СПИСОК ЛИТЕРАТУРЫ

1. Griffiths L. J. Signal extraction using real-time adaptation of a linear multichannel filter / Stanford University. Stanford, Calif., 1968. 8 p.

2. Адаптивные антенные системы / Б. Уидроу, П. Е. Мантей, Л. Д. Гриффитс, Б. Б. Гуд // ТИИЭР. 1976. Т. 55, № 12. С. 78–95.

3. Daniell T. P. Adaptive estimation with manually correlated tracing samples / Stanford Electron. Labs. Stanford, Calif., 1968. 14 p.

D. M. Klionskiy, A. M. Golubkov, D. I. Kaplun, M. S. Kupriyanov
Saint Petersburg Electrotechnical University «LETI»

ADAPTIVE ALGORITHM FOR HYDROACOUSTIC SIGNAL PROCESSING

The paper discusses an adaptive algorithm for processing signals of antenna arrays in real time. The results of our analysis of the algorithm are provided. The algorithm is based on an iterative procedure for finding a set of weighting coefficients. We have also provided recommendations for using the algorithm in various conditions.

Adaptive algorithm, hydroacoustic monitoring, hydroacoustic signal

УДК 004.056

В. И. Воробьев, Р. Р. Фаткиева
Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН)

Ю. А. Шичкина
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)

Автоматизация процесса корректировки регламентирующих документов в соответствии со стандартами информационной безопасности

Рассмотрен подход к анализу стандартов и алгоритмов с использованием онтологического моделирования. Для разработки «Политики безопасности» и «Профиля пользователя» предприятия и изучения его предпочтений использовался аппарат онтологий.

Гармонизация стандартов, нормативно-правовые акты, онтологии, модель защиты

Стандарты и нормативно-правовые акты в области информационной безопасности определяют необходимость, архитектуру, методику и последовательность применения средств защиты любых информационных ресурсов и данных, в том числе персональных, неправомерное оперирование с которыми может нанести ущерб их собственнику, владельцу, пользователю или иному лицу [1].

С другой стороны, в представленных правовых актах отсутствуют методологические рекомендации по измерению, интерпретации и оценке параметров информационной безопасности, которые представляют собой разнородные данные, полученные как прямым измерением, так и косвенным. При этом практически не учитываются ошибки измерения. Особенно это актуально при комплексной оценке комбинированных средств защиты и организационно-технических мер.

Проблема формирования методологического подхода представляет сложность при выборе как непосредственно самих показателей, так и средств измерения. В частности, отдельным звеном стоят

вопросы анализа, позволяющего не только оценить результат, но и осуществить необходимые меры по защите информации. В настоящее время в законодательной базе не приводятся необходимые показатели защищенности и их доверительные интервалы, на базе которой возможно создание сбалансированной системы измерения информационной безопасности. При этом существующие методики не позволяют оценить системы в целом. Также отсутствует перечень применяемых средств измерений, алгоритмов обработки результатов измерения, методы сравнения и выбора наилучшего варианта защиты при минимальных затратах на обеспечение безопасности.

Вторая проблема – выбор показателей, что особенно важно в условиях, когда возникает необходимость принятия превентивных мер в режиме реального времени. В качестве примера можно привести необходимость оценки состояния сетевой безопасности в условиях атаки. В данном случае мониторинг сети ложится дополнительной нагрузкой на каналы связи, что в свою очередь только усугубляет ситуацию. При этом для распространенных атак полностью отсутствует методологический аппарат, позволяющий произвести указанную оценку [2]–[4].

Решение проблемы выбора показателей для большого количества разнообразных средств защиты информации, работа которых может не подпадать ни под один из существующих стандартов, требует введения ведомственных законодательных актов в отрасли или внесения изменений в существующую политику безопасности в пределах предприятия. Обоснование подобных изменений в регламентирующих документах чаще всего основываются на оценке интегрального показателя информационной безопасности по критерию максимизации целевой функции, что не всегда может обеспечить заданный уровень защиты информации.

Приведенные факты подтверждают необходимость введения процедуры гармонизации, которая рассматривается далее на примере автоматизированного анализа документов «Политика безопасности» и «Профиль пользователя» предприятия. Предлагаемый анализ направлен на выявление проблемных цепочек, которые влекут за собой ошибку в способе доступа к системе, что приводит к утере или искажению корпоративной информации.

