УДК 004.056

ИСПОЛЬЗОВАНИЕ МЕТОДА АНАЛИЗА ИЕРАРХИЙ ПРИ ОЦЕНКЕ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ

Чусавитин М.О.

ГАОУ ВПО «Национальный исследовательский университет «Высшая школа экономики», Москва, e-mail: gala_m27@mail.ru

Применение ИКТ в образовательной деятельности сопряжено с рисками нарушения информационной безопасности. В статье дано определение категории «риски, порождаемые применением ИКТ в системе высшего профессионального образования». Рассмотрены основные программные средства, используемые для автоматизации управления рисками информационной безопасности. Автором разработана методика оценки рисков информационной безопасности образовательного учреждения с использованием метода анализа иерархий (Т. Саати). В качестве программного средства использована система Super Decisions. Предлагаемая методика позволяет, с наименьшими затратами на внедрение и обучение персонала, провести оценку рисков, выявив наиболее критичные бизнес-процессы и ИТ-сервисы образовательного учреждения, нуждающиеся в обеспечении информационной безопасности. Публикация выполнена в рамках выполнения проекта РГНФ № 11-06-01006 «Разработка и апробация модели подготовки научно-педагогических кадров к обеспечению информационной безопасности в ИКТ-насыщенной среде».

Ключевые слова: информационная безопасность, управление рисками, электронное обучение, дистанционное образование, ИКТ, критичные бизнес-процессы и ИТ-сервисы образовательного учреждения, метод анализа иерархий

APPLYING THE ANALYTIC HIERARCHY PROCESS FOR RISK ASSESSMENT IN EDUCATIONAL INSTITUTIONS

Chusavitin M.O.

National Research University «Higher School of Economics», Moscow, e-mail: gala_m27@mail.ru

The use of ICT in educational activities involve risks breach information security. The paper provides a definition of the category «risks posed by the use of ICT in higher education». The main software tools utilized by the automation of information security risk management. The author developed a method of risk assessment of information security educational institution using the analytic hierarchy process (T. Saaty). As a software tool used by system Super Decisions. The proposed method makes it possible, with the lowest cost of implementation and training, conduct a risk assessment to identify the most critical business processes and IT-SERV of educational institutions in need of information security. Publication of you -complete in the framework of the implementation of the project RFH № 11-06-01006 «Development and testing of the model prepared ki of the teaching staff to ensure information security in ICT – rich environment».

Keywords: informationsecurity, risk management, distance education, e-learning, Information and Communication Technologies, critical business processes and IT services with an educational institution, analytic hierarchy process

В условиях глобальной информатизации возрастает зависимость всех сфер деятельности образовательных организаций от негативных воздействий природного, техногенного или социального характера. Инциденты информационной безопасности ведут к нарушению непрерывности функционирования критичных бизнес-процессов и ИТ-сервисов электронной информационно-образовательной среды(ЭИОС) вуза, что в свою очередь приводит к снижению качества предоставляемых образовательных услуг и эффективности информационного обеспечения научно-образовательной и организационной деятельности, потери конкурентных преимуществ образовательного учреждения и др. [3; 5 и др.].

Оценить эффективность системы информационной безопасности образовательного учреждения можно посредством понятия риска – возможных потерь организации от реализации определенных угроз. Под категорией «риски, порождаемые применением ИКТ в системе высшего профессионального образования», мы понимаем возможность возникновения неблагоприятных условий или воздействий на образовательную деятельность вуза (включая миссию, функции, образ, репутацию, активы, ресурсы), обуславливаемые взаимодействием образовательной системы с угрозами и опасностями, индуцируемыми и производимыми в результате функционирования в ИКТ-насыщенной образовательной среде [4].

