УДК 330.1:332.1:614.8:658.5

ПРОБЛЕМЫ И ЗАДАЧИ ЗАЩИТЫ ПАТЕНТНОЙ ИНФОРМАЦИИ

В.О. Сиротюк
Институт проблем управления им. В.А. Трапезникова РАН
Россия, 117997, Москва, Профсоюзная ул., 65
E-mail: vsirotyuk@ipu.ru

С.А. Косяченко
Институт проблем управления им. В.А. Трапезникова РАН
Россия, 117997, Москва, Профсоюзная ул., 65
E-mail: sakos@ipu.ru

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

Аннотация: В работе рассмотрены теоретические и практические вопросы построения эффективной системы защиты патентной информации. Описаны угрозы информационной безопасности патентных баз данных, сформулированы цели и задачи защиты патентной информации, обеспечения информационной безопасности патентных баз данных. Предложены формализованные модели и методы анализа и оценки рисков информационной безопасности, синтеза эффективных механизмов защиты канонических, логических и физических структур патентных баз данных и системы защиты патентного информационного фонда. Рассмотрено построение эффективной системы управления информационной безопасностью Евразийского патентного ведомства.

1. Введение

Централизация хранения патентно-информационных ресурсов в соответствующих базах данных патентной информации (патентных базах данных или ПБД) и децентрализация их использования выдвигают проблему обеспечения требуемого уровня защиты патентной информации от преднамеренного или непреднамеренного несанкционированного доступа, модификации или разрушения.

Основными угрозами информационной безопасности (ИБ) ПБД являются:

- раскрытие конфиденциальной информации, к которой относятся материалы дел заявок и патентов до их публикации, входящая и исходящая корреспонденция, документы электронного обмена и др. данные;
- компрометация патентной информации (внесение несанкционированных изменений в ПБД);
- несанкционированный обмен патентной информацией;
- отказ от информации (непризнание экспертом патентного ведомства или заявителем (патентным поверенным)) фактов получения или отправки информации;
- отказ в обслуживании (отсутствие доступа к патентной информации).

Высокий уровень защиты патентной информации может быть обеспечен разработкой и внедрением оптимальной системы защиты ПБД и системы управления информационной безопасностью (СУИБ) патентного информационного фонда (ПИФ) [1-3].

В работе предложены формализованные модели и методы анализа и синтеза оптимальных механизмов защиты структур ПБД и системы защиты ПИФ. Полученные результаты применялись при построении СУИБ международной патентной организации - Евразийского патентного ведомства Евразийской патентной организации.

2. Цели и задачи защиты патентной информации

Целями защиты патентной информации является обеспечение конфиденциальности, неизменности, достоверности и доступности информационных материалов по заявкам на изобретения и патентов, официальных изданий, а также других информационных активов ПИФ.

Для достижения этих целей в организации – владельце ПИФ внедряется СУИБ. Разработка эффективной СУИБ должна базироваться на использовании формализованных моделей и методов анализа и синтеза оптимальных механизмов и системы защиты ПБД от несанкционированного доступа [1,3].

Создание СУИБ предполагает организацию и регулярное проведение мероприятий по инвентаризации и классификации информационных активов ПИФ, оценке рисков информационной безопасности.

Для оценки рисков ИБ может использоваться следующая формула:

$$R=D\cdot P(V),$$

где R – риск информационной безопасности; D – критичность актива (ущерб); P(V) – вероятность реализации уязвимости.

Основными задачами информационной безопасности ПБД являются:

- определение сферы (границ) СУИБ;
- распределение обязанностей по обеспечению информационной безопасности;
- обучение и подготовка персонала по поддержанию режимов ИБ;
- уведомление о случаях нарушения защиты;
- защита от вирусов и спама;
- планирование бесперебойной работы ПБД;
- контроль над копированием информации и программ;
- защита патентной информации от несанкционированного доступа;
- контроль соответствия принятой политике информационной безопасности;
- управление рисками в области информационной безопасности;
- выбор контрмер, обеспечивающих требуемый уровень ИБ;
- контроль за функционированием и аудит СУИБ.

3. Модели и методы проектирования механизмов защиты структур ПБД и системы защиты ПИФ

Механизм защиты структур ПБД должен обеспечивать такую структуризацию хранимой в ПБД патентной 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 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 ПИФ и СУИБ [2, 3].

