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

Том 8, №2 (2016) http://naukovedenie.ru/index.php?p=vol8-2

URL статьи: http://naukovedenie.ru/PDF/117TVN216.pdf

DOI: 10.15862/117TVN216 (http://dx.doi.org/10.15862/117TVN216)

Статья опубликована 16.05.2016.

Ссылка для цитирования этой статьи:
Ларионов И.П., Хорев П.Б. Проблемы создания и основные задачи экспертной системы поддержки проектирования комплексной системы защиты информации // Интернет-журнал «НАУКОВЕДЕНИЕ» Том 8, №2 (2016) http://naukovedenie.ru/PDF/117TVN216.pdf (доступ свободный). Загл. с экрана. Яз. рус., англ. DOI: 10.15862/117TVN216

УДК 004.891.2

Ларионов Игорь Павлович[1]
ФГБОУ ВО «Российский государственный социальный университет», Россия, Москва[2]
Аспирант
E-mail: cmpara@mail.ru
РИНЦ: http://elibrary.ru/author_items.asp?authorid=828881

Хорев Павел Борисович
ФГБОУ ВО «Национальный исследовательский университет «Московский энергетический институт», Россия, Москва
Преподаватель
Кандидат технических наук, доцент
E-mail: cmpara@mail.ru
РИНЦ: http://elibrary.ru/author_items.asp?authorid=620811

Проблемы создания и основные задачи экспертной системы поддержки проектирования комплексной системы защиты информации

Аннотация. В данной статье описываются проблемы разработки и основные задачи экспертной системы поддержки проектирования комплексных систем защиты информации. Проектирования комплексных систем защиты информации является нетривиальной задачей, и ее автоматизация является актуальной проблемой. Основная проблема состоит в том, что задача проектирования комплексных систем защиты информации относится к классу слабо формализованных задач с неполной информацией. В качестве решения данной проблемы предлагается использовать экспертную аналитическую систему поддержки проектирования, которая будет способна работать со слабо формализованными знаниями благодаря наличию специализированной базы знаний, а возможность уточнять входную информацию у пользователя позволяет преодолевать проблему изначальной неполноты информации. Такая система будет решать задачу многокритериальной оптимизации набора признаков, описывающих комплексную систему защиты информации для проектирования оптимального состава средств и методов защиты информации в комплексной системе защиты информации.

Ключевые слова: экспертные системы; принятие решений; система поддержки принятия решений; комплексная система защиты информации; экспертная система

[1] https://ru.linkedin.com/in/larionovigor

[2] 140180, Российская Федерация, Московская область, г. Жуковский, ул. Семашко, д. 8, корп. 2, кв. 41

поддержки проектирования; информационная безопасность; защита информации; многокритериальная оптимизация; система, основанная на знаниях; моделирование систем

Комплексные системы защиты информации (КСЗИ) на сегодняшний день стали неотъемлемой обязательной частью в составе каждой организации для обеспечения информационной безопасности своих бизнес-процессов. Проектирование КСЗИ на предприятии не является тривиальным и однозначным: нужно обеспечить выполнение базовых требований законодательства по информационной безопасности в отношении обработки коммерческой тайны, персональных данных сотрудников и клиентов или других типов конфиденциальной информации, защитить основные информационные активы предприятия, разработать организационно-распорядительные документы, разработать технический проект внедрения или модернизации существующей КСЗИ, соблюсти дополнительные требования заказчика [6].

Для разработки проекта такой системы надо рассмотреть множество различных факторов и добиться оптимального соотношения между уровнем обеспечиваемой информационно безопасности, ценой и качеством данной системы. Следовательно, надо рассмотреть несколько альтернативных вариантов проектов, сравнить их по критериям и выбрать не лучший или худший вариант по одному признаку, а оптимальный по всей совокупности ключевых признаков. Решение многокритериальных задач оптимизации в условиях неполной определенности трудоемкий и долговременный процесс, хорошо изложен в [5, 7, 9, 10]. Автоматизация процесса проектирования, включающей в себя такие этапы как формирования концептуальных требований, создания и расчета модели, формирования альтернатив и ее выбор (принятие решений) позволяет значительно упростить работу по проектированию и снизить расходы на КСЗИ в целом. [1]

КСЗИ состоит из следующих взаимосвязанных частей [6]:

- средства программно-аппаратной защиты информации;
- средства инженерно-технической защиты информации;
- организационные меры и организационно-распорядительная документация;

и направлена на обеспечение:

- конфиденциальности защищаемой информации – предотвращение несанкционированного доступа и распространения информации за пределы защищаемого объекта;
- целостности защищаемой информации – предотвращение несанкционированных изменений (модификация, удаление) существующей информации;
- доступности защищаемой информации – обеспечение непрерывности информационных процессов и предотвращение отказов в доступе к важным информационным ресурсам.

