Сиротюк В.О.

Механизмы управления безопасностью баз данных патентной информации

Аннотация: В работе рассмотрены формализованные механизмы управления безопасностью баз данных патентной информации (БДПИ). Описаны угрозы и риски информационной безопасности патентной информации. Предложены модели синтеза оптимальных механизмов защиты структур БДПИ на различных уровнях их представления (концептуальном, логическом и физическом). Предложенные модели и методы использовались при разработке системы защиты патентного информационного фонда региональной патентной организации.

Ключевые слова: база данных патентной информации, угроза информационной безопасности, риск информационной безопасности, конфиденциальность данных, неизменность данных, доступность данных, механизм защиты структур баз данных, система защиты патентной информации

Введение

Патентные информационные фонды (ПИФ) являются важным стратегическим ресурсом высокотехнологических предприятий и организаций XXI века. Принятие решений на основе анализа и использования патентной информации позволяет повысить эффективность НИР и ОКР, создавать конкурентоспособною продукцию, развивать предпринимательство и дает важные стратегические преимущества.

Центральное место в ПИФ занимают базы данных патентной информации (БДПИ), на которые возложены функции хранения, интеграции и консолидации патентно-информационных ресурсов. БДПИ содержат уникальную информацию по различным аспектам научно-технических, экономических, военно-стратегических, социальных, культурных и других видов знаний. Информация, содержащаяся в БДПИ и формируемых на их основе тематических подборках, обладает значительными преимуществами перед другими видами информации.

Вместе с этим возрастают потенциальные угрозы и риски информационной безопасности (ИБ) ПИФ и, как следствие этого, возрастает потребность в надежных и эффективных методах и средствах защиты данных БДПИ, информационной и обеспечивающей инфраструктуры ПИФ [1].

В работе предложены формализованные модели и методы анализа и синтеза оптимальных механизмов защиты канонических, логических и физических структур БДПИ и системы защиты ПИФ от преднамеренного или непреднамеренного несанкционированного доступа, модификации или разрушения данных.

Угрозы и уязвимые элементы ИБ ПИФ

Основными угрозами ИБ ПИФ являются:

- раскрытие конфиденциальной информации,
- компрометация информации,
- несанкционированный обмен информацией,
- отказ от информации,
- отказ в обслуживании.

Уязвимыми элементами ПИФ являются содержимое БДПИ, программное обеспечение, оборудование, люди (пользователи, администраторы ПИФ), документация [1].

Принципиально возможными путями утечки патентной информации могут быть:

- прямое хищение носителей информации и документов,
- копирование конфиденциальной информации,
- несанкционированное подключение к терминалу пользователей и незаконное его использование,
- несанкционированный доступ к данным.

Методы построения механизмов защиты структур БДПИ

Исходной информацией для построения механизмов защиты структур БДПИ является информация о спецификациях требований пользователей, требованиях к обеспечению необходимой степени секретности данных, а также профилях полномочий пользователей.

Требования к механизму защиты канонической структуры ПБД формируются на этапе анализа требований пользователей и формирования канонической структуры БДПИ.

Пусть $S = \{s_v\}, v = \overline{1, V_0}$ - множество формируемых БДПИ, $U = \{u_k / k = \overline{1, K_0}\}$ - множество запросов пользователей.

Формально каноническая структура отдельной *v*-й БДПИ представляется в виде графа $G_v(D_v, R_v)$, где $D_v = \{d_\varepsilon / \varepsilon \in L_v^{ob}, L_{ob}^v \subseteq L_v\}$ – множество объектов данных, R_v – множество взаимосвязей (отношений) между элементами. Каждый объект $d_\varepsilon \in D_v$ характеризуется множеством информационных элементов $D_l = \{d_l / l \in L_v^{el}\}$ и функций $H_l^{pr} = \{h_j / j \in J_v\}$ [2].

Пусть $A = \{a_j : j = \overline{1, m_q}\}$ - множество типов доступа к данным БДПИ. Для каждого объекта данных и информационного элемента указываются степени их секретности $\varphi_i \in \Phi$. Профиль полномочий пользователя k - го пользователя зададим в виде множества $\Pi_k = \{\pi_k : k = \overline{1, K_0}, l \in L_k \subseteq L, \phi_l \in \Phi\}$.

Механизм защиты канонической структуры БДПИ $M(G_к)$ есть отображение $\{(u_k, \pi_k, a_j, d_\varepsilon, \phi_i)\} \to \{0,1\}$. Случай «1» соответствует правомочности доступа типа a_j k-го пользователя, имеющего профиль полномочий π_k, к объекту данных d_ε, который имеет степень секретности φ_i, а случай «0» - запрету такого доступа. Механизм защиты $M(G_v)$ формируется в результате реорганизации канонической структуры БДПИ с учетом требований к защите данных. Алгоритмы реорганизации рассмотрены в работе [2]. После реорганизации механизм защиты *v–й* ПБД $M(G_v)$ описывается матрицей смежности канонической структуры *v-й* ПБД $W_v = \|w_{\varepsilon\varepsilon'}^v\|$, матрицей степеней секретности объектов данных

$F_v = \|f_{\varepsilon i}^v\|$ и матрицей полномочий пользователей $P = \|p_{ki}\|$.

