Сиротюк В.О.

Разработка эффективной системы управления безопасностью патентных организаций

Аннотация: В работе рассмотрены требования, цели и задачи построения эффективной системы управления информационной безопасностью (СУИБ) патентной организацией. Предложена ролевая структура СУИБ, рассмотрен перечень основных нормативных документов, регламентирующих правила и процедуры обеспечения эффективной защиты патентных информационных ресурсов.

Ключевые слова: патентная информация, система управления информационной безопасностью, защита данных, конфиденциальность данных, неизменность данных, достоверность данных, доступность данных, патентная база данных, система защиты патентной информации.

Введение

Патентные организации с каждым годом расширяют свое информационное представительство, как в регионе, стране, так и в мировом патентном информационном пространстве, наращивают свой информационный потенциал, переходят на безбумажные технологии работы, совершенствуют информационные и поисковые системы, расширяют электронное взаимодействие с внешними организациями [1]. Вместе с этим возрастают потенциальные угрозы и риски информационной безопасности организаций и, как следствие этого, возрастает потребность в надежных и эффективных методах и средствах защиты патентных баз данных (ПБД), информационных систем, информационной и обеспечивающей инфраструктуры, обеспечения их сохранности и восстановления в случае сбоев, в основе которых должна лежать сбалансированная и эффективная система управления информационной безопасностью (СУИБ) [1, 2].

В работе рассмотрены предпосылки и требования по созданию СУИБ, цели и задачи создания СУИБ, ролевая структура СУИБ, нормативно-методическое обеспечение СУИБ.

Основные предпосылки создания и требования по формированию эффективной СУИБ патентной организации

Основными предпосылками создания и требованиями по формированию эффективной СУИБ патентной организации являются следующие:

1. Несоблюдение требований конфиденциальности, неизменности, достоверности и доступности информационных ресурсов и активов патентной организации при наличии потенциальных угроз безопасности может нарушить нормальный режим ее функционирования и, тем самым, подорвать ее репутацию.

2. Часть представленной в патентном фонде информации, например, материалы заявок на изобретения до их публикации, носит конфиденциальный характер, доступ к которой должен быть ограничен и строго регламентироваться соответствующими правилами и процедурами. Другая часть информации является открытой, но ее значительные объемы требуют специальных мер по обеспечению сохранности, достоверности и доступности данных.

3. Количество пользователей патентной информации неуклонно растет. Вместе с тем наибольшую опасность для организации, как показывает мировая практика, представляют свои сотрудники, которые неумышленными или умышленными действиями приводят к нарушению ИБ. Поэтому эффективная СУИБ должна строиться на основе надежной и проверенной практикой информационной и обеспечивающей инфраструктуры, обеспечивающей интеграцию информационных технологий и систем (ИТ и ИС соответственно), централизованное управление пользователями и политиками доступа к ресурсам.

4. К различным ИС и ИТ организации могут предъявляться различные требования по обеспечению их ИБ и надежности функционирования.

5. В области ИБ существует ряд международных и национальных стандартов, которые должны в обязательном порядке учитываться и использоваться при разработке СУИБ.

6. При построении СУИБ должен использоваться комплексный подход, включающий меры следующих видов:

– нормативные (нормативные акты, стандарты, требования, технические условия, положения, регламенты, инструкции и т.п.);

– административные (действия общего характера, предпринимаемые руководством организации);

– процедурные (меры безопасности, реализуемые служащими организации);

– аппаратно-программные (конкретные технические меры).

7. Затраты на создание СУИБ не должны превышать риски, связанные с потерей информации и восстановлением ПБД, ИС, ИТ и инфраструктуры патентной организации.

8. Эффективная СУИБ патентной организации должна быть распределенной – подразделение, ответственное за сбор, хранение, передачу, обработку, предоставление и распространение той или иной информации, сопровождение ИС и ИТ должно самостоятельно разрабатывать предложения по обеспечению ее безопасности и использовать соответствующие методы и средства защиты в соответствии с принятой в организации политикой ИБ. При этом координацию, планирование и организацию всех работ по ИБ организации, выбору методов и средств защиты данных, приобретению соответствующих аппаратно-программных средств должна осуществлять специальное подразделение по ИБ (СПИБ).