Для решения поставленной задачи по автоматизации процесса предлагается использовать методы искусственного интеллекта, в частности экспертные системы (ЭС). Экспертные системы [9] – это специальный вид интеллектуальных систем, которые содержат знания экспертов в определенной области и оперируют ими для выдачи рекомендации или принятия решения. Как правило, экспертные системы решают задачи следующего рода:

- извлечение информации из первичных данных и интерпретация этих данных (сигналы от датчиков, или информация от пользователя);

- диагностика неисправностей технических систем и заболеваний человека;
- структурный анализ сложных объектов;
- определение конфигурации и проектирование (компонентов систем, компьютеров, сложных объектов);
- инструктаж или обучение навыкам;
- контроль и управления процессами;
- прогнозирование;
- планирование;
- устранение нарушений в работе.

Рассмотрим основные составные части ЭС поддержки проектирования КСЗИ, задачи ЭС и проблемы, связанные с непосредственной реализацией ЭС поддержки проектирования КСЗИ.

ЭС поддержки проектирования КСЗИ должна иметь в своем составе подсистему поддержки принятия решений (СППР) для решения задачи оптимального проектирования подсистем КСЗИ с помощью многокритериальной оптимизации. Для этого необходимо чтобы различные варианты КСЗИ (альтернативы в теории принятия решений) были оценены по некоторым заранее выделенным критериям оценки, которые позволяют описать КСЗИ с точки зрения надежности, эффективности, экономичности. Критерии оценки могут состоять из подкритериев, формируя таким образом дерево принятия решений. Однако при проектировании КСЗИ возникает не только задача оптимального проектирования, но необходимость системного подхода к проектированию КСЗИ. Также для учета требований законодательства, внутренних положений организации и требований заказчика необходимо решить задачу информационно-аналитической поддержки проектирования КСЗИ, то есть ЭС должна иметь информационно-справочную подсистему для консультации и интерпретации введенных данных, аналитическую расчетную систему [8] для диагностирования и мониторинга текущего уровня защищенности и сравнения его с требуемым уровнем. ЭС должна не только получать данные на входе, но и предлагать решения, поясняя их – содержать подсистему объяснений и логического вывода. Для ЭС дополнительной задачей также является формализация методики оценки рисков ИБ и поддержка возможности создания дополнительных (пользовательских) методик с возможностью редактирования. ЭС может осуществить такую формализацию на основе базы знаний, фактов и правил, при этом для поддержки разработки собственных методик по оценки рисков ИБ необходимо создать некий шаблон правил и фреймов знаний для каждого из этапов, что подробнее изложено в [3, 4]. Таким образом, основные задачи ЭС поддержки проектирования, подлежащие решению, включают в себя:

1. сбор входных данных о состоянии уровня информационной безопасности предприятия, наличия средств защиты информации и организационных мер по обеспечению информационной безопасности на основе анкетирования – подготовка и утверждение технического задания для КСЗИ;
2. диагностирование уровня информационной безопасности, выявление несоответствий с предъявленными требованиями законодательства и учетом пожеланий заказчика на основе методики предложенной в [4];

3. формирование набора рекомендаций (альтернативных проектов) по повышению уровня информационной безопасности до требуемого уровня – создание технических предложений КСЗИ и их моделей;
4. выделение ключевых параметров сравнения (оптимизации) для поддержки принятия решения и ведения переговоров по окончательному варианту КСЗИ, формирование эскизного проекта;
5. получение (вывод) решения – формирование технического проекта;
6. поддержка разработки сопровождающей документации на систему, а также организационно-технических мер и организационно-распорядительных документов по защите информации;
7. повторное диагностирование уровня информационной безопасности предприятия после внедрения и опытной эксплуатации системы, внесение корректив и сравнение с исходными требованиями – формирование рабочего проекта и поддержка опытной эксплуатации;
8. завершение внедрения или модернизации КСЗИ, ее сертификация в соответствии с требованиями законодательства – информационно-правовая поддержка процесса сертификации КСЗИ.

Проектирование КСЗИ происходит на основе иерархической модели уровней:

1. физический уровень;
2. технологический уровень;
3. пользовательский уровень;
4. сетевой уровень;
5. уровень управления.