Для гармонизации предлагается использовать онтологическое описание, включающее построение таксономий терминов предметной области, предикативных отношений между терминами, учитывающих семантику концептов предметной области, а также средства интеграции онтологий: встраивание, связывание и объединение [1]. Задачей гармонизации является построение непротиворечивого формального описания предметной области и построение прикладного программного обеспечения для поддержки унифицированной схемы данных, включая построение терминологических таксономий, предикативных отношений, дескриптивных ограничений для вывода новых типов данных и расширение множества правил вывода. Важным моментом является возможность уточнения терминологии и предикативных отношений.

Онтологическое моделирование позволит дать эффективное метаописание регламентирующих документов в виде формальной компьютерной модели (семантической сети), автоматизировать их смысловое сопоставление средствами семантического анализа, обеспечить программный механизм доступа к документам при использовании Web-технологий (XML, RDF, OWL, SPARQL) для их описания.

Уже имеется определенный опыт семантического анализа понятийного аппарата стандартов Common Criteria и ISMS с применением средств полуформального моделирования [4], [5]: объектно-ориентированная модель общего контекста безопасности; модель угрозы, контекста угрозы; полная функциональная модель оценки ИТ по Common Criteria; функциональная модель требований к СУИБ по стандартам ISO 27001, ISO 27001.

Существуют программные продукты (ПП), используемые для проверки соответствия политики информационной безопасности требованиям стандарта ISO 17799: Cobra (компания C & A Systems Security Ltd); КОНДОР+ (компания Digital Security); Метод CRAMM (CCTA Risk Analysis and Management Method); Risk Watch; ГРИФ 2006 из состава Digital Security Office и др., которые имеют свои недостатки, в частности, отсутствие возможности установки пользователем веса на каждое требование; отсутствие русскоязычной версии; требование специальной подготовки и высокой квалификации аудитора; высокая стоимость лицензии.

Предлагается онтологическая модель политики безопасности предприятия на основе системы Protégé. Процесс создания онтологий начинается с создания «чернового варианта» политики безопасности с последующей детализацией для

определения деталей, со следующей итерацией, до тех пор пока создаваемая онтология не будет отражать концепцию предметной области с определенной степенью точности. На практике данная технология включает: определение классов в онтологии, иерархии классов (базовый класс –> подкласс); определение слотов и их допустимых значений; заполнение значений слотов для экземпляров классов [5], [6].

Покажем классы онтологии на примере условного предприятия, описывающие понятия предметной области. Каждый из классов может иметь свой подкласс, который изображает более подробное описание, чем его надкласс.

Общая структура организации представлена на рис. 1.

Рис. 1

Представленный способ хранения и доступа к информации позволяет ранжировать информацию по носителям. Общий вид представлен на рис. 2.

Рис. 2

Создание свойств и их ограничений позволяют специфицировать общие факты о членах классов. Различают 2 типа свойств: свойства-значения – отношения между представителями классов и типами данных; свойства-объекты – отношения между представителями двух классов.

Заполнение классов и слотов онтологии политики безопасности конкретными экземплярами – довольно долгий процесс, поэтому покажем заполнение одной группы экземпляров. В качестве примера возьмем класс Director (Генеральный директор). Вначале необходимо заполнить те слоты, которые являются типом слот-значение: фамилия, имя сотрудника, стаж работы сотрудника и его заработная плата, рабочая станция, телефон. Результат работы представлен на рис. 3.

Используя разработанную политику безопасности, генеральный директор имеет доступ ко всем компьютерам сотрудников, подписывает документацию, организует работу сотрудников, управляет персоналом, принимает участие в формировании бюджета и контролирует его выполнение. Для выявления несоответствия учетной политики политике безопасности сформируем поисковые запросы. В качестве примера запроса представим запрос на поиск лиц, ответственных за учет запчастей. Для этого в поле Slot выберем «Otherduties» и соответствующий экземпляр «Ведение базы запчастей». После нажатия кнопки Find результат запроса отобразится в поле Search Results справа (рис. 4).

Как видно из рисунка, имеется ошибка в разграничении доступа к корпоративной информации. Онтологическая модель выявила ошибку в распределении прав доступа. К данной информации имеет право доступа (чтение/запись) только лишь бухгалтер.

Структуру представленной онтологической модели можно расширить, при необходимости, добавив большое количество сотрудников и обязанностей, сделав поиск ошибки автоматизированным.

