DOI: 10.25728/iccss.2023.77.30.025

Сиротюк В.О.

Управление информационной безопасностью евразийского экспертно-информационного пространства

Аннотация: Выявлены проблемы и сформулированы цели защиты патентно-информационных ресурсов Евразийского экспертно-информационного пространства (ЕАЭИП). Рассмотрены задачи построения эффективной системы управления информационной безопасностью (СУИБ) патентно-информационных фондов ЕАЭИП. Приведен опыт практического использования предложенных методов и средств управления информационной безопасностью при построении СУИБ ЕАЭИП.

Ключевые слова: евразийское экспертно-информационное пространство, информационная безопасность, защита данных

Введение

Как известно [1, 2], Евразийская патентная система предоставляет возможность физическим и юридическим лицам защитить права на свои изобретения на основе единого евразийского патента, действующего на территории 8 государств-участников Евразийской патентной конвенции (ЕАПК) – Туркменистана, Республики Беларусь, Республики Таджикистан, Российской Федерации, Республики Казахстан, Азербайджанской Республики, Кыргызской Республики и Республики Армения. Пользователями Евразийской патентной системы являются заявители более чем из 80 стран мира.

Образование Евразийской патентной организации (ЕАПО) и ее исполнительного органа – Евразийского патентного ведомства (ЕАПВ) – дало возможность для формирования единого евразийского экспертно-информационного пространства (ЕАЭИП) с целью обеспечения экспертов ЕАПВ и национальных патентных ведомств (НПВ), а также заинтересованных лиц полной и качественной патентной и научно-технической информацией. В

своем современном виде ЕАЭИП представляет собой логически интегрированную и физически распределенную совокупность мировых, региональных и национальных патентных информационных фондов (ПИФ), организованных виде соответствующих баз данных (БД), а также функциональных средств доступа к БД, поиска в них, обработки и формирования тематических БД. На евразийском пространстве сложилась эффективная система рабочих и экспертных контактов между НПВ и ЕАПВ. Экспертам ведомств и пользователям из ведущих ВУЗов и публичных библиотек предоставляется доступ к БД ПИФ ЕАЭИП на базе российской (PatSearch) и евразийской (ЕАПАТИС) информационно-поисковых систем.

Цифровизация Евразийской патентной системы несет потенциальные угрозы и риски ее информационной безопасности (ИБ), поэтому возрастает потребность в надежных и эффективных методах и средствах защиты данных, информационных систем, цифровых технологий и информационной инфраструктуры ЕАЭИП, обеспечения их сохранности и восстановления в случае сбоев [3, 6].

В работе рассмотрены проблемы и задачи обеспечения информационной безопасности ЕАЭИП, предложены методы построения эффективной системы управления информационной безопасностью ЕАЭИП.

Проблемы и цели информационной безопасности ЕАЭИП

Предоставление свободного доступа к патентно-информационным ресурсам ЕАЭИП коллективам пользователей выдвигает проблему обеспечения требуемого уровня защиты данных от преднамеренного или непреднамеренного несанкционированного доступа, модификации или разрушения данных [4, 5].

Основными угрозами безопасности объектов ЕАЭИП являются:

- 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).

В условиях цифровизации Евразийской патентной системы большую актуальность приобретают также вопросы обеспечения ИБ организаций-субъектов ЕАПО, связанных с возможностью работы отдельных сотрудников организаций (экспертов ведомств, ученых, исследователей) в режиме удаленного доступа. При таком режиме работы сотрудники с помощью мобильных устройств получают доступ к локальной сети организации, информационным ресурсам, системам и средствам автоматизации, возможность проводить телеконференции, совещания, находясь вне защищаемого периметра, что, в свою очередь, приводит к увеличению рисков (инцидентов) ИБ [3, 4, 6].

В таких условиях высокий уровень информационной безопасности можно обеспечить путем построения комплексной системы защиты БД ПИФ ЕАЭИП, информационной и обеспечивающей инфраструктуры ЕАЭИП.

