Интернет-журнал «Науковедение» ISSN 2223-5167 https://naukovedenie.ru/

Том 9, №6 (2017) https://naukovedenie.ru/vol9-6.php

URL статьи: https://naukovedenie.ru/PDF/06TVN617.pdf

Статья опубликована 02.12.2017

Ссылка для цитирования этой статьи:
Сиротюк В.О. Модели, методы и средства разработки и внедрения эффективной системы управления информационной безопасностью патентного ведомства // Интернет-журнал «НАУКОВЕДЕНИЕ» Том 9, №6 (2017) https://naukovedenie.ru/PDF/06TVN617.pdf (доступ свободный). Загл. с экрана. Яз. рус., англ.

УДК 62

Сиротюк Владимир Олегович
ФГБУН «Институт проблем управления им. В.А. Трапезникова Российской академии наук», Россия, Москва[1]
Ведущий математик
Доктор технических наук, доцент
E-mail: vsirotyuk.55@icloud.com

Модели, методы и средства разработки и внедрения эффективной системы управления информационной безопасностью патентного ведомства

Аннотация. В статье рассмотрены теоретические и прикладные задачи построения эффективной системы управления информационной безопасностью патентного ведомства на примере региональной патентной организации – Евразийского патентного ведомства Евразийской патентной организации. Предложены формализованные модели и методы описания, анализа и структуризации предметной области системы управления информационной безопасностью патентного ведомства; анализа и оценки рисков информационной безопасности; синтеза эффективных механизмов и системы защиты структур патентных баз данных от несанкционированного доступа. Определена область действия системы управления информационной безопасностью Евразийского патентного ведомства, приведено описание характеристик основных процессов ведомства, входящих в область действия системы управления информационной безопасностью, определены владельцы процессов и требуемые активы для их реализации. Рассмотрены основные положения политики патентного ведомства в области информационной безопасности и защиты патентных информационных ресурсов, информационной и обеспечивающей инфраструктуры патентного ведомства. Приведена ролевая структура системы управления информационной безопасностью, определены роли служащих ведомства в системе информационной безопасности. Рассмотрены вопросы обеспечения резервного копирования и восстановления дел заявок на изобретения и патентов, внедрения системы защиты от утечек конфиденциальной информации, организации и проведения данных работ в патентном ведомстве.

Ключевые слова: региональная международная патентная организация; угроза информационной безопасности; система управления информационной безопасностью; патентная база данных; механизм защиты структур патентных баз данных от несанкционированного доступа; система защиты патентных баз данных; политика

[1] 117997, Москва, ул. Профсоюзная, 65

информационной безопасности; система резервного копирования; система защиты от утечек конфиденциальной информации

Введение

В современных условиях обеспечение информационной безопасности и защиты патентно-информационных ресурсов, информационной и обеспечивающей инфраструктуры патентных ведомств является важной и актуальной задачей. Согласно данным компании InfoWatch[2] по проблемам утечки конфиденциальной информации, в 2016 году по сравнению с 2015 годом число утечек информации в мире выросло на **3,4 %**, число «российских» утечек по сравнению с данными 2015 года выросло на **80 %**. При этом большая часть ставших известными утечек (около **62 %**) происходит не по злому умыслу, а из-за ошибок, невнимательности и небрежности персонала. Основным каналом утечки информации по-прежнему является сеть Интернет (около **70 %**). В Евразийском патентном ведомстве (ЕАПВ) большинство технологических и производственных процессов автоматизировано и выполняется с использованием средств вычислительной и оргтехники. Специфика деятельности ведомства требует также наличия доступа служащих к ресурсам сети Интернет. В то же время такие общедоступные сервисы Интернет, как электронная почта (типа mail.ru, gmail), облачные хранилища данных (Cloud), социальные сети и др. хотя и обеспечивают ряд удобств их пользователям, но так как они предоставляются сторонними организациями, то несут ряд угроз безопасности, в частности, связанных с потерей организацией контроля над хранением, распространением и ограничением доступа к конфиденциальной информации. Эти особенности деятельности патентного ведомства создают следующие основные угрозы информационной безопасности:

- возможность раскрытия конфиденциальной информации (несанкционированный доступ, копирование данных, кража информации) и компрометации информации (внесение несанкционированных изменений в массивы данных и базы данных) вследствие ее хранения в электронной форме в системах хранения данных (как во внутренних, так и в облачных);
- несанкционированное использование служащими облачных хранилищ данных и социальных сетей для передачи информации и обмена данными;
- отказ от информации;
- отказ в обслуживании;
- неразрешенное использование служащими съемных носителей информации (USB-носителей, смартфонов, планшетных устройств) для записи информации.

Решение задачи обеспечения информационной безопасности позволяет ведомствам обеспечить конфиденциальность, достоверность, доступность, неизменность и сохранность патентной информации, предотвратить раскрытие формулы и описания изобретения до проведения патентной экспертизы и публикации заявки, а также повысить надежность функционирования систем и средств сбора, хранения, обработки, передачи и отображения патентной информации [1, 2, 3].

Анализ зарубежных и отечественных методологий, методов и средств обеспечения информационной безопасности и защиты информации, а также процедур и правил в области

[2] Отчет «Исследование утечек конфиденциальной информации в 2016 году» – https://www.infowatch.ru/analytics/reports/17479.

информационной безопасности, содержащихся в соответствующих стандартах[3,4], показывает, что все они носят общий рекомендательный характер и не учитывают специфику и особенности конкретной предметной области. Кроме того, ими практически не обеспечивается получение эффективных проектных решений по созданию системы управления информационной безопасностью (СУИБ) организации. Это не позволяет рассматривать их как эффективный и адекватный инструмент при создании системы информационной безопасности патентного ведомства с его особенностями формирования и использования патентно-информационных ресурсов, информационной и обеспечивающей инфраструктурой [4, 5, 6].