Сотруднику ответственному за информационную безопасность в образовательном учреждении часто приходится обосновывать необходимость выделения средств на реализацию мероприятий, связанных с повышением уровня информационной безопасности. Анализ негативных последствий предполагает обязательную идентификацию возможных источников угроз, факторов, способствующих их проявлению и, как

следствие, определение актуальных угроз безопасности информации. В настоящее время подготовлено более десятка различных стандартов и спецификаций, детально регламентирующих процедуры управления информационными рисками, среди которых наибольшую известность приобрели международные спецификации и стандарты: ISO 177992002 (BS 7799), GAO и FISCAM, SCIP, NIST, SAS 78/94 и COBIT [1 и др.]. Для обеспечения информационной безопасности сегодня активно используются программные средства автоматизации процесса управления рисками. На текущий момент на рынке представлены следующие решения, обладающие уникальными алгоритмами анализа рисков: Digital Security Office 2006; CRAMM v5.1 Information Security Toolkit; RiskWatch и др. Приобретение готового продукта управления рисками решает большинство проблем, связанных с оценкой ИБ организации и управления рисками, однако требует серьезных затрат, таких как: капитальные вложения на приобретение программного продукта; профессиональные услуги по интеграции программного продукта на предприятии; обучение сотрудников работе с информационной системой; регулярное поддержание контракта на поддержку программного продукта у производителя. Вложение большого объема денежных средств на покупку подобных решений не оправдано для большинства небольших образовательных учреждений.

Для оценки рисков информационной безопасности мы воспользуемся методом анализа иерархий, разработанным Т. Саати [2]. Метод анализа иерархий (МАИ) является систематической процедурой для иерархического представления элементов, определяющих суть проблемы практически любой природы.

МАИ помогает структурировать проблему (в том числе плохо формализуемую) в виде иерархии, построить набор альтернатив, выделить характеризующие их факторы, задать значимость этих факторов, сравнить и выполнить количественную оценку альтернативных вариантов решения, найти неточности и противоречия в суждениях эксперта, проранжировать альтернативы, провести анализ решения и обосновать полученные результаты. Метод применяется для построения шкалы отношений, как из дискретных, так и из непрерывных парных сравнений объектов в многоуровневых иерархических структурах. Сравнения проводят на основе реальных измерений или с помощью численной шкалы, отражающей относительную силу предпочтений экспертов в отношении объектов сравнения. МАИ используется во всем мире для принятия решений в разнообразных ситуациях: от управления на межгосударственном уровне до решения отраслевых и частных проблем в бизнесе, промышленности, здравоохранении и образовании [2 и др.].

На первом этапе применения МАИ проводится структурирование проблемы в виде иерархии или сети. В наиболее общем виде иерархия строится с вершины (цели), через промежуточные уровни – критерии (технико-экономические параметры) к самому нижнему уровню, который, как правило, является набором альтернатив. После иерархического представления проблемы назначаются критерии, вычисляются их приоритеты и по ним оценивается каждая из альтернатив. Элементы сравниваются попарно по отношению к их воздействию на общую для них характеристику. Результат такого сравнения может быть представлен в виде обратно симметричной матрицы. Элементом такой матрицы *aij* является интенсивность проявления элемента иерархии i относительно элемента иерархии j, оцениваемая по шкале интенсивности от 1 до 9, предложенной автором метода (табл. 1).

Таблица 1

Значение экспертных оценок в системе анализа иерархий

Шкала интенсивности	Качественные суждения
1	Равная важность
3	Умеренное превосходство одного над другими
5	Существенное превосходство одного над другими
7	Значительное превосходство одного над другими
9	Очень сильное превосходство одного над другими
2, 4, 6, 8	Соответствующие промежуточные значения

Если при сравнении одного фактора *i* с другим *j* получено *aij = b*, то при сравнении второго фактора с первым автоматически получаем (исходя из свойств обратно симметричной матрицы) *aij = 1/b* . Относительная сила, величина или вероятность каждого отдельного объекта в иерархии определяются оценкой соответствующего ему элемента собственного вектора матрицы приоритетов, нормализованного на единицу. Процедура определения собственных векторов матриц поддается приближению с помощью вычисления геометрической средней. Приоритеты синтезируются, начиная со второго уровня вниз. Локальные

приоритеты перемножаются на приоритет соответствующего критерия на вышестоящем уровне и суммируются по каждому элементу в соответствии с критериями, на которые воздействует элемент. Для контроля мнений экспертов в МАИ вводят т.н. индекс согласованности (ИС) который дает информацию о степени нарушения согласованности:

$$\text{ИС} = \frac{\lambda_{\max} - n}{n-1}. \qquad (1)$$

Если индекс согласованности(ИС) превышает установленные пределы, то тому, кто проводит суждения, следует их перепроверить. Для той же цели в МАИ вводится также величина, которая получилась бы при случайном выборе количественных суждений из фундаментальной шкалы и образовании обратно симметричной матрицы (табл. 2).

