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

Том 9, №4 (2017) http://naukovedenie.ru/vol9-4.php

URL статьи: http://naukovedenie.ru/PDF/84TVN417.pdf

Статья опубликована 01.09.2017

Ссылка для цитирования этой статьи:
Кульба В.В., Сиротюк В.О. Модели и методы синтеза оптимальной системы защиты патентного информационного фонда международной патентной организации от несанкционированного доступа // Интернет-журнал «НАУКОВЕДЕНИЕ» Том 9, №4 (2017) http://naukovedenie.ru/PDF/84TVN417.pdf (доступ свободный). Загл. с экрана. Яз. рус., англ.

УДК 62

Кульба Владимир Васильевич
ФГБУН «Институт проблем управления им. В. А. Трапезникова Российской академии наук», Россия, Москва[1]
Заведующий лабораторией
Доктор технических наук, профессор
E-mail: kulba@ipu.ru

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

Модели и методы синтеза оптимальной системы защиты патентного информационного фонда международной патентной организации от несанкционированного доступа

Аннотация. В работе предложены формализованные модели и методы синтеза оптимальной системы защиты патентного информационного фонда международной патентной организации от несанкционированного доступа на примере Евразийского патентного ведомства Евразийской патентной организации. Сформулированы цели и задачи Евразийского патентного ведомства в области информационной безопасности, рассмотрены особенности формирования и развития патентного информационного фонда, создаваемого в Евразийском патентном ведомстве в виде виртуального патентно-информационного хранилища. Введены показатели эффективности и качества патентного информационного фонда, используемые при подготовке баз данных патентной информации, непатентной литературы и патентно-ассоциированной документации. На основе проведенного анализа выявлены основные угрозы информационной безопасности патентно-информационного фонда и сформулированы предпосылки и требования по созданию системы управления информационной безопасностью международной патентной организации.

Дано формальное определение системы защиты патентного информационного фонда от несанкционированного доступа и описаны ее характеристики. Поставлена общая задача синтеза оптимальной системы защиты баз данных патентного информационного фонда от несанкционированного доступа и выполнена ее декомпозиция на ряд последовательно

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

решаемых подзадач. Предложены критерии эффективности задач синтеза системы защиты от несанкционированного доступа, коррелированные с требованиями защиты.

Разработана математическая модель задачи синтеза оптимальной системы защиты данных патентного информационного фонда от несанкционированного доступа по критерию минимума межпользовательского информационного интерфейса. Задача синтеза представлена в виде задачи нелинейного целочисленного программирования с булевыми переменными. Для ее решения предложены соответствующие методы и алгоритмы. Результаты решения поставленной задачи синтеза использовались при построении эффективной системы управления информационной безопасностью Евразийского патентного ведомства Евразийской патентной организации.

Ключевые слова: региональная международная патентная организация; патентный информационный фонд; база данных патентного информационного фонда; угроза информационной безопасности патентного информационного фонда; система защиты патентного информационного фонда от несанкционированного доступа; система управления информационной безопасностью

Введение

Обеспечение высокого уровня безопасности патентных информационных ресурсов является важной и актуальной задачей, стоящей перед патентными ведомствами [1].

Патентные ведомства 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 автоматизированные, информационные и поисковые системы, расширяют электронное взаимодействие с внешними организациями.

Вместе с этим возрастают потенциальные угрозы и риски информационной безопасности ведомств и, как следствие этого, возрастает потребность в надежных и эффективных методах и средствах защиты данных, информационных систем и информационной инфраструктуры, обеспечения их сохранности и восстановления в случае сбоев, в основе которых должна лежать сбалансированная и эффективная система информационной безопасности организации [2, 3].

Не является исключением в этом отношении Евразийское патентное ведомство (ЕАПВ) – региональная международная патентная организация и национальные патентные ведомства государств-участников Евразийской патентной конвенции (ЕАПК)[2], входящие в состав Евразийской патентной организации (ЕАПО) (Россия, Беларусь, Казахстан, Киргизия, Армения, Азербайджан, Таджикистан, Туркменистан). В ЕАПВ ЕАПО накоплен значительный патентно-информационный потенциал, сформированы фонды патентной, непатентной и патентно-ассоциированной информации, продолжаются работы по формированию и развитию единого евразийского патентно-информационного пространства [4]. Для полноценного информационного обеспечения пользователей евразийского региона на протяжении многих лет поддерживается функционирование Евразийской патентно-информационной системы (ЕАПАТИС), в которой хранится более 60 млн патентных документов [5]. Разработана и эффективно используется заявителями и их представителями (патентными поверенными) автоматизированная система электронной подачи евразийских заявок и электронного обмена ЕАПВ-ОНЛАЙН. С 2014 года ЕАПВ ЕАПО перешло на официальное электронное интернет-

[2] Евразийская патентная конвенция. М.: ВОИС, 1995.

издание – Евразийский сервер публикаций, представляющий собой специализированную информационную систему, предназначенную для хранения и оперативного доступа к опубликованным евразийским патентным документам (патентам и заявкам) и сведениям о них. Внедрены и находятся в промышленной эксплуатации автоматизированные информационные системы и информационные технологии, позволяющие автоматизировать основные технологические процессы на этапах формальной экспертизы заявок и экспертизы по существу, делопроизводства, патентного поиска, публикации информации, формирование электронных досье дел евразийских заявок и патентов, выдачи и поддержания в силе евразийских патентов.

Краткая характеристика ЕАПВЕАПО

ЕАПО является международной межправительственной организацией со штаб-квартирой в г. Москве. ЕАПО выполняет административные задачи, связанные с функционированием Евразийской патентной системы и выдачей евразийских патентов[3].