В работе рассмотрен широкий круг проблем и задач обеспечения информационной безопасности патентных ведомств и построения эффективной системы управления информационной безопасностью патентного ведомства на примере региональной международной патентной организации – Евразийского патентного ведомства Евразийской патентной организации (ЕАПВ ЕАПО) [7]. Впервые в отечественной практике создания систем информационной безопасности для патентных ведомств предложена формализованная методология, модели и методы анализа и структуризации предметной области СУИБ патентного ведомства, построения объектной канонической структуры патентной базы данных (ПБД), анализа и оценки рисков информационной безопасности, синтеза оптимальных механизмов защиты структур и системы защиты ПБД от несанкционированного доступа, построения эффективной СУИБ патентного ведомства.

Разработка формализованной методологии построения СУИБ патентного ведомства

Разработанные формализованная методология, модели, методы и средства анализа и синтеза СУИБ обеспечивают комплексное решение следующих задач:

- проведение обследования и анализа предметной области СУИБ патентного ведомства и ее формализованное описание;
- формирование спецификаций информационных требований пользователей патентной информации и построение объектной канонической структуры ПБД;
- выявление уязвимых элементов и угроз информационной безопасности;
- определение области действия СУИБ;
- проектирование оптимальных по заданным критериям эффективности механизмов и системы защиты структур ПБД (канонической, логической и физической) патентного информационного фонда от несанкционированного доступа;
- разработка политики информационной безопасности ведомства и нормативных документов в области обеспечения информационной безопасности;
- обеспечение физической защиты информационных систем и ресурсов;
- проведение организационно-технических мероприятий по внедрению СУИБ;

[3] ISO/IEC 27001:2013, Information technology – Security Techniques – Code of practice for information security controls.

[4] ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью.

- разработка мероприятий по поддержанию работоспособности существующих автоматизированных информационных систем ведомства;
- разработка планов восстановительных работ при попытке взлома защиты и несанкционированного доступа к ТПБД.

Методы и процедуры описания и структуризации предметной области СУИБ патентного ведомства

Под предметной областью СУИБ патентного ведомства понимается взаимосвязанная совокупность пользователей, объектов данных, в том числе подлежащих защите, процедур поиска и обработки патентной информации, сведения о которых хранятся в ПБД и используется при решении задач электронного делопроизводства по заявкам и патентам, патентного поиска, выдачи, публикации и поддержании патентов в силе [1, 8, 9].

Описание предметной области СУИБ включает следующие основные компоненты:

- пользователи ПБД, к которым относятся служащие патентных ведомств, изобретатели, заявители, патентообладатели, патентные поверенные и третьи лица;
- процедуры поиска и обработки данных, последовательность их выполнения и характеристики;
- объекты данных, информационные элементы и их характеристики;
- отношения между объектами данных, информационными элементами и процедурами поиска и обработки данных.

Данная информация формируется на этапе изучения предметной области и фиксируется в стандартных формах обследования.

Модель предметной области СУИБ патентного ведомства представим в виде множества $M_{pro} = \{H, U, O, E, R\}$, где $H = \{h_j \mid j = \overline{1, J}\}$ – множество процедур, состоящее из подмножества процедур поиска данных $H_n \subseteq H$ и подмножества процедур обработки данных $H_{обр} \subseteq H$; $U = \{u_k / k = \overline{1, K_0}\}$ – множество пользователей; $O = \{o_m \mid m = \overline{1, M}\}$ – множество объектов данных, в качестве которых выступают такие элементы, как информация из полных описаний изобретений к заявкам и патентам, формула, реферат изобретения и их части, документы определенной тематики, классифицированные в соответствии с классами международной патентной классификации (МПК), а также сведения о патентообладателях, фирмах, изобретателях, и др. элементы. $E = \{e_p \mid p = \overline{1, P}\}$ – множество информационных элементов предметной области, к которым относятся библиографические данные патентных документов и другие элементы, описывающие объекты (части) патентных документов; $R = \{r_y \mid y = \overline{1, Y}\}$ – множество отношений (взаимосвязей) между компонентами $\{H, U, O, E\}$.

Выделяются следующие типы отношений:

$r_1(H, U)$ – отношения «процедуры – пользователи». Каждый кортеж отношения r_1 определяет использование процедур поиска и/или обработки данных пользователями;

$r_2(H_n, H_n)$ – отношение «процедура поиска – процедура поиска». Каждый кортеж отношения r_2 определяет последовательность выполнения процедур поиска, которая формирует структуру запроса пользователя;

$r_3(H,O)$ – отношение «процедуры – объекты данных» Каждый кортеж отношения r_3 определяет перечень объектов данных, используемых процедурами поиска и/или обработки данных;

$r_4(H,E)$ – отношение «процедуры – данные». Каждый кортеж отношения r_4 определяет использование информационных элементов при выполнении определенных поисковых процедур и/или процедур обработки данных;

$r_5(O,E)$ – отношение «объекты – данные». Каждый кортеж отношения r_5 характеризует информационное содержание (описание) определенного объекта данных.

Формализовано модель предметной области СУИБ описывается с помощью множеств $\{H,U,O,E\}$ и булевых матриц смежности:

$$HU = \|hu_{jk}\|, HH = \|hh_{jj'}\|, HO = \|ho_{jm}\|, HE = \|he_{jp}\|, OE = \|oe_{mp}\|,$$

которые описывают соответствующие отношения R между компонентами предметной области. Элементы данных матриц равны 1, если между соответствующими компонентами имеется отношение (взаимосвязь), и равны 0, в противном случае.

Разработанная модель предметной области СУИБ используется в дальнейшем при формировании моделей спецификаций информационных требований пользователей, задаваемых в виде кортежей $M^{к}_{спец} =< \alpha R \beta >$, где *к* – индекс пользователя, α и β – структурные элементы предметной области, R – отношение между элементами. Структурными элементами моделей являются элементы множеств $O = \{o_m \,|\, m = \overline{1,M}\}$ и $E = \{e_p \,|\, p = \overline{1,P}\}$. Обозначим полное множество структурных элементов как $D = \{d_l \,|\, l = \overline{1,L}\}$.

