УДК 330.1:332.1:614.8:658.5

МОДЕЛИ И МЕТОДЫ ПОСТРОЕНИЯ ЭФФЕКТИВНЫХ МЕХАНИЗМОВ ЗАЩИТЫ СТРУКТУР ПАТЕНТНЫХ БАЗ ДАННЫХ

В.О. Сиротюк

Рассмотрены особенности формирования и характеристики патентных баз данных. Приведена классификация патентной информации. Выявлены угрозы информационной безопасности патентной информации и пути ее утечки в патентном ведомстве. Введено формализованное определение механизма защиты патентной базы данных и предложены модели и методы построения оптимальных механизмов защиты структур патентных баз данных патентно-информационного фонда на разных уровнях их представления — концептуальном, логическом и физическом. Полученные результаты использованы при построении системы управления информационной безопасностью Евразийского патентного ведомства.

Ключевые слова: патентная информация, классы патентной информации, патентная база данных, патентный информационный фонд, информационная безопасность, методы защиты, механизмы защиты.

ВВЕДЕНИЕ

В условиях возрастающих рисков и угроз информационной безопасности патентных ведомств, направленных на взлом систем защиты патентной информации, ее раскрытие, подмену, модификацию и искажение, обеспечение информационной безопасности и защиты патентно-информационных ресурсов, информационной и обеспечивающей инфраструктуры патентных ведомств является важной и актуальной задачей. Ее решение позволит ведомствам обеспечить конфиденциальность, достоверность, доступность и сохранность патентной информации, предотвратить раскрытие формулы и описания изобретения до проведения патентной экспертизы и публикации заявки на изобретение, а также повысить надежность функционирования систем и средств сбора, хранения, обработки, передачи и отображения патентной информации [1—5].

1. ОСОБЕННОСТИ ФОРМИРОВАНИЯ И ХАРАКТЕРИСТИКИ ПАТЕНТНЫХ БАЗ ДАННЫХ (ПБД)

Патентные базы данных патентно-информационного фонда (ПИФ) содержат информацию о патентных документах (заявках и патентах на изобретения, полезных моделях и промышленных образцах), непатентной литературе и патентно-ассоциированной документации и предназначены для обеспечения специалистов патентных ведомств полной и качественной информацией об объектах интеллектуальной собственности, о последних достижениях науки и практики в рассматриваемых предметных областях заявок на изобретения, а также об актуальной патентной нормативно-правовой и справочной документации. Информационное обеспечение работы экспертов патентного ведомства реализуется путем предоставления им доступа к соответствующим ПБД. При проведении экспертизы должна использоваться патентная документация стран, входящих в минимум документации согласно Договору о патентной кооперации (PCT — Patent Cooperation Treaty), рекомендуемая по списку Всемирной организации интеллектуальной собственности непатентная литература и патентно-ассоциированная документация [1, 6].

Основные показатели качества ПБД: полнота, достоверность, актуальность, глубина ретроспективы данных, время загрузки информации в ПБД

и обслуживания запросов пользователей патентной информации.

Информация ПИФ делится на открытую (общедоступную), конфиденциальную и информацию для внутреннего пользования [1, 2].

К открытой относится информация, предназначенная для размещения в СМИ, на веб-сайте ведомства, информация рекламного характера, а также другая информация, которая признается общедоступной в соответствии с национальным законодательством и может быть обнародована. К открытой информации патентного ведомства, в частности, относятся: патентные и библиотечные фонды, официальные издания; БД опубликованной патентной и непатентной документации; информационные ресурсы веб-сайта патентного ведомства; нормативные и правовые документы; справочная и другого рода информация; международные договоры и соглашения; новости и пресс-релизы.

Доступ к этой информации не ограничен, и к ней, в первую очередь, предъявляются требования по обеспечению достоверности и сохранности данных, защиты информации от разрушений и модификации.

К конфиденциальной информации патентного ведомства, как правило, относятся:

— материалы заявок на изобретение (на бумажном носителе и в электронном виде) до их публикации;

— персональные данные служащих патентного ведомства;

— данные бухгалтерской отчетности, информация о заработной плате служащих патентного ведомства;

— архив дел заявок;

— складская документация;

— входящая и исходящая корреспонденция;

— договоры со сторонними организациями;

— информация, разглашение которой запрещено нормативными правовыми документами патентного ведомства.

Требования по защите конфиденциальной информации при ее обработке, передаче, хранении и уничтожении должны соответствовать требованиям национального законодательства.

Доступ к конфиденциальной информации должен регламентироваться соответствующими нормативными правовыми документами ведомства н осуществляться по специальному перечню (разрешению) на основании соответствующих трудовых договоров или соглашений и в объемах, не превышающих минимально необходимых для исполнения данным лицом своих обязанностей (должностных или функциональных).