В соответствии с Соглашением между Правительством Российской Федерации и Евразийской патентной организацией о штаб-квартире ЕАПО имущество Организации не подлежит обыску, реквизиции, экспроприации, конфискации и какой-либо другой форме принудительных действий со стороны соответствующих властей. Архивы ЕАПО, включая корреспонденцию и документы на бумажных, магнитных и электронных носителях информации, а также компьютерные программы, принадлежащие ЕАПО или находящиеся в ее владении, неприкосновенны. Организация имеет право пользоваться шифрами, отправлять и получать свою официальную корреспонденцию с курьером или в запечатанных вализах, на которые распространяются иммунитеты, аналогичные тем, которые распространяются на дипломатическую почту.

Органами ЕАПО являются Административный совет и Евразийское патентное ведомство.

Официальным языком Организации является русский язык.

Главной задачей ЕАПВ является получение, рассмотрение евразийских заявок и выдача евразийских патентов, действующих на территории государств-участников Евразийской патентной конвенции. Основными выполняемыми функциями ЕАПВ являются: поиск и экспертиза; выдача патентов и публикация информации; рассмотрение возражений; распространение информации; формирование евразийского патентно-информационного пространства. ЕАПВ обладает в каждом Договаривающемся государстве правоспособностью, которая признана за юридическими лицами в соответствии с национальным законодательством данного государства.

Цели и задачи ЕАПВ ЕАПО в области информационной безопасности

Основной стратегической целью ЕАПВ ЕАПО в области информационной безопасности (ИБ) является обеспечение конфиденциальности, достоверности, неизменности и доступности материалов и информационных активов патентно-информационного фонда (ПИФ) ЕАПВ[4].

Частными целями ИБ являются:

[3] Материалы веб-портала Евразийской патентной организации: http://www.eapo.org/.

[4] Годовые отчёты ЕАПО: http://www.eapo.org/ru/publications/reports/.

- обеспечение уровня безопасности, соответствующего принятым нормативным документам;
- обеспечение заданного уровня безопасности информационной и обеспечивающей инфраструктуры ЕАПВ;
- обеспечение регистрации всех действий пользователей с информацией и ресурсами;
- разработка планов восстановительных работ после аварий и иных критических ситуаций с целью обеспечения непрерывности работы локальной вычислительной сети.

Для достижения сформулированных целей руководители подразделений ЕАПВ должны отвечать за доведение положений политики информационной безопасности до служащих, а администраторы локальной сети и информационных систем – обеспечивать непрерывное функционирование сети и автоматизированных информационных систем и отвечать за реализацию технических мер, необходимых для обеспечения необходимого уровня информационной безопасности. Пользователи должны работать с локальной сетью и информационными системами в соответствии с принятой политикой информационной безопасности, подчиняться распоряжениям лиц, отвечающих за отдельные аспекты безопасности, ставить в известность руководство обо всех подозрительных ситуациях и угрозах безопасности и нести персональную ответственность за нарушение политики безопасности.

Особенности формирования и характеристики ПИФ ЕАПВ

Целью создания и развития ПИФ ЕАПВ является обеспечение экспертов ЕАПВ, а также изобретателей (заявителей), патентовладельцев и их представителей (патентных поверенных) и широкой общественности полной, достоверной и качественной информацией об объектах интеллектуальной собственности (евразийских заявках и патентах) и последних достижениях науки и практики в рассматриваемых предметных областях заявок на изобретения.

При формировании ПИФ необходимо руководствоваться требованиями правил 34 PCT и 36 PCT Инструкции к Договору о патентной кооперации (PCT)[5].

В соответствии с этими правилами ПИФ ЕАПВ создается в виде виртуального патентно-информационного хранилища, обеспечивающего предоставление доступа к локальным (внутренним) фондам ПИФ и к внешним патентным информационным ресурсам, доступным по каналам связи.

Для экспертов ЕАПВ крайне важно также иметь доступ к фондам патентной документации национальных патентных ведомств государств-участников Евразийской патентной конвенции и других независимых государств на территории бывшего СССР.

ПИФ ЕАПВ включает:

- электронные поисковые фонды, отвечающие основным требованиям, предъявляемым к международному поисковому органу;
- электронные фонды евразийских заявок и патентов;

[5] Patent Cooperation Treaty (PCT). Geneva: WIPO, 2000.

- электронные фонды национальной патентной документации стран минимума PCT, а также фонды стран-членов ЕАПО;
- электронный архив (досье) дел евразийских заявок и патентов;
- электронный фонд патентно-ассоциированной литературы;
- электронный фонд непатентной литературы, формируемый на основе поиска и подбора ссылочной документации по евразийским заявкам, а также статей из периодических изданий, получаемых в электронной форме по подписке;
- справочно-поисковый аппарат и средства унифицированного доступа к электронным фондам патентной информации и непатентной литературы внутренних источников данных и к внешним патентно-информационных ресурсам стран минимума PCT и непатентной литературы.

Формирование ПИФ ЕАПВ осуществляется ведомством на основе внутренних и внешних источников.

Внутренними источниками формирования ПИФ ЕАПВ являются: евразийская патентная документация (заявки и патенты); законодательная, нормативно-правовая и справочная документация ЕАПВ.

К *внешним источникам* относятся: патентная документация стран минимума PCT (США, России, Великобритании, Канады, Франции, Германии, Японии, и др. стран) и региональных патентных организаций (ЕПВ, ARIPO, OAPI); международные заявки PCT (ВОИС), национальная патентная документация, получаемые по обмену; патентная информация, получаемая по каналам связи из внешних БД; непатентная документация, получаемая из специализированных патентных и научно-технических библиотек (включая электронные), а также из БД электронных журналов и с сайтов издательств.

