ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

Павленко А.В., аспирант,
Ковалева Е.Г., канд. техн. наук, ст. препод.
Радоуцкий В.Ю., канд. техн. наук, проф.
Белгородский государственный технологический университет им. В.Г. Шухова

АНАЛИЗ ПОДХОДОВ К ОЦЕНКЕ РИСКА*

vs1606@mail.ru

При анализе риска для ресурсов высшего учебного заведения, лица принимающие решения сталкиваются со следующими трудностям: количественная оценка исходных параметров; сложная организация объекта обеспечения безопасности; учет вероятностной природы угроз безопасности. В статье приведен анализ различных подходов к оценке риска воздействия угроз на объект защиты, таких как: метод экспертной оценки информационных ресурсов (метод CRAMM); метод «матрицы рисков»; метод на получение оценок рисков с использованием нечеткой логики; метод основанный на теории игр; метод основанный на модели системы «с полным перекрытием».

Ключевые слова: *анализ, риск, эксперт, матрица, вероятность, логика, теория игр, модель.*

Введение. На современном этапе осуществление образовательной деятельности невозможно без обеспечения безопасности и защиты обучающихся, преподавателей и сотрудников от действия неблагоприятных и опасных факторов террористического, природного, техногенного, социального, медико-биологического и иного характера.[1]

Существующие многочисленные угрозы обусловлены не только объективно существующими потенциальными источниками и факторами опасности, но и недостаточной защитой от их воздействия, а нередко и отсутствием такой защиты. [2]

Основой для принятия решений и планирования мероприятий по повышению безопасности личности (учащегося, студента, преподавателя, сотрудника) в образовательном учреждении должна стать теория и основанная на ней система управления рисками.[3] С помощью экспертно-аналитических методов необходимо дать количественную оценку угроз для безопасности образовательных учреждений и установить их приоритеты. Количественный подход позволяет трансформировать угрозы в риски и произвести оценку этих рисков.

Прежде всего, необходима идентификация, классификация и ранжирование всех опасностей и угроз. Далее, на основе имеющихся статистических данных с использованием методов теории вероятностей, теории надежности с привлечением современных вычислительных средств необходимо количественно оценить вероятности возникновения критических и чрезвычайных ситуаций.

Количественный анализ рисков создает базу для разработки методов и приемов управления рисками – правовых, организационных, экономических, технических и др.

Методология. При работе использованы методы системного анализа, теории вероятности, теории принятия решений, методы оптимизации.

Основная часть. Для защиты обучающихся, преподавателей и сотрудников от действия неблагоприятных и опасных факторов различного характера в высших учебных заведениях создаются системы комплексной безопасности (СКБ) [4]. Функционирование СКБ происходит в условиях воздействия неопределенных факторов, в первую очередь, человеческого. Проникновение злоумышленника на объект, возникновение пожара - все это факторы вероятностные. Однако такие показатели, как ценность ресурса или стоимость средства защиты, имеют вполне определенные количественные значения и тоже должны браться в рассмотрение. Таким образом, чтобы учесть и вероятностную природу функционирования СКБ, и детерминированные значения используемых показателей, возможно использование такого агрегированного критерия, как риск [5]. Риск - это потенциальный ущерб от реализации воздействия угроз на объект защиты. Анализ риска позволяет определить наиболее актуальные для объекта угрозы, меры противодействия им, наиболее критичные уязвимости, а также оптимизировать стоимостные затраты на построение системы безопасности.

В настоящее время известно множество методов экспертной оценки информационных рис-

ков [6]. Эти методы рекомендованы международными стандартами информационной безопасности, главным образом, ISO 17799 (BS7799).

Одним из наиболее известных методов оценки риска по данному стандарту является метод CRAMM (CCTA Risk Analysis & Management Method) [7]. Данный метод позволяет производить анализ рисков и решать ряд других аудиторских задач: обследование информационной системы, проведение аудита в соответствии с требованиями стандарта BS 7799, разработка политики безопасности. CRAMM предполагает разделение всей процедуры анализа риска на три последовательных этапа.

Задачей первого этапа является ответ на вопрос: «Достаточно ли для защиты применения средств базового уровня, реализующих традиционные функции безопасности, или необходимо проведение более детального анализа?»

На втором этапе производится идентификация рисков и оценивается их величина.

На третьем этапе решается вопрос о выборе адекватных контрмер. В случае принятия решения о внедрении новых контрмер или модификации старых, на аудитора может быть возложена задача подготовки плана внедрения новых контрмер и оценки эффективности их использования [8]. Решение этих задач выходит за рамки метода CRAMM.

