**.

Функционирование схемы шифрования SBE, реализующей распределенный монитор безопасности иерархического информационного ресурса представлена на рис. 2.

Таким образом, общее правило онтологической модели управления доступом [1], формируется доверенным центром криптосистемы на основе семантического критерия доступа $S_{\text{kr}}(c_1, c_2)$ посредством предоставления закрытых ключей расшифрования ответа d_{c21},dsc_{22}...$d_{c2i} \in G_1$ иерархического ресурса на запрос пользователя.

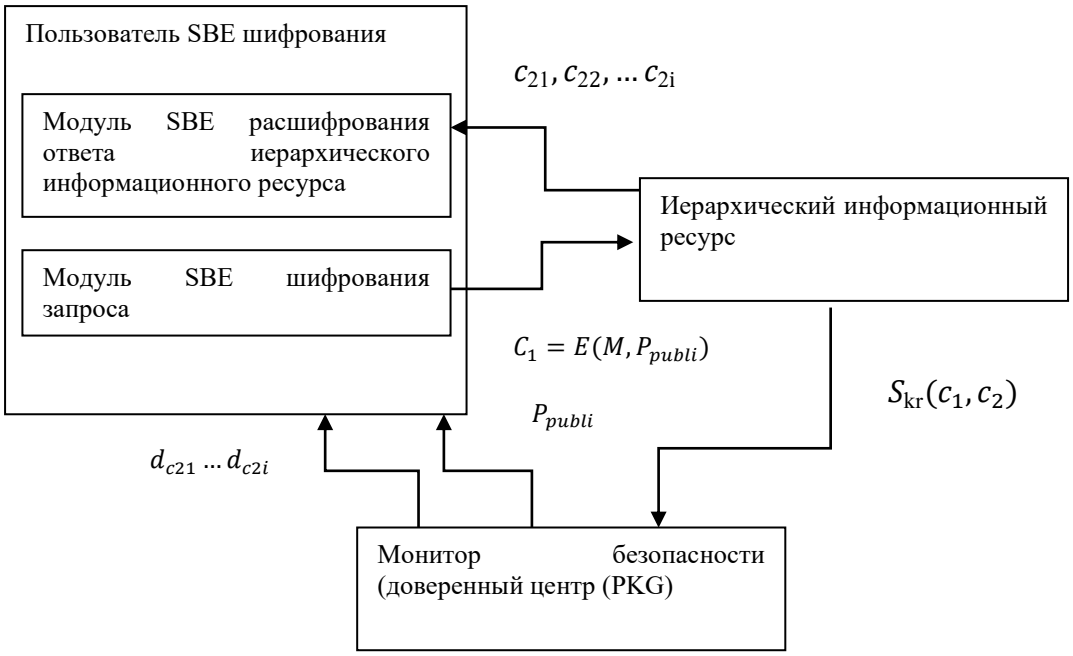

Рис. 2. Схема шифрования SBE, реализующая распределенный монитор безопасности иерархического информационного ресурса

Заключение

В статье предложен метод реализации распределенных мониторов безопасности, реализующих онтологическую модель управления доступом в МИС которые внедрены в деятельность всех медицинских организаций в рамках создания Единой государственной информационной системы в сфере здравоохранения. В качестве ядра СЗИ с распределенным монитором безопасности предложено использовать ассиметричную криптографическую схему основанные на использовании билинейных групп. Для адаптации предложенной схемы с учетом логики онтологической модели управления доступом ассиметричный алгоритм шифрования предложено модернизировать в части генерации и использования пар ключей. Для существующих алгоритмов идентификационного шифрования Hierarchical Identity Based Encryption, предложено заменить идентификационные данные содержанием семантики запроса пользователя к иерархическому ресурсу. При этом, полученная ассиметричная схема шифрования названа семантической схемой шифрования Semantic Based Encryption system.

Стойкость к криптоанализу SBE шифрования определяется сложностью решения задачи дискретного логарифмирования в группе точек эллиптической кривой.

Проведенный в статье анализ подходов к формированию иерархических классификаторов позволил в качестве наиболее приемлемого, выбрать фасетный

подход. Данный подход позволяет получить наиболее гибкий распределенный монитор безопасности, обеспечить минимизацию использования пар ключей и, соответственно, снижения требований к производительности ЭВМ для развертывания онтологической модели управления доступа.

Дальнейшим направлением совершенствования криптографических методов формирования мониторов безопасности видится в проведении анализа возможности их применения при построении традиционных моделей управления доступа (дискреционной, полномочной, ролевой). Применение криптографических методов построения мониторов безопасности, не только определяют возможность построения распределенных мониторов, но и помогут решить ряд практических проблем возникающих при практической реализации мониторов безопасности. Таких как изоляция модулей СЗИ, сопоставления пользователя с устройством, защита вывода конфиденциальной информации на отчуждаемый носитель.