Вся информация, поступающая в ЕАПВ, подлежат регистрации, учету и контролю. Порядок выполнения данных операций и сопровождения ПИФ определяется на основе нормативных актов ЕАПВ, иных регламентирующих документов с учетом особенностей носителей, на которых представлена информация (бумажных, электронных). Состав и структура ПИФ ЕАПВ подвергается периодическому пересмотру и актуализации в соответствии с информационными потребностями пользователей, требованиями обеспечения информационной безопасности, а также с учетом требований полноценного и качественного информационного обеспечения технологических и производственных процессов, предоставления легких и удобных инструментов и средств доступа к источникам информации ПИФ.

Показатели эффективности и качества ПИФ

В современных условиях общим показателем эффективности и качества ПИФ ведомства является *степень представления входящих в него документов в электронной форме*. Этот показатель рассчитывается как отношение количества документов ПИФ, представленных в электронном виде, к общему количеству документов, хранящихся в ПИФ.

Другие (частные) показатели качества ПИФ, представленного в электронном виде, характеризуют соответствие состава, содержания, структуры, эксплуатационных и сервисных характеристик ПИФ спецификациям требований, предъявляемых стандартами ВОИС к фондам патентной и непатентной документации и литературы, а также рекомендациями к эксплуатационным характеристикам их использования.

Частными показателями качества ПИФ являются: полнота, достоверность, актуальность, глубина ретроспективы.

Показатель полноты определяется как отношение количества хранимых в БД ПИФ документов к их общему числу, определенному в эталонной БД. При этом в качестве эталонной БД выбирается БД либо источника информации (патентная БД национального патентного ведомства, например, БД USPTO, или БД JPO, или БД Роспатента и т. д.), либо БД всемирных патентных информационных систем типа espacenet или Patentscope.

Показатель достоверности характеризует степень соответствия данных об объектах, зафиксированных в БД ПИФ, реальным объектам в данный момент времени. Показатель достоверности рассчитывается как отношение количества правильных (безошибочных) документов к их общему числу в ПИФ.

Актуальность данных определяется как отношение разности между общим числом документов в БД ПИФ и числом документов, информация о которых морально устарела, к общему числу документов. Актуальность данных в БД ПИФ рекомендуется определять на основе представительной выборки, в которой число документов определяется экспертным путем.

Глубина ретроспективы определяется как интервал времени от даты публикации документа и/или записи в БД ПИФ ЕАПВ самого раннего документа до настоящего времени. Показатель глубины ретроспективы тесно связан с показателем полноты БД ПИФ.

Для патентной информации наиболее важными являются показатели полноты и глубины ретроспективы информации, т. к. они напрямую влияют на качество патентного поиска, проводимого в первую очередь в массиве патентной документации.

Для непатентной документации наиболее важным является показатель актуальности информации, т. к. в эпоху научно-технического прогресса научные разработки быстро развиваются, и эксперт должен иметь доступ к наиболее «свежей» информации.

Для законодательной, нормативно-правовой и справочной информации наиболее актуальным является показатель достоверности данных, т. к. данная информация может быстро устаревать и все изменения должны оперативно отражаться в ПИФ.

ПИФ ЕАПВ содержит большие объемы разнородной, многоаспектной информации, исчисляемые миллионами документов (в первую очередь, патентных), для хранения которой в электронной форме требуются терабайты памяти. Для надежного и безопасного хранения и эффективного использования таких больших объемов информации в ЕАПВ разработана специализированная система электронного хранения данных (СЭХД).

Таким образом, формирование, ведение и развитие ПИФ ЕАПВ представляет собой комплексную проблему, предполагающую решение ряда организационных, методологических и технических задач, среди которых одной из важных является задача обеспечения высокого уровня защиты патентно-информационных ресурсов от несанкционированного доступа.

Основные предпосылки и требования по созданию СУИБ ЕАПВ ЕАПО.

Основными предпосылками и требованиями для создания эффективной СУИБ ЕАПВ являются следующие [1, 4, 6]:

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

2. В ЕАПВ накоплен значительный патентно-информационный фонд. Часть представленной в ПИФ информации 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 патентно-информационных ресурсов и информационных систем неуклонно растет. Эффективная система информационной безопасности ведомства должна строиться на основе надежной и проверенной практикой информационно-технологической инфраструктуры, обеспечивающей интеграцию информационных технологий и систем, централизованное управление пользователями и политиками доступа к ресурсам.

4. К различным автоматизированным информационным системам ЕАПВ предъявляются различные требования по обеспечению их информационной безопасности и надежности функционирования. Например, автоматизированная система делопроизводства SOPRANO, информационно-поисковая система ЕАПАТИС, автоматизированная система подготовки к публикации Hive, автоматизированная система поиска и подбора ссылочной документации SRP, используемые в основном технологическом процессе ведомства должны быть доступны служащим ЕАПВ постоянно (в режиме 5х8), независимо от надежности функционирования аппаратно-программных средств их реализации. Доступ к Интернет-версии системы ЕАПАТИС, к системе электронной подачи евразийских заявок ЕАПВ-ОНЛАЙН, а также к Серверу публикаций должен быть предоставлен в режиме 7х24 для обеспечения нормальной работы с системами внешних пользователей. Время на восстановление этих систем в случае сбоев в работе оборудования, программного, информационного и технологического обеспечения должно быть минимальным и исчисляться часами. Веб-портал ЕАПО, выполняющий роль веб-представительства ЕАПО в Интернет и обеспечивающий ряд веб-сервисов для пользователей Евразийской патентной системы с учетом разницы во времени в часовых поясах, несовпадением выходных и праздничных дней в различных государствах и России (где расположена штаб-квартира ЕАПО) должен быть доступен в режиме 7х24.

5. В области информационной безопасности и защиты данных существует ряд международных стандартов. Положения этих стандартов должны учитываться и использоваться при разработке СУИБ патентного ведомства.

6. При построении СУИБ ведомства должен использоваться комплексный подход, включающий меры следующих видов [7, 8]:

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

6.2. Административные (действия общего характера, предпринимаемые руководством ведомства).

6.3. Процедурные (меры безопасности, реализуемые служащими ведомства).