Для организации доступа к конфиденциальной информации должны применяться средства усиленной двухфакторной аутентификации, а также должны быть реализованы механизмы протоколирования событий, позволяющие однозначно идентифицировать допущенных к этой информации лиц и их действия. Обработка конфиденциальной информации допускается только с применением сертифицированных программно-аппаратных средств, эксплуатация которых разрешена руководством патентного ведомства.

Методы и средства передачи конфиденциальной информации должны обеспечивать ее передачу только адресатам с обязательной идентификацией и подтверждением авторства отправителя и факта получения (например, по электронной почте). При передаче конфиденциальной информации в цифровой (электронной) форме обязательно ее шифрование с помощью криптостойких алгоритмов и ключей шифрования, а при ее передаче на носителях информации необходимо обеспечить безопасность этих носителей при транспортировке.

Конфиденциальная информация должна храниться с применением средств контроля актуальности и достоверности данных. Процессы уничтожения конфиденциальной информации должны обеспечивать невозможность ее последующего восстановления.

К информации для внутреннего пользования должны быть отнесены внутренние организационно-распорядительные документы, нормативно-справочная информация, внешняя и внутренняя служебная переписка, проекты договоров и прочая информация, которая не отнесена к открытой и конфиденциальной.

Методы и средства передачи информации внутри ведомства должны обеспечивать ее передачу только соответствующим адресатам, а также идентифицировать и гарантировать авторство отправителя.

Доступ лиц к информации данного класса при ее обработке, хранении, передаче и уничтожении должен осуществляться на основании трудовых соглашений или договорных отношений в объемах, минимально необходимых для исполнения своих должностных обязанностей допущенным лицом.

2. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ПУТИ УТЕЧКИ ПАТЕНТНОЙ ИНФОРМАЦИИ

Под угрозой информационной безопасности понимается любой объект, событие или лицо, представляющие определенную опасность для информационной системы. Угрозы могут быть умыш-

ленными (прямое хищение, умышленная модификация информации), случайными (ошибки в вычислениях, случайное удаление файла), природными (наводнение, ураган, молния и т. п.) или техногенными (скачки напряжения, пожары, аварии в системах коммунального обеспечения помещений и т. п.) [3, 4].

Анализ особенностей формирования и характеристик ПИФ, классификации патентной информации, требований запросов пользователей ПИФ показал, что основными угрозами информационной безопасности ПБД являются [2]:

— раскрытие конфиденциальной информации (несанкционированный доступ, копирование данных, тиражирование данных, кража информации);

— компрометация информации (внесение несанкционированных изменений в массивы данных и базы данных);

— несанкционированный обмен информацией;

— отказ от информации (непризнание получателем или отправителем фактов получения или отправки информации соответственно);

— отказ в обслуживании (отсутствие доступа к информации).

Принципиально возможными путями утечки информации в патентном ведомстве могут быть:

— прямое хищение носителей информации и документов;

— копирование конфиденциальной информации;

— несанкционированное подключение к персональной рабочей станции (терминалу) пользователей и незаконное использование устройства доступа к информации;

— несанкционированное использование специальных программных средств для доступа к конфиденциальным данным.

Особое значение вопросы обеспечения информационной безопасности патентно-информационных ресурсов приобретают в настоящее время в связи с активным использованием технологий облачных вычислений (cloud computing) при построении систем хранения данных ПИФ. Возникающие при этом дополнительные риски информационной безопасности, связанные с «перемещением» бизнес-процессов, программного и информационного обеспечения в облако, обусловливают необходимость повышения доступности и надежности хранения данных на основе разработки новых моделей безопасности, предполагающих, в частности, делегирование отдельному прокси-серверу полномочий для идентификации, выгрузки, обработки и удаленной проверки достоверности и неизменности данных в облаке, а также проверки, не хранятся ли данные внешнего источника, не загружая при этом все данные [5].

3. МЕТОДЫ, СРЕДСТВА И МЕХАНИЗМЫ ЗАЩИТЫ ПБД

Различают организационные, процедурные, структурные, аппаратные и программные методы и средства защиты информации ПБД [7—9].

Рассмотрим структурные методы защиты.

Структурные методы применяются на этапах анализа и синтеза канонических, логических и физических структур ПБД. Проектируемые при этом механизмы защиты структур ПБД должны обеспечивать такую структуризацию хранимой в ПБД информации, которая позволяла бы разделять данные на общедоступные и конфиденциальные; обеспечивала бы установление разрешенных прав доступа пользователей к данным в соответствии с их полномочиями; защиту структурных элементов ПБД (объектов данных, логических и физических записей) и отношений (взаимосвязей) между ними. Информация о механизмах защиты канонической, логической и физической структур ПБД используется в дальнейшем при построении эффективной системы защиты ПБД и в целом системы управления информационной безопасностью (СУИБ) патентного ведомства.

