URL: https://www.iso.org/standard/64120.html (дата обращения 10.10.2024).

3. *Голованов В.Б.* Модель зрелости как подход измерения эффективности процессов информационной безопасности // НиКа. – 2006. – URL: https://cyberleninka.ru/article/n/model-zrelosti-kak-podhod-izmereniya-effektivnosti-protsessov-informatsionnoy-bezopasnosti (дата обращения 10.10.2024).

4. CIS Critical Security Controls V7 Measures & Metrics. – URL: https://www.cisecurity.org/insights/white-papers/cis-controls-v7-measures-metrics (дата обращения 10.10.2024).

5. *Слепов А.В., Зефиров С.Л.* Способ риск-ориентированной оценки информационной безопасности организации // Инжиниринг и технологии. – 2018. – Т. 3(2). – С. 32-35.

6. *Егоров И.А., Кондратьев В.Ю.* Методика анализа совокупной стоимости владения (TCO) // Инновации и инвестиции. – 2022. – №11. – URL: https://cyberleninka.ru/article/n/metodika-analiza-sovokupnoy-stoimosti-vladeniya-tco (дата обращения 10.10.2024).

7. *Правиков Д.И., Мурашкин В.А.* Оптимизация процессов управления информационной безопасностью на предприятии ТЭК / Сборник научных трудов Всероссийской научно-технической конференции «Кибернетика и информационная безопасность» «КИБ-2023», Москва, 18-19 октября 2023 года. – Москва: Национальный исследовательский ядерный университет «МИФИ», 2023. – С. 102-103.

Сиротюк В.О.

Решение задач повышения безопасности цифровых систем управления интеллектуальной собственностью

Аннотация: Рассмотрены проблемы обеспечения безопасности и качества патентно-информационных фондов, информационно-технологической инфраструктуры цифровых систем управления интеллектуальной собственностью (ИС), возникающие при решении задач цифровой трансформации традиционных систем

управления ИС. Сформулированы требования к цифровым органам управления ИС. Предложены методы и средства решения задач повышения безопасности цифрового органа управления ИС и цифровой экосистемы патентно-информационной деятельности. Разработанные модели, методы и средства использовались при построении эффективной системы менеджмента безопасности и качества международной патентной организации.

Ключевые слова: цифровая система управления ИС, цифровой информационный фонд ИС, информационная инфраструктура, цифровая экосистема патентно-информационной деятельности, качество данных, информационная безопасность

Введение

Цифровизация управления интеллектуальной собственностью (ИС) предполагает трансформацию традиционной системы управления ИС путем перевода бизнес-процессов патентно-информационной деятельности субъектов системы управления ИС (патентных организаций, научных институтов, библиотек, издательств и др.) на новые (в т.ч. оптимизационные) модели, методы и информационные технологии (ИТ) управления, построение на этой основе цифровой системы управления ИС (ЦСУИС) и цифровой экосистемы (ЦЭС) патентно-информационной деятельности (ПИД). Создание ЦСУИС и ЦЭС ПИД способствуют совершенствованию и развитию изобретательства и предпринимательства, творческой и инновационной деятельности, расширению рынка научно-информационной продукции и услуг, обеспечению надежной защиты прав патентообладателей и интеллектуального суверенитета экономики страны [1-2].

Вместе с тем, их построение несет многочисленные угрозы и риски снижения качества и информационной безопасности (ИБ), что обусловливает необходимость разработки надежных и эффективных методов и средств защиты цифрового информационного фонда ИС (ЦИФИС), информационной и обеспечивающей инфраструктуры ЦСУИС. Должна быть

разработана эффективная система менеджмента безопасности и качества патентно-информационной продукции и услуг ЦСУИС.

В работе рассмотрены проблемы обеспечения безопасности цифровой системы управления ИС. Сформулированы требования и задачи по обеспечению качества и защиты баз данных (БД) ЦИФИС, информационно-технологической инфраструктуры ЦСУИС и предложены методы их решения.

Особенности цифровой трансформации и построения цифровой системы управления ИС

ЦСУИС позволяет перейти к новой парадигме проведения патентных исследований, НИР и ОКР, основанной на предоставлении унифицированного доступа к разнообразным источникам научной, технической и патентной информации, их обработки и использования. Построение эффективного цифрового органа управления ИС осуществляется на принципах клиентоориентированности и омниканальности, оперативного обслуживания запросов пользователей, использования современных ИТ и цифровых платформ для доступа к данным, хранения, обработки и распространения информации.