6.4. Аппаратно-программные (конкретные технические меры).

6.5. Структурные (методы оптимизации структур хранения данных ПИФ по критериям эффективности, коррелированным с требованиями защиты данных от несанкционированного доступа).

7. Исходя из необходимости экономного расходования бюджетных средств ведомства, затраты на создание системы информационной безопасности не должны превышать риски, связанные с потерей информации и восстановлением БД, информационных систем и информационной инфраструктуры ведомства.

8. Эффективная СУИБ ведомства должна быть распределенной. Это означает, что подразделение, ответственное за сбор, хранение, передачу, обработку, предоставление и распространение той или иной информации, сопровождение информационных систем должно самостоятельно разрабатывать предложения по обеспечению ее защиты и безопасности и использовать соответствующие методы и средства защиты в соответствии с принятой в ведомстве политикой информационной безопасности. Например, в ЕАПВ ответственными за обеспечение информационной безопасности являются отраслевые отделы экспертизы Управления экспертизы, отдел реестра евразийских патентов, отдел права, канцелярия и др. подразделения. Для координации и управления работами создана Рабочая группа по безопасности (РГБ) из представителей пользователей и ИТ-специалистов.

Угрозы безопасности могут быть умышленными (прямое хищение, умышленная модификация информации), случайными (ошибки в вычислениях, случайное удаление файла), природными (наводнение, ураган, молния и т. п.) или техногенными (скачки напряжения, пожары, аварии в системах коммунального обеспечения помещений и т. п.) [9].

При этом основными угрозами информационной безопасности ПИФ ЕАПВ являются:

- раскрытие конфиденциальной информации (несанкционированный доступ, копирование данных, кража информации);
- компрометация информации (внесение несанкционированных изменений в массивы данных и базы данных);
- несанкционированный доступ к данным с помощью специальных программных средств и несанкционированный обмен информацией;
- несанкционированное (неразрешенное) использование рабочих станций пользователей для доступа к конфиденциальной информации,
- отказ от информации (непризнание получателем или отправителем фактов получения или отправки информации, соответственно);
- отказ в обслуживании (отсутствие доступа к информации).

Формализованное определение и характеристики системы защиты БД ПИФ.

Формально система защиты $S^3 = \{m_s : s = \overline{1, S}\}$ представляет собой взаимосвязанную совокупность методов и средств защиты, где m_s есть s-й метод (средство), а S – общее число методов и средств. Под эффективной системой защиты информационных ресурсов ПИФ будем понимать такую совокупность методов и средств защиты S_{opt}, $S_{opt} \subseteq S$, комплексное использование которых по установленным правилам обеспечивает оптимальное значение заданного критерия эффективности разработки и/или эксплуатации системы защиты ПИФ. При построении системы защиты должны соблюдаться требования по обеспечению нормального функционирования информационной и обеспечивающей инфраструктуры ПИФ, выполнению запросов пользователей, структурных и функциональных ограничений, накладываемых СЭХД ПИФ.

Основными характеристиками системы защиты ПИФ являются: вероятность преодоления выбранных методов и средств защиты злоумышленниками; время безопасного функционирования информационной системы, под которым понимается среднее время, необходимое для получения защищенных конфиденциальных данных путем опробования различных вариантов доступа; стоимость разработки и внедрения системы, затраты на

сопровождение и развитие системы защиты; время выполнения множества запросов пользователей.

Методы защиты характеризуются системой параметров, которые описываются следующими векторами:

- $V=\{v_1,v_2,...,v_s,...,v_S\}$ – вектор стоимостей разработки и эксплуатации методов защиты, где v_s – затраты на разработку и эксплуатацию m_s-го метода защиты;
- $\tau = \{\tau_1, \tau_2, ..., \tau_s, ..., \tau_S\}$ -вектор математических ожиданий безопасных времен методов защиты, где τ_s – математическое ожидание безопасного времени метода защиты m_s;
- $T=\{t_1,t_2,...,t_s,...,t_S\}$ – вектор средних затрат процессорного времени на реализацию методов защиты;
- $\Phi=\{\phi_1,\phi_2,...,\phi_s,...,\phi_S\}$ – вектор затрат дополнительных объемов оперативной памяти на реализацию заданных методов защиты (последние два параметра характеризуют программные методы защиты; в случае использования аппаратных и/или организационных методов они принимают значения, соответственно, $t_s=0$, $\phi_s=0$);
- $P=\{p_1,p_2,...,p_{s,...},p_S\}$ – вектор вероятностей преодоления используемых методов защиты, где p_s – вероятность взлома s-го метода защиты.

Постановка задачи, модели и методы синтеза оптимальной системы защиты БД ПИФ от несанкционированного доступа.

Исходной информацией для постановки и решения задачи синтеза оптимальной системы защиты ПИФ является информация о предметной области и спецификациях информационных требований пользователей, требования к обеспечению необходимой степени секретности данных, профили полномочий пользователей на использование данных ПИФ, а также информация о механизмах защиты канонической и логической структур БД ПИФ, методы построения которых и их формализованные описания приводятся в работах [7, 11, 12].

Задачи синтеза оптимальной системы защиты ПИФ решаются на этапе формирования структур хранения и физической организации данных. Их решение обеспечивает выбор оптимальных методов и средств непосредственной защиты и их распределение между элементами структур хранения физической организации данных.

Управление доступом пользователей к информационным ресурсам ПИФ включает осуществление следующих основных процедур защиты:

- идентификацию пользователей, терминалов, рабочих станций и других ресурсов информационной инфраструктуры;
- аутентификацию пользователей;
- проверку полномочий пользователей и принятие решений о правомерности доступа пользователей к затребованным ими ресурсам ПИФ;
- регистрацию обращений пользователей к защищаемым данным, хранящимся в ПИФ;
- оповещение соответствующих служб в случае попыток несанкционированного доступа к информации ПИФ.

