

## **VIІ. Автоматизированные системы и средства обеспечения безопасности сложных систем**

**Сиротюк В.О., Богатырева Л.В., Потапова О.А.**

### **Построение системы защиты цифровых фондов интеллектуальной собственности**

**Аннотация:** В работе рассмотрены особенности формирования и использования цифровых информационных фондов интеллектуальной собственности (ЦФИС). Рассмотрены требования к базам данных (БД) интеллектуальной собственности и ЦФИС. Предложены постановка задачи, формализованные модели и методы построения оптимальных по различным критериям эффективности систем защиты БД ЦФИС от несанкционированного доступа. Предложенные модели и методы использовались при разработке системы управления информационной безопасностью БД евразийского патентно-информационного пространства.

**Ключевые слова:** база данных интеллектуальной собственности, цифровой информационный фонд интеллектуальной собственности, конфиденциальность данных, неизменность данных, доступность данных, система защиты данных

#### **Введение**

Системы управления интеллектуальной собственностью (ИС) играют важную роль при проведении хозяйствующими субъектами патентных и научных исследований с целью принятия обоснованных решений в различных областях науки и техники. Используемая при этом патентная и научно-техническая информация обладает значительными преимуществами перед другими видами информации [1].

В совокупности информационные фонды ИС, хранимые в соответствующих базах данных интеллектуальной собственности (БД ИС), информационные технологии сбора, хранения, обработки и передачи данных, информационно-телекоммуникационные и сетевые инфраструктуры образуют цифровой фонд интеллектуальной собственности (ЦФИС), который формируется для эффективного выполнения научно-исследовательскими институтами, организациями и предприятиями различных отраслей экономики поставленных перед ними задач.

Формирование, хранение и развитие данных ЦФИС включает операции, связанные с получением документов, комплектованием и организацией хранения документов фондов, переводом их в цифровую форму и загрузкой в БД ИС, представленных БД патентной информации (ПБД) и БД научно-технической информации (БД НТИ) [1,2].

Создание БД ИС по материалам первоисточников является весьма мощным средством активизации национальных информационных ресурсов за счет перевода значительной их части в цифровую форму и последующего многоаспектного использования в процессе исследований и разработок.

Современный ЦФИС имеет распределенную информационно-управляющую структуру и предоставляет доступ к локальным и внешним удаленным ПБД и БД НТИ, поиск информации и ее использование через единый пользовательский интерфейс [1,2]. Это обуславливает необходимость логической интеграции (или консолидации) данных локальных и внешних ПБД и БД НТИ.

Большие объемы хранимой в БД ИС информации, относимых к классу сверхбольших баз данных (VLDB), обуславливают необходимость не только разработки методов и средств оптимизации их проектирования, организации и использования, но и создания эффективных методов, средств и технологий защиты БД, информационной и обеспечивающей инфраструктуры ЦФИС [1,3].

В работе рассмотрены требования к БД ИС и ЦФИС, предложены формализованные модели и методы построения оптимальных по различным критериям эффективности систем защиты данных ЦФИС от преднамеренного или непреднамеренного несанкционированного доступа, модификации или разрушения данных.

## **Требования к БД ИС, обеспечивающей и информационной инфраструктуре ЦФИС**

ПБД и БД НТИ (БД ИС) ЦФИС хранят информацию о патентных документах и научно-технической литературе. Они относятся к типу документальных мультимедийных баз данных. Требования, предъявляемые к их составу и структуре более высокие, чем к традиционным документальным, библиографическим или фактографическим БД [1-3]. Сложность их создания и эксплуатации увеличиваются в связи с тем, что в них загружаются и хранятся очень большие объемы информации (от сотен гигабайт до десятков терабайт). Эти особенности обуславливают повышенные требования к качеству и безопасности информационной и обеспечивающей инфраструктуры ЦФИС.

Оценка эффективности построения ЦФИС проводится с использованием критериев максимума обеспечиваемых уровней полноты, достоверности, гарантированной защиты ПБД и БД НТИ от несанкционированного доступа, непреднамеренных искажений, разрушения и других неблагоприятных факторов.

С учетом распределенной структуры доступа к данным ЦФИС представляется в виде виртуального информационного хранилища. Инфраструктура ЦФИС должна удовлетворять следующим основным требованиям:

1. Обеспечивать защиту данных БД ИС от несанкционированного доступа, преднамеренного или непреднамеренного искажения, разрушения и модификации информации.