Модель системы защиты предприятия. Для формального описания систем защиты требуется разработка модели системы защиты, в которой рассматривается взаимодействие «области угроз», «защищаемой области» (ресурсов АС) и «системы защиты» (механизмов безопасности АС):

$T = \{t_i\}$ – множество угроз безопасности;

$O = \{o_j\}$ – множество объектов (ресурсов) защищенной системы;

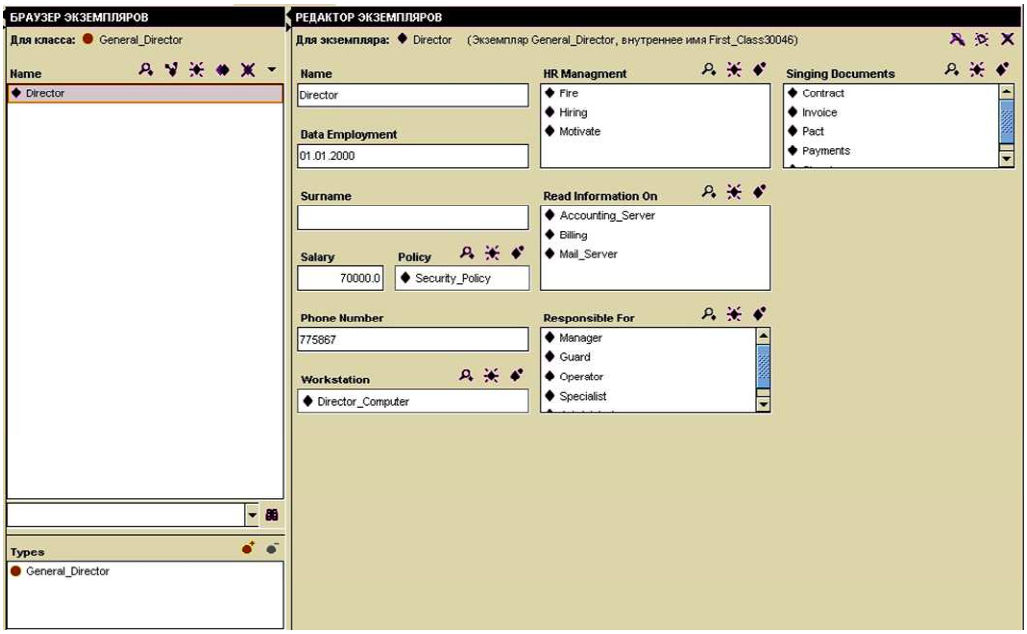

Рис. 3

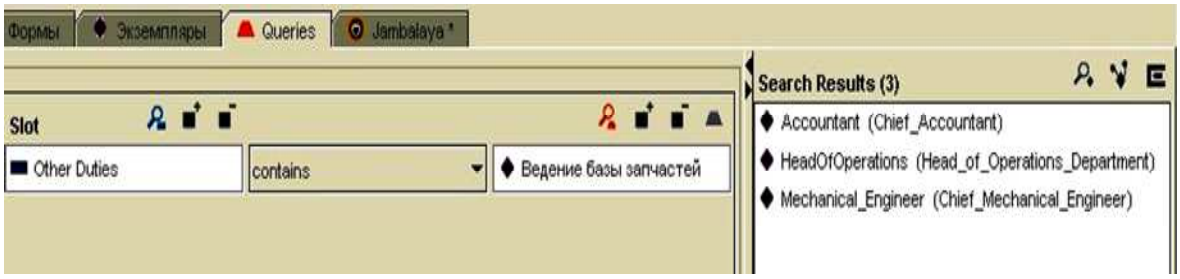

Рис. 4

$M = \{m_k\}$ – множество механизмов безопасности.

Для описания системы защиты обычно используется графовая модель, представленная на рис. 5. Множество отношений угроза-объект образует двухдольный граф {<*T*, *O*>}. Цель защиты состоит в том, чтобы перекрыть все возможные ребра в графе. Это достигается введением третьего набора *M*. В результате получается трехдольный граф {<*T*, *M*, *O*>}.

Развитие этой модели предполагает введение еще двух элементов:

V – набор уязвимых мест, определяемый подмножеством декартова произведения *T***O*: $v_r = <t_i, o_j>$. Таким образом, под уязвимостью системы защиты будем понимать возможность осуществления угрозы *t* в отношении объекта o (на практике под уязвимостью системы защиты обычно понимают не саму возможность осуществления угрозы безопасности, а те свойства системы, которые способствуют успешному осуществлению угрозы либо могут быть использованы злоумышленником для осуществления угрозы);