Общая задача синтеза оптимальной системы защиты БД ПИФ от несанкционированного доступа включает последовательное решение следующего комплекса подзадач:

1. Формирование структур хранения данных (файлов) БД ПИФ с учетом степеней секретности логических записей и взаимосвязей между ними, зафиксированных в механизме защиты логической структуры БД, и характеристик запросов пользователей.
2. Распределение файлов между внешними запоминающими устройствами информационной инфраструктуры ПИФ в соответствии с требованиями обеспечения безопасности хранения данных и эффективности доступа к ним.
3. Распределение пользователей ПИФ по рабочим станциям (терминалам), при котором исключается несанкционированный доступ к базам данных ПИФ.
4. Выбор варианта сопряжения множества терминалов с множеством внешних носителей, обеспечивающего выполнение требований к секретности данных.
5. Закрепление методов и средств непосредственной защиты за объектами защиты различных структурных уровней.

Критериями эффективности при решении задачи синтеза системы защиты ПИФ от несанкционированного доступа могут служить максимум информационной независимости пользователей ПИФ, минимум затрат на разработку и эксплуатацию системы защиты, минимум суммарных потерь от несанкционированного доступа к конфиденциальной информации ПИФ.

В качестве ограничений выступают ограничения на степень защищенности данных ПИФ, на стоимость проектирования, разработки и эксплуатации системы защиты, ограничения, обусловленные используемыми СУБД и ОС, ограничения, определяемые требованиями к эффективности использования ресурсов информационной инфраструктуры и др.

Обозначим через G=$\{ g_\delta / \delta = \overline{1,\Delta} \}$ множество проектируемых файлов БД ПИФ, C=$\{ c_b / b = \overline{1,B} \}$ – множество терминалов (рабочих станций) пользователей, U=$\{ u_k / k = \overline{1,K_0} \}$ – множество пользователей ПИФ, Y=$\{ y_f / j = \overline{1,F} \}$ – множество устройств хранения данных (внешних запоминающих устройств). Степени секретности логических записей (объектов данных и информационных элементов записи) задаются множеством Ф=$\{ \varphi_i / i \in R \}$, а профили полномочий пользователей – матрицей П=$\| \pi_{ki} \|$.

Логическая структура БД ПИФ представляет собой ориентированный граф $G_л(N, W_л)$, где $N = \{n_j : j = \overline{1,J}\}$ – множество логических записей, $W_л = \{ (n_j, n_{j'}) / j, j' = \overline{1,J} \}$ – множество взаимосвязей между записями. Формально логическая структура БД ПИФ описывается матрицей смежности $\hat{B} = \| \hat{b}_{jj'} \|$. Структура запросов пользователей к информации ПИФ задается с помощью матрицы D=$\| d_{kj} \|$. где d_{kj}=1, если k-му пользователю требуется запись n_j, d_{kj} = 0, в противном случае. Периодичность выполнения запросов представляется в виде вектора $\sigma = \{\sigma_k / k = \overline{1,K}\}$, где σ_k – частота выполнения запроса k-го пользователя.

Механизм защиты логической структуры БД ПИФ M($G_л$) формально задается матрицей смежности $\hat{B} = \| \hat{b}_{jj'} \|$, матрицей степеней секретности логических записей $F = \| f_{ji} \|$, а также

матрицей профилей полномочий пользователей $P = \|p_{ki}\|$. Матрица F индексируется по строкам множеством типов записей N логической структуры БД и множеством связей между ними $W_л$, которые требуют защиты, а по столбцам – множеством установленных для записей и связей степеней секретности $\Phi = \{\varphi_i : i \in R\}$. Элемент $f_{ji}(f_{jj',i})$=1, если для логической записи (связи) $n_j \in N((n_j, n_{j'}) \in W_ë)$ установлена степень секретности φ_i, $f_{ji}(f_{jj',i})$=0, в противном случае.

Множество внешних запоминающих устройств У={y_f}, используемых для размещения информации БД ПИФ, описываются следующей системой векторов:

- $\Lambda = \{\lambda_f / f = \overline{1,F}\}$ – вектор объемов памяти внешних запоминающих устройств, где λ_f – объем f-го ВЗУ;
- W={w_f/ $f = \overline{1,F}$} – вектор средних стоимостей хранения байта информации на внешних носителях;
- $\Psi = \{\psi_f / f = \overline{1,F}\}$ – вектор средних времен доступа к внешним запоминающим устройствам.

Ценность информации ПИФ будем выражать через условную стоимость, определяемую затратами на ее сбор, подготовку и формирование требуемых структур хранения; средствами, вложенными в проектирование, изготовление и испытание объектов предметной области, сведения о которых размещены в базе данных. Ценность информации представляется в виде вектора условных стоимостей сведений, содержащихся в множестве логических записей БД E={e_1,e_2,...,e^j,...,e^J}, где e j – условная стоимость j-й логической записи.

Угрозы безопасности можно классифицировать по вероятностям их проявления и представить в виде вектора $\mu = \{\mu_1, ..., \mu_j, ..., \mu_J\}$, где μ_j – вероятность проявления угрозы несанкционированного доступа со стороны неавторизованных пользователей к j-му типу логической записи.