Механизмы защиты канонической, логической и физической структур ПБД предназначены для обеспечения доступа и допуска к контенту ПБД, только обладающих соответствующими полномочиями пользователей ПИФ. Системы защиты ПБД реализуются путем одного или нескольких методов защиты.

Функционирование механизма защиты ПБД задается матрицей доступа, в которой каждый ее элемент указывает, какое подмножество типов доступа разрешено конкретному пользователю в отношении определенного информационного элемента. Фактически данная матрица устанавливает правила взаимодействия пользователей с патентными информационными ресурсами (активами) посредством информационных технологий.

Механизм защиты структур ПБД позволяет установить правомочность действий пользователей ПБД, предотвратить несанкционированное (умышленное или непреднамеренное) использование и модификацию информации ПБД и прикладного программного обеспечения (ППО).

4. ФОРМАЛИЗОВАННОЕ ОПРЕДЕЛЕНИЕ МЕХАНИЗМА ЗАЩИТЫ ПБД

Обозначим $U = \{u_k / k = \overline{1, K_0}\}$ — множество пользователей БД ПИФ, в качестве которых выступают сотрудники ведомства, заявители и па-

тентообладатели, патентные поверенные и третьи лица; $D = \{d_l | l = \overline{1, L}\}$ — полное безызбыточное множество структурных элементов предметной области (объектов данных и информационных элементов), $D = \bigcup_{k}^{K_0} D_k$, где $D_k = \{d_l | l \in L_k,\ L_k \subseteq L\}$, $DB = \{db_i : i = \overline{1, I_B}\}$ — проектируемая ПБД; $AS = \{as_j : j = \overline{1, J_B}\}$ — ППО, где db_i и as_j — компоненты проектируемой ПБД и ППО соответственно, к которым относятся объекты данных, логические и физические записи, файлы, информационные элементы, процедуры обработки и поиска данных, отношения (взаимосвязи) между элементами, интерфейсные средства, программные модули, утилиты и т. п.

Механизм защиты ПБД можно представить в виде отображения θ: $\{(u_k, db_i, as_j)\} \xrightarrow{\theta} \{0, 1\}$, где «1» соответствует правомочности доступа пользователя $u_k \in U$ к элементам $db_i \in DB$ и/или $as_j \in AS$, а «0» — запрету на такой доступ.

Пусть $A = \{a_j : j = \overline{1, m_q}\}$ — множество типов доступа к информационным ресурсам ПБД (поиска, выборки, модификации (корректировки), копирования, тиражирования, добавления, удаления данных и других операций).

Для каждого объекта данных и информационного элемента предметной области ПИФ указываются степени их секретности $\varphi_i \in \Phi$, где $\Phi = \{\varphi_i : i \in \Phi\}$ — множество степеней секретности структурных элементов ПБД. Степень секретности является важным метаданным структурного элемента, их хранение и ведение осуществляется в базе метаданных репозитария ПБД. Степень секретности устанавливается для каждого элемента в отдельности при подготовке документа СУИБ «Политика информационной безопасности патентного ведомства» экспертным путем на основе анализа степени важности структурного элемента и возможных потерь организации в случае несанкционированного доступа к элементу и/или его искажения (модификации). Для разных экземпляров структурных элементов могут назначаться разные степени секретности. Например, степень секретности экземпляра объекта «Заявка на изобретение» по заявке, находящейся на этапе экспертизы, выше степени секретности экземпляра опубликованной заявки того же объекта данных. То же можно отнести к объекту «Патент» для экземпляров опубликованных и неопубликованных патентов.

Сведения о секретности структурных элементов пользователей представляется матрицами секретности $F_k = \|f_{li}^k\|$, $k = \overline{1, K_0}$, $i \in R$, $l \in L_k \subseteq L$. В данной матрице элемент $f_{li}^k = 1$, если для экземпляров элемента $d_l \in D_k$ k-го пользователя установлена степень секретности $\varphi_i \in \Phi$, и $f_{li}^k = 0$ в противном случае. Матрицы F_k используются для построения обобщенной матрицы секретности структурных элементов предметной области $F = \|f_{li}\|$, также заносимой и хранимой в базе метаданных репозитария ПБД. Матрица F формируется путем объединения матриц F_k по правилу, согласно которому степень секретности $\varphi_i \in \Phi$, присвоенная элементу $d_l \in D_k$, покрывает степень секретности $\varphi_{l'} \in \Phi$, которая установлена для элемента $d_l \in D_k$, если степень секретности φ_i более сильная в смысле ограничений доступа, чем степень секретности $\varphi_{l'}$.