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.

Исходной информацией для построения механизмов защиты структур ПБД является информация о предметной области ПИФ, спецификациях информационных и функциональных требований пользователей и канонической структуре ПБД, требованиях к обеспечению необходимой степени секретности данных, а также профилях полномочий пользователей на использование данных.

Пусть $A = \{a_j : j = \overline{1, m_q}\}$ – множество типов доступа к информационным ресурсам ПБД. Для каждого структурного элемента предметной области (объекта данных и информационного элемента) с учетом их ценности указываются степени их секретности $\varphi_i \in \Phi$, где $\Phi = \{\varphi_i : i \in R\}$ – множество степеней секретности патентной информации.

Информация о секретности структурных элементов представляется в виде матрицы $F = \|f_{li}\|$, элемент которой f_{li} = 1, если для элемента $d_l \in D$ установлена степень секретности $\varphi_i \in \Phi$, и равен нулю в противном случае.

Профиль полномочий пользователя *k*-го пользователя зададим в виде множества $\Pi_k = \{\pi_{kl} : k = \overline{1, K_0}, l \in L_k \subseteq L, \phi_l \in \Phi\}$. Формально профиль полномочий пользователей представляется матрицей $P = \|p_{ki}\|$, элемент которой $p_{ki} = a_j$, если k-й пользователь имеет право выполнять доступа типа a_j к данным ПБД, имеющим степень секретности φ_i, и равен нулю в противном случае.

С учетом введенных формальных определений и обозначений механизм защиты канонической структуры ПБД $M(G_к)$ есть отображение $\{(u_k, \pi_{kl}, a_j, d_l^{ob}, \phi_i)\} \to \{0,1\}$. Случай «1» соответствует правомочности доступа типа a_j *k*-го пользователя, имеющего профиль полномочий π_{kl}, к объекту данных d_l^{ob}, который имеет степень секретности φ_i, а случай «0» соответствует запрету такого доступа. Эффективный механизм защиты $M(G_k)$ формируется в результате анализа канонической структуры ПБД и ее реорганизации с целью построения разрешенных с учетом требований к защите путей доступа к данным, требуемым для удовлетворения санкционированных запросов пользователей. Для построения оптимального механизма защиты $M(G_к)$ канонической структуры ПБД могут использоваться методы и алгоритмы, рассмотренные в [4].

Механизм защиты логической структуры ПБД $M(G_л)$ формируется на этапе логического проектирования ПБД. Логическая структура задается графом $G_.(N, W)$, где $N = \{n_j : j = \overline{1, J}\}$ - множеством логических записей и W –множество связей между ними. Механизм защиты логической структуры ПБД $M(G_л)$ 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 связи $(n_j, n_{j'})$ и логической записи n_j, которые имеют степени секретности $\hat{\varphi}_{jj'} \in \widetilde{\Phi}$ и $\hat{\varphi}_J \in \widetilde{\Phi}$ соответственно. Значение «0» соответствует неправомочности такого доступа. Механизм защиты логической структуры ПБД формируется в результате отображения механизма защиты канонической структуры ПБД в механизм защиты логической структуры

ПБД. В качестве критериев эффективности синтеза оптимального механизма защиты логической структуры ПБД используются минимум суммарного числа подсхем пользователей, а также минимум суммарной длины путей доступа к данным [1,2].

Механизм защиты физической структуры ПБД $M(G_ф)$ создается на этапе проектирования структуры хранения ПБД, представляемой графом $G_ф(D^Ф,W^Ф)$, вершинами которого $D^Ф=\{ d_l^Ф : l \in L^ф \}$ является множество физических записей (блоков, файлов), а дугами $W^Ф$ – множество связей между элементами физической структуры. Механизм защиты физической структуры ПБД устанавливает правомочность доступа пользователей к элементам структуры хранения (физическим записям, блокам, файлам и т.д.) ПБД. Механизм защиты физической структуры ПБД $M(G_ф)$ есть отображение $\{(u_k, \pi_{kl}, a_j, v_p, \varphi_i)\} \to \{0,1\}$, 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.