Использование методов и средств обеспечения безопасности информации на различных уровнях защиты БД ПИФ описывается с помощью матрицы смежности W=$\|w_{\nu s}\|$, $\nu = \overline{1,\nu_0}, s = \overline{1,S}$, где индекс ν указывает уровень защиты. Элемент матрицы $w_{\nu s}$ = 1, если на ν-м уровне защиты БД ПИФ может быть использован s-й метод защиты и равен нулю в противном случае. В общем случае злоумышленнику требуется преодолеть четыре препятствия, чтобы получить доступ к конфиденциальной информации, т. е. ν_0=4. Первое препятствие обусловлено комплексом организационно-технических и программных мер и мероприятий по обеспечению контроля доступа в помещения ЦОД. При этом, если инфраструктура СЭХД ПИФ размещается в «облаке» с использованием соответствующих облачных ИТ, то для данного уровня защиты требуются дополнительно методы и средства защиты механизмов доступа к облачным данным, проверки достоверности и неизменности данных в облаке [10]. Второе препятствие связано с наличием программно-технических методов и средств защиты рабочих станций и терминалов. Следующее препятствие – это методы, обеспечивающие защиту внешних запоминающих устройств от несанкционированного доступа к размещенным на них данным. Методы защиты,

предназначенные для предупреждения неправомочного обращения к файлам ТПБД, образуют четвертый уровень защиты.

Для формализации постановки задачи синтеза оптимальной системы защиты ПИФ от несанкционированного доступа введем следующие переменные:

$x_{j\delta}=1$, если j-я логическая запись включена в состав δ-го файла БД ПИФ, $x_{j\delta}=0$, в противном случае;

$x_{\delta}^{k}=1$, если $\sum_{j=1}^{J} x_{j\delta} d_{kj} \geq 1$, $x_{\delta}^{k}=0$, если $\sum_{j=1}^{J} x_{j\delta} d_{kj}=0$. Переменные x_{δ}^{k} определяют требования пользователей на доступ к файлам БД ПИФ;

$x_{\delta k}=1$, если $x_{\delta}^{k}\prod_{j\in J_\delta} x_{j\delta}\sum_{i=1}^{I} f_{ji}\pi_{ki}\geq 1$, $x_{\delta k}=0$, если $x_{\delta}^{k}\prod_{j\in J_\delta} x_{j\delta}\sum_{i=1}^{I} f_{ji}\pi_{ki}=0$, где J_δ – индексы элементов множества логических записей, включенных в структуру файла q_δ. Переменная $x_{\delta k}$ идентифицируют правомочность доступа k-го пользователя ПИФ к δ-му файлу;

$x_{\delta f}^{'}=1$, если файл g^{δ} размещается на f-м ВЗУ, $x_{\delta f}^{'}=0$, в противном случае;

$y_{kf}=1$, если $\sum_{\delta=1}^{\Delta} x_{\delta}^{k} x_{\delta f}^{'}\geq 1$, $y_{kf}=0$, если $\sum_{\delta=1}^{\Delta} x_{\delta}^{k} x_{\delta f}^{'}=0$. Переменная y_{kf} равна единице в том случае, когда требуемая k-му пользователю информация размещена на f-м ВЗУ;

$y_{k}^{f}=1$, если $y_{kf}\prod_{\delta\in\Delta_f}(\sum_{i=1}^{I} x_{\delta j}^{'} f_{\delta i}\pi_{ki})=1$, $y_{k}^{f}=0$, если $y_{kf}\prod_{\delta\in\Delta_f}(\sum_{i=1}^{I} x_{\delta f}^{'} f_{\delta i}\pi_{ki})=0$, где Δ_f – множество файлов ПИФ, размещенных на f-м ВЗУ, $f_{\delta i}$ - степень секретности δ-го файла, которая определяются следующим образом: $f_{\delta i}=\max\{f_{ji}/j\in J_\delta\}$. Переменная $y_{k}^{f}=1,$ если на требуемом k-му пользователю ПИФ f-м ВЗУ не хранится информация, степень секретности которой превышает уровень полномочий рассматриваемого пользователя;

$\bar{y}_{kb}=1$, если k-му пользователю для доступа к БД ПИФ выделен b-й терминал, $\bar{y}_{kb}=0$, в противном случае;

$y_{bf}^{'}=1$, если $\sum_{k=1}^{K}\bar{y}_{kb} y_{kf}\geq 1$, $y_{bf}^{'}=0$, если $\sum_{k=1}^{K}\bar{y}_{kb} y_{kf}=0$. Переменная $y_{bf}^{'}$ устанавливает необходимость отображения на b-й терминал информации, размещенной на f-м ВЗУ;

$z_{\varepsilon s}^{\nu}=1$, если для защиты ε-го объекта, расположенного на ν-м структурном уровне выбран s-й метод, $z_{\varepsilon s}^{\nu}=0$, в противном случае. Значения индекса ε определяются рассматриваемым структурным уровнем защиты, т. е. конкретным значением индекса ν. Если ν=1, то ε=1, а при значениях ν=2, ν=3, ν=4 имеем $\varepsilon=\overline{1,B}$, $\varepsilon=\overline{1,F}$, $\varepsilon=\overline{1,\Delta}$, соответственно;

$\tilde{x}_{\delta k}=1$, если $(\sum_{f\in F_b}\sum_{b\in B_k} y_{bf}^{'}\bar{y}_{kb} y_{kf} x_{\delta f}^{'})(1-x_{\delta k})\prod_{s=1}^{S}(1-z_{\delta s}^{4})\geq 1$,

$\tilde{x}_{\delta k}=0$, если $(\sum_{f\in F_b}\sum_{b\in B_k} y'_{bf}\,\bar{y}_{kb}\,y_{kf}x'_{\delta f})(1-x_{\delta k})\prod_{s=1}^{S}(1-z^4_{\delta s})=0$, где F_b – множество индексов ВЗУ, на которых размещен δ-й файл, B_k – множество индексов терминалов, доступных k-му пользователю. Ненулевое значение переменной $\tilde{x}_{\delta k}$ означает, что пользователь u_k может осуществить беспрепятственно несанкционированный доступ к файлу g_δ, т. к. он имеет право обращаться к ВЗУ, на котором размещен файл g_δ и к связанному с этим ВЗУ терминалу, а указанный файл непосредственно не защищен хотя бы одним методом из множества M={m_s/s=$\overline{1,S}$};