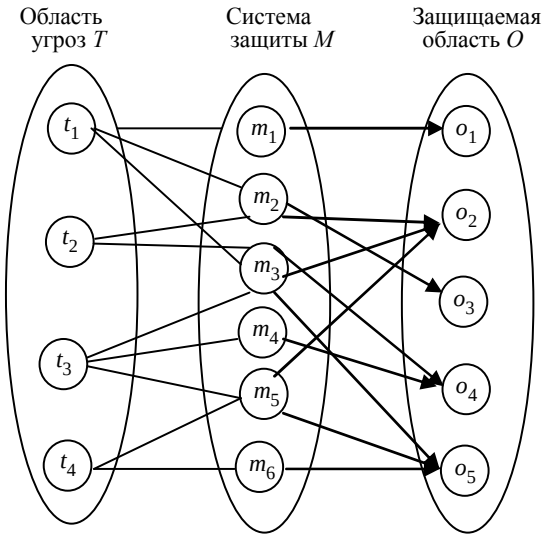

Рис. 5

B – набор барьеров, определяемый декартовым произведением *V***M*: $b_l = <t_i, o_j, m_k>$, представляющих собой пути осуществления угроз безопасности, перекрытые средствами защиты.

В результате получаем систему, состоящую из пяти элементов: <*T*, *O*, *M*, *V*, *B*>, описываю-

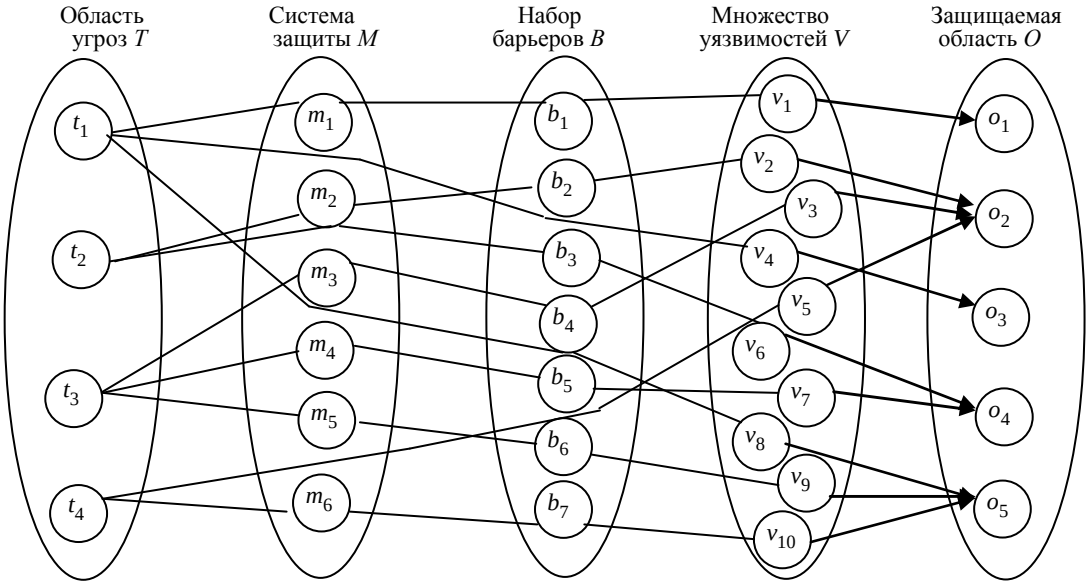

Рис. 6

щую систему защиты с учетом наличия в ней уязвимостей (рис. 6).

Для системы с полным перекрытием выполняется условие: для любой уязвимости имеется соответствующий барьер, устраняющий эту уязвимость.

Таким образом, в системе защиты с полным перекрытием для всех возможных угроз безопасности существуют механизмы защиты, препятствующие осуществлению этих угроз. Данное условие является первым фактором, определяющим защищенность АС. Вторым фактором является прочность существующих механизмов защиты.

Защищенность АС от угроз безопасности S определяется количеством уязвимостей v, для которых в системе не создано барьеров b, перекрывающих эти уязвимости, а также прочностью существующих барьеров [7].

Механизм защиты должен блокировать соответствующий путь осуществления угрозы $<t_i, o_j>$. На практике механизмы защиты обеспечиваются частично. В связи с этим в качестве характеристик элемента набора барьеров $b_l = <t_i, o_j, m_k>$ может рассматриваться набор $<P_l, L_l, R_l>$, где P_l – вероятность появления угрозы; L_l – размер ущерба при удачном осуществлении угрозы в отношении защищаемых объектов (уровень серьезности угрозы); R_l – степень сопротивляемости механизма защиты m_k, характеризующаяся вероятностью его преодоления.

Стойкость барьера $b_l = <t_i, o_j, m_k>$ характеризуется значением остаточного риска Riskl, связанного с возможностью осуществления угрозы безопасности t_i в отношении объекта АС o_j, при использовании механизма защиты m_k, т. е. Riskl = $= P_k L_k (1 - \mathrm{R_k})$.

Далее защищенность S можно оценить следующим образом:

$$S = 1 \Big/ \left[\Sigma_{\forall b_k \in B} \left(P_k L_k \left(1 - R_k\right)\right)\right],$$

где P_k, L_k Є (0, 1), R_k Є [0, 1].

Знаменатель определяет суммарное значение условных рисков, связанных с возможностью осуществления угроз безопасности T в отношении объектов АС, при использовании механизмов защиты M. Суммарное значение условных рисков характеризует уязвимость системы защиты в целом, а защищенность АС определяется как обратная величина. При отсутствии в системе барьеров b_k, перекрывающих определенные уязвимости, стойкость средств защиты R_k принимается равной нулю.

На практике получение приемлемых значений характеристик барьеров затруднено, но даже модельные расчеты по данному алгоритму позволяют выделить бреши в системе барьеров защиты. С другой стороны, балансировка средств защиты с угрозами должна осуществляться с соблюдением регламентирующих документов. Включение оценок рисков в онтологическое описание документа «Политика безопасности» позволит автоматизировать проверку данного документа с учетом минимизации рисков.

СПИСОК ЛИТЕРАТУРЫ

1. Theory and Practice of Cryptography Solutions for Secure Information Systems / А. Ю. Атисков, В. И. Воробьев, Л. Н. Федорченко и др. // IGI Global, 701 E. Chocolate Ave. Hershey, PA 17033, USA. 2012. Dec. P. 101–130.
2. Воробьев В. И., Фаткиева Р. Р. Природа уязвимостей программного кода // Программируемые инфокоммуникационные технологии: сб. статей / под ред. В. В. Александрова, В. А. Сарычева. М.: Радиотехника, 2009. С. 53–55.
3. ISO/IEC Standing document 11. URL: http://www.din.de/blob/78920/e0cb93d9370a69c2e6b7b0f46571854b/sc27-sd11-overview-of-work-of-sc27-data.pdf.
4. Сайт компании Аудит информационной безопасности. URL: http://www.audit-ib.ru/audit/security-audit/information-flows/program-risk-analysis/ ©2011–2015 audit-ib.ru.
5. IT Governance Green Paper INFORMATION SECURITY& ISO 27001. URL: https://www.itgovernance.co.uk/files/RiskAssessmentSoftware (3).pdf.
6. Перспективные направления развития науки в Петербурге / отв. ред. Ж. И. Алферов, О. В. Белый, Г. В. Двас, Е. А. Иванова. СПб.: Изд-во ИП Пермяков С. А., 2015.

V. I. Vorobiev, R. R. Fatkieva
Saint Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS)

Yu. A. Shichkina
Saint Petersburg Electrotechnical University «LETI»

AUTOMATION OF THE CORRECTION PROCESS REGULATORY DOCUMENTS IN ACCORDANCE WITH INFORMATION SECURITY STANDARDS

Deals with an approach to standards and algorithms analysis on the basis of ontological modeling. Ontology apparatus was also applied to the development of Security Policy of an enterprise and of User's Profile as well as to User's Preferences studies.

Standards harmonization, regulatory acts, ontologies, protection model

УДК 51-37/.004

М. С. Попова
Международный государственный экологический институт им. А. Д. Сахарова БГУ (г. Минск, Беларусь)

Сравнительный анализ алгоритмов поиска информации в различных средах

Выполнен анализ существующих методов и алгоритмов поиска информации в различных видах информационно-поисковых систем. Рассмотрены основные типы информационно-поисковых систем. Кратко рассмотрена история развития технологий информационного поиска. Рассмотрены различные классификации алгоритмов поиска информации. Рассмотрены некоторые методы построения онтологии для задач библиографического поиска документов, их классификации и аннотирования.

Информационно-поисковая система, алгоритм информационного поиска, индексирование, ранжирование, поисковый запрос, библиографический поиск, онтология

Одним из основных информационных процессов является поиск информации. Вместе с ростом количества информации в доступных документах для решения этой задачи разрабатываются новые, все более совершенные, методы поиска необходимых документов. Существующие методы поиска информации разнообразны, что определяется условиями конкретных задач поиска, например