Если разделить ИС на число, соответствующее случайной согласованности матрицы того же порядка, получим отношение согласованности (ОС):

$$\text{ОС} = \frac{\text{ИС}}{\text{СС}}. \qquad (2)$$

Таблица 2

Зависимость коэффициента случайной согласованности от размера матрицы

Размер матрицы	1	2	3	4	5	6	7	8	9	10
Случайная согласованность	0	0	0,58	0,9	1,12	1,24	1,32	1,41	1,45	1,49

Чтобы быть приемлемой, величина ОС не должна превышать 10%. В некоторых случаях допускается значение ОС не более 20%. Если это условие не выполняется, необходимо потребовать от экспертов, принимающих участие в опросе, перепроверить свои суждения [2].

Рис. 1. Иерархия принятия решения об оценке критичности сервиса

Метод анализа иерархий содержит процедуру синтеза приоритетов, вычисляемых на основе субъективных суждений экспертов. Число суждений может измеряться десятками или сотнями. Математические вычисления для задач небольшой размерности можно выполнить даже с помощью калькулятора, однако для задач большой размерности целесообразно использовать программное обеспечение для ввода

и обработки суждений. В настоящее время МАИ реализован во многих пакетах прикладных программ, таких как Expert Choice, SuperDecisions, MPRIORITY, СППР «Выбор»; Император 3.1 и др. Для решения задачи многокритериального анализа мы использовали программное обеспечение Super Decisions. Super Decisions – простой удобный в работе пакет для того, чтобы построить модели решения с зависимостью и обратной связью и вычислить результаты. Это программное обеспечение было разработано для многих операционных системах, в том числе существует веб-версия программы.

Рассмотрим более подробно процесс выявления наиболее критического ИТ-сервиса с точки зрения информационной безопасности на примере высшего образовательного учреждения. На рис. 1 представлена соответствующая иерархия задачи.

В качестве программного средства мы использовали Super Decisions.

Шаг 1. Расчет состоит из трёх последовательных шагов.

Эксперт определяет относительный «вес» источников угроз, руководствуясь косвенными показателями, такими как:

- Вероятность возникновения источника угроз;
- Возможность реализации угрозы;
- Вероятный ущерб, нанесенный реализованной угрозой.

Программный продукт предоставляет интерфейс для относительной оценки параметров, как представлено на рис. 2.

Рис. 2. Интерфейс оценки относительного веса угроз в кластере «Выявление наиболее критичного сервиса образовательного учреждения»

Шаг 2. Эксперты оценивают вероятность реализации каждого источника относительно всех угроз информационной безопасности.

Шаг 3. Эксперт оценивает совокупный ущерб от реализации каждой из угроз информационной безопасности в контексте заданных альтернатив.

Шаг 4. На основе окончательного ранжирования объектов эксперт делает выводы о степени уязвимости объектов (рис. 3).

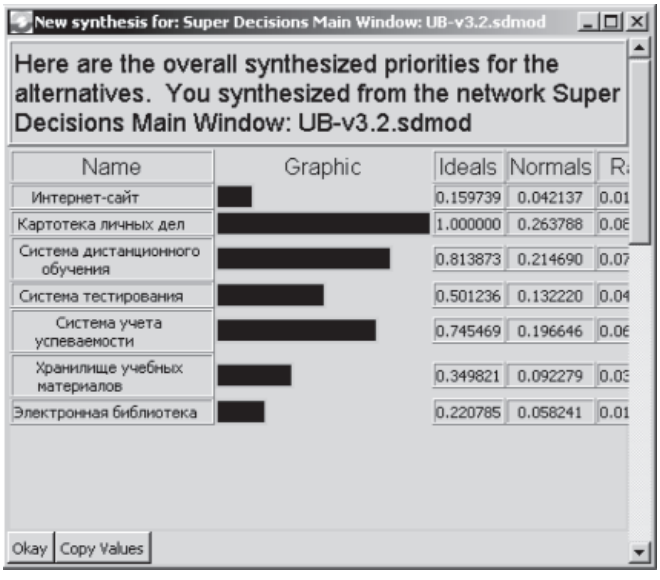

Рис. 3. Окончательное ранжирование объектов

В соответствии с данными окончательного ранжирования определяется рекомендуемая приоритетность повышения защищенности объектов.