$z_{\delta\delta'}=1$, если $\sum_{j=1}^{J}\sum_{j'=1}^{J}x_{j\delta}x_{j'\delta'}\xi_{j'j}\geq 1$, $z_{\delta\delta'}=0$, если $\sum_{j=1}^{J}\sum_{j'=1}^{J}x_{j\delta}x_{j'\delta'}\xi_{j'j}=0$, где $\xi_{j'j}$ – элемент матрицы достижимости логических записей, формируемой на основе матрицы смежности $\hat{B}=\left\|\hat{b}_{jj'}\right\|$. Переменная $z_{\delta\delta'}$ определяет достижимость файла g_δ из файла $g_{\delta'}$;

$z^{\delta}_{\delta'}=1$, если $\sum_{j=1}^{J}\sum_{j'=1}^{J}x_{j\delta}x_{j'\delta'}\hat{b}_{j'j}\geq 1$, $z^{\delta}_{\delta'}=0$, если $\sum_{j=1}^{J}\sum_{j'=1}^{J}x_{j\delta}x_{j'\delta'}\hat{b}_{j'j}=0$. Переменная $z^{\delta}_{\delta'}$ определяет отношения смежности между файлами физической структуры БД;

$z_\delta=1$, если $\sum_{j\in J_t}x_{j\delta}\geq 1$, $z_\delta=0$, если $\sum_{j\in J_t}x_{j\delta}=0$, где J_t – множество типов логических записей, которые могут служить точками входа в базу данных. Переменная z_δ равна единице, если δ-й файл представляет собой возможную точку входа в БД;

$\hat{x}^k_{\delta'}=1$, если $\sum_{\delta=1}^{\Delta}x^k_{\delta}z_{\delta'\delta}\geq 1$, $\hat{x}^k_{\delta'}=0$, если $\sum_{\delta=1}^{\Delta}x^k_{\delta}z_{\delta'\delta}=0$. Переменная $\hat{x}^k_{\delta'}$ принимает значение равное единице, если q_k-й пользователь использует δ-й файл для формирования ответа на запрос, либо для поиска требуемых ему данных.

Одним из достаточно эффективных средств повышения уровня защиты информации ПИФ от несанкционированного доступа является обеспечение максимальной информационной независимости пользователей. Поэтому в качестве критерия эффективности при решении задачи синтеза системы защиты ПИФ целесообразно использовать минимум межпользовательского информационного интерфейса. Математическая модель в этом случае имеет вид:

$$\min_{\{x_{j\delta},\,x'_{\delta f},\,\bar{y}_{kb},\,z^{\nu}_{\varepsilon s}\}}\sum_{\delta=1}^{\Delta}\sum_{k=1}^{K-1}\sum_{k'=k+1}^{K}\hat{x}^k_{\delta}\hat{x}^{k'}_{\delta} \quad (1)$$

при ограничениях:

- на суммарные затраты на разработку и эксплуатацию:

$$\sum_{S=1}^{S}v_s\left[Z^1_{\varepsilon s}+\sum_{b=1}^{B}Z^2_{bs}+\sum_{f=1}^{F}(Z^3_{fs}+\sum_{\delta=1}^{\Delta}Z^4_{\delta s}\cdot x'_{\delta f})\right]\leq V_{\max}, \quad (2)$$

где V_{max} – средства, выделенные на разработку и эксплуатацию множества методов защиты информации ПИФ;

- на допустимость использования методов защиты на различных структурных уровнях:

$$w_{vs} - z_{\varepsilon s}^{v} \geq 0, \ \forall v = \overline{1, v_0}, \ \forall s = \overline{1, S}; \quad (3)$$

- на обязательность правомочного доступа пользователей к требуемым им файлам:

$$x_{\delta}^{k} - x_{\delta k} = 0, \ \forall k = \overline{1, K}, \ \forall \delta = \overline{1, \Delta}; \quad (4)$$

- на обязательность правомочного доступа пользователей к ВЗУ, на которых размещены требуемые им файлы:

$$y_{kf} - y_{k}^{f} = 0, \ \forall k = \overline{1, K}, \ f = \overline{1, F}; \quad (5)$$

- на потери от несанкционированного доступа пользователей ТПБД к конфиденциальной информации:

$$\sum_{k=1}^{K} \sum_{\delta=1}^{\Delta} \tilde{x}_{\delta k} \cdot \sum_{j=1}^{J} x_{j\delta} \cdot e_j \leq \tilde{\mathrm{E}}, \quad (6)$$

где $\tilde{E}$ – максимально допустимые суммарные потери от несанкционированных действий пользователей ПИФ;

- на затраты процессорного времени, требуемого для реализации используемых программных методов защиты:

$$\sum_{s \in S.} t_S \left[\sum_{\varepsilon=1}^{B} z_{\varepsilon s}^{2} + \sum_{f=1}^{F} \left(z_{fs}^{3} + \sum_{\delta=1}^{\Delta} z_{\delta s}^{4} \cdot x'_{\delta f} \right) \right] \leq T^{*}, \quad (7)$$

где T* – максимально допустимые затраты процессорного времени на реализацию программных методов защиты;

- на число терминалов, закрепляемых за пользователем:

$$1 \leq \sum_{b=1}^{B} \bar{y}_{kb} \leq B_{k}^{*}, \ \forall k = \overline{1, K}, \quad (8)$$

где B_k^* – максимальное число терминалов, которые могут быть предоставлены для работы k-му пользователю;

- на допуск для работы на одних и тех же терминалах пользователей с разными уровнями полномочий:

$$y_{kb} \cdot \pi_{ki} + y_{k'b} \cdot \pi_{k'i'} \leq 1, \quad (9)$$

для заданных i, i'; $k, k' = \overline{1, K}$, $k \neq k'$, $\forall b = \overline{1, B}$;

- на число типов логических записей, объединяемых в один файл:

$$1 \leq \sum_{j=1}^{J} x_{j\delta} \leq L^{*}, \ \forall \delta = \overline{1, \Delta}, \quad (10)$$

где L* – максимально допустимое число типов логических записей, объединенных в один файл;

- на допустимость объединения в один файл отдельных типов логических записей:

$$x_{j\delta} + x_{j'\delta} \le 1 \text{, для заданных } n_j, n_{j'} \in N;\ \forall \delta = \overline{1,\Delta} \quad (11)$$

Поставленная задача синтеза оптимальной системы защиты ПИФ от несанкционированного доступа относятся к классу задач нелинейного целочисленного программирования с булевыми переменными. Для их решения могут использоваться универсальные методы и алгоритмы, предложенные в [11] для решения разнообразных задач анализа и синтеза оптимальных структур БД различного класса и назначения с учетом специфики поставленной задачи и ограничений (2)-(11).