Алгоритм формирования спецификаций информационных требований пользователей состоит из следующих шагов:

1. На основании анализа матриц *HU* и *HH* определяется перечень процедур поиска и процедур обработки данных по каждому пользователю и последовательность их выполнения.
2. На основании информации, полученной в п. 1. с использованием матрицы *HO* формируются пары структурных элементов $< OR_{об} O >$, где $R_{об}$ – отношения между объектами патентного фонда.
3. На основании анализа матрицы *OE* формируются пары $< OR_{а} E >$, где R_a – отношение принадлежности (входимости) информационных элементов объектам данных.
4. Проводится совместный анализ матриц *HE, HH* и *OE,* в результате которого устанавливается противоречивость и несогласованность описаний объектов.
5. На основании полученных в пп.1÷4 результатов по каждому требованию пользователя формируются бинарные модели спецификаций $M^{к}_{спец} =< \alpha R \beta >$, представляемые в виде списка парных отношений между структурными элементами $d_l \in D$:

$$S_k = \{(d_l R d_{l'})\}, \text{ где } d_l, d_{l'} \in D_k, D_k \subseteq D.$$

В дальнейшем в соответствии с разработанной методологией осуществляется формирование внешних моделей пользователей, обобщенной внешней модели и ее нормализация, в также построение объектной канонической структуры ПБД. Для построения и нормализации используются методы и алгоритмы, приведенные в работах [10, 11].

В результате выполнения данных процедур структура внешней модели пользователя формализовано представляется в виде орграфа $G_k(D_k, R)$ и описывается с помощью матрицы семантической смежности $B_k = \|b_{ll'}^k\|, l, l' \in L_k$ элементы которой $b_{ll'}^k = 1$, если $d_{kl} R d_{kl'}$; $b_{ll'}^k = 0$ в противном случае.

Структура обобщенной внешней модели задается в виде матрицы семантической смежности $W = \|w_{ij}\|$. Элемент матрицы $w_{ij} = 1$, если хотя бы в одной из матриц семантической смежности внешних моделей пользователей между элементами d_i и d_j имеется связь, в противном случае $w_{ij} = 0$. Полученной таким образом матрице смежности, ставится в соответствии орграф $G(D, R)$. В обобщенной внешней модели задаются множество запросов, инициируемых пользователями, и множество транзакций.

Этап нормализации обобщенной внешней модели ПБД заканчивается формированием структурированной матрицы смежности W = $\|w_{ll'}\|$ и соответствующего орграфа объектной канонической структуры ПБД $G_к(D,U)$, где $D=\{d_l / l=\overline{1,L}\}$ – полное множество структурных элементов (объектов данных и информационных элементов, среди которых выделены ключи и атрибуты данных), $U = U_1 \bigcup U_2$ – полное множество взаимосвязей между структурными элементами (объектами данных U_1 и ключами и атрибутами объектов данных U_2). Построенная таким образом объектная каноническая структура ПБД отвечает требованиям полноты и безызбыточности [8, 10, 11]. Она описывает структуру, особенности и характеристики предметной области пользователей патентного ведомства и не зависит от информационной и обеспечивающей инфраструктуры. В дальнейшем объектная каноническая структура ПБД используется при построении оптимальных механизмов и системы защиты ПБД от несанкционированного доступа.

Методы анализа и оценки рисков информационной безопасности патентных ведомств

Анализ рисков информационной безопасности патентных ведомств позволяет идентифицировать имеющиеся угрозы, оценить вероятность их успешного осуществления, возможные последствия для организации и правильно расставить приоритеты при реализации контрмер. На основе проводимого анализа рисков разрабатывается система первоочередных мероприятий по уменьшению величины рисков до приемлемого уровня.

Процесс анализа и оценки рисков включает в себя решение следующих задач [3, 4]:

- анализ ресурсов, включая информационные ресурсы, программные и технические средства, людские ресурсы, и построение модели ресурсов, учитывающей их взаимозависимости;
- анализ задач, решаемых информационными системами, позволяющий оценить критичность информационных ресурсов, с учетом их взаимозависимостей;

- идентификация угроз безопасности в отношении ресурсов информационной системы и уязвимостей защиты, делающих возможным осуществление этих угроз;
- оценка вероятности осуществления угроз, величины уязвимостей и ущерба, наносимого ведомству;
- определение величины рисков для каждой тройки: угроза – группа ресурсов – уязвимость;
- ранжирование существующих рисков.

Для каждого вида ресурсов необходима своя методика определения ценности элементов, помогающая выбрать подходящий набор критериев. Эти критерии служат для описания потенциального ущерба, связанного с нарушением конфиденциальности и достоверности информации, уровня ее доступности. Физические ресурсы оцениваются с точки зрения стоимости их замены или восстановления работоспособности. Эти стоимостные величины затем преобразуются в ранговую (качественную) шкалу, которая используется также и для информационных ресурсов. Программные ресурсы оцениваются также на основе определения затрат на их разработку, приобретение или восстановление.

Оценка информационных рисков заключается в расчете рисков, который выполняется с учетом сведений о критичности активов, а также вероятностей реализации уязвимостей. Для оценки рисков может использоваться следующая формула:

$$R = D*P(V),$$

где: R – риск информационной безопасности;

D – критичность актива (ущерб);

P(V) – вероятность реализации угрозы.

Одним из примеров практической реализации вышеописанного подхода к определению уровней риска является матрица рисков, приведенная в табл. 1.

Таблица 1

Матрица рисков (согласно рекомендациям NIST "Risk Management Guide for Information Technology Systems")

Угроза (ее вероятность)	**Ущерб**		
	(низкий) – 10	***(средний) – 50***	***(высокий) – 100***
(высокая) – 1	(низкий) 10x1 = 10	(средний) 50x1 = 50	(высокий) 100x1 = 100
(средняя) – 0.5	(низкий) 10x0.5 = 5	(средний) 50x0.5 = 25	(средний) 100x0.5 = 50
(низкая) – 0.1	(низкий) 10x0.1 = 1	(низкий) 50x0.1 = 5	(низкий) 100x0.1 = 10
Уровень риска: Высокий (от 50 до 100); Средний (от 10 до 50); Низкий (от 1 до 10).			