Стратегическими целями безопасности патентно-информационных ресурсов (активов) ЕАЭИП являются:

- обеспечение конфиденциальности материалов заявок на изобретение;
- обеспечение восстановления автоматизированных информационных систем и бизнес-процессов после аварий;
- обеспечение контроля выполнения всех требований по ИБ и эффективности работы мер по защите;
- обеспечение осведомленности служащих в вопросах ИБ;
- обеспечение соответствия правовым и нормативным требованиям Российской Федерации (как места нахождения штаб-квартиры ЕАПО) в области защиты информации;
- обеспечение соответствия договорным обязательствам с заявителями и их представителями (патентными поверенными).

Частными целями защиты БД ПИФ ЕАЭИП могут быть [3, 4]:

– обеспечение уровня безопасности, соответствующего принятым нормативным документам ведомства;

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

– обеспечение заданного уровня безопасности информационной и обеспечивающей инфраструктуры ЕАЭИП;

– обеспечение регистрации всех действий пользователей с информацией и ресурсами;

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

– выработка планов восстановления после аварий и иных критических ситуаций для всех функциональных областей с целью обеспечения непрерывности работы сети;

– обеспечение строгого соответствия нормативным актам и политике информационной безопасности организации.

Для достижения данных целей в организации – владельце ПИФ ЕАЭИП (ЕАПВ, НПВ) разрабатывается и внедряется система управления информационной безопасностью (СУИБ). Построение эффективной СУИБ проводится на основе использования формализованной методологии, предложенной в [3-5], а также с учетом положений, требований и рекомендаций международного стандарта в области ИБ ISO/IEC 27001:2013 [5].

Для поддержания патентной информации в защищенном состоянии адекватно существующим угрозам безопасности должны регулярно проводиться мероприятия по инвентаризации и классификации (реклассификации) информационных ресурсов ЕАЭИП, оценке полноты и достоверности БД, оценке рисков и угроз информационной безопасности объектов ПИФ, уязвимых элементов и путей утечки информации об объектах ПИФ ЕАЭИП.

Задачи и мероприятия по построению эффективной системы управления информационной безопасностью патентно-информационных фондов ЕАЭИП. Методы защиты данных

Исходя из необходимости обеспечения требований конфиденциальности, неизменности, достоверности и доступности информации, основными задачами информационной безопасности ПИФ ЕАЭИП являются:

– определение сферы (границ) СУИБ;

– распределение обязанностей по обеспечению ИБ;

– обучение и подготовка персонала по поддержанию режимов информационной безопасности;

– уведомление о случаях нарушения защиты;

– защита от вирусов и спама;

– планирование бесперебойной работы организации;

– контроль над копированием информации и программ;

– защита документации организации;

– защита данных (особенно конфиденциальных) от несанкционированного доступа;

– контроль соответствия принятой политике ИБ;

– управление рисками в области ИБ;

– выбор контрмер, обеспечивающих требуемый уровень ИБ;

– контроль за функционированием и аудит системы обеспечения информационной безопасности.

Первоочередными мерами по созданию СУИБ ЕАЭИП являются следующие [3-6]:

1. Создание рабочей группы (подразделения) по ИБ.

Рабочая группа (подразделение) создается из специалистов ЕАПВ и НПВ для координации, планирования, организации и проведения работ по обеспечению информационной безопасности БД ПИФ ЕАЭИП, выбору методов и средств защиты данных, приобретению соответствующих аппаратно-программных средств.

2. Определение сферы (границ) СУИБ.

Описание сферы (границ) СУИБ ЕАЭИП должно включать: описание оргструктур организаций-субъектов ЕАПО и изменений, которые предполагается внести в них в связи с внедрением и модернизацией информационных систем и ИТ; схему размещения оборудования информационной и поддерживающей инфраструктуры ЕАЭИП, описание объектов защиты, описание технологии обработки информации и решаемых задач, описание уязвимых элементов и угроз безопасности, результаты анализа и оценки рисков, т.е. возможных последствий угроз безопасности, описание требований к режимам информационной безопасности.

3. Разработка политики информационной безопасности ведомства.

Разработка политики ИБ является наиболее ответственной и важной задачей при построении СУИБ. Политика ИБ представляет

собой набор формальных правил, которым должны подчиняться лица, получившие доступ к информационным системам, технологиям и информации организации.