Заключение

Предложенные в работе модели и методы синтеза обеспечивают:

- распределение логических записей по файлам БД ПИФ с учетом степеней секретности логических записей и характеристик запросов пользователей;
- распределение файлов ПИФ между ВЗУ в соответствии с требованиями безопасности данных и эффективности доступа к ним;
- закрепление пользователей ПИФ за терминалами;
- сопряжение множества терминалов с множеством внешних носителей;
- закрепление методов непосредственной защиты за объектами защиты различных структурных уровней;
- размещения БД ПИФ на устройствах внешней памяти, т. е. позволяют сформировать оптимальную по заданному критерию эффективности, коррелированному с требованиями информационной безопасности, систему защиты баз данных патентного информационного фонда от несанкционированного доступа.

Разработанные модели, методы и средства построения эффективной системы защиты ПИФ использовались при создании СУИБ ЕАПВ ЕАПО, которая в 2015 году была введена в промышленную эксплуатацию. Их применение позволило на 30-50 % сократить время и затраты на проектирование и разработку структур ряда патентных БД ПИФ, содержащих конфиденциальную информацию: БД «Евразийские заявки на изобретения», БД «Неопубликованные евразийские патенты», БД «Реестр евразийских патентов», БД электронных досье дел евразийских заявок и патентов и других с учетом требований защиты данных, а также системы защиты ПИФ ЕАПВ ЕАПО с одновременным повышением качества вырабатываемых проектных решений.

ЛИТЕРАТУРА

1. В. О. Сиротюк Проблемы и задачи обеспечения информационной безопасности патентно-информационных ресурсов. М.: Патентная информация сегодня, №1 / 2012, с. 3-10.
2. Информационная безопасность систем организационного управления. Теоретические основы: в 2 т. / Н. А. Кузнецов, В. В. Кульба, Е. А. Микрин и др. – М.: Наука, 2006.
3. 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.
4. 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.
5. Х. Ф. Фаязов, В. О. Сиротюк, А. В. Овчинников, А. Б. Бурцев Использование Евразийской патентно-информационной системы (ЕАПАТИС) при проведении патентных поисков. – М.: ИНИЦ «ПАТЕНТ», 2009. – 92 с.
6. 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.
7. В. О. Сиротюк Методы и средства обеспечения информационной безопасности патентных ведомств. М: Патентная информация сегодня, №2 / 2012, с. 3-11.
8. Kizza Joseph Migga. Guide to Computer Network Security. Springer, 2017. – 569 p. – ISBN 978-3-319-55606-2.
9. Brdarevic Omega. HackerTools Crack With Disassembling, 2016. – 517 p. – ASIN B01MTKQGQ9.
10. H. Wang. Identity-Based Distributed Provable Data Possession in Multicloud Storage // IEEE Trans. Services Computing. – 2015. Vol. 8, № 2. – P. 328-340.
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. Кульба В. В., Курочка Н. П. Математическая модель обеспечения безопасности информации в базах данных // Интернет-журнал «Науковедение» Том 7, №3 (2015) http://naukovedenie.ru/PDF/108TVN315.pdf.

Kul'ba Vladimir Vasil'evich
Institute of control science of Russian academy of science, Russia, Moscow
E-mail: kulba@ipu.ru

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

Models and methods of synthesis of the optimal protection system of the patent information fund of the international patent organization against unauthorized access

Abstract. The paper proposes formalized models and methods for synthesizing an optimal system for protecting the patent information fund of an international patent organization against unauthorized access by the example of the Eurasian Patent Office of the Eurasian Patent Organization. The goals and objectives of the Eurasian Patent Office in the field of information security are formulated, the specifics of the formation and development of the patent information fund created in the Eurasian Patent Office in the form of a virtual patent information store are considered. The indicators of efficiency and quality of the patent information fund, used in the preparation of databases of patent information, non-patent literature and patent-associated documentation, are introduced. Based on the analysis, the main threats to the information security of the patent information fund were identified and the prerequisites and requirements for the creation of an information security management system for an international patent organization were formulated.

A formal definition of the protection system of patent information fund against unauthorized access is given and its characteristics are described. The general task of synthesis of the optimal system of protection of databases of the patent information fund from unauthorized access is set and its decomposition into a series of successively solved subtasks is performed. The criteria of efficiency of the problems of synthesis of the system of protection from unauthorized access, correlated with the requirements of protection, are proposed.

A mathematical model of the problem of synthesizing the optimal system for protecting the data of the patent information fund from unauthorized access by the criterion of the minimum of the inter-user information interface was developed. The synthesis problem is presented as a non-linear integer programming problem with Boolean variables. To solve it, appropriate methods and algorithms are proposed. The results of the solution of the stated synthesis problem were used in the construction of an effective information security management system of the Eurasian Patent Office of the Eurasian Patent Organization.

Keywords: the Regional International Patent Organization; patent information fund; Database of the patent information fund; the threat of information security of the patent information fund; system of patent information fund protection against unauthorized access; Information security management system