Еще одной актуальной средой медицинского применения предлагаемого инструментария следует считать нейросетевую диагностику, где управление доступом должно быть особенно тщательным. Внешние и внутренние угрозы, присутствующие в данном случае, могут привести к фатальным последствиям для пациентов. Вторжение в средства машинного обучения нейросети способно привести к трагическим ошибкам в ходе лечения целого множества клиентов системы. В этом контексте уместно использовать базу MITRE-ATLAS и усилить контроль за доступом на различных уровнях применения медицинской автоматизированной системы диагностики, что представляется возможным и с использованием предлагаемого в настоящей статье инструментария. При этом надо понимать, что арсенал средств вторжения довольно развит и совершенствуется в реальном масштабе времени. Это требует дальнейших шагов по модернизации методического и программного обеспечения данной разработки в темпе экспансии искусственного интеллекта как в системах обработки медицинских данных, так и подсистемах их защиты, а также, конечно, в средствах реализации кибератак.

Список литературы

1. Организация управления доступом к медицинским информационным системам с использованием методов семантической близости / В. П. Гулов, В. П. Косолапов, Г. В. Сыч, В. А. Хвостов // Системный анализ и управление в биомедицинских системах. 2021. Т. 20, № 2. С. 79-87.

2. S.G. Akl and P.D. Taylor. Cryptographic Solution to a Multi Level Security Problem. InAdvancesinCryptology – CRYPTO, 1982.

3. R. Blom. An optimal class of symmetric key generation systems, in Advances in Cryptology — Eurocrypt ’84, Lecture Notes in Computer Science 209 (1984), Springer. P. 335–338.

4. D. Boneh, B. Lynn, and H. Shacham. Short signatures from the Weil pairing, in Advances in Cryptology — Asiacrypt 2001, Lecture Notes in Computer Science 2248 (2001), Springer. P. 514–532.

5. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками / П.Н. Девянин, 3-е. М.: Горячая Линия – Телеком, 2020. 352 с.

6. Menezes A. J., van Oorschot P. C., and Vanstone S. A. Handbook of Applied Cryptography. CRC Press, 1996. 816 p.

7. Shamir A. Identity-based cryptosystems and signature schemes // Workshop on the theory and application of cryptographic techniques. Springer, Berlin, Heidelberg, 1984. С. 47–53.

8. Joux. A one round protocol for tripartite Diffie-Hellman. In W. Bosma, editor, Proceedings of Algorithmic Number Theory Symposium IV, volume 1838 of LNCS. P. 385–394. Springer, 2000.

Воронежский государственный университет инженерных технологий
Voronezh State University of Engineering Technologies

Воронежский государственный медицинский университет им. Н.Н. Бурденко
Voronezh State Medical University N.N. Burdenko

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 20.02.25

Информация об авторах

Хвостов Виктор Анатольевич– канд. техн. наук, доцент кафедры информационной безопасности, Воронежский государственный университет инженерных технологий, e-mail: hvahva1@mail.ru

Сыч Галина Владимировна –канд. матем. наук, доцент, доцент кафедры управления в здравоохранении, Воронежский государственный медицинский университет имени Н.Н. Бурденко, e-mail: sichgala@gmail.com

Гулов Владимир Павлович– д-р биол .наук, профессор, профессор кафедры управления в здравоохранении, Воронежский государственный медицинский университет имени Н.Н. Бурденко, e-mail: voldemar1908@mail.ru

Чопоров Олег Николаевич– д-р техн. наук, профессор, проректор по цифровой трансформации, Воронежский государственный университет им. Н.Н. Бурденко; профессор, Воронежский государственный технический университет, e-mail: choporov_oleg@mail.ru

IMPLEMENTATION OF A DISTRIBUTED SECURITY MOGITOR FOR MEDICAL INFORMATION SYSTEMS BY THE CRYPTOGRAPHIC METHOD OFSEMANTIC ENCRYPTION

V.A. Khvostov, G.V. Sych, V.P. Gulov, O.N. Choporov

Construction of network security monitors implementing a unified policy for distributing access rights in geographically distributed medical information systems (MIS) currently has no regulatory solution.Traditional access control models (discretionary, mandatory, etc.) are significantly resource-intensive when organizing the work of a large number of users, which is typical for MIS.In these conditions of the need to provide access to a large number of users external to the information system, an ontological access control model is proposed.The measures of semantic proximity of the user's request and the heading of the subject classifier of the information resource are used as an access granting criterion that forms the main security theorem.It is proposed to use a cryptographic scheme of semantic encryption as a security monitor for a distributed ontological access control model.The proposed cryptographic scheme is a variation of asymmetric algorithms based on elliptic curves and implements a faceted approach to constructing a hierarchical information resource.

Keywords: security monitor, ontological model, semantic criterion, faceted approach.

Submitted 20.02.25

Information about the authors

Victor A.Khvostov – Cand. Sc. (Technical), Associate Professor of the Department of Information Security, Voronezh State University of Engineering Technologies, e-mail: hvahva1@mail.ru

Galina V. Sych – Cand. Sc. (Medical), Associate Professor of the Department management in healthcare, Voronezh State Medical University named after N.N. Burdenko, e-mail: sichgala@gmail.com

Vladimir P. Gulov – Dr. Sc. (Biological), Professor, Professor of the Department management in healthcare, Voronezh State Medical University named after N.N. Burdenko, e-mail: voldemar1908@mail.ru

Oleg N. Choporov – Dr. Sc. (Technical), Professor, Vice-Principial for Digital Transformation, Voronezh State Medical University named after N.N. Burdenko; Professor, Voronezh State Technical University, e-mail: choporov_oleg@mail.ru