III. Проблемы обеспечения информационной безопасности

Сиротюк В.О.

Цели, задачи и принципы обеспечения безопасности цифровых систем управления интеллектуальной собственностью

Аннотация: В работе рассмотрены особенности и характеристики систем управления интеллектуальной собственностью (ИС) в условиях их цифровой трансформации, описаны объекты ИС, угрозы и риски информационной безопасности объектов ИС. Сформулированы цели, задачи и принципы обеспечения информационной безопасности цифровых систем управления ИС. Предложенные принципы и задачи использовались при разработке мероприятий по обеспечению информационной безопасности системы управления ИС международной патентной организации.

Ключевые слова: система управления ИС, объект интеллектуальной собственности, база данных патентной информации, база данных научно-технической информации, угроза информационной безопасности, риск информационной безопасности, система информационной безопасности

Введение

Становление цифровой экономики является одним из приоритетных направлений научно-технического прогресса [1]. Переход к цифровой экономике предполагает цифровую трансформацию традиционных систем управления предприятиями и организациями или целой экономической отрасли на основе использования новых (в т.ч. формальных) моделей бизнес-процессов, менеджмента и способов производства и их оптимизации, применения современных информационно-телекоммуникационных (цифровых) технологий.

Под влиянием новой цифровой парадигмы происходят радикальные изменения в организации и методах проведения

научных исследований и опытно-конструкторских работ. Научное сообщество переходит к новой концепции проведения научных исследований и разработок, основанной на возможности доступа к разнообразным распределенным источникам научной, технической и патентной информации, их обработки и использования, интеллектуального анализа Больших Данных (Big Data) в различных предметных областях.

Цифровая трансформация системы управления интеллектуальной собственности (ИС) позволяет повысить эффективность и качество работы патентных и научных организаций, перейти на новые бизнес-модели и методы управления, избавить сотрудников от рутинных работ и повысить производительность труда и конкурентоспособность организаций. Цифровизация информационных фондов ИС, создание баз данных патентной и научно-технической информации, повышение их полноты, качества, защищенности и доступности является важной и актуальной задачей, решаемой в рамках перехода к цифровой экономике в одной из важных ее отраслей – управление ИС [2].

В работе рассмотрены характеристики системы управления ИС, особенности ее цифровой трансформации и связанные с этим угрозы и риски информационной безопасности объектов ИС; сформулированы цели и принципы информационной безопасности объектов ИС от преднамеренного или непреднамеренного несанкционированного доступа, модификации или разрушения данных; предложен перечень задач обеспечения информационной безопасности цифровой системы управления ИС.

Характеристики системы управления ИС. Угрозы, риски и уязвимые элементы информационной безопасности

Система управления ИС обеспечивает регистрацию, экспертизу и выдачу охранных документов, сопровождение, хранение и охрану объектов ИС с помощью патентов, авторского права и товарных знаков, что позволяет авторам добиваться признания или получать финансовое вознаграждение за свои изобретения или произведения. Обеспечивая баланс интересов изобретателей и широкой публики, система управления ИС способствует созданию условий для развития творчества и инноваций.

Объектами ИС являются результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации юридических лиц, товаров, работ, услуг и предприятий, которым предоставляется правовая охрана. К объектам ИС относятся изобретения, промышленные образцы, полезные модели, литературные, художественные и научные произведения, символика, названия и изображения, используемые в коммерческих целях. ИС охватывает широкий спектр деятельности и играет важную роль в научной, образовательной, культурной и хозяйственной жизни.

Цифровая трансформация традиционной системы управления ИС приводит к построению цифрового органа управления ИС. Эффективная цифровая система управления ИС должна создаваться на принципах и моделях клиентоориентированности и омниканальности, максимизации эффективности обслуживания запросов пользователей. Одной из главных функций цифровой системы управления ИС является формирование, сопровождение и развитие баз данных патентной (ПБД) и научно-технической информации (БД НТИ), информационного поиска по фондам патентной документации и научно-технической литературы.

ПБД и БД НТИ содержат уникальную информацию по различным аспектам научно-технических, экономических, социальных, культурных и других видов знаний, которая используется при выполнении НИР и ОКР, проведении экспертизы работ, принятии решений по приоритетным направлениям научно-технологического развития и в других областях человеческой деятельности. С учетом наличия многочисленных разрозненных источников научно-технической и патентной информации инфраструктура цифровой системы управления ИС должна иметь распределенную структуру и обеспечивать оперативный доступ к локальным и внешним удаленным ПБД и БД НТИ и поиск информации через единый пользовательский интерфейс [2,3].

Цифровизация системы управления ИС, несмотря на все ее преимущества, несет потенциальные угрозы и риски информационной безопасности объектов ИС, поэтому возрастает потребность в надежных и эффективных методах и средствах защиты данных ПБД и БД НТИ, информационной и обеспечивающей инфраструктуры цифрового органа ИС [3].

Основными угрозами безопасности объектов ИС являются [4]:

- раскрытие конфиденциальной информации (кража информации, несанкционированный доступ, копирование данных),
- компрометация информации (внесение несанкционированных изменений в массивы данных и БД),
- несанкционированный обмен информацией,
- отказ от информации (непризнание получателем или отправителем фактов получения/отправки информации),
- отказ в обслуживании (отсутствие доступа к информации).