4. Разработка нормативных документов в области обеспечения информационной безопасности.

Должны быть разработаны следующие основные нормативные документы: положение о рабочей группе (подразделении) по ИБ, документ Политика информационной безопасности, положение о ПИФ ЕАЭИП; должностные инструкции служащих и др. [5].

5. Разработка планов восстановительных работ.

Планы восстановительных работ должны быть направлены на ликвидацию последствий угроз информационной безопасности.

6. Обеспечение антивирусной защиты.

7. Обеспечение физической защиты информационных систем и ресурсов.

Безопасность систем, инфраструктуры и ресурсов ЕАЭИП в значительной степени зависит от физического окружения, в котором они функционируют и используются. Физическая защита предполагает не только отражение попыток несанкционированного доступа, но и предохранение от вредных влияний окружающей среды, таких, как жара, холод, влага, магнетизм.

Рассмотрим методы и средства защиты данных и систем.

Множество существующих методов защиты патентно-информационных ресурсов ЕАЭИП включают в себя организационные, процедурные, структурные, аппаратные и программные методы [4, 5]. Кратко рассмотрим их особенности и характеристики.

Организационные методы защиты используются для ограничения числа лиц, которые получают право доступа в помещение центра обработки данных (ЦОД). Эти меры включают организацию режима доступа в ЦОД, а также к терминалам, мероприятия по обеспечению надежного хранения носителей информации, регламентируют технологические схемы обработки защищаемой информации, процесс взаимодействия пользователей с системой, задачи и обязанности обслуживающего персонала ЦОД и пользователей БД и т.д.

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

соответствующие разрешения. Реализация процедурных методов защиты обеспечивается установлением паролей пользователей и терминалов, грифов секретности данных, созданием физических ограждений, а рост их эффективности достигается путем соответствующего обучения и повышения уровня ответственности персонала.

Структурные методы защиты применяются на этапах проектирования БД ПИФ ЕАЭИП. Они обеспечивают такую структуризацию данных БД, которая позволяет повысить уровень защищенности и безопасности 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. Эти устройства отличаются высокой надежностью исполнения функций идентификации, но при этом имеют высокую стоимость. Широко используются аппаратные средства в системе охраны территории и помещений ЦОД. Криптографическая защита информации может быть реализована также с помощью специальной аппаратуры шифрования или кодирования.

Программные методы играют важную роль при создании эффективных систем защиты информационных ресурсов БД от несанкционированного доступа. Программные методы защиты реализуются путем включения разработанных программных средств в состав используемых операционных систем и СУБД, либо выделения их в специальные самостоятельные пакеты программ. Программные методы защиты могут поддерживать различные стратегии разграничения доступа пользователей к ресурсам БД.

Методы и средства защиты информации характеризуются определенными технико-экономическими показателями. К основным характеристикам методов защиты относятся затраты на их разработку и эксплуатацию, безопасное время, под которым понимается математическое ожидание времени раскрытия метода защиты путем опробования множества возможных вариантов проникновения. Безопасное время может служить оценкой эффективности метода защиты.

Опыт практического построения СУИБ ЕАЭИП

Разработанная и внедренная в ЕАПВ в промышленную эксплуатацию СУИБ обеспечивает высокий уровень информационной безопасности БД ПИФ ЕАЭИП, информационной и обеспечивающей инфраструктуры ЕАЭИП [3-5].

Основными задачами, решаемыми СУИБ ЕАЭИП, являются: защита БД ПИФ; восстановление автоматизированных информационно-управляющих систем; обеспечение контроля выполнения требований к ИБ и осведомленности служащих ЕАПВ в вопросах ИБ; обеспечение соответствия правовым и нормативным требованиям Российской Федерации в области ИБ, как страны пребывания штаб-квартиры ЕАПО; обеспечение выполнения обязательств перед заявителями и их представителями.

В рамках функционирования СУИБ регулярно проводятся мероприятия по инвентаризации и классификации информационных активов ПИФ ЕАЭИП, производится оценка рисков ИБ, разработан пакет документации, регламентирующий функционирование СУИБ (Политика ЕАПВ в области ИБ и документы, регламентирующие требования к ИБ). Все документы СУИБ в обязательном порядке доводятся до сведения служащих ЕАПВ.