Составлено автором

Определение области действия СУИБ

Область действия СУИБ определяется в результате проведения работ по обследованию предметной области СУИБ с использованием рассмотренных выше методов формального описания, анализа и структуризации данных и разработанных на их основе соответствующих алгоритмов и методик.

СУИБ ЕАПВ распространяется на основной вид деятельности ведомства – обеспечение процесса функционирования Евразийской патентной системы и выдачи евразийских патентов, общая схема которого приведена на рис. 1. На рис. 1 представлены обрабатываемые массивы информации и используемые для этого автоматизированные информационные системы ЕАПВ.

Область действия СУИБ охватывает шесть основных подпроцессов, связанных с технологической и производственной деятельностью ЕАПВ:

- обработка входящей информации по евразийским заявкам и евразийским патентам, включая общее делопроизводство (1.1);
- проведение формальной экспертизы (1.2);
- проведение экспертизы по существу и принятие решений (1.3);
- обеспечение публикаций (1.4);
- выдача евразийского патента (1.5);
- поддержание патента, регистрация изменений правового статуса патента (1.6).

Рисунок 1. *Процесс функционирования Евразийской патентной системы (разработано автором)*

Область действия СУИБ распространяется на все структурные подразделения ЕАПВ.

Рассмотрим описание процесса и подпроцессов с выделением их владельцев, описание требований к процессам, а также активов. На рис. 2 представлена детальная схема основного процесса. Владельцами подпроцессов являются:

- подпроцесса 1.1 – группы делопроизводства Управления экспертизы;
- подпроцесса 1.2 – отдел формальной экспертизы Управления экспертизы;
- подпроцесса 1.3 – отраслевые отделы экспертизы (химии и медицины, физики и электротехники), отдел по рассмотрению возражений, жалоб и контролю качества Управления экспертизы;
- подпроцесса 1.4 – Управление патентной информации и автоматизации;
- подпроцесс 1.5 – отдел реестра евразийских патентов;
- подпроцесса 1.6 – отдел реестра евразийских патентов и отдел права.

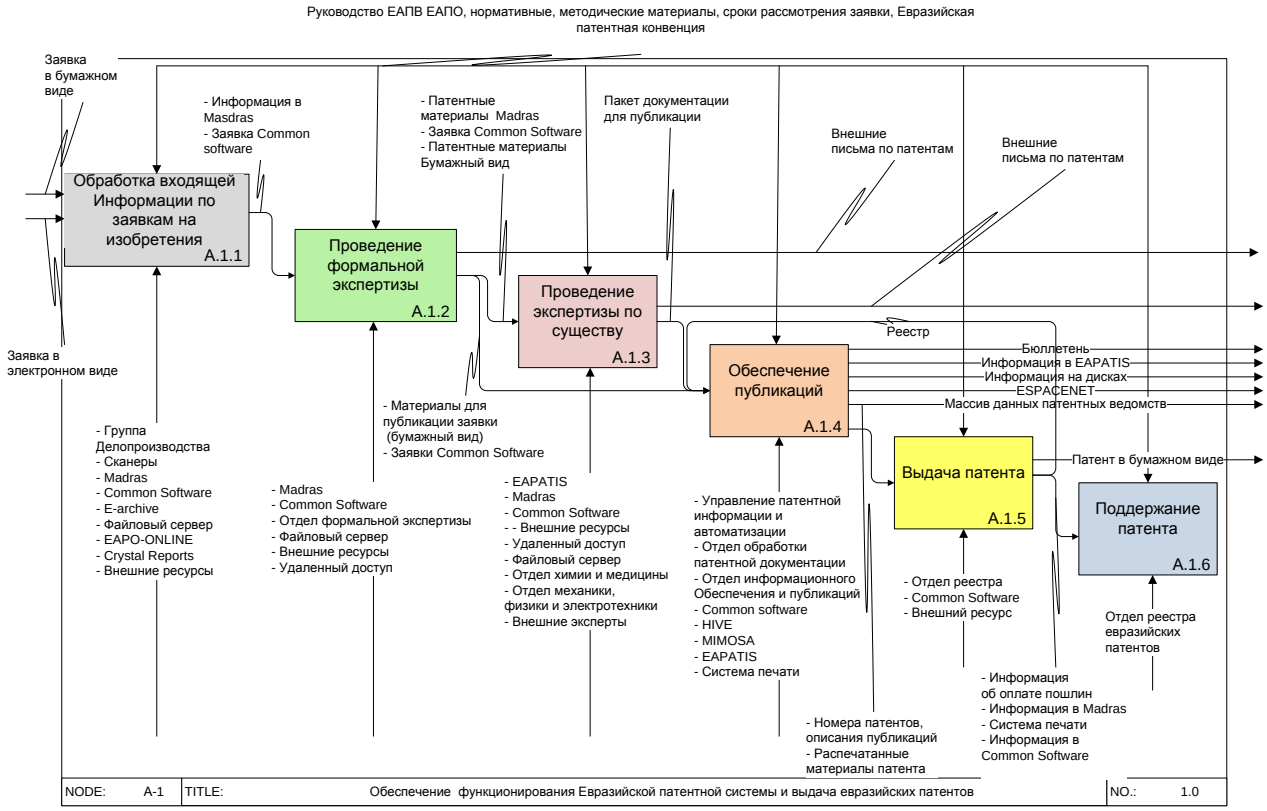

Рисунок 2. *Детальная схема основного процесса (разработано автором)*

Для реализации основного вида деятельности ЕАПВ необходимы следующие активы:

1. Персонал.
2. Структурные подразделения ведомства.
3. Информационные активы, к которым относятся:
   - материалы заявок на изобретения (на бумажном носителе и в электронном виде);
   - материалы опубликованных патентов на электронном носителе;
   - нормативно-методическая документация;
   - патентная документация и непатентная литература;
   - договорная и складская документация;
   - входящая и исходящая корреспонденция.