В результате решения задач синтеза системы защиты ПИФ осуществляется выбор совокупности методов непосредственной защиты (программных, организационных и др.) с учетом характеристик их эффективности и закрепление их за определенными структурными элементами логической и физической организации ПБД. В качестве критериев эффективности при решении задач синтеза оптимальной системы защиты ПИФ используются максимум информационной независимости пользователей ПИФ, минимум потерь от несанкционированного доступа пользователей. Постановки задач, модели и методы синтеза оптимальной системы защиты ПИФ рассмотрены в [1,4].

4. Построение эффективной системы управления информационной безопасностью

Рассмотрим построение эффективной системы управления информационной безопасностью международной патентной организации – Евразийского патентного ведомства (ЕАПВ) Евразийской патентной организации (ЕАПО) [1,3].

СУИБ ЕАПВ разработана на основе предложенных в работе формализованной методологии, моделях и методах анализа и оценки рисков ИБ, синтеза оптимальных механизмов защиты структур ПБД и системы защиты ПИФ.

СУИБ ЕАПВ обеспечивает комплексное решение следующих задач:

- выявление уязвимых элементов и угроз информационной безопасности;
- оценку рисков ИБ;
- построение оптимальных механизмов и системы защиты ПБД и ПИФ;
- мониторинг выполнения политики информационной безопасности ЕАПВ;
- обеспечение физической защиты информационных систем и ресурсов;
- разработку мероприятий по поддержанию работоспособности автоматизированных информационных систем ведомства и планов восстановительных работ.

СУИБ ЕАПВ является неотъемлемой составляющей (подсистемой) общей административной системы управления ЕАПВ со встроенными в нее функциями, обязанностями и ролями служащих по обеспечению надлежащего уровня информационной безопасности. Область ее действия распространяется на все структурные подразделения ЕАПВ, основные технологические и производственные процессы [1, 3].

Полный цикл функционирования СУИБ ЕАПВ состоит из следующих этапов:

- планирование – определение приоритетов и целей СУИБ, выбор механизмов, необходимых для их достижения, планирование работ и ресурсов;
- выполнение – выполнение запланированных работ, внедрение выбранных механизмов и систем защиты;
- проверка – сбор информации, контроль результативности достижения запланированных работ;
- совершенствование – принятие мер по устранению причин отклонений от запланированного результата, изменения в планировании и распределении ресурсов.

Политика информационной безопасности ЕАПВ включает набор общих формальных правил и требований, которым должны подчиняться служащие ЕАПВ и третьи лица, получившие доступ к информационным ресурсам, системам и технологиям ЕАПВ. К ним относятся правила доступа к информационным системам и ресурсам, требования и рекомендации по защите аппаратного, программного и информационного обеспечения ПБД и ПИФ, правила пользования электронной почтой и др. [3].

Создание СУИБ ЕАПВ ЕАПО на основе предложенных в работе формализованных моделей, методов и средств защиты патентной информации позволило повысить уровень информационной безопасности ЕАПВ, свести к минимуму угрозы и риски ИБ, обеспечить конфиденциальность, неизменность, достоверность, сохранность и доступность патентной информации.

5. Заключение

В работе рассмотрены проблемы, цели и защиты патентной информации, играющей важную роль при проведении НИР и ОКР и используемой при разработке высокоэффективной техники и технологий. В работе предложены методы оценки информационных рисков, модели и методы анализа и синтеза оптимальных механизмов защиты структур патентных БД и системы защиты патентной информации.

Эффективность практического применения предложенной методологии, моделей, методов и алгоритмов подтверждена разработкой и внедрением СУИБ международной патентной организации.

Список литературы

1. Кульба В.В., Сиротюк В.О., Косяченко С.А. Информационная безопасность патентных ведомств: теория и практика. М.:ИПУ РАН, 2017, 166с.
2. Сиротюк В.О. Модели и методы построения эффективных механизмов защиты структур патентных баз данных // Проблемы управления. 2017. № 5. С. 43-51.
3. Сиротюк В.О. Модели, методы и средства разработки и внедрения эффективной системы управления информационной безопасностью патентного ведомства // Науковедение. 2017. Т. 9, № 6. https://naukovedenie.ru/PDF/06TVN617.pdf.

4. 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.