Таким образом, рассмотренная методика применения метода анализа иерархий в целях анализа рисков и классификации ИТ-сервисов образовательного учреждения позволила структурировать проблему, построить набор альтернатив, выделить характеризующие их факторы, оценить альтернативы по каждому из факторов, определить согласованность мнений эксперта, проранжировать альтернативы, провести анализ решения и обосновать полученные результаты. Методика позволяет с наименьшими затратами на внедрение и обучение персонала провести оценку рисков, выявив наиболее критичные бизнес-процессы, нуждающиеся в обеспечении информационной безопасностью.

Публикация выполнена в рамках выполнения проекта РГНФ № 11-06-01006 «Разработка и апробация модели подготовки научно-педагогических кадров к обеспечению информационной безопасности в ИКТ-насыщенной среде».

Список литературы

1. Петренко С.А., Симонов С.В. Управление информационными рисками. Экономически оправданная безопасность. – М.: Компания АйТи; ДМК Пресс, 2004. – 384 с.

2. Саати Т.Л. Принятие решений при зависимостях и обратных связях: Аналитические сети. – М.: Изд-во ЛКИ, 2008. – 360 с.

3. Чусавитина Г.Н. Информационная безопасность в открытом образовании // Информационная безопасность в открытом образовании: сборник трудов участников IV всероссийской научно-практической конференции / под общ. ред. Г.Н. Чусавитиной, Л.З. Давлеткиреевой. – Магнитогорск: МаГУ, 2011. – С. 5–10.

4. Чусавитина Г.Н. Управление рисками, порождаемыми применением информационно-коммуникативных технологий в образовательном процессе вуза// Международная научная конференция «Информационные технологии и телекоммуникации в образовании и науке» (IT&T ES'2008). – М.: ЭГРИ, 2008. – С. 142–143.

5. Чусавитина Г.Н., Чусавитин М.О. Анализ непрерывности бизнес-процессов и поддерживающей инфраструктуры вуза в сфере электронного образования // Современные проблемы науки и образования. – 2012. – № 5; URL: http://www.science-education.ru/105-7275.

References

1. Petrenko S.A., Simonov S.V. (2004). Information Risk Management. Economically justified security. Moscow, IT Co., DMK Press.

2. Saati T.L. (2008). Prinjatie reshenij pri zavisimostjah i obratnyh svjazjah: Analiticheskie seti. Moscow, LKI.

3. Chusavitina G.N. (2011). Informacionnaja bezopasnost' v otkrytom obrazovanii: Sbornik trudov uchastnikov IV vserossijskoj nauchno-prakticheskoj konferencii, pod obshh. red. G.N.Chusavitinoj. L.Z. Davletkireevoj. *Informacionnaja bezopasnost v otkrytom obrazovanii.* Magnitogorsk, MaGU, pp. 5–10.

4. Chusavitina G.N. (2008). Management of risk posed by the use of awareness-communication technologies in the educational process of high school. International Scientific Conference on-«Information Technology and Telecommunications in Education and Science» (IT & T ES2008). Moscow, AGRE.

5. Chusavitina G.N., Chusavitin M.O. (2012). Analiz nepreryvnosti biznes-processov i podderzhivajushhej infrastruktury vuza v sfere jelektronnogo obrazovanija. *Sovremennye problemy nauki i obrazovanija*.

Рецензенты:

Кузнецов В.А., д.ф.-м.н., профессор, декан физико-математического факультета, ФГБОУ ВПО «Магнитогорский государственный университет», г. Магнитогорск;

Гневэ О.В., д.п.н., профессор, проректор по учебной работе, ФГБОУ ВПО «Магнитогорский государственный университет», г. Магнитогорск.

Работа поступила в редакцию 17.10.2013.