Механизм защиты $M(G_v)$ логической структуры БДПИ формируется на этапе построения логической структуры, задаваемой графом *G(N,L),* где $N = \{n_j / j = \overline{1, J}\}$ – множество логических записей, $L = \{(n_j, n_{j'}) / j, j' = \overline{1, J}\}$ - множество взаимосвязей между записями. Организация эффективной защиты БДПИ на этом

уровне требует защиты не только данных, но и защиты отношений (связей) между данными.

Обозначим степени секретности *j-й* логической записи и отношений между логическими записями n_j и $n_{j'}$ через $\hat{\varphi}_j \in \hat{\Phi}$ и $\hat{\varphi}_{jj'} \in \hat{\Phi}$ соответственно. Тогда механизм защиты $M(G_л)$ логической структуры БДПИ есть отображение:

$$\{(u_k, \pi_k, a_j, (n_j, n_{j'}), \hat{\varphi}_{jj'}, n_j, \hat{\varphi}_j)\} \to \{0,1\}.$$

Значение «1» означает, что пользователь $u_k \in U$ с уровнем полномочий $\pi_k \in \Pi$ обладает правом доступа типа $a_j \in A$ в отношении элементов логической структуры БДПИ (связи и логической записи) $(n_j, n_{j'})$ и n_j, которые имеют степени секретности $\hat{\varphi}_{jj'} \in \hat{\Phi}$ и $\hat{\varphi}_j \in \hat{\Phi}$ соответственно. Значение «0» соответствует неправомочности такого доступа.

Критериями оптимизации при решении задачи синтеза механизма защиты логической структуры БДПИ, коррелированными с требованиями защиты данных, являются минимум суммарного числа подсхем, используемых пользователями, минимум суммарной длины путей доступа к данным, минимум интерфейса между подсхемами БДПИ. Постановки задач синтеза, математические модели и методы их решения приведены в [1, 2]. Формируемый в результате их решения оптимальный механизм защиты логической структуры БДПИ $M\left(G_л\right)$ обеспечивает идентификацию правомочности доступа пользователей к подсхемам БДПИ, логическим записям, а также к объектам данных и информационным элементам. Формализованное описание механизма защиты $M(G_л)$ задается матрицей описания логической структуры БДПИ $B = \left\| b_{jj'} \right\|$, матрицей степеней секретности $\hat{F} = \left\| \hat{f}_{lj} \right\|$, а также матрицей полномочий пользователей $P = \left\| p_{ki} \right\|$.

Механизм защиты физической структуры ПБД позволяет идентифицировать правомочность доступа пользователей к

компонентам физической структуры ПБД. Механизм защиты $M(G_ф)$ физической структуры ПБД есть отображение $\{(u_k, \pi_k, a_j, v_p, \varphi_i)\} \to \{0,1\}$, где $v_p \in V$ - множество компонентов физической организации ПБД (физических записей, блоков, файлов и т.д.). При этом «1» означает для пользователя $u_k \in U$ с уровнем полномочий $\pi_k \in \Pi$ возможность доступа типа $a_j \in A$ к элементам $v_p \in V$ физической организации БДПИ, которые имеют степени секретности $\varphi_i \in \Phi$, а «0» - невозможность такого доступа.

Рассмотрим задачи синтеза оптимальной системы защиты ПИФ. Синтез оптимальной системы защиты ПИФ включает решение следующего множества задач [1,2]:

1. Формирование структуры файлов БДПИ с учетом степеней секретности логических записей и характеристик запросов.
2. Распределение файлов БДПИ между устройствами памяти.
3. Выбор варианта закрепления пользователей за терминалами.
4. Выбор варианта сопряжения терминалов с устройствами памяти.
5. Распределение методов защиты между объектами защиты.

Критериями оптимальности при решении задачи синтеза системы защиты ПИФ являются максимум информационной независимости пользователей БДПИ, минимум суммарных потерь от несанкционированного доступа к конфиденциальной информации БДПИ и др. В качестве ограничений выступают ограничения на уровень защищенности информационных ресурсов БДПИ, на стоимость разработки и эксплуатации системы защиты, ограничения, определяемые требованиями к эффективности использования ресурсов вычислительной системы и др. [1,2].

Заключение

В работе рассмотрены модели и методы построения эффективных механизмов управления безопасностью баз данных патентной информации и системы защиты патентных информационных фондов. Полученные результаты используются в дальнейшем при построении оптимальной системы управления информационной безопасностью (СУИБ) ПИФ. Предложенные модели, методы и программное обеспечение использовались при

решении задач обеспечения защиты информационных ресурсов ПИФ евразийского патентного информационного пространства [3].

Литература:

1. *В.В. Кульба, В.О. Сиротюк, С.А. Косяченко* Информационная безопасность патентных ведомств: теория и практика. – М.: ИПУ РАН., 2017. – 166с.

2. *Кульба В.В., Ковалевский С.С., Косяченко С.А., Сиротюк В.О.* Теоретические основы проектирования оптимальных структур распределенных баз данных. Серия «Информатизации России на пороге XXI века». – М.: СИНТЕГ, 1999. – 660 с.

3. *Х.Ф. Фаязов, В.О. Сиротюк, А.В. Овчинников, А.Б. Бурцев* Формирование и развитие евразийского патентно-информационного пространства. – М.: ИНИЦ «Патент», 2010. – 124 с.