4. Автоматизированные информационные системы (АИС), к которым относятся:
   - АИС электронного делопроизводства;
   - информационно-поисковая система;
   - АИС публикации;
   - АИС электронного архива;
   - АИС Сервер публикаций;
   - веб-портал ЕАПО и внутренний сайт ЕАПВ;
   - АИС электронной подачи евразийских заявок и электронного обмена;
   - вспомогательные ИТ системы.
5. Программные активы:
   - системное и прикладное программное обеспечение;
   - программные средства защиты информации;
   - внешние программные сервисы и утилиты.
6. Средства обслуживания обеспечивающей и информационной инфраструктуры:
   - физическая охрана;
   - коммутационное оборудование;
   - коммуникационное оборудование.

Перечень информационных активов, программных активов, автоматизированных систем и других технических средств регулярно пересматривается и актуализируется в соответствии с методикой анализа рисков и результатами классификации информации.

Модели и методы проектирования эффективных механизмов защиты структур ПБД

Механизм защиты ПБД определяется перечнем требований к ПБД по обеспечению исключения несанкционированного (преднамеренного или непреднамеренного) использования информации ПБД и позволяет идентифицировать законных пользователей ПБД и правомочность их действий, а также предотвратить незаконные действия пользователей.

Проектирование механизма защиты ПБД осуществляется путем последовательного построения механизмов защиты структур ПБД на каноническом, логическом и физическом уровнях представления патентной информации.

Исходной информацией для построения механизмов защиты структур ПБД является информация о предметной области СУИБ, спецификациях информационных и функциональных требований пользователей и объектной канонической структуре ПБД, требования к обеспечению необходимой степени секретности данных, профили полномочий пользователей на использование данных при решении различных функциональных задач.

Пусть $A = \{a_j : j = \overline{1, m_q}\}$ – множество типов доступа к информационным ресурсам ПБД (поиска, выборки, редактирования, отображения и т. п.). Для каждого структурного элемента предметной области (объекта данных и информационного элемента) с учетом их ценности указываются степени их секретности $\varphi_i \in \Phi$, где $\Phi = \{\varphi_i : i \in R\}$ – множество степеней секретности патентно-информационных ресурсов. Степень секретности является

устанавливается на основе анализа степени их важности и экспертной оценки возможных потерь организации в случае утечки этих данных или их искажения (модификации). Если разные экземпляры некоторого элемента $d_l \in D$ имеют разные степени секретности, то для этого элемента вводится несколько степеней секретности $\{\varphi_{li} : i \in R\} \subseteq \Phi$.

Информация о секретности структурных элементов предметной области СУИБ представляется в виде матрицы $F = \|f_{li}\|$, элемент которой f_{li} = 1, если для экземпляров элемента $d_l \in D$ установлена степень секретности $\varphi_i \in \Phi$, и равен нулю в противном случае.

Пусть $\Pi = \{\pi_k : k = \overline{1, K_0}\}$ – множество профилей полномочий пользователей ПБД. Под профилем полномочий пользователя ПБД понимается право пользователя осуществлять доступ к защищенным данным. Профиль полномочий пользователей представляется матрицей $P = \|p_{ki}\|$. Элемент p_{ki} матрицы P равен $a_j \in A$, если пользователь u_k имеет полномочия выполнять доступ типа a_j к ресурсам, имеющим степень секретности $\varphi_i \in \Phi$, и равен нулю в противном случае. Профили полномочий пользователей устанавливаются руководством патентного ведомства в соответствии с возложенными на пользователей функциями по обработке информации и должностными инструкциями.

С учетом введенных формальных определений и обозначений механизм защиты $M(G_к)$ канонической структуры ПБД представим в виде отображения $\{(u_k, \pi_k, a_j, d_l^{об}, \varphi_i)\} \to \{0,1\}$, где $u_k \in U$, $\pi_k \in \Pi$, $\mathrm{a_j} \in \mathrm{A}$, $d_l^{об} \in D^{об}$, $\varphi_i \in \Phi$.

В случае правомочности доступа типа a_j k-го пользователя, имеющего профиль полномочий π_k, к объекту данных $d_l^{об}$, который имеет степень секретности φ_i механизм защиты $M(G_к)$ принимает значение «1», в противном случае (неправомочности доступа) механизм защиты $M(G_к)$ принимает значение «0», что соответствует запрету такого доступа. Эффективный механизм защиты $M(G_к)$ формируется в результате анализа сформированной на предпроектной стадии объектной канонической структуры ПБД и ее реорганизации с целью построения разрешенных с учетом требований к защите путей доступа к данным, требуемым для удовлетворения санкционированных запросов пользователей. Для построения оптимального механизма защиты $M(G_к)$ объектной канонической структуры ПБД, содержащей разрешенные пути, могут использоваться методы и алгоритмы реорганизации канонической структуры баз данных, рассмотренные в работе [11]. После реорганизации механизм защиты $M(G_к)$ формально описывается матрицей смежности объектной канонической структуры ПБД $W = \|w_{ll'}\|$, матрицей степеней секретности данных $F = \|f_{li}\|$ и матрицей профилей полномочий пользователей $P = \|p_{ki}\|$.

Механизм защиты $M(G_л)$ логической структуры ПБД формируется на этапе ее логического проектирования в результате отображения объектной канонической структуры ПБД в логическую структуру с учетом требований и ограничений выбранной СУБД и программно-аппаратной среды ее реализации [10, 11]. Логическая структура формально представляется в виде графа $G_л(N, W_л)$, где $N = \{n_j : j = \overline{1, J}\}$ _ множество типов логических записей, а $\mathrm{W^л} = \{(n_j, n_{j'}) / j, j' = 1, J\}$ – множество отношений (взаимосвязей) между ними. Логическая структура ПБД описывается матрицей смежности $\hat{B} = \|\hat{b}_{jj'}\|$, в которой элемент $\hat{b}_{jj'}$ = 1, если запись $n_{j'}$ взаимосвязана с записью n_j и равен нулю в противном случае.

Организация эффективной защиты ПБД от несанкционированного использования на логическом уровне требует защиты не только данных, но и обеспечения защиты отношений (связей) между данными. Защита взаимосвязей требуется, например, в том случае, если некоторый пользователь имеет право доступа только к одному из двух типов логических записей, связанных отношением, но не должен получать эти записи вместе. Обозначим степень секретности отношений между логическими записями n_j и $n_{j'}$ через $\hat{\varphi}_{jj'} \in \hat{\Phi}$.

