Леуцкий Евгений Александрович

МЕТОДЫ УПРАВЛЕНИЯ РИСКАМИ ПРИ ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Статья посвящена разработке методов управления рисками, возникающими при обеспечении информационной безопасности предприятий и организаций. Основными направлениями исследования были выявление отличительных особенностей существующих систем анализа и управления рисками, а также проведение анализа существующих решений и методов и эффективности их использования. В основу исследования положен качественно новый прецедентный подход, который использовался для построения системы анализа и управления рисками (Risk Panel).

Адрес статьи: www.gramota.net/materials/1/2013/11/26.html

Статья опубликована в авторской редакции и отражает точку зрения автора(ов) по рассматриваемому вопросу.

Источник

Альманах современной науки и образования

Тамбов: Грамота, 2013. № 11 (78). С. 96-98. ISSN 1993-5552.

Адрес журнала: www.gramota.net/editions/1.html

Содержание данного номера журнала: www.gramota.net/materials/1/2013/11/

© Издательство "Грамота"

Информация о возможности публикации статей в журнале размещена на Интернет сайте издательства: www.gramota.net

Вопросы, связанные с публикациями научных материалов, редакция просит направлять на адрес: almanac@gramota.net

УДК 004.4
Технические науки

Статья посвящена разработке методов управления рисками, возникающими при обеспечении информационной безопасности предприятий и организаций. Основными направлениями исследования были выявление отличительных особенностей существующих систем анализа и управления рисками, а также проведение анализа существующих решений и методов и эффективности их использования. В основу исследования положен качественно новый прецедентный подход, который использовался для построения системы анализа и управления рисками (Risk Panel).

Ключевые слова и фразы: информационная безопасность; риск; угроза; уязвимость; информационная система; база знаний; прецедентный подход; модель угроз; онтология; *Risk Panel*.

Леуцкий Евгений Александрович
Новосибирский государственный университет
statusqwr@gmail.com

МЕТОДЫ УПРАВЛЕНИЯ РИСКАМИ ПРИ ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ©

Исследование выполнено при поддержке Министерства образования и науки Российской Федерации, соглашение 14.B37.21.0400 «Методы извлечения и порождения знаний для обеспечения информационной безопасности».

Ни для кого не секрет, что анализ информационных рисков – это одна из актуальных задач как для современного бизнеса, так и для государства. Согласно статистике [7], количество киберпреступлений в мире и, в частности, в России увеличивается из года в год. Например, в октябре 2012 года МВД опубликовало статистику относительно киберпреступлений за первое полугодие 2012 года. По данным Министерства, в России было зафиксировано 5696 киберпреступлений, что почти на 11% больше, чем за аналогичный период 2011 года [12]. Таким образом, можно сделать вывод, что способность компаний конкурировать между собой и даже, наверное, выживать в современных условиях зависит от наличия развитой системы информационной безопасности.

В последние годы в России почти на каждой конференции по информационной безопасности можно услышать довольно серьезные доклады, связанные с созданием систем анализа рисков и управления уязвимостями [8]. При этом остаются незатронутыми такие вопросы, по большей степени затрагивающие сами основы, как: что именно представляет собой задача анализа рисков, какие существуют методы ее решения, а также, какие трудности возникают в процессе выбора метода решения.

Анализ информационных рисков – это, прежде всего, процесс комплексной оценки степени защищенности информационной системы с переходом к качественным или количественным показателям рисков. Риск рассматривается как вероятный ущерб, который зависит от степени защищенности информационной системы. Таким образом, согласно определению, на выходе алгоритма анализа риска можно получить либо качественную оценку рисков (уровень риска: высокий, средний, низкий), либо количественную (например, риск можно измерить в деньгах). Также стоит отметить, что анализ рисков может осуществляться в соответствии с двумя подходами, которые отличаются уровнем анализа рисков. Как правило, выделяют базовый и полный уровень. Базовый состоит только из проверки того, что существует риск невыполнения некоторых требований общепринятого стандарта безопасности (обычно ISO 17799) [13]. В результате такой проверки получают качественную оценку уровня рисков (низкий, средний и высокий). Для того чтобы провести полный анализ рисков требуется построение полной модели анализируемой информационной системы. Такая модель должна включать: все типы ценной информации, объекты ее хранения (например, оборудование); группы пользователей и виды доступа к информации; средства защиты и политика безопасности, а также всевозможные виды угроз.

Таким образом, несомненно, что доступ к данным, которые используются для анализа рисков, должен быть организован в соответствии со всеми требованиями к качественному анализу, который предполагает работу с правильной, стандартизованной и достоверной информацией.

На сегодняшний момент существует разнообразное количество систем анализа и управления рисками, например, CRAMM [10], RiskWatch [9], ГРИФ [11] и т.д. Как правило, перед созданием подобного рода систем сначала выбирается подход, которой в дальнейшем определит функционал, возможности и эффективность системы. В основе каждого из подходов лежит свой метод, знание и понимание которого существенно поможет при выборе подходящей системы анализа и управления рисками. И, несмотря на то, что существует достаточное количество хорошо себя зарекомендовавших и широко используемых методов оценки и управления рисками, одной из классических проблем алгоритмов анализа информационных рисков по-прежнему остается выбор методики анализа и определения угроз безопасности информации.