Цели и задачи построения СУИБ патентной организации

Создание эффективной СУИБ требует для ее решения сочетания законодательных, нормативно-правовых, организационных и программно-технических мер. Основные задачи администрации организации при этом состоят в выработке политики информационной безопасности с учетом специфики в области действия СУИБ, назначении и распределении функций в области ИБ, доведении основных положений политики безопасности до служащих организации, расстановке и повышении квалификации кадров, обеспечении надлежащего аудита.

Главной целью СУИБ патентной организации является обеспечение конфиденциальности материалов заявок на изобретения, а также достоверности, доступности, неизменности и конфиденциальность информационных активов патентной организации, в том числе персональных данных служащих.

Основными задачами СУИБ патентной организации являются:

– обеспечение мер защиты информационных активов организации, основанных на анализе рисков ИБ;

– обеспечение восстановления ИС и ИТ после аварий в соответствии с установленными требованиями организации;

– обеспечение контроля выполнения требований к ИБ и эффективности работы мер по защите информационных активов организации;

– обеспечение осведомленности служащих организации в вопросах ИБ;

– обеспечение соответствия СУИБ требованиям стандартов и рекомендаций в области ИБ;

– обеспечение выполнения обязательств перед заявителями и их представителями с учетом требований стандарта.

Для реализации поставленных целей и задач СУИБ регулярно проводятся мероприятия по инвентаризации и классификации информационных активов патентной организации, производится оценка рисков ИБ и разрабатывается нормативно-правовая документация, регламентирующая функционирование СУИБ.

Политика организации в области информационной безопасности и документы, регламентирующие требования к ИБ, в обязательном порядке доводятся до сведения каждого служащего патентной организации.

Разработка ролевой структуры СУИБ патентной организации

СУИБ патентной организации является неотъемлемой составляющей (подсистемой) общей административной системы управления организации со встроенными в нее функциями и обязанностями служащих по обеспечению надлежащего уровня информационной безопасности.

В целях распределения функций по поддержанию ИБ организации используется ролевая структура СУИБ, которая представляет собой иерархию ролей по ИБ, минимально достаточную для поддержания работоспособности СУИБ ее соответствия стандарту по ИБ ISO/IEC 27001:2013.

Роли ИБ распределяются по служащим организации либо непосредственно выделенным для выполнения задач СУИБ сотрудникам (например, СПИБ), либо в качестве дополнительных обязанностей к уже имеющимся у служащих организации.

В рамках СУИБ выделяются следующие роли:

- руководство ЕАПВ;
- председатель СПИБ;
- 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.

Назначение и область действия каждой роли описаны в [2].

Нормативно-методическое обеспечение СУИБ патентной организации

Перечень нормативных документов и записей СУИБ патентной организации устанавливает состав, уровень, название и обозначение документации по ИБ. Состав документации должен быть достаточным для обеспечения соответствия требованиям международного стандарта по ИБ ISO/IEC 27001:2013.

В целях обеспечения внедрения и реализации СУИБ в патентной организации разрабатываются следующие нормативно-правовые документы (полный перечень документов и их содержание приведен в работе [2]):

1. Стратегия в области информационной безопасности.
2. Классификатор информации.
3. Перечень конфиденциальной информации.
4. Область действия СУИБ.
5. Управление ролями в области информационной безопасности.
6. Управление рисками информационной безопасностью.
7. Руководство по управлению информационной безопасностью.
8. Показатели результативности процессов СУИБ.
9. Технические и организационные меры обеспечения ИБ.
10. Процедура проведения аудитов СУИБ.

Заключение

В работе рассмотрены требования по созданию эффективных систем управления информационной безопасностью патентных организаций, цели и задачи построения СУИБ, ролевая структура системы, нормативно-методическое обеспечение функционирования СУИБ в патентных организациях. Разработанные методы и документы использовались при построении СУИБ региональной патентной организации – Евразийского патентного ведомства [1, 2].

Литература:

1. *В.О. Сиротюк.* Проблемы и задачи обеспечения информационной безопасности патентно-информационных ресурсов // Патентная информация сегодня. – 2012. – №1. – С. 3-10.

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