Тогда механизм защиты *M(Gл)* логической структуры ПБД $G_л(N, W_л)$ представим в виде отображения $\{(u_k, \pi_k, a_j, (n_j, n_{j'}), \hat{\varphi}_{jj'}, n_j, \hat{\varphi}_j)\} \to \{0,1\}$. Значение «1» означает, что пользователь $u_k \in U$ с профилем полномочий $\pi_k \in \Pi$ обладает правом доступа типа $a_j \in A$ в отношении элементов логической структуры ПБД (связи и логической записи) $(n_j, n_{j'})$ и n_j, которые имеют степени секретности $\hat{\varphi}_{jj'} \in \tilde{\Phi}$ и $\hat{\varphi}_J \in \tilde{\Phi}$ соответственно. Значение «0» соответствует неправомочности такого доступа. Степень секретности $\hat{\varphi}_j$ логической записи n_j определяется на основании данных о степени секретности объектов канонической структуры ПБД, которые входят в ее состав. Пользователь имеет право доступа к логической записи в том случае, если ему доступны все объекты данных, образующие эту запись.

Исходными данными для решения задач синтеза оптимального механизмов защиты логической структуры ПБД являются: описание механизма защиты объектной канонической структуры ПБД; описание структуры запросов пользователей и транзакций; характеристики запросов пользователей и транзакций; ограничения на возможность использования конкретными пользователями отдельных типов логических записей и взаимосвязей между записями, ограничения выбранной СУБД и инфраструктуры и др. [11].

В качестве критериев оптимизации при решении задачи синтеза механизма защиты логической структуры ПБД могут использоваться минимум суммарного числа подсхем, используемых заданным множеством пользователей, а также минимум суммарной длины путей доступа пользователей к данным.

Постановки задач синтеза, математические модели и методы их решения приведены в [11]. Оптимальный механизм защиты логической структуры ПБД $M(G_л)$, получаемый в результате решения задач синтеза, описывается матрицей смежности логической структуры ПБД $\hat{B} = \|\hat{b}_{jj'}\|$, матрицей степеней секретности $\hat{F} = \|\hat{f}_{lj}\|$, а также матрицей полномочий пользователей $P = \|p_{ki}\|$. Механизм защиты логической структуры ПБД обеспечивает возможность идентификации правомочности доступа к защищенным типам логических записей и взаимосвязям между ними со стороны всех пользователей.

Механизм защиты *M(Gф)* физической структуры ПБД синтезируется в результате поиска эффективного варианта отображения логической структуры ПБД в физическую, при котором обеспечивается неизменность логических взаимосвязей между данными и достигается экстремальное значение критерия эффективности ее разработки с учетом требований по защите данных.

Механизм защиты *M(Gф)* физической структуры ПБД есть отображение $\{(u_k, \pi_k, a_j, v_p, \varphi_i)\} \to \{0,1\}$, где $v_p \in V$ – множество компонентов физической организации ПБД. При этом «1» означает для пользователя $u_k \in U$ с уровнем полномочий $\pi_k \in \Pi$ возможность доступа типа $a_j \in A$ к элементам $v_p \in V$ физической организации ПБД, которые имеют степени секретности $\varphi_i \in \Phi$, а «0» означает невозможность такого доступа. Механизм

защиты физической структуры ПБД позволяет идентифицировать правомочность доступа пользователей к различным компонентам физической структуры ПБД.

Эффективный механизм защиты физической структуры обеспечивает возможность обращения пользователей к требуемым элементам данных при условии исключения несанкционированного доступа путем соответствующего размещения ПБД на устройствах внешней памяти.

На этапе синтеза системы защиты ПБД осуществляется выбор совокупности методов непосредственной защиты (программных, организационных и др.) с учетом характеристик их эффективности и закрепление их за определенными структурными элементами физической организации ПБД. Постановка задачи, модель и метод синтеза оптимальной системы защиты ПБД от несанкционированного доступа рассмотрены в работе [12].

Предотвращение утечек конфиденциальной информации

Для снижения рисков разглашения (утечки) конфиденциальной информации в патентном ведомстве должны быть внедрены средства предотвращения утечек информации.

Основным техническим решением, позволяющим обеспечить защиту от угроз утечки информации, являются аппаратно-программные системы класса DLP (Data Leakage Prevention – система предотвращения утечек конфиденциальной информации). Внедрение системы класса DLP позволило решить следующие задачи:

1. Снижение рисков утечки информации за счет:
   - контроля (или блокирования) записи конфиденциальной информации на съемные носители информации;
   - контроля передачи конфиденциальных данных за границы периметра локальной сети;
   - информирования и предостережения пользователей о возможных попытках несанкционированной передачи конфиденциальной информации;
   - своевременного оповещения ответственных за обеспечение ИБ о нарушении или попытках нарушения конфиденциальности защищаемой информации и принятия мер реагирования.
2. Выявление недобросовестных служащих:
   - нарушение внутренних требований и инструкций по пользованию электронной почтой и сетью Интернет (разглашение адреса рабочей электронной почты, использование электронной почты не в служебных целях);
   - выявление фактов неэтичного поведения при общении с внешними организациями.
3. Анализ процессов передачи данных и потоков конфиденциальной информации в ведомстве.

Системы класса DLP выполняют мониторинг в автоматическом фоновом режиме и в случае выявления нарушения распространения конфиденциальной информации сигнализируют об этом ответственному персоналу для принятия мер по устранению последствий и недопущению таких инцидентов в будущем.

Наиболее известными системами данного класса являются SecureTower (компания «Falcongaze»), lnfoWatch Traffic Monitor (компания «ИнфоВотч»), Гарда Предприятие (компания «МФИ Софт»).

Разработка политики информационной безопасности патентного ведомства

Политика информационной безопасности патентного ведомства представляет собой набор общих формальных правил, которым должны подчиняться служащие ведомства и третьи лица, получившие доступ к информационным ресурсам, системам, технологиям, информационной и обеспечивающей инфраструктуре патентного ведомства.