Множество уровней полномочий пользователей ПБД, под которыми понимается право пользователя осуществлять доступ к конфиденциальным данным, обозначим через $\Pi = \{\pi_k : k = \overline{1, K_0}\}$. Уровень полномочий пользователей устанавливается руководством патентного ведомства.

Перечень полномочий k-го пользователя по отношению к данным, хранимым в ПБД в соответствии с их степенью секретности, образует профиль полномочий пользователя k-го пользователя $\Pi_k = \{\pi_{kl} : k = \overline{1, K_0},\ l \in L_k \subseteq L,\ \varphi_l \in \Phi\}$. Профиль полномочий пользователей формально представляется матрицей полномочий $P = \|p_{ki}\|$, элемент которой $p_{ki} = a_j$, если k-й пользователь имеет право выполнять доступ типа a_j к данным ПБД, имеющим степень секретности φ_i и равен нулю в противном случае.

5. МЕТОДЫ ПОСТРОЕНИЯ МЕХАНИЗМА ЗАЩИТЫ КАНОНИЧЕСКОЙ СТРУКТУРЫ ПБД

Каноническая структура ПБД формально представляется в виде орграфа $G_k(D, U)$ и матрицы смежности $W = \|w_{ll'}\|$ [10]. Вершинами графа D служат структурные элементы предметной области ПБД (объекты данных и информационные элементы), а дугами U — взаимосвязи (отношения) между структурными элементами. Степени секретности объектов данных $D^{об} \subseteq D$ зависят от их состава. Степень секретности φ_i объекта данных $d_l^{об} \in D^{об}$ соответствует максимальной степени среди степеней секретности образующих его информационных элементов. Очевидно, что в один объ-

ект данных не должны попадать информационные элементы d_l и $d_{l''}$, которые имеют разные степени секретности, так как если профиль полномочий k-го пользователя позволяет ему обращаться к элементу d_l, но не дает ему право доступа к элементу данных $d_{l''}$, то он не должен иметь права обращаться и к объекту данных, в состав которого входит элемент $d_{l''}$, а поэтому не получит требуемый ему информационный элемент d_l.

Механизм защиты $M(G_к)$ канонической структуры ПБД есть отображение $\{(u_k, \pi_{kl}, a_j, d_l^{об}, \varphi_i)\} \to \to \{0, 1\}$, где $u_k \in U$, $\pi_{kl} \in \Pi_k$, $a_j \in A$, $d_l^{об} \in D^{об}$, $\varphi_i \in \Phi$. Случай «1» соответствует правомочности доступа типа a_j k-го пользователя, имеющего профиль полномочий π_{kl}, к объекту данных $d_l^{об}$, со степенью секретности φ_i, а случай «0» соответствует запрету такого доступа.

Механизм защиты $M(G_к)$ создается в результате выполнения процедур преобразования сформированной на этапе предпроектного анализа канонической структуры ПБД, осуществляемых с учетом требований к обеспечению секретности данных предметной области ПИФ и профилей полномочий пользователей, а также ограничений на типы отношений между объектами данных, налагаемых выбранной системой управления базами данных (СУБД). Механизм защиты $M(G_к)$ представляет собой средство установления правомочности доступа пользователей ко всем типам требуемых им объектов данных и отношений (взаимосвязей), зафиксированных на канонической структуре ПБД. Эффективность и качество механизма защиты канонической структуры $M(G_к)$ определяется существованием на канонической структуре ПБД разрешенных путей доступа ко всем данным, требуемым для удовлетворения множества санкционированных запросов пользователей, и допустимых типов отношений (взаимосвязей) между ними при заданных профилях полномочий пользователей. Путь доступа к требуемым объектам данных и информационным элементам канонической структуры ПБД считается разрешенным, если все объекты, через которые он проходит из одной из точек входа в каноническую структуру, имеют степени секретности, покрываемые профилем полномочий пользователя, а связи удовлетворяют ограничениям выбранной СУБД. Для решения поставленной задачи могут применяться универсальные методы преобразования структур БД на различных уровнях их представления, предложенные в работе [10], с учетом ограничений, налагаемых на структуры данных профилями полномочий пользователей, ограничений выбранной СУБД на типы отношений и взаимосвязей между объектами данных и требований секретности данных. Суть разработанного алгоритма заключается в выполнении операций перекомпоновки объектов данных с учетом требований профилей полномочий пользователей, формирования при необходимости новых типов объектов данных, распределения информационных элементов и их экземпляров по объектам данных с учетом степеней секретности данных и установления взаимосвязей между объектами, обеспечивающих разрешенные пути доступа к информационным элементам, проверки типов отношений между сформированными объектами данных и их преобразование с учетом ограничений СУБД. При выполнении данных операций анализируется формируемая обобщенная структура, в результате устраняются дублируемые структурные элементы и избыточные взаимосвязи.

