комитета на 41 ассамблею Международной гражданской авиации (ИКАО) A41-WP/72, 2022. – URL: https://www.icao.int/Meetings/a41/Documents/WP/wp_072_ru.pdf (дата обращения 06.11.2023).

DOI: 10.25728/iccss.2023.86.11.051

Сиротюк В.О., Богатырева Л.В.

Повышение безопасности тематических баз данных цифрового информационного фонда интеллектуальной собственности

Аннотация: В работе рассмотрены особенности построения и характеристики тематических баз данных (ТБД), формируемых в результате проведения патентно-информационных поисков в базах данных патентной и научно-технической информации цифрового информационного фонда интеллектуальной собственности. Сформулированы требования, цели и задачи обеспечения информационной безопасности ТБД в условиях цифровизации систем управления интеллектуальной собственностью.

Ключевые слова: система управления интеллектуальной собственностью, цифровой информационный фонд интеллектуальной собственности, тематическая база данных, защита данных, информационная безопасность

Введение

В условиях цифровизации систем управления интеллектуальной собственностью (ИС) происходят радикальные изменения в организации и методах проведения НИР и ОКР, коммерциализации результатов интеллектуальной деятельности [1]. Научное сообщество переходит к новой концепции проведения научных исследований и разработок, основанной на возможности доступа к разнообразным, распределенным источникам научной, технической и патентной информации, формирования на основании извлекаемой из них информации баз данных определенной тематики (тематик) (тематических БД, ТБД), их обработки и использования в различных предметных областях.

Создание ТБД позволяет научному сообществу пользоваться широким кругом источников информации, причем не только исходных, но и вторичных, структурированных, созданных на основе первичных патентных, научных и технических данных.

ТБД содержат консолидированную патентную и научно-техническую информацию, используемую организациями и предприятиями для разработки документов, связанных с деятельностью хозяйствующего субъекта и обоснованием принимаемых им решений: прогнозов, программ, бизнес-планов, планов создания и развития производства объектов техники и оказания услуг; документации, связанной с формированием и реализацией инвестиционной политики; планово-технической документации на выполнение НИР и ОКР; документации, связанной с оценкой технического уровня и качества продукции, модернизацией или снятием ее с производства и др. [2].

В условиях цифровой трансформации систем управления ИС значительно возрастают риски и угрозы информационной безопасности (ИБ) баз данных (БД), информационных систем, цифровых сервисов, информационной и обеспечивающей инфраструктуры и поэтому возрастает потребность в надежных методах и средствах их защиты. От эффективности используемых методов и средств обеспечения ИБ во многом зависит эффективность и качество функционирования самих цифровых органов управления ИС и оказываемых ими услуг.

В работе рассмотрены особенности построения и характеристики ТБД, критерии эффективности и модели их формирования. Разработаны требования по обеспечению ИБ ТБД. Сформулированы цели и описаны задачи повышения защиты ТБД.

Особенности построения, характеристики и модели формирования ТБД ЦИФИС. Критерии эффективности создания ТБД

ТБД формируются в результате проведения хозяйствующими субъектами тематических патентно-информационных поисков в базах данных патентной (ПБД) и научно-технической информации (БД НТИ) цифрового информационного фонда интеллектуальной собственности (ЦИФИС) и отбора из них релевантной информации.

ТБД могут создаваться как централизовано (в виде сетевых БД или в составе облачных сервисов), так и децентрализовано в виде федеративных БД [1, 2]. Независимо от выбранной модели формирования ТБД основным их назначением является полное, качественное, безопасное и оперативное удовлетворение информационных и функциональных требований пользователей. Вследствие этого, основными критериями эффективности их создания являются их эксплуатационные характеристики (минимум суммарного времени обслуживания тематических запросов пользователей, минимум суммарной длины путей доступа к данным и др.), а также показатели повышения качества ТБД (уровня защиты, полноты, достоверности и доступности данных) [2, 3].

Наиболее эффективной по отмеченным критериям моделью является технология федерализации данных, обеспечивающая создание виртуальной (в т.ч. облачной) федеративной ТБД, предоставляющей доступ к источникам ПБД и БД НТИ и извлечение данных из них на основании тематических запросов. Эта технология обеспечивает доступ к текущим (актуальным) данным источников данных, что избавляет администраторов ТБД от необходимости консолидации данных в едином хранилище данных и связанных с этим проблем, связанных с задержкой формирования ТБД, их обновлением и актуализацией [1].

Требования по обеспечению безопасности патентной и научно-технической информации ЦИФИС

Централизованное хранение патентно-информационных ресурсов в ПБД и БД НТИ ЦИФИС и децентрализованное их использование в составе формируемых на их основе ТБД выдвигают проблему обеспечения требуемого уровня защиты данных ЦИФИС от преднамеренного или непреднамеренного несанкционированного доступа, модификации или разрушения данных со стороны неавторизованных пользователей [3, 4].

Учитывая, что ТБД формируется на основании выполнения операций доступа к определенным в соответствии с тематическими запросами пользователей ПБД и БД НТИ, поиска в БД, выборки и извлечения данных из БД и формирования массивов ТБД, обеспечение их информационной безопасности напрямую зависит от требований, предъявляемых к защите ПБД и БД НТИ ЦИФИС.

Рассмотрим эти требования [1-3].

Главной целью защиты патентной и научно-технической информации ЦИФИС является обеспечение конфиденциальности, неизменности и доступности информационных материалов по заявкам на изобретения и патентов, научных публикаций, нормативно-правовых документов и официальных изданий, других информационных ресурсов ПБД и БД НТИ ЦИФИС.