Главной целью политики ИБ является информирование служащих ведомства об их обязанностях и ответственности по обеспечению защиты информационных ресурсов, систем, информационной и обеспечивающей инфраструктуры.

Политика ИБ патентного ведомства устанавливает правила и требования доступа служащих ведомства и внешних пользователей к патентно-информационным системам и ресурсам; порядок доступа и пользования ресурсами сети Интернет; требования по защите аппаратного, программного и информационного обеспечения; правила пользования электронной почтой; ответственность за сохранность данных на стационарных и портативных персональных компьютерах. Для ИТ-подразделений ведомства политика ИБ определяет правила доступа и пользования центром обработки данных (ЦОД), в котором находятся объекты инфраструктуры, наиболее критичные с точки зрения обеспечения информационной безопасности: серверы, телефонная станция, маршрутизаторы, файерволы, RAID-массивы, источники бесперебойного питания и другое оборудование.

Политика регламентирует процедуры обеспечения резервного копирования и восстановления дел заявок на изобретения и патентов. В частности, пользователям предписывается необходимость регулярно делать резервные копии всех основных служебных данных и программного обеспечения, а при использовании электронных носителей для хранения данных периодически проверять на читаемость, как самих носителей, так и форматов данных в течение срока их хранения.

Служащие обязаны сообщать ответственному за ИБ подразделению об известных или подозреваемых ими нарушениях информационной безопасности, в том числе, о наличии вирусов или вредоносного программного обеспечения и не пытаться использовать ставшие им известными слабые стороны системы безопасности. Ответственное за ИБ подразделение должно информировать служащих об известных способах или предполагаемых случаях нарушения информационной безопасности.

Служащих ведомства необходимо обучать процедурам безопасности и правильному использованию информационных систем, ресурсов и инфраструктуры с целью сведения к минимуму возможные риски информационной безопасности. Необходимо повышать квалификацию специалистов ИТ-подразделений в области ИБ с целью обеспечения высокого уровня информационной безопасности патентного ведомства, развития и совершенствования информационно-технологического и нормативно-правового регулирования в области ИБ.

Реализация политики ИБ на примере ЕАПВ

Реализация политики ИБ патентного ведомства предусматривает принятие необходимых мер в целях защиты информационных ресурсов, информационных систем и инфраструктуры от случайного или преднамеренного изменения, раскрытия или уничтожения,

обеспечения конфиденциальности, достоверности, неизменности и доступности информации, а также непрерывности технологических процессов автоматизированной обработки данных в ведомстве.

Политика ИБ ЕАПВ реализуется на основе подготовки и выпуска соответствующих распорядительных документов:

- нормативных документов в области обеспечения ИБ. Состав документации является достаточным для обеспечения соответствия требованиям международного стандарта по ИБ ISO/IEC 27001:2013;
- уточненных положений о структурных подразделениях и рабочей группы по безопасности (РГБ);
- инструкций пользователей по работе с информационными системами, ресурсами и технологиями;
- инструкций администраторов информационных систем;
- инструкций (правил, памяток) по проведению рабочих встреч и переговоров с представителями сторонних организаций, заключению договоров с третьими лицами;
- планов мероприятий по поддержанию работоспособности находящихся в эксплуатации автоматизированных информационных систем, включая планы проведения регламентных работ;
- планов восстановительных работ, направленных на ликвидацию последствий нарушений информационной безопасности.

Для обеспечения постоянной доступности дел евразийских заявок и дел евразийских патентов в электронной форме необходимо обеспечивать резервное копирование АИС, используемых для их обработки и хранения.

Резервирование осуществляется системой резервного копирования (СРК), которая производит копирование файлов баз данных и сетевых каталогов с делами евразийских заявок и делами евразийских патентов, хранимых в соответствующих АИС.

Резервное копирование проводится автоматически по настроенному расписанию с использованием штатного программного обеспечения СРК.

Полное резервное копирование на магнитные ленты может осуществляться со следующей частотой: ежедневно, еженедельно, ежемесячно и ежегодно.

Разработка структуры системы управления ИБ ЕАПВ

В основе построения СУИБ заложен процессный подход, при котором СУИБ рассматривается как циклически повторяющийся процесс постоянного совершенствования.

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

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

Назначение ролей ИБ служащим ЕАПВ проводится в установленном порядке посредством подписания соответствующего обязательства по ИБ.

В рамках СУИБ ЕАПВ выделяются следующие роли:

- руководство ЕАПВ;
- председатель 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.

Функционирование СУИБ на основе введенных ролей осуществляется следующим образом.

Представитель руководства ЕАПВ в области ИБ предъявляет общие требования по распределению функций и обязанностей по защите информационных активов ЕАПВ и организует работу по обеспечению ИБ информационных активов. Председателем РГБ инициируется первичное назначение ролей ИБ, обеспечивается координация, планирование, контроль и анализ работ в области ИБ, принимаются решения по обеспечению соответствующего уровня информационной безопасности, которые представляются руководству.

Специалист по управлению ИБ отвечает за работоспособность процессов управления СУИБ. Специалист по управлению ИТ обеспечивает предоставление ИТ- услуг. Специалист по управлению непрерывностью деятельности ЕАПВ обеспечивает функционирование основных ИТ и ИБ сервисов ведомства в случае наступления чрезвычайных ситуаций, он же поддерживает в актуальном состоянии документации по управлению непрерывностью деятельности ведомства. Специалист по управлению физической безопасностью назначается из руководящего состава структурного подразделения ЕАПВ. Его задачей является обеспечение физической безопасности информационной и обеспечивающей инфраструктуры ЕАПВ.

Внутренним аудитором СУИБ назначается служащий структурного подразделения ЕАПВ, который осуществляет внутренние проверки на соответствие СУИБ требованиям стандартов и нормативных документов ведомства в области ИБ.