Уязвимыми элементами цифрового органа управления ИС являются содержимое БД, программное обеспечение, оборудование, пользователи, администраторы данных, документация.

Возможными путями утечки информации об объектах ИС могут быть:

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

Цели и принципы обеспечения информационной безопасности цифровой системы управления ИС

Главной целью информационной безопасности (ИБ) цифровой системы управления ИС является обеспечение конфиденциальности, достоверности, неизменности и доступности информационных материалов объектов ИС.

Частными целями и задачами защиты информации об объектах ИС могут быть:

– обеспечение заданного уровня безопасности ПБД и БД НТИ, соответствующего принятым нормативным документам;

– обеспечение экономической целесообразности при выборе защитных мер, основанном на анализе рисков ИБ;

– обеспечение высокого уровня безопасности информационной и обеспечивающей инфраструктуры цифрового органа управления ИС;

– обеспечение регистрации всех действий пользователей с информацией и ресурсами ПБД и БД НТИ;

– обеспечение эффективного анализа регистрационной информации, предоставление пользователям достаточной информации для поддержания режима безопасности;

– разработка планов восстановительных работ после аварий и иных критических ситуаций с целью обеспечения непрерывной работы цифровой системы управления ИС;

– обеспечение строгого соответствия нормативным актам и политике информационной безопасности.

Основными принципами обеспечения информационной безопасности цифровой системы управления ИС являются [3]:

1. *Принцип невозможности «обхода» средств защиты данных.* Означает, что все информационные потоки и пути доступа к данным должны контролироваться средствами защиты.

2. *Принцип слабого звена.* Предполагает в первую очередь усиление с точки зрения безопасности наиболее уязвимых элементов системы.

3. *Принцип гарантированного выполнения функций.* Означает, что при любых обстоятельствах (в том числе нештатных), система защиты информации должна полностью выполнять свои функции, либо полностью блокировать все возможные пути доступа.

4. *Принцип минимизации привилегий.* Предполагает выделение пользователям и администраторам системы только тех прав, которые необходимы им для выполнения служебных обязанностей.

5. *Принцип разделения обязанностей.* Предполагает при распределении прав и ответственности пользователей системы исключение возможности нарушения критически важных для системы функций и процессов одним человеком.

6. *Принцип многоуровневой защиты.* Гарантирует многоуровневую структуру систем обеспечения информационной безопасности с целью повышения ее надежности и эффективности.

7. *Принцип разнообразия средств защиты.* Предполагает одновременное использование различных по своей природе и принципам действия механизмов и методов защиты данных.

8. *Принцип простоты и управляемости.* Предполагает возможность анализа эффективности и доказательства корректности реализации функций автоматизированной системы в целом и используемых механизмов защиты.

9. *Принцип открытости.* Требует разработки комплекса организационных мер, направленных на обеспечение лояльности персонала, его обучение и повышение квалификации при работе с системой, разъяснения прав и обязанностей каждого пользователя.

10. *Принцип непрерывности защиты.* Означает, что информационная безопасность системы управления ИС должна обеспечиваться на всех стадиях жизненного цикла информационных систем.

11. *Принцип избирательного управления доступом.* Средства защиты должны контролировать доступ пользователей к объектам ИС.

Основные задачи информационной безопасности цифровой системы управления ИС

Исходя из необходимости обеспечения требований конфиденциальности, неизменности, достоверности и доступности информации ПБД и БД НТИ, основными задачами информационной безопасности (ИБ) цифровой системы управления ИС являются:

- определение границ системы ИБ;
- распределение обязанностей по обеспечению ИБ;
- подготовка персонала по поддержанию режимов ИБ;
- уведомление о случаях нарушения защиты;
- защита информации ПБД и БД НТИ от вирусов и спама;
- контроль копирования информации ПБД и БД НТИ;
- защита конфиденциальной информации от несанкционированного доступа;
- контроль соответствия принятой политике ИБ;
- управление рисками в области ИБ;
- выбор контрмер, обеспечивающих требуемый уровень ИБ;
- контроль функционирования и аудит системы ИБ.

Заключение

В работе сформулированы цели, принципы и задачи построения эффективной системы информационной безопасности цифровых систем управления ИС. Полученные результаты использовались при подготовке комплекса организационных, технических,

структурных и процедурных мероприятий по построению эффективной системы управления информационной безопасностью Евразийского патентного ведомства – международной региональной патентной организации [2,3].

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. Программа «Цифровая экономика Российской Федерации». Утверждена распоряжением Правительства Российской Федерации от 28 июля 2017 г. № 1632-р. – URL: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf (дата обращения 14.10.2021).

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., Грузман В.А., Косяченко С.А.* Структура и характеристики объектов информационной безопасности и классификация информационных ресурсов / Материалы XXVIII Международной конференции «Проблемы управления безопасностью сложных систем» (ПУБСС-2020) (16 декабря 2020 г. Москва). – М.: ИПУ РАН, 2020. – С. 446-451.