СУИБ ПИФ ЕАЭИП является неотъемлемой составляющей (подсистемой) Евразийской патентной системы со встроенными в нее функциями, обязанностями и ролями служащих по обеспечению надлежащего уровня информационной безопасности.

Основными ролями СУИБ являются: представитель руководства ЕАПВ, председатель рабочей группы по ИБ (РГБ); специалист по управлению ИТ; специалист по управлению ИБ; владелец актива; владелец процесса; специалист по обеспечению непрерывности деятельности; специалист по обеспечению физической безопасности; внутренний аудитор СУИБ [4, 5].

Область действия СУИБ ЕАПВ охватывает следующие подпроцессы основного технологического бизнес-процесса функционирования региональной евразийской системы управления интеллектуальной собственностью: обработка входящей информации (материалов) по евразийским заявкам (цифровизация данных); проведение формальной экспертизы; проведение экспертизы по существу; обеспечение публикаций; выдача

евразийского патента; поддержание патента, регистрация изменений правового статуса патента; формирование и развитие БД ПИФ ЕАЭИП; предоставление патентно-информационных услуг.

Важное место в СУИБ ЕАЭИП отводится методам и мероприятиям обеспечения физической сохранности дел евразийских заявок и евразийских патентов в цифровой форме, надежного и длительного хранения данных. Эти задачи решаются путем организации и проведения резервного копирования данных и их восстановления при необходимости из резервных копий, что обеспечивает высокую доступность информации ПБД ЕАПВ.

Заключение

В работе рассмотрены особенности построения и характеристики евразийского экспертно-информационного пространства, выявлены проблемы информационной безопасности патентно-информационных фондов ЕАЭИП. Сформулированы цели и задачи обеспечения безопасности патентной и научно-технической информации ПИФ ЕАЭИП, построения эффективной системы управления информационной безопасностью ЕАЭИП. Разработанная СУИБ, ее ролевая структура и комплекс взаимосвязанных методов, мероприятий, нормативно-методических документов и инструментальных средств обеспечивает высокий уровень доступности и защиты данных БД ЕАЭИП, безопасности информационной и обеспечивающей инфраструктуры ЕАЭИП.

Литература:

1. *Григорьев А.Н.* Евразийская патентная организация в документах и лицах. – М.: Изд. дом «Городец», 2023. – 304 с.

2. *Ивлиев Г.П.* Евразийская патентная система: возможности и перспективы // Инженер. Наука, Техника. Производство. Образование. – 2022. – № 11. – С. 2-6.

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

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.

6. *Сиротюк В.О.* Цели, задачи и принципы обеспечения безопасности цифровых систем управления интеллектуальной собственностью / Проблемы управления безопасностью сложных систем: материалы XXIX Международной конференции. 15 декабря 2021 г., Москва. – Москва: ИПУ РАН, 2021. – С. 182-188.

DOI: 10.25728/iccss.2023.99.45.026

Чубуков М.А., Коровин А.С., Хабибулин Р.Ш.

Классификация программного обеспечения, направленного на работу с данными, используемыми при предотвращении и ликвидации чрезвычайных ситуаций

Аннотация: В работе приводятся некоторые результаты обзора специализированного программного обеспечения (СПО), работающего с информацией, связанной с обеспечением управленческих функций, направленных на мониторинг, предотвращение и ликвидацию чрезвычайных ситуаций (ЧС). Рассматриваются критерии поиска программ для ЭВМ, обеспечивающих указанные функции при ЧС, анализ количества типов программного обеспечения по различным характеристикам, позволяющим выделять специфические особенности и функционал данных программ.

Ключевые слова: специализированное программное обеспечение, мониторинг, управление, чрезвычайные ситуации

В настоящее время современные системы поддержки принятия решений (СППР) состоят из специализированного программного обеспечения (СПО) с различным функционалом [1-3]. Данное исследование представляет собой анализ имеющегося СПО, работающего с информацией, связанной с чрезвычайными