Основными угрозами безопасности данных являются [1, 3]:

– раскрытие конфиденциальной информации (кража информации, несанкционированный доступ, копирование данных),

– компрометация информации (внесение несанкционированных изменений в массивы данных и структуры БД),

– несанкционированный обмен информацией,

– отказ от информации (непризнание получателем или отправителем фактов получения/отправки информации),

– отказ в обслуживании (отсутствие доступа к информации).

Данные факторы обусловливают необходимость повышения уровня информационной безопасности патентно-информационных ресурсов БД ЦИФИС, информационной и обеспечивающей инфраструктуры цифрового органа управления ИС.

Инфраструктура ЦИФИС при этом должна удовлетворять следующим основным требованиям:

Обеспечивать защиту данных ПБД, БД НТИ и ТБД от несанкционированного доступа, преднамеренного или непреднамеренного искажения, разрушения и модификации информации.

Обеспечивать доступность данных по схеме 24часа*365дней.

Для обеспечения высокого уровня сохранности данных ПБД, БД НТИ и ТБД должны обладать свойством «самообслуживания», предполагающим возможность самостоятельного восстановления работоспособности БД.

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

Серверное оборудование ЦИФИС 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.

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

Обладать развитой системой диагностики и автоматического информирования о произошедших неполадках.

Цели и задачи обеспечения информационной безопасности ТБД

С учетом сформулированных требований к защите данных первоисточников (ПБД и БД НТИ), а также того факта, что ТБД формируются, как правило, на основании общедоступной опубликованной патентной документации, информации, извлекаемой из открытых библиотечных фондов, архивов, официальных изданий и других открытых источников целями информационной безопасности ТБД являются обеспечение заданного уровня неизменности (имманентности) и доступности данных ТБД, повышение полноты и достоверности данных.

Основными задачами повышения безопасности информационных ресурсов и построения эффективной системы защиты ТБД являются следующие:

– анализ требований тематических запросов пользователей и определение перечня (подмножества) ПБД и БД НТИ ЦИФИС для поиска и извлечения данных при формировании ТБД определенной тематики (тематик);

– анализ требований политики информационной безопасности данных и лицензионных ограничений, установленных владельцами отобранных для поиска ПБД и БД НТИ, запрещающих (ограничивающих) доступ и допуск к данным и их использование, определение показателя доступности данных ПБД и БД НТИ;

– анализ и оценка рисков ИБ ТБД (анализ информационных ресурсов ТБД, анализ функциональных задач и бизнес-процессов использующих ТБД, идентификация угроз безопасности в отношении ресурсов ТБД и уязвимостей существующей в

организации системы защиты, оценка вероятности осуществления угроз, показателей уязвимостей и ущерба, наносимого организации, определение величины рисков ИБ и их ранжирование);

– проектирование оптимальных механизмов защиты структур ТБД на различных уровнях их представления (каноническом, логическом, физическом) с учетом требований доступности ПБД\БД НТИ ЦИФИС и результатов оценки рисков и угроз ИБ;

– построение системы защиты ТБД от несанкционированного доступа, модификации или разрушения данных по критериям эффективности, коррелированным с требованиями защиты данных.

Модели и методы решения этих задач рассмотрены в [1, 3, 4].

При наличии разрешений владельца БД ЦИФИС на доступ к конфиденциальной информации (например, к материалам неопубликованных заявок на изобретения, рукописям научных трудов до их публикации и т.п.) этот доступ регламентируется соответствующими нормативными правовыми документами организаций (например, документом Политика информационной безопасности). Для организации доступа к конфиденциальной информации применяются средства усиленной двухфакторной аутентификации, а также методы протоколирования событий.

Заключение

В работе рассмотрены особенности построения и характеристики тематических БД, играющих важную роль при проведении пользователями патентно-информационных поисков, оказании цифровых услуг в процессе выполнения НИР и ОКР. Разработаны требования к обеспечению информационной безопасности патентной и научно-технической информации, инфраструктуре ЦИФИС. Сформулированы цели и описаны задачи повышения информационной безопасности и защиты ТБД в условиях цифровизации систем управления ИС.

Литература:

1. *Неретин О.П., Кульба В.В., Сиротюк В.О.* Оптимизация структур данных цифровых информационных фондов систем управления интеллектуальной собственностью. – М.: ФИПС, 2023. – 260 с.

2. *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.

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

4. *Сиротюк В.О., Богатырева Л.В.* Построение эффективной системы управления качеством и информационной безопасностью цифровых фондов интеллектуальной собственности / Проблемы управления безопасностью сложных систем: материалы XXX Международной конференции. 14 декабря 2022 г., Москва. – Москва: ИПУ РАН, 2022. – С. 385-393.

DOI: 10.25728/iccss.2023.78.53.052

Клочач Е.В., Ткаченко В.А.

Производственный контроль как элемент управления промышленной безопасностью

Аннотация: Рассмотрен полученный в течение нескольких десятилетий опыт внедрения и функционирования производственного контроля за соблюдением требований промышленной безопасности в организациях, эксплуатирующих опасные производственные объекты. Отмечены факторы, снижающие результативность использования этого инструмента регулирования промышленной безопасности. Предложены пути развития производственного контроля.

Ключевые слова: производственный контроль, управление, промышленная безопасность

С момента вступления в силу Федерального закона «О промышленной безопасности опасных производственных объектов» [1] в 1997 году прошло достаточно времени для того, чтобы провести анализ результативности использования тех или иных элементов управления промышленной безопасностью,