2. Обеспечивать доступность данных по схеме 24часа\*365дней.

3. Для обеспечения высокого уровня сохранности данных ПБД и БД НТИ должны обладать свойством «самообслуживания», предполагающим возможность самостоятельного восстановления работоспособности БД. Например, технологии ORACLE обеспечивают такую возможность на основе концепции создания т.н. автономных БД [4].

4. Предоставлять удобный интерфейс доступа к локальным и внешним удаленным ПБД и БД НТИ, базирующийся на принципе «одного окна» и средств метапоиска [1,2].

5. Серверное оборудование ЦФИС должно быть легко масштабируемым по объему хранимой информации. Подключение

дополнительных модулей хранения, расширяющих объем хранилища, должно осуществляться автоматически, и при этом должна обеспечиваться интеграция с существующими компонентами хранилища без перестройки уже развернутого информационного хранилища.

6. Обладать современными средствами поддержания готовности данных, обеспечивающими полное резервирование, упреждающий мониторинг, обнаружение и исправление ошибок.

7. Обладать развитой системой диагностики и автоматического информирования о произошедших неполадках.

С учетом сформулированных требований ЦФИС в современных условиях должен создаваться на основе специализированной системы аппаратно и программно конфигурируемой и масштабируемой платформы хранения, например, на основе платформы Oracle Exadata Cloud&Customer [4].

### **Формализованные методы построения оптимальной системы защиты данных ЦФИС**

Как известно, множество существующих методов защиты данных БД включают в себя организационные, процедурные, структурные, аппаратные и программные методы [3,5].

Организационные методы защиты используются для ограничения числа лиц, которые получают право доступа в помещение центра обработки данных (ЦОД).

Процедурные методы защиты делают возможным доступ к данным и передачу их только тем пользователям, которые имеют соответствующие разрешения.

Структурные методы защиты применяются на этапах проектирования структур БД (канонической, логической и физической) и системы защиты данных ЦФИС. Они должны обеспечивать такую структуризацию и организацию данных, которая позволяет повысить уровень защищенности хранимых данных.

Аппаратные средства защиты информации представляют собой различные электронные устройства, встраиваемые в состав технических средств вычислительной системы или сопрягаемые с ними с помощью стандартного интерфейса.

Программные методы защиты реализуются путем включения специализированных программных средств в состав используемых операционных систем и СУБД, либо выделения их в самостоятельные приложения, которые иницируются перед началом процесса обслуживания запросов пользователей.

Различные методы защиты информации характеризуются определенными технико-экономическими показателями, к которым относятся затраты на их разработку и эксплуатацию, безопасное время раскрытия методов защиты и др. [3,5].

Рассмотрим постановку задачи и модели синтеза оптимальной системы защиты данных ЦФИС [3,5].

При синтезе системы защиты данных ЦФИС требуется сформировать структуры файлов БД ИС и их распределение между устройствами памяти, выбрать варианты взаимодействия пользователей с ЦФИС при которых обеспечивался бы заданный критерий эффективности функционирования системы защиты, возможность выполнения ею функций защиты информационных ресурсов ПБД и БД НТИ в условиях заданных ограничений.

Синтез оптимальной системы защиты ЦФИС включает решение следующих задач:

1. Формирование структуры файлов БД ИС с учетом степеней секретности логических записей и характеристик запросов.
2. Распределение файлов БД ИС 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.

Исходной информацией при решении задач синтеза оптимальной системы защиты БД ИС являются описания механизмов защиты канонической и логической структур ПБД и БД НТИ, представляемые отображениями  $\{(u_k, db_i, as_j)\} \xrightarrow{\theta} \{0,1\}$ , где «1» соответствует правомочности доступа пользователя  $u_k \in U$  к элементам (объектам, данным) БД  $db_i \in DB$  и/или приложениям  $as_j \in AS$ , а «0» – запрету на такой доступ [3].