Далее рассмотрим несколько упомянутых выше методов. Начнем с метода OCTAVE. Этот метод состоит в том, что для оценки рисков используется серия так называемых внутренних семинаров, которые проводятся

© Леуцкий Е. А., 2013

с целью выяснения различных вопросов информационной безопасности. В соответствии с этим методом, перед тем как проводить поэтапную оценку рисков, обычно организуют ряд подготовительных мероприятий, состоящих, как правило, из согласования графика семинаров, назначения ролей, планирования, координации действий участников проектной группы и т.д.

Подобный подход также используется и в широко известном методе оценки рисков *CRAMM*. В основу метода *CRAMM* положена концепция, которая состоит в том, что анализ рисков, прежде всего, включает в себя идентификацию и определение уровней мер (или рисков) на основе оценок, сопоставленных угрозам, ресурсам и уязвимостям ресурсов. В свою очередь, оценки строятся, исходя из тщательно организованных интервью с подробнейшими опросниками. Если сравнивать метод *OCTAVE* с методом *CRAMM*, то можно сказать, что методы построения величин рисков и последовательность действий имеют существенные различия. В первую очередь в *CRAMM* определяется целесообразность оценки рисков. Если оказывается, что информационная система организации не так критична, то к ней применяется классический набор механизмов контроля, прописанных в международных стандартах и содержащихся в базе знаний *CRAMM*. Обычно контроль рисков состоит в идентификации и выборе контрмер, с помощью который риски снижаются до приемлемого уровня.

Теперь рассмотрим метод *RiskWatch*. В этом методе для управления и оценки рисков используются такие критерии, как оценка «возврата от инвестиций» и «предсказание годовых потерь». По сути, метод предполагает жесткую ориентацию на точную количественную оценку соотношения потерь от угроз безопасности и затрат на создание системы защиты. Стоит отметить, что большая часть алгоритмов и, в частности, американский *RiskWatch*, основана на следующем подходе: пользователь системы указывает максимально полный список угроз безопасности, имеющих место именно для используемой им системы, а также оценку ущерба в случае реализации каждого вида угроз. С точки зрения алгоритма, такой подход не совсем удачный, так как конечный элемент защиты – это информация, потеря или повреждение которой в дальнейшем и определяют ущерб. Следствием того, что ущерб устанавливается только по специфичным для данной системы угрозам, является завышенная оценка нанесенного ущерба по отношению к реальному ущербу по видам информации, что неверно.

Как альтернатива решению такого противоречия, рассмотрим алгоритм *ГРИФ*. В соответствии с работой данного алгоритма, требуется указать ущерб по трем видам угроз (угроза доступности, целостности и конфиденциальности) для каждого вида ценной информации. Во-первых, такой метод позволяет строить модель системы, не задумываясь о конкретных угрозах безопасности (каждая конкретная угроза делится на три стандартных непересекающихся вида угроз, которые указаны выше). Во-вторых, с его помощью есть возможность исключить избыточное суммирование по ущербу ввиду того, что оно ведется по непересекающимся угрозам. В-третьих, анализ защищенности информационной системы дробится на множество элементарных ситуаций, благодаря чему алгоритм осуществляет анализ всевозможных реализаций данных классических угроз безопасности для каждого вида информации на каждом ресурсе. Также на этапе анализа нет какой-либо привязки алгоритма к конкретным реализациям угроз.

В дополнение ко всему вышесказанному отметим, что, несмотря на различия всех рассмотренных методов, каждый из них обладает весьма развитым программным инструментарием, который, обычно, состоит из базы знаний по рискам и механизмов их минимизации; средств формирования отчетов; средств сбора информации и алгоритмов для вычисления величины рисков.

Таким образом, методики, позволяющие осуществлять анализ и управление рисками организации, а также инструментальные средства, поддерживающие их, следует искать с учетом таких факторов, как наличие статистики по инцидентам нарушения информационной безопасности; наличие экспертов в области оценки риска; а также наличие достаточно точной качественной и количественной оценки.

Из всех программных продуктов в сфере информационной безопасности большая часть систем работает на основе модели угроз и уязвимостей, которые обычно строятся по введенным пользователем данным. Принципы, относительно которых строятся такие системы, очень важны, так как именно от них будут зависеть процесс оценки риска информации, анализ вероятности реализации угроз информационной безопасности на каждый ресурс, указанный в системе, и т.д. Если сравнивать с имеющимися системами систему *RiskPanel* [5], то сразу можно отметить ее преимущество перед остальными. Как правило, многие системы анализа и управления рисками используют подход, при котором информация сначала оцифровывается, а потом обрабатывается. Иными словами, работа происходит с числовыми оценками возможности осуществления рисков. *RiskPanel* построена на базе принципиально нового подхода, при котором работа ведется с множеством прецедентов, на которые сработали риски. Такой подход дает возможность работать с полноценной информацией, которая не подвергалась искажению ввиду оцифровки. Подход использует онтологии предметной области информационной безопасности, формализованные на основе применения теоретико-модельных методов [3, с. 7-9]. Помимо этого, можно добавить, что у *RiskPanel* есть еще одно преимущество. Эта система, помимо того, что работает с данными, которые были введены вручную или переданы в некотором формате, периодически обновляет прецедентную базу и тем самым увеличивает спектр возможных угроз. Также стоит отметить, что система была расширена интерфейсом, который позволяет осуществлять доступ к нужной информации в базе знаний.