Владелец процесса СУИБ – служащий ЕАПВ, который несет ответственность за результат и качество выполняемого процесса обеспечения или управления ИБ. Владельцы должны быть определены для каждого процесса СУИБ, например, владелец процесса антивирусной защиты, владелец процесса резервного копирования, владелец процесса управления инцидентами ИБ и т. д. Владелец актива – служащий ЕАПВ, уполномоченный управлять созданием, использованием и безопасностью информационного актива ЕАПВ.

Заключение

В работе предложены формализованная методология, модели, методы и средства анализа и синтеза эффективных механизмов и системы защиты патентных баз данных от несанкционированного доступа, построения эффективной системы управления информационной безопасностью патентного ведомства.

Разработанная методология обеспечивает комплексное решение следующих задач: проведение обследования предметной области СУИБ патентного ведомства и ее формализованное описание; определение области действия СУИБ на основе формализованного описания предметной области и выявленных уязвимых элементов и угроз информационной безопасности; проектирование оптимальных по заданным критериям эффективности механизмов и системы защиты ПБД от несанкционированного доступа; разработка политики информационной безопасности ведомства и нормативных документов в области обеспечения информационной безопасности; обеспечение физической защиты информационных систем и ресурсов; разработка мероприятий по поддержанию работоспособности существующих автоматизированных информационных систем ведомства; разработка планов восстановительных работ; проведение ряда организационно-технических мероприятий (создание рабочей группы (подразделения) по информационной безопасности; назначение ролей СУИБ; внесение изменений в должностные инструкции служащих ведомства и др.).

Эффективность практического применения предложенной методологии, моделей, методов и алгоритмов подтверждена разработкой и внедрением СУИБ в региональной патентной организации – Евразийском патентном ведомстве Евразийской патентной организации.

Полученные в работе результаты могут использоваться в качестве типовых проектных решений при создании СУИБ национальных патентных ведомств стран – участниц Евразийской патентной конвенции.

ЛИТЕРАТУРА

1. В. О. Сиротюк, А. В. Бителева. Особенности и задачи обеспечения безопасности патентного информационного фонда международной патентной организации. Проблемы управления безопасностью сложных систем. Материалы IX Международной конференции. М.: РГГУ, 2002, с. 220-221.
2. В. О. Сиротюк Проблемы и задачи обеспечения информационной безопасности патентно-информационных ресурсов. М.: Патентная информация сегодня, №1 / 2012, с. 3-10.
3. В. О. Сиротюк Методы и средства обеспечения информационной безопасности патентных ведомств. М: Патентная информация сегодня, №2 / 2012, с. 3-11.
4. Информационная безопасность систем организационного управления. Теоретические основы: в 2 т. / Н. А. Кузнецов, В. В. Кульба, Е. А. Микрин и др. – М.: Наука, 2006.
5. Garcia-Alfaro Joaquin, Kranakis Evangelos. Foundations and Practice of Security. Springer, 2016. – 325 p. – (Lecture Notes in Computer Science). – ISBN-10: 3319303023. – ISBN-13: 978-3319303024.
6. Kizza Joseph Migga. Guide to Computer Network Security. Springer, 2017. – 569 p. – ISBN 978-3-319-55606-2.
7. Х. Ф. Фаязов, В. О. Сиротюк, А. В. Овчинников, А. Б. Бурцев Формирование и развитие евразийского патентно-информационного пространства. М.: ИНИЦ «Патент», 2010. – 124 с.
8. Сиротюк В. О., Сиротюк О. В. Методы повышения эффективности и качества структур тематических патентных баз данных в патентных автоматизированных информационно-управляющих системах. Автоматика и телемеханика. М.: Наука, №8/2002, с. 168-177.
9. Сиротюк В. О., Бителева А. В. Обеспечение сохранности патентных баз данных в евразийской патентной информационной системе. Труды международной научно-практической конференции «Теория активных систем». Секция 3 «Проблемы безопасности сложных систем». Том 1. М.: ИПУ РАН, 2001, с. 138-139.
10. А. Г. Мамиконов, В. В. Кульба, С. А. Косяченко, В. О. Сиротюк и др. Оптимизация структур данных в АСУ. М.: Наука, 1988, – 256 с.
11. Кульба В. В., Ковалевский С. С., Косяченко С. А., Сиротюк В. О. Теоретические основы проектирования оптимальных структур распределенных баз данных. Серия «Информатизации России на пороге XXI века». М.: СИНТЕГ, 1999, – 660 с.
12. В. В. Кульба, В. О. Сиротюк Модели и методы синтеза оптимальной системы защиты патентного информационного фонда международной патентной организации от несанкционированного доступа. – Интернет-журнал «Науковедение», т.9, вып.№4, http://naukovedenie.ru/PDF/84TVN417.pdf, – 16 с.

Sirotyuk Vladimir Olegovich
Institute of control science of Russian academy of science, Russia, Moscow
E-mail: vsirotyuk.55@icloud.com

Models, methods and tools for developing and implementing an effective information security management system of the patent office

Abstract. The theoretical and applied problems of constructing an effective information security management system of the patent office are considered in the article by the example of the regional patent organization – the Eurasian Patent Office of the Eurasian Patent Organization. Formalized models and methods for describing, analyzing and structuring the subject area of the information security management system of the Patent Office are proposed; analysis and assessment of information security risks; synthesis of effective mechanisms and system of protection of structures of patent databases from unauthorized access. The scope of the information security management system of the Eurasian Patent Office has been defined, the characteristics of the main processes of the department within the scope of the information security management system have been described, and the owners of the processes and the required assets have been identified for their implementation. The main provisions of the patent office policy in the field of information security and protection of patent information resources, information and providing infrastructure of the patent office are considered. The role structure of the information security management system is given; the roles of the agency employees in the information security system are defined. The issues of ensuring the backup and recovery of applications for inventions and patents, the introduction of a system to protect against the leakage of confidential information, the organization and conduct of these works in the patent office are considered.

Keywords: the Regional International Patent Organization; threat of information security; information security management system; patent database; mechanism for protecting the structures of patent databases from unauthorized access; protection system of patent databases; information security policy; system of backup; system of protection from leaks of confidential information