После реорганизации формально механизм защиты $M(G_к)$ описывается матрицей смежности $B = \|b_{ll'}\|$ графа канонической структуры ПБД, обобщенной матрицей степеней секретности объектов данных $F = \|f_{li}\|$ и матрицей полномочий пользователей $P = \|p_{ki}\|$.

6. МОДЕЛИ И МЕТОДЫ ПОСТРОЕНИЯ МЕХАНИЗМА ЗАЩИТЫ ЛОГИЧЕСКОЙ СТРУКТУРЫ ПБД

Механизм защиты $M(G_л)$ логической структуры ПБД формируется на этапе логического проектирования ПБД. Логическая структура задается графом $G_л(N, W_л)$, где $N = \{n_j : j = \overline{1, J}\}$ — множество логических записей и $W_л$ — множество связей между ними [7, 8]. Логическая структура формально описывается матрицей смежности $\hat{B} = \|\hat{b}_{jj'}\|$, где элемент $\hat{b}_{jj'}$ равен единице, если запись $n_{j'}$ подчинена записи n_j, и равен нулю в противном случае.

Степень секретности отношений между логическими записями n_j и $n_{j'}$ обозначим через $\hat{\varphi}_{jj'} \in \hat{\Phi}$.

Механизм защиты $M(G_л)$ логической структуры ПБД есть отображение $\{(u_k, \pi_{kj}, a_j, (n_j, n_{j'}), \hat{\varphi}_{jj'}, n_j, \hat{\varphi}_j\} \to \{0, 1\}$, где значение «1» означает, что k-й пользователь с профилем полномочий π_{kj} обладает правом доступа типа a_j в отношении элементов логической структуры ПБД (связи и логической

записи) (n_j, n_j) и n_j, которые имеют степени секретности $\hat{\varphi}_{jj'} \in \tilde{\Phi}$ и $\hat{\varphi}_j \in \tilde{\Phi}$ соответственно. Значение «0» соответствует неправомочности такого доступа. Механизм защиты логической структуры ПБД устанавливает правомочность доступа пользователей к конфиденциальной информации логических записей и защищенным взаимосвязям между ними. Он формируется в результате отображения механизма защиты канонической структуры ПБД в механизм защиты логической структуры ПБД. При отображении степень секретности $\hat{\varphi}_j$ логической записи n_j определяется на основании данных о степени секретности объектов и информационных элементов механизма защиты канонической структуры ПБД, вошедших в ее состав. Пользователь имеет право доступа к логической записи в том случае, если ему доступны все объекты данных, образующие эту запись. Формализовано механизм защиты $M(G_л)$ задается матрицей описания логической структуры ПБД $\hat{B} = \|\hat{b}_{jj'}\|$, матрицей степеней секретности $\hat{F} = \|\hat{f}_{lj}\|$, а также матрицей полномочий пользователей $P = \|p_{ki}\|$. Элемент матрицы $\hat{F}\,\hat{f}_{li}(\hat{f}_{jj',i}) = 1$, если для логической записи (связи) $n_j \in N((n_j, n_{j'}) \in W_л)$ установлена степень секретности $\hat{\varphi}_i$, и $\hat{f}_{li}(\hat{f}_{jj',i}) = 0$ в противном случае.

Каждому варианту отображения механизма защиты канонической структуры ПБД в логическую структуру соответствует конкретный механизм защиты $M^0(G_л)$ логической структуры.

В качестве критерия эффективности при решении задачи синтеза механизма защиты логической структуры ПБД предлагается принять минимум суммарного числа подсхем, используемых заданным множеством пользователей. Механизм подсхем служит эффективным средством защиты связей между логическими записями путем разнесения записей в разные подсхемы (логические БД одной ПБД), а минимизация используемых пользователями подсхем облегчает администратору ПБД контроль за правильностью их использования. На формируемой при этом логической структуре ПБД обеспечивается правомочный доступ пользователей к типам логических записей, включенным в состав выделенных ими подсхем. В качестве другого критерия оптимизации может быть взят минимум суммарной длины путей доступа пользователей к данным.

Исходные данные для постановки задачи синтеза оптимального механизма защиты логической структуры ПБД: описание характеристик канонической структуры ПБД и механизма ее защиты; описание запросов пользователей ПБД и их характеристик; ограничения на возможность использования отдельными пользователями конкретных типов логических записей и взаимосвязей между записями и др.

Для описания характеристик канонической структуры ПБД задаются: $R = \{r_1, r_2, ..., r_1, ..., r_L\}$ — вектор количества экземпляров объектов данных, где r_l — количество экземпляров объекта d_l; $\rho = \{\rho_1, \rho_2, ..., \rho_l, ..., \rho_L\}$ — вектор длин каждого объекта в байтах; $\Delta = \{\delta_{ll'}/l, l' \in \overline{1, L}\}$ — множество усредненных коэффициентов связей.