Наибольшее распространение среди методов оценки рисков получил метод «матрицы рисков». В процессе оценки экспертами определяются вероятность возникновения каждого риска и размер связанных с ним потерь (стоимость риска), причем оценивание производится по шкале с тремя градациями: «высокая», «средняя», «низкая». На базе оценок для отдельных рисков выставляется оценка системе в целом, а сами риски ранжируются. К сожалению, дать интерпретацию полученных результатов не всегда возможно [6]. При расчете риска чаще всего пользуются формулой [9], представляющей риск как произведение трех параметров:

-стоимость (ценность) ресурса;

-мера уязвимости ресурса к угрозе (показывает, в какой степени тот или иной ресурс уязвим по отношению к рассматриваемой угрозе);

-оценка вероятности реализации угрозы (насколько вероятна реализация той или иной угрозы за определенный период времени).

Большинство из описанных параметров принимается на основе мнения эксперта. Это связано с тем, что количественная оценка вероятности реализации угрозы затруднена ввиду относительной новизны информационных технологий и, как следствие, отсутствия достаточного количества статистических данных [9].

Известны методы, основанные на получении оценок рисков с использованием *нечеткой логики* [10]. Механизм оценивания рисков на основе нечеткой логики, по существу, является экспертной системой, в которой базу знаний составляют правила, отражающие логику взаимосвязи входных величин (уровень угрозы, ценность ресурса, уровень уязвимости) и риска. В общем случае, эта сложная логика отражает реальные взаимосвязи, которые могут быть формализованы с помощью продукционных правил вида «Если..., то...». Механизм нечеткой логики требует формирования оценок ключевых параметров и представления их в виде нечетких переменных. Необходимо определить вид функций принадлежности данных переменных, что для человека без соответствующего опыта может оказаться довольно трудной задачей. Однако, всё же механизм нечеткой логики позволяет заменить приближенные методы экспертной оценки рисков количественными оценками, основанными на хорошо разработанном математическом методе [11].

Среди методов анализа риска следует также отметить метод, основанный на *теории игр* [12]. Метод позволяет оценить эффект от внедрения различных средств защиты. Например, если x_i; - вариант применения i-го метода защиты, а a_j - идентифицированные входные данные (идентифицированная угроза), то $f(x_i, a_j)$ представляет собой блокированную угрозу, выраженную численно. В задачах защиты функция f (x, a) имеет дискретный характер, т.е. любому допустимому решению x; соответствуют различные входные данные (угрозы) a_j и результаты решений f_{ij}. Семейство решений в этом случае можно описать некоторой матрицей $||f_{ij}||$, строками которой являются решения, или стратегии, а столбцами — входные данные. При выборе наилучшего решения необходимо учитывать все возможные последствия варианта x_i. Для этого необходимо ввести подходящие оценочные (целевые) функции. При этом матрица решений $||f_{ij}||$ сведется к одному столбцу — вектору результатов f_{ir} в котором любому варианту x_i приписывается некоторый результат f_{ir}, являющийся функцией всех последствий этого решения. Эта функция может иметь различный вид, в зависимости от позиций лица, принимающего решения (ЛПР), которые в теории принятия решений различают следующим образом: оптимистическая, пессимистическая, позиция компромисса, позиция нейтралитета [13]. К недостаткам метода следует отнести сложность определения значения функции $f(x_i,$

a_j), характеризующей эффективность блокирования j-й угрозы i-м методом защиты. Также трудности вызывает введение оценочных (целевых) функций, отражающих стратегию ЛПР.

Одним из наиболее распространенных методов оценки риска является метод, основанный на модели системы *«с полным перекрытием»,* представляющей собой триаду «угрозы - средства защиты информации - объекты защиты» в виде трехдольного графа. Удобство данной модели — возможность введения и анализа количественных мер уязвимости (вероятность преодоления средств защиты информации, ущерб от реализации угроз) на основе взвешивания вершин и ребер графа.

При анализе риска для ресурсов вуза, ЛПР сталкивается со следующими трудностями [14]:

1. Количественная оценка исходных параметров.