Подводя итог, можно сделать вывод, что инструментальные средства анализа рисков, в основе которых лежат современные базы знаний и процедуры логического вывода, открывают возможность для построения как структурных, так и объектно-ориентированных моделей информационных активов компании. Помимо этого, с их помощью можно построить модели угроз и рисков, связанных с отдельными информационными

и бизнес-транзакциями. В рамках проделанной работы было установлено, что подобного рода инструментальные средства должны обеспечивать надежное, своевременное и достаточно быстрое пополнение базы знаний, а также предоставлять высокую скорость доступа к данным. Все это, несомненно, увеличит скорость реагирования как на возникшие угрозы, так и на их симптомы.

Список литературы

1. **Нестеров С. А.** Анализ и управление рисками в информационных системах на базе операционных систем Microsoft: учебный курс. СПб., 2009.
2. **Пальчунов Д. Е.** Поиск и извлечение знаний: порождение новых знаний на основе анализа текстов естественного языка // Философия науки. 2009. № 4. С. 70-90.
3. **Пальчунов Д. Е.** Решение задач поиска информации на основе онтологий // Бизнес-информатика. 2008. № 1. С. 3-13.
4. **Пальчунов Д. Е.** Теоретико-модельная формализация онтологии и рефлексии // Философия науки. 2006. № 4. С. 86-114.
5. **Пальчунов Д. Е., Яхъяева Г. Э., Хамутская А. А.** Программная система управления информационными рисками *RiskPanel* // Программная инженерия. 2011. № 7. С. 29-36.
6. **Baader F., Calvanese D., McGuinness D.** The Description Logic Handbook. Theory, Implementation, and Applications. Cambridge University Press, 2003.
7. **http://d-russia.ru/ugrozhayushhaya-statistika-rosta-kiberprestupnosti-v-mire.html** (дата обращения: 03.09.2013).
8. **http://expolink-company.ru/templates/business_conf.php?show=95** (дата обращения: 01.09.2013).
9. **http://riskwatch.com/** (дата обращения: 23.09.2013).
10. **http://www.cramm.com** (дата обращения: 23.09.2013).
11. **http://www.dsec.ru/about/articles/grif_ar_methods/** (дата обращения: 23.09.2013).
12. **http://www.tadviser.ru/index.php/Статья:Киберпреступность** (дата обращения: 04.09.2013).
13. **http://17799.denialinfo.com/** (дата обращения: 23.09.2013).
14. **Undercoffer J., Joshi A., Pinkston J.** Modeling Computer Attacks: an Ontology for Intrusion Detection. University of Maryland, 2003.

RISKS MANAGEMENT METHODS WHILE ENSURING INFORMATION SECURITY

Leutskii Evgenii Aleksandrovich
Novosibirsk State University
statusqwr@gmail.com

The article is devoted to working out the management methods of the risks arising while ensuring the information security of enterprises and organizations. The main research directions were the revelation of the distinctive features of the existing analysis and risks management systems and the analysis of the existing solutions and methods, and the efficiency of their use. The research base is a qualitatively new precedent approach, which was used for constructing the system of analysis and risks management *(Risk Panel)*.

Key words and phrases: information security; risk; threat; vulnerability; information system; knowledge base; precedent approach; model of threats; ontology; *Risk Panel*.

УДК 378.09:004.38
Педагогические науки

В статье описывается веб-квест «Joining a Global Company», разработанный автором для обучения студентов-экономистов в свете современных требований к курсу иностранного языка для профессионального общения. Представив структуру веб-квеста, автор выделяет умения, необходимые для поэтапного выполнения заданий веб-квеста, целью которого является обучение будущих экономистов устному профессионально-ориентированному монологическому выступлению в сопровождении компьютерной презентации.

Ключевые слова и фразы: веб-квест; устное профессионально-ориентированное выступление; компьютерная презентация; умения; опоры.

Лямзина Наталия Константиновна
Львовская коммерческая академия, Украина
lyamzina_n@mail.ru

ВЕБ-КВЕСТ ДЛЯ ОБУЧЕНИЯ СТУДЕНТОВ-ЭКОНОМИСТОВ ПРОФЕССИОНАЛЬНО-ОРИЕНТИРОВАННОМУ МОНОЛОГУ В СОПРОВОЖДЕНИИ КОМПЬЮТЕРНОЙ ПРЕЗЕНТАЦИИ©

Стремительные информатизация и глобализация всех сфер современной жизни и связанные с ними требования к подготовке специалистов разных отраслей находят свое отражение и в изменениях, происходящих

© Лямзина Н. К., 2013