Структура запросов пользователей к ПБД задается с помощью матрицы $T = \|t_{kl}\|$, проиндексированной по строкам множества пользователей $U = \{u_k/k = \overline{1, K}\}$, а по столбцам — множеством типов объектов данных, требуемых пользователям, $t_{kl} = 1$, если k-му пользователю требуется данные объекта $d_l \in D^{об}$; $t_{kl} = 0$ в противном случае. Частота реализации запросов пользователей к ПБД задается вектором $\sigma = \{\sigma_1, \sigma_2, ..., \sigma_k, ..., \sigma_K\}$, где σ_k — частота выполнения запроса k-го пользователя.

Для формализации задачи построения эффективного механизма защиты логической структуры ПБД введем переменные:

$x_{lj} = 1$, если l-й объект включен в состав j-й логической записи, $x_{lj} = 0$ в противном случае;

$x'_{jn} = 1$, если j-я логическая запись входит в состав n-й подсхемы, $x'_{jn} = 0$ в противном случае;

$y_{kj} = 1$, если $\prod\limits_{l \in L_j^{K'}} x_{lj}\left(\sum\limits_{i=1}^{I} f_{li} p_{ki}\right) = 1$, $y_{kj} = 0$ в противном случае, где $L_j^{K'}$ — множество объектов, включенных в состав j-й логической записи. Переменная y_{kj} устанавливает покрываемость степени секретности j-й логической записи уровнем полномочий k-го пользователя ($y_{kj} = 1$) либо отсутствие такой покрываемости ($y_{kj} = 0$);

$y'_{kn} = 1$, если $\sum\limits_{j=1}^{J}\sum\limits_{l=1}^{L} x'_{jn} x_{lj} t_{kl} \geq 1$, $y'_{kn} = 0$ в противном случае. Переменная y'_{kn} определяет необходимость использования k-м пользователем n-й подсхемы для реализации своих функциональных задач;

$z_{kn} = 1$, если $y'_{kn} \prod_{j \in L_n^n} x'_{jn} y_{kj} = 1$, $z_{kn} = 0$ в противном случае, где L_n^n — множество логических записей, образующих n-ю подсхему; переменная $z_{kn} = 1$, если n-я подсхема не содержит в своем составе данных, недоступных k-му пользователю по уровню секретности, в противном случае $z_{kn} = 0$;

$s_{jj'} = 1$, если $\sum_{l=1}^{L} \sum_{l'=1}^{L} x_{lj'} x_{lj} d_{ll'} \geq 1$, $s_{jj'} = 0$ в противном случае, где $d_{ll'}$ — элемент матрицы достижимости графа канонической структуры ПБД ($d_{ll'} \in \{1, 0\}$). Переменная s_{jj} определяет достижимость искомой логической записи j из некоторой, предшествующей ей на графе логической структуры ПБД, j'-й логической записи. Достижимость логических записей вытекает из условия необходимости сохранения семантических связей между элементами канонической структуры ПБД;

$s'_{j'j} = 1$, если $\sum_{l \in 1}^{L} \sum_{l' \in 1}^{L} x_{lj} x_{lj'} b_{ll'} \geq 1$, $s'_{j'j} = 0$ в противном случае, переменная $s'_{j'j}$ определяет отношения смежности между логическими записями, т. е. запись j' непосредственно предшествует записи j на логической структуре ПБД, если $s'_{j'j} = 1$;

$$z'_{kn} = 1, \text{ если } z_{kn} \prod_{j = L_n^n} \left(x'_{jn} \prod_{j = L_j^d} s_{jj'} y_{kj'} \right) = 1, \; z'_{kn} = 0$$

в противном случае, где L_j^d — множество типов записей, предшествующих на логической структуре ПБД j-й записи n-й подсхемы, переменная z'_{kn} определяет возможность доступа k-го пользователя к логическим записям, вошедшим в n-ю подсхему, без нарушения требований защиты данных ПБД от несанкционированного доступа.

Задача построения эффективного механизма защиты логической структуры ПБД по критерию минимума суммарного числа подсхем, используемых множеством запросов пользователей, имеет вид:

$$\min_{\left\{ \begin{matrix} x_{lj} \\ x_{jn} \end{matrix} \right\}} \sum_{k=1}^{K} \sum_{n=1}^{N} \delta_k y'_{kn} \qquad (1)$$

при ограничениях:

— на число объектов в логической записи:

$$\sum_{l=1}^{L} x_{lj} \leq I, \quad j = \overline{1, J}, \qquad (2)$$

где I — максимально допустимое число объектов в составе логической записи;

— на длину логической записи в байтах:

$$\sum_{l=1}^{L} x_{lj} \rho_1 \leq V, \quad j = \overline{1, J}, \qquad (3)$$

где V — максимально допустимая длина логической записи;