Разработка ЦСУИС осуществляется с использованием моделей и методов интеллектуального анализа больших данных (Big Data), обеспечивающих обнаружение и обработку новых источников данных; моделей и методов оптимизации информационно-управляющей структуры ЦСУИС и структур БД; сервисных бизнес-моделей, основанных на использовании технологии облачных вычислений и др. [1, 3-4].

Построение ЦСУИС и ЦЭС ПИД предъявляют высокие требования к качеству и защите БД ЦИФИС. От эффективности используемых методов и средств их проектирования, создания и эксплуатации во многом зависит эффективность и качество самих цифровых систем управления ИС и оказываемых ими услуг.

Основные ИТ цифровой системы управления ИС и формализованная методология ее построения

Основными ИТ ЦСУИС, обеспечивающими ее полноценное функционирование, являются следующие [1-3]:

– ИТ электронной подачи дел заявок на объекты ИС;

– ИТ цифрового доступа к БД ЦИФИС;
– ИТ ЦЭС ПИД, обеспечивающих межпроцессную интеграцию данных и систем и управление жизненным циклом патентно-информационной продукции и услуг;
– ИТ электронных платежей;
– ИТ взаимодействия с внешними организациями.

Формализованная методология построения эффективной ЦСУИС включает решение следующих задач [1, 3-5]:

– построение онтологической модели предметной области патентных и научных исследований системы управления ИС;
– формирование спецификаций объектных моделей требований пользователей системы управления ИС;
– построение модели распределенной информационно-управляющей структуры ЦСУИС;
– проектирование оптимальных структур распределенных, локальных и автономных БД ЦИФИС;
– проектирование оптимальных структур тематических БД, формируемых в виде федеративных и облачных БД;
– построение цифровой экосистемы ПИД;
– управление качеством данных БД ЦИФИС;
– обеспечение ИБ и защиты данных БД ЦИФИС;
– построение комплексной системы менеджмента безопасности и качества патентно-информационной продукции ЦСУИС и ее ролевой организационной структуры.

Разработанные базовые ИТ и формализованная методология использовались при проведении работ по цифровой трансформации и построению эффективного цифрового органа управления ИС региональной Евразийской патентной организации (ЕАПО) [1, 3].

Требования, цели и задачи обеспечения информационной безопасности цифровых систем управления ИС

Большую актуальность в условиях цифровой трансформации системы управления ИС приобретают вопросы обеспечения ИБ организаций – субъектов системы управления ИС, допускающих возможность работы отдельных ее сотрудников в режиме удаленного доступа. Учитывая, что в этом режиме сотрудники с помощью мобильных устройств получают доступ к информационно-вычислительным ресурсам организации, находясь

вне защищаемого периметра, комплексную безопасность можно обеспечить решением задач защиты каналов связи, подключений и информации на мобильном или стационарном устройстве.

Помимо этого, наличие многочисленных гетерогенных источников патентной, научной и технической информации, распределенный характер их хранения в БД большого объема, разнообразие требований, предъявляемых владельцами (провайдерами) информации по ее использованию, и в то же время необходимость логической интеграции данных с целью проведения полноценных патентно-информационных поисков выдвигают проблему повышения качества и защиты данных.

Инфраструктура современного цифрового органа управления ИС должна удовлетворять следующим требованиям:

1. Обеспечивать защиту БД ЦИФИС от несанкционированного доступа, преднамеренного или непреднамеренного искажения, разрушения и модификации информации.
2. Обеспечивать максимальную доступность данных.
3. Функционал ЦИФИС должен содержать средства самообслуживания БД, обеспечивающие возможность самостоятельного восстановления работоспособности БД.
4. Предоставлять удобный интерфейс доступа к локальным и внешним удаленным БД ЦИФИС.
5. Серверное оборудование ЦСУИС должно быть легко масштабируемым по объему хранимой информации и при этом должна обеспечиваться интеграция с существующими компонентами хранилища без перестройки уже развернутого информационного хранилища.
6. Обладать современными средствами поддержания готовности данных, обеспечивать полное резервирование, упреждающий мониторинг, обнаружение и исправление ошибок.
7. Обладать развитой системой диагностики и автоматического информирования о произошедших неполадках.

С учетом рассмотренных требований построение инфраструктуры ЦСУИС должно производиться на основе специализированной цифровой платформы (в т.ч. облачной), аппаратно и программно конфигурируемой и масштабируемой.