Основные проблемы, встречающиеся в ходе выполнения поставленной задачи, согласно [2] являются:

1. наполнение ЭС знаниями, фактами и правилами логического вывода в соответствие с [3];
2. формирование набора критериев для оценки альтернативных вариантов КСЗИ;
3. выбор стратегии многокритериальной оптимизации принятия решений для поиска оптимального варианта КСЗИ.
4. формирование подсистемы объяснений;
5. обеспечение простоты и удобства обновления знаний, правил и фактов экспертом;
6. обеспечение простоты и удобства пользования для конечного пользователя;
7. обеспечение детализации и наглядности подсистемы объяснений с поддержкой формирования таблиц, графиков, диаграмм и отчетов для выбранного решения;
8. обеспечение актуальности информационно-справочной подсистемы, содержащие основные требования и положения законодательства в области обеспечения информационной безопасности.

Таким образом, целью данной ЭС является поддержка принятия решений на различных этапах проектирования КСЗИ, создание оптимального набора средств и методов защиты информации на предприятии.

Формальное описание КСЗИ производится на основе системного подхода и математического моделирования. Однако создание формальной математической модели КСЗИ имеет ряд факторов, осложняющих эту задачу:

- модель должна обладать большим числом критериев для оценки КСЗИ и учитывать требования и ограничения, накладываемые действующим законодательством, причем требования и ограничения могут изменяться со временем, т.е. модель должна быть полной и адаптивной;
- ряд критериев КСЗИ взаимозависят от других показателей ИС, которые данная КСЗИ защищает (например, показатель качества, эффективности);
- критерии трудно выразить в точных количественных оценках, преобладает качественный, нечеткий характер в оценках;
- критерии взаимосвязаны, но взаимозависимость может иметь противоречивый характер (стоимость напрямую зависит от степени надежности КСЗИ, однако одновременно увеличивать надежность и снижать стоимость невозможно);
- на ранних этапах их проектирования КСЗИ собрать исходные данные для оценки альтернативных проектов согласно модели затруднительно.

Исходя из описанных условий, математическая модель КСЗИ не может быть построена на только традиционных методах математической статистики, теории вероятностей и методов оптимизации для решения задачи проектирования КСЗИ (анализа КСЗИ и синтеза средств защиты информации в КСЗИ). При этом процесс принятия решения основывается на качественных экспертных оценках, а не количественных в условиях неполной и неточной информации. Поэтому вместо классических методов необходимо использовать обработку экспертной исходной информации на базе теории нечетких множеств и лингвистической переменной. Подробнее теория нечетких множеств, нечеткой логики и лингвистических переменных рассмотрена в литературе [2], в том числе применительно к ее использованию в экспертных системах.

Пользователями данной системы могут являться сотрудники отдела или службы информационной безопасности предприятия. Они могут применять ее в целях контроля уровня информационной безопасности, проведения внутреннего аудита на предмет соответствия КСЗИ требованиям законодательства.

Поскольку любая ЭС перенимает опыт и знания экспертов в конкретных областях, то именно эксперты занимаются наполнением ЭС правилами и фактами, отлаживают ее работу, формируют систему понятий и объяснений, иными словами, занимаются инженерией знаний [8]. Такими экспертами для данной системы могут выступать инженеры, специалисты по защите информации, юристы (наполнение информационно-правовой справочной системы в области информационной безопасности).

Рассмотрев выше изложенное, можно сказать, что мы также рассмотрели первый этап разработки ЭС поддержки проектирования КСЗИ на предприятии, который включает в себя идентификацию целей, задач и проблем, которые должна решать система, определение круга пользователей и экспертов.

Применение ЭС для поддержки принятия решений при проектировании КСЗИ на предприятии позволяет существенно улучшить качество таких систем, дать четкое пояснение

необходимости применения тех или иных компонентов системы, разрабатывать несколько вариантов проекта КСЗИ для ведения переговоров с заказчиком, использовать опыт экспертов в области информационной безопасности.