— на возможность попадания в состав одной логической записи объектов, имеющих разные степени секретности:

$$x_{lj} f_{li} + x_{lj} f_{li'} \leq 1 \text{ для заданных } i, i'; \qquad (4)$$

— на степень дублирования объектов в одной логической записи:

$$\sum_{l=1}^{L} x_{lj} = 1, \quad j = \overline{1, J}; \qquad (5)$$

— на степень дублирования объектов в различных логических записях:

$$\sum_{j=1}^{J} x_{lj} \leq \mu, \quad l = \overline{1, L}, \qquad (6)$$

где μ — допустимая степень дублирования объекта в логических записях;

— на степень дублирования логических записей в одной подсхеме:

$$\sum_{j=1}^{J} x'_{jn} = 1, \quad n = \overline{1, N}; \qquad (7)$$

— на степень дублирования логических записей в различных подсхемах:

$$\sum_{n=1}^{N} x'_{jn} \leq \psi, \quad j = \overline{1, J}, \qquad (8)$$

где ψ — максимально допустимая степень дублирования логических записей в подсхемах;

— на возможность существования в одной подсхеме заданных типов логических записей:

$$x'_{jn} + x'_{j'n} \leq 1 \text{ для заданных } j, j'; \qquad (9)$$

— на возможность попадания в состав одной подсхемы отдельных типов объектов данных:

$$x'_{jn} x_{lj} + x'_{j'n} x_{lj'} \leq 1 \text{ для заданных } dl, dl'; \qquad (10)$$

— на объем оперативной памяти, выделяемой пользователям при запросе требуемых им подсхем:

$$\sum_{n=1}^{N} \sum_{j=1}^{J} x'_{jn} \left(\sum_{l=1}^{L} x_{lj} \rho_l \right) \leq V_{\text{о.п}}, \qquad (11)$$

где $V_{\text{о.п}}$ — максимально допустимый объем оперативной памяти, выделяемый для суммарного числа подсхем, используемых множеством пользователей ПБД;

— на обязательность включения логических записей, требуемых пользователям, в одну из формируемых подсхем:

$$\sum_{n=1}^{N} x'_{jn} \geq 1,\ \forall j / \sum_{k=1}^{K} \sum_{l=1}^{L} x_{lj} t_{kl} \geq 1; \qquad (12)$$

— на обязательность доступности для пользователей используемых ими подсхем:

$$\prod_{n \in N_k} y'_{kn} z'_{kn} = 1, \quad k = \overline{1, K}, \qquad (13)$$

— на отказ в доступе пользователю к отдельным типам объектов данных даже при покрываемости степеней секретности этих объектов уровнями полномочий пользователей:

$$z'_{kn} = 0 \text{ для заданных } u_k,\ d_l; \qquad (14)$$

— на недопустимость совместного использования пользователями отдельных типов объектов данных:

$$z'_{kn} x'_{jn} x_{lj} + z'_{kn} x'_{j'n} x_{lj'} = 1$$
$$\text{для заданных } d_l,\ d_{l'} \in D^{\text{об}},\ u_k \in U. \qquad (15)$$

Поставленная задача синтеза относится к классу задач нелинейного целочисленного программирования с булевыми переменными. Для ее решения могут применяться методы и алгоритмы, предложенные в работе [10] для решения задач синтеза оптимальных по различным критериям эффективности логических структур БД различного класса и назначения, с учетом ограничений (2)—(15). В результате решения поставленной задачи (1)—(15) механизм защиты логической структуры ПБД формально описывается совокупностью трех бинарных матриц Z, X, Y, которые строятся на основе значений переменных z'_{kn}, x'_{jn}, x_{lj} соответственно. Единичные записи в k-й строке матрицы Z идентифицируют доступные k-му пользователю подсхемы. Матрицы X и Y определяют составы сформированных логических записей и подсхем соответственно. Механизм защиты $M(G_{\text{л}})$ обеспечивает правомочность доступа пользователей ПБД к подсхемам, логическим записям, а также типам объектов данных и информационным элементам.

7. МОДЕЛИ И МЕТОДЫ ПОСТРОЕНИЯ МЕХАНИЗМА ЗАЩИТЫ ФИЗИЧЕСКОЙ СТРУКТУРЫ ПБД

Механизм защиты $M(G_{\text{ф}})$ физической структуры создается на этапе проектирования физической структуры (структуры хранения) ПБД, представляемой графом $G_{\text{ф}}(D^{\text{ф}}, W^{\text{ф}})$, вершинами которого $D^{\text{ф}} = \{d_l^{\text{ф}} : l \in L^{\text{ф}}\}$ служит множество физических записей (блоков, файлов), а дугами $W^{\text{ф}}$ — множество связей между элементами физической структуры. Формально структура хранения ПБД описывается матрицей смежности $B^{\text{ф}} = \| b_{ll'}^{\text{ф}} \|$, проиндексированной по обеим осям множеством типов физических записей (блоков, файлов) $D^{\text{ф}} = \{d_l^{\text{ф}} : l \in L^{\text{ф}}\}$. Элемент $b_{ll'}^{\text{ф}}$ матрицы $B^{\text{ф}}$ равен единице, если физическая запись $d_l \in D^{\text{ф}}$ подчиняется записи $d_l \in D^{\text{ф}}$.