Главной целью повышения безопасности и качества ЦИФИС, информационно-технологической инфраструктуры цифрового

органа управления ИС является обеспечение уровня безопасности, соответствующего требованиям и рекомендациям международных стандартов в области управления ИБ и менеджмента качества.

Основными задачами обеспечения безопасности и качества ЦСУИС являются [3-5]:

- защита от вирусов и спама;
- обеспечение работоспособности инфраструктуры ЦСУИС;
- контроль над копированием информации и программ;
- защита конфиденциальных данных от несанкционированного доступа;
- контроль соответствия принятой в организации политике информационной безопасности и качества данных;
- управление рисками в области ИБ;
- выбор контрмер, обеспечивающих требуемый уровень ИБ;
- контроль функционирования и аудит системы менеджмента качества и безопасности цифрового органа управления ИС;
- уведомление о случаях нарушения конфиденциальности, целостности и доступности информации.

Построение эффективной системы менеджмента безопасности и качества цифровой системы управления ИС Евразийского патентного ведомства (ЕАПВ)

Комплексное решение поставленных в работе задач повышения защищенности и качества данных, информационно-технологической инфраструктуры осуществляется в рамках построения единой системы менеджмента безопасности и качества (СМБК) патентно-информационной продукции ЦСУИС с назначенными ролями и функциональными обязанностями служащих организации. Построение СМБК ЕАПВ осуществляется на основе разработанных моделей, методов и инструментальных средств управления качеством данных и информационной безопасностью, предложенных в [1, 4-5].

Область действия СМБК ЕАПВ охватывает восемь основных бизнес-процессов, связанных с производственно-хозяйственной и информационно-технологической деятельностью организации:

- обработка входящей информации по объектам ИС;
- формирование и обслуживание БД ЦИФИС;
- проведение патентно-информационных поисков;

– проведение экспертизы по заявкам на изобретения;
– выполнение НИР и ОКР;
– выдача охранных документов на объекты ИС;
– публикация информации по заявкам и патентам;
– сопровождение опубликованных документов на объекты ИС.

В соответствии с международными стандартами в ЕАПВ используется ролевая организационная структура СМБК. Каждая роль сопровождает определенные процессы управления качеством и ИБ и оснащена соответствующими инструментальными средствами и ИТ. Выделяются следующие основные роли:

– представитель руководства ЕАПВ (советник президента ЕАПВ);
– менеджер данными (сотрудник управления ИТ);
– администратор данных (сотрудники отделов ИПС, стандартизации и управления качеством данных);
– специалист по обработке и непрерывности данных (сотрудник отдела подготовки и публикации патентной информации);
– специалист по управлению ИБ (сотрудник отдела информационной и обеспечивающей инфраструктуры);
– специалист по управлению информационными технологиями (сотрудник управления ИТ);
– владелец информационного актива (сотрудники экспертных и публикационных подразделений по принадлежности);
– владелец технологического бизнес-процесса (сотрудники отдела делопроизводства, отделов экспертизы, публикационного отдела по принадлежности);
– внутренний аудитор СМБК (сотрудники отдела организационно-правового управления и управления ИТ по принадлежности).

Заключение

В работе рассмотрены проблемы, цели и задачи обеспечения безопасности цифровых систем управления интеллектуальной собственностью, возникающие на этапе их цифровой трансформации. Определены базовые ИТ цифровой системы управления ИС и приведена формализованная методология построения цифрового органа. Сформулированы требования по

обеспечению безопасности ЦИФИС, информационно-технологической инфраструктуры цифрового органа управления ИС. Предложены методы и комплекс мероприятий для решения задач повышения безопасности и качества ЦСУИС. Рассмотрено построение эффективной ролевой системы менеджмента безопасности и качества патентно-информационной продукции цифрового органа управления Евразийского патентного ведомства.

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.* Концептуальные основы цифровизации системы управления интеллектуальной собственностью // Вестник ФИПС. – 2023. – Т. 2, №1 (3). – С. 32-35.

3. *Кульба В.В., Сиротюк В.О.* Основные положения по созданию эффективной цифровой системы управления интеллектуальной собственностью в евразийском регионе / Материалы XIV Всероссийского совещания по проблемам управления (ВСПУ-2024). Москва, 17-20 июня 2024 г. – М.: ИПУ РАН, 2024. – С. 3176-3180.

4. *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.

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