DOI: 10.17117/na.2015.11.03.156

<http://ucom.ru/doc/na.2015.11.03.156.pdf>

Поступила (Received): 13.11.2015

Кадочникова Н.А., Цырульник В.Ф. Оценка рисков информационной безопасности на основе метода построения матрицы General Electric/McKinsey

Kadochnikova N.A , Tsyrulnik V.F.
Assessment of risks of information security on the basis of
the method of creation the matrix General Electric/McKinsey

В информационной безопасности методы оценки рисков появились для прогнозирования возможного ущерба, связанного с реализацией угроз, и оценки необходимого объема инвестиций на построение систем защиты информации. В данной статье предложен способ оценки рисков информационной безопасности на основе метода построения матрицы Мак-Кинзи

The information security risk assessment techniques appeared to predict potential damages associated with the implementation of the threats, and assess the necessary volume of investment in the construction of systems of information protection. This article provides a method of assessing information security risks based on the method of constructing matrix McKinsey

Ключевые слова: информация, безопасность, риск, метод оценки, защита информации

Key words: information, security, risk, assessment method, protection of information

Кадочникова Наталья Александровна

Студент

Омский государственный технический университет

г. Омск, пр. Мира, 11

Kadochnikova Natalia Alexandrovna

Student

Omsk state technical university

Omsk, Mira ave., 11

Цырульник Валерия Федоровна

Студент

Омский государственный технический университет

г. Омск, пр. Мира, 11

Tsyrulnik Valeria Fedorovna

Student

Omsk state technical university

Omsk, Mira ave., 11

В современном мире управление информационными рисками представляет собой одно из наиболее актуальных направлений в области защиты информации. В настоящее время широко используются как качественные, так и количественные международные методики управления информационными рисками.

В данной работе для оценки состояния защищенности автоматизированной системы (АС) предложено воспользоваться принципом построения модели Мак-Кинзи. Модель представляет собой матрицу, состоящую из 9 ячеек для

сравнительного анализа состояния АС. Для правильного построения матрицы можно выделить 4 ключевых последовательных шага:

Шаг первый: выбор критериев для оценки.

В основе матрицы лежат два показателя: сильные стороны системы и ее уязвимости. Критерии сильных сторон и уязвимостей системы рождаются из анализа системы. Не существует универсального списка критериев сильных сторон и уязвимостей системы. Под каждый конкретный анализ составляются отдельные множества критериев на основе имеющейся информации у специалиста: сильные стороны = $\{x_1, x_2, \dots, x_n\}$, уязвимости = $\{y_1, y_2, \dots, y_n\}$.

Шаг второй: определение веса (= важности) критериев.

Присвоить вес каждому фактору, который отражает его значимость в состоянии защиты АС (сумма весов равна единице) (Таблица 1) (Таблица 1.1).

Шаг третий: оценка каждого из критериев.

Дать оценку системе по каждому из выбранных критериев от единицы (не привлекательный) до пяти (очень привлекательный) (Таблица 1) (Таблица 1.1).

Шаг четвертый: определение потенциала и стратегии развития АС.

Умножить вес на оценку и просуммировать полученные значения по всем факторам, в итоге получается взвешенная оценка / рейтинг состояния защищенности АС.

Таблица 1

Сильные стороны	Относительный вес	Оценка	Результат
x_1	0,3	5	$0,3 \cdot 5 = 1,5$
x_2	0,5	2	$0,5 \cdot 2 = 1$
...	...	...	...
x_n	0,2	5	$0,2 \cdot 5 = 1$
Оценка сильных сторон системы			$1,5 + 1 + 1 = 3,5$

Таблица 1.1

Уязвимости	Относительный вес	Оценка	Результат
y_1	0,4	4	$0,4 \cdot 4 = 1,6$
y_2	0,3	3	$0,3 \cdot 3 = 0,9$
...	...	...	...
y_n	0,3	5	$0,3 \cdot 5 = 1,5$
Оценка уязвимостей системы			$1,6 + 0,9 + 1,5 = 4$

Анализируемые единицы отражаются в виде кружков с центрами на пересечении соответствующих им значениям. В зависимости от того, какой итоговый балл получила система по оценке сильных сторон и уязвимостей, зависит ее положение в матрице.

Интерпретация полученных значений:

- от 0-1 баллов: низкая
- от 2-3 баллов: средняя
- от 4-5 баллов: высокая

Таблица 1.2

Уязвимости системы	Высокая (4-5)			
	Средняя (2-3)			
	Низкая (0-1)			
		Высокая (4-5)	Средняя (2-3)	Низкая (0-1)
		Сильные стороны системы		

Каждый кружок соответствует общему состоянию определенной системы (Таблица 1.3).

Образуются три области:

- Системы с высоким потенциалом защищенности;
- Системы с низким потенциалом защищенности;
- Системы с средним потенциалом защищенности (по диагонали);

Таблица 1.3

Уяз-вимо-сти си-стемы	Высокая(4-5)	?	Низкий потен-циал	Низкий потенциал
	Средняя(2-3)	Высокий по-тенциал	Средний потен-циал	Низкий потенциал
	Низкая (0-1)	Высокий по-тенциал	Высокий потен-циал	Средний потенциал
		Сильное (4-5)	Среднее (2-3)	Слабое (0-1)
		Сильные стороны системы		

В матрице выделяются три области