Формально механизмы защиты канонической и логической структуры  $v$ -й БД ИС  $M(G_v)$  и  $M(G_n)$  описываются, соответственно,

матрицами смежности канонической структуры  $\nu$ -й БД ИС  $W_\nu = \|w_{\varepsilon\varepsilon}^\nu\|$ , матрицей степеней секретности объектов данных  $F_\nu = \|f_{\varepsilon i}^\nu\|$  и матрицей полномочий пользователей  $P = \|p_{ki}\|$  канонической структуры; матрицей описания логической структуры БД ИС  $B = \|b_{ij}\|$ , матрицей степеней секретности  $\hat{F} = \|\hat{f}_{lj}\|$ , а также матрицей полномочий пользователей  $P = \|p_{ki}\|$  логической структуры данных. Методы и алгоритмы их построения приводятся в [3,4].

Система защиты  $S^3 = \{m_s : s = \overline{1, S}\}$  представляет собой взаимосвязанную совокупность методов защиты, где  $m_s$  есть  $s$ -й метод, а  $S$  – общее число методов. Под оптимальной системой защиты данных ЦФИС понимается такая совокупность (подмножество) методов защиты  $S_{opt} \subset S^3$ , которые в совокупности обеспечивают экстремальное значение некоторого заданного критерия эффективности разработки и/или эксплуатации системы защиты БД ЦФИС при условии соблюдения требований к функционированию БД ИС, выполнению структурных и функциональных ограничений, накладываемых ЦФИС, СУБД и пользователями.

В качестве исходных данных, помимо формального описания механизмов защиты канонической и логической структур БД ИС, используются также характеристики логической структуры БД ИС, запросов пользователей и транзакций, ограничения на возможность доступа пользователей к отдельным типам логических записей, параметры методов защиты информации от несанкционированного доступа и технических средств хранения информации и взаимодействия пользователей с БД.

Для формализации задачи синтеза оптимальной системы защиты вводятся следующие переменные [3,5]:

- переменные, определяющие требования пользователей на доступ к файлам ПБД и БД НТИ;
- переменные, идентифицирующие правомочность доступа пользователей к файлам БД ИС;

- переменные о размещении файлов на внешних устройствах памяти;
- переменные прикрепления пользователей к терминалам;
- переменные выбора метода защиты для объектов БД ИС;
- производные переменные.

Критериями эффективности при решении задач синтеза оптимальной системы защиты данных ЦФИС являются максимум информационной независимости пользователей БД ИС, минимум суммарных потерь от несанкционированного доступа к конфиденциальной информации БД ИС и др. В качестве ограничений выступают ограничения на уровень защищенности информационных ресурсов БД ИС, на стоимость разработки и эксплуатации системы защиты, ограничения, определяемые требованиями к эффективности использования ресурсов вычислительной системы и др. [3].

Поставленные задачи синтеза относятся к классу задач нелинейного целочисленного программирования с булевыми переменными. Методы и алгоритмы решения данных задач приводятся в [5].

В результате решения поставленных задач формируется оптимальная по заданному критерию эффективности, коррелированному с требованиями информационной безопасности, система защиты БД ЦФИС, обеспечивающая:

- распределение логических записей по файлам ПБД и БД НТИ с учетом степеней секретности логических записей и характеристик запросов пользователей;
- распределение файлов ПБД и БД НТИ между устройствами памяти в соответствии с требованиями безопасности данных и эффективности доступа к ним;
- закрепление пользователей ЦФИС за терминалами;
- сопряжение множества терминалов с множеством внешних носителей;
- закрепление методов непосредственной защиты за объектами защиты различных структурных уровней.

### **Заключение**

В работе рассмотрены особенности построения ЦФИС, характеристики и требования к БД ИС, обеспечивающей и

информационной инфраструктуре ЦФИС. Рассмотрены постановка задачи, модели и методы построения оптимальной системы защиты данных ЦФИС. Полученные результаты использовались при построении оптимальной системы защиты БД ЦФИС евразийского патентного информационного пространства [1,2].

*Работа выполнена в рамках темы: «Фундаментальные исследования по направлению «Модели, методы анализа и синтеза структуры и сценариев развития социально-экономических и технических систем управления, повышения их управляемости и безопасности функционирования в условиях неопределенности, структурных возмущений и чрезвычайных ситуаций» № 0052-2019-0011*

Литература:

1. Кульба В.В., Сиротюк В.О. Формализованная методология повышения эффективности и качества патентных информационных фондов и опыт ее использования при формировании и развитии евразийского патентно-информационного пространства. – М.: ИПУ РАН, 2019. – 236 с.

2. 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.

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

4. Материалы сайта ORACLE. – URL: <https://www.oracle.com/> (дата обращения 14.10.2021).

5. 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.

---