Механизм защиты физической структуры ПБД устанавливает правомочность доступа пользователей к элементам структуры хранения (физическим записям, блокам, файлам и др.) ПБД. Механизм защиты $M(G_{\text{ф}})$ физической структуры ПБД есть отображение $\{(u_k, \pi_{kj}, a_j, v_p, \varphi_i)\} \to \{0, 1\}$, где $v_p \in V$ — множество элементов физической организации ПБД. Значение «1» означает для k-го пользователя с профилем полномочий π_{kl} возможность доступа типа $a_j \in A$ к элементам $v_p \in V$ структуры хранения и физической организации ПБД, которые имеют степени секретности $\varphi_i \in \Phi$, а «0» означает невозможность такого доступа.

Эффективный механизм защиты физической структуры ПБД обеспечивает возможность обращения пользователей к требуемым элементам физической организации данных и структуры хранения ПБД, обеспечивая исключение несанкционированного доступа к физическим записям, блокам и файлам путем соответствующего размещения их на устройствах внешней памяти. Данный механизм защиты формируется на этапе синтеза системы защиты информации от несанкционированного доступа, используемой в дальнейшем при построении системы управления информационной безопасностью организации [11].

ЗАКЛЮЧЕНИЕ

Предложенные в работе модели и методы позволяют построить эффективные механизмы защиты структур патентных баз данных (ПБД) на кано-

ническом, логическом и физическом уровнях их представления, обеспечивающие доступ и допуск к содержимому ПБД только обладающих соответствующими полномочиями пользователей и устанавливающие правила взаимодействия пользователей с патентными информационными ресурсами по критериям оптимальности, коррелированным с требованиями защиты ПБД.

Разработанные модели, методы и средства построения эффективных механизмов защиты ПБД использовались при создании системы управления информационной безопасностью Евразийского патентного ведомства Евразийской патентной организации, которая в 2015 г. была введена в эксплуатацию.

ЛИТЕРАТУРА

1. *Фаязов Х.Ф., Сиротюк В.О., Овчинников А.В., Бурцев А.Б.* Формирование и развитие евразийского патентно-информационного пространства. — М.: ИНИЦ «Патент», 2010. — 124 с.
2. *Сиротюк В.О.* Проблемы и задачи обеспечения информационной безопасности патентно-информационных ресурсов // Патентная информация сегодня. — 2012. — № 1. — С. 3—10.
3. *Информационная* безопасность систем организационного управления. Теоретические основы: в 2 т. / Н.А. Кузнецов, В.В. Кульба, Е.А. Микрин и др. — М.: Наука, 2006.
4. *Kizza J.M.* Guide to Computer Network Security. — London: Springer, 2017. — 569 p.
5. *Wang H., He D., Tang S.* Identity-Based Proxy-Oriented Data Uploading and Remote Data Integrity Checking in Public Cloud // IEEE Trans. Information Forensics and Security. — 2016. — Vol. 11, N 6. — P. 1165—1176.
6. *Patent* Cooperation Treaty (PCT). — Geneva.: WIPO, 2000.
7. *Сиротюк В.О.* Методы и средства обеспечения информационной безопасности патентных ведомств // Патентная информация сегодня. — 2012. — № 2. — С. 3—11.
8. *Кульба В.В., Курочка Н.П.* Математическая модель обеспечения безопасности информации в базах данных // Науковедение. — 2015. — Т. 7, № 3.
9. *Gregg M.* The Network Security Test Lab: A Step-by-Step Guide. — John Wiley & Sons, 2015. — 488 p.
10. *Кульба В.В., Ковалевский С.С., Косяченко С.А., Сиротюк В.О.* Теоретические основы проектирования оптимальных структур распределенных баз данных / Сер.: Информатизация России на пороге XXI века. — М.: СИНТЕГ, 1999. — 660 с.
11. *Vacca J.R.* Computer and Information Security Handbook. — Morgan Kaufmann, 2017. — 1280 p.

Статья представлена к публикации членом редколлегии В.М. Вишневским.

Сиротюк Владимир Олегович *— д-р техн. наук, вед. математик, Институт проблем управления им. В.А. Трапезникова РАН, г. Москва,*
✉ *vsirotyuk@ipu.ru.*