На начальном этапе при обследовании объекта защиты возникают проблемы с выделением и количественной оценкой ресурсов, подлежащих защите. Неясно, что брать в качестве ценности ресурса — стоимость восстановления, потери от дискредитации (вообще, расплывчатый параметр), ценность для конкурентов. Одним из видов защищаемых ресурсов для СКБ вуза являются люди. Ценность человеческой жизни несравнима ни с какими материальными потерями. Таксономия угроз информационным ресурсам содержится в [15]. Для материальных ценностей и людей будут рассматриваться свойственные им угрозы. Проблема возникает опять при количественной оценке угроз. Какой-то адекватной статистики по различным видам угроз до сих пор не собрано; надо привлекать экспертов, что неизбежно вносит субъективизм.

2.Сложная организация объекта обеспечения безопасности.

При анализе риска необходимо рассматривать все множество ресурсов, расположенных на объекте защиты, в том числе и людских. Таких ресурсов может насчитываться до нескольких тысяч. Учет данного факта, а также потоков движения информационных и людских ресурсов - одна из задач, которые необходимо решить.

3.Учет вероятностной природы угроз безопасности

Появление злоумышленника на объекте обеспечения безопасности всегда носит вероятностный характер. Порядок его дальнейших действий зависит уже от степени инженерной укрепленности самого объекта — прочности дверей и окон, наличия решеток, технических средств задержки. Учет вероятности появления злоумышленника, а также анализ его пути к защищаемым ресурсам являются еще одной задачей, которую должна решить используемая модель анализа риска.

Вывод. Данные трудности необходимо решить при разработке модели анализа риска для ресурсов вуза. Наиболее перспективной моделью анализа риска с нашей точки зрения является модель, основанная на модели системы с полным перекрытием каналов воздействия угроз и использовании марковских моделей, которая учитывает возможность столкновения с различными типами злоумышленников, а так же различные распределения вероятности выбора данными злоумышленниками угроз.

** Работа выполнена в рамках программы стратегического развития БГТУ им. В.Г. Шухова на 2012 – 2016 годы.*

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Радоуцкий В.Ю., Шаптала В.Г. Характеристика внутренних опасностей и угроз образовательных учреждений высшего профессионального образования // Вестник Белгородского государственного технологического университета им. В.Г. Шухова. 2009. №3м. С. 124-126.

2. Радоуцкий В.Ю., Шаптала В.В., Ветрова Ю.В., Шаптала В.Г. Оценка рисков чрезвычайных ситуаций и пожаров: уч. пос. Белгород: Изд-во. БГТУ, 2011. 116 с.

3. Радоуцкий В.Ю. Шаптала В.Г., Шульженко В.Н., Глызин В.Л. Нормирование рисков техногенных чрезвычайных ситуаций // Вестник Белгородского государственного технологического университета им. В.Г. Шухова. 2008. №4. С. 65-68.

4. Радоуцкий В.Ю., Шаптала В.Г. Методологические основы моделирования систем обеспечения комплексной безопасности ВУЗов // Вестник Белгородского государственного технологического университета им. В.Г. Шухова. 2008. №3. С. 64-66.

5. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях/ Под ред. В.Ф. Шаньгина. М.: Радио и связь, 1999. 328 с.

6. Лопарев С., Куканова Н. Современные методы и средства анализа и управление рисками информационных систем компаний. http://www.dsec.ru/about/articles/ar_compare/

7. Risk Management Guide for Information Technology Systems, NIST, Special Publication 800-30. 34 p.

8. Лопарев С., Шелупанов А. Анализ инструментальных средств оценки рисков утечки информации в компьютерной сети предприятия // Вопросы защиты информации. 2003. №4. С. 43 - 46.

9. Покровский П. Защита информации: анализ рисков // LAN. Журнал сетевых решений. Октябрь, 2004. С. 35-38.

10. Zadeh I. Fuzzy Logic, Neural Networks and Soft Computing // Communication on the ACM-1994. - Vol. 37, №3. 77-84 pp

11. Wang L.X. Analysis and design of hierarchical fuzzy systems // IEEE Transactions on Fuzzy Systems, 7(5), 1999. 617-624 pp.

12. Волобуев С.В. О принципах построения модели изменяющейся системы защиты // Вопросы защиты информации. 2004. №2. С. 34-41.

13. Gibbons Robert. Game Theory for Applied Economists. Princeton University Press, 1992. 198 pp.

14. Гузаиров М.Б. Васильев В.И., Зарипов С.Н., Иванова Т.А. Методологические проблемы проектирования комплексной системы безопасности вуза // Мавлютовские чтения: Российская научно-техническая конференция: сб. трудов. Том 1. Уфа: УГАТУ, 2006. С. 70 - 76.

15. ГОСТ Р 51275 - 99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. М.: Изд-во стандартов, 2003. 9 с.