ЛИТЕРАТУРА

1. Баранова Е.К. Методы принятия решений в разработке комплексной системы защиты информации, РГСУ, М: 2010 – 12 с.
2. Джозеф Джарратано, Гари Райли. Экспертные системы. Принципы разработки и программирование. М: Вильям, 2007. – 1152 с.
3. Ларионов И.П., Хорев П.Б. Особенности представления знаний в экспертной системе поддержки проектирования комплексной системы защиты информации // Материалы XXV международной научно-практической конференции «Современные проблемы гуманитарных и естественных наук» 08-09 октября 2015 г. / РФ, Москва, 2015.
4. Ларионов И.П., Хорев П.Б. Особенности разработки методики оценки информационной безопасности предприятия для экспертных систем // Современная наука: актуальные проблемы и пути их решения. Сборник научных статей. Труды международной дистанционной научной конференции №9, 23-24 мая 2014 г. / РФ, г. Липецк, 2014.
5. Лотов А.В., Бушенков В.А., Каменев Г.К., Черных О.Л. Компьютер и поиск компромисса, метод достижимых целей, издательство «Наука», М: 1997 – 404 с.
6. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб. пособие для вузов – М.: Горячая линия – Телеком, 2004. - 280 с.
7. Ногин В.Д. Принятие решений в многокритериальной среде: количественный подход. - М.: ФИЗМАТЛИТ, 2005, 176 с.
8. Советов Б.Я. Интеллектуальные системы и технологии: учебник для студ. Учреждений высш. проф. образования. – М.: Издательский центр «Академия», 2013. – 320 с.
9. А.Г. Трифонов. Многокритериальная оптимизация. Режим доступа: http://matlab.exponenta.ru/optimiz/book_1/16.php (свободный).
10. Matthias Ehrgott. Multicriteria Optimization. - Springer, 2nd edition, 2005. – 323 p.

Larionov Igor Pavlovich
Russian State Social University, Russia, Moscow
E-mail: cmpara@mail.ru

Khorev Pavel Borisovich
National research institute «Moscow Power Engineering Institute», Russia, Moscow
E-mail: pbkh@yandex.ru

Problems of making and main objectives of expert support system for complex information security system engineering

Abstract. This article describes problems of making and main objectives of expert support system for complex information security system engineering. Engineering of complex information security system is not trivial task and its automation is an actual problem. Main problem is that the task of complex information security engineering belongs to the class weakly formalized task with incomplete information. Analytical expert support engineering system is considered to be the solution of that problem because it is capable to work with weakly formalized knowledge due to its specialized knowledge base and possibility to refine the input information from the user, that allows to overcome the problem of initial incompleteness of data. Such system will solve the problem of multicriteria optimization over the set of chosen criteria that describe the complex information security system for engineering the optimal composition of information security components and means of information protection in complex information security system.

Keywords: expert system; decision making; decision making system; complex information security system; engineering expert support system; information security; protection of information; multicriteria optimization; knowledge-based systems; system modeling

REFERENCES

1. Baranova E.K. Metody prinyatiya resheniy v razrabotke kompleksnoy sistemy zashchity informatsii, RGSU, M: 2010 – 12 s.
2. Dzhozef Dzharratano, Gari Rayli. Ekspertnye sistemy. Printsipy razrabotki i programmirovanie. M: Vil'yam, 2007. – 1152 s.
3. Larionov I.P., Khorev P.B. Osobennosti predstavleniya znaniy v ekspertnoy sisteme podderzhki proektirovaniya kompleksnoy sistemy zashchity informatsii // Materialy XXV mezhdunarodnoy nauchno-prakticheskoy konferentsii «Sovremennye problemy gumanitarnykh i estestvennykh nauk» 08-09 oktyabrya 2015 g. / RF, Moskva, 2015.
4. Larionov I.P., Khorev P.B. Osobennosti razrabotki metodiki otsenki informatsionnoy bezopasnosti predpriyatiya dlya ekspertnykh sistem // Sovremennaya nauka: aktual'nye problemy i puti ikh resheniya. Sbornik nauchnykh statey. Trudy mezhdunarodnoy distantsionnoy nauchnoy konferentsii №9, 23-24 maya 2014 g. / RF, g. Lipetsk, 2014.
5. Lotov A.V., Bushenkov V.A., Kamenev G.K., Chernykh O.L. Komp'yuter i poisk kompromissa, metod dostizhimykh tseley, izdatel'stvo «Nauka», M: 1997 – 404 s.
6. Malyuk A.A. Informatsionnaya bezopasnost': kontseptual'nye i metodologicheskie osnovy zashchity informatsii. Ucheb. posobie dlya vuzov – M.: Goryachaya liniya – Telekom, 2004. - 280 s.
7. Nogin V.D. Prinyatie resheniy v mnogokriterial'noy srede: kolichestvennyy podkhod. - M.: FIZMATLIT, 2005, 176 s.
8. Sovetov B.Ya. Intellektual'nye sistemy i tekhnologii: uchebnik dlya stud. Uchrezhdeniy vyssh. prof. obrazovaniya. – M.: Izdatel'skiy tsentr «Akademiya», 2013. – 320 s.
9. A.G. Trifonov. Mnogokriterial'naya optimizatsiya. Rezhim dostupa: http://matlab.exponenta.ru/optimiz/book_1/16.php (svobodnyy).
10. Matthias Ehrgott. Multicriteria Optimization. - Springer, 2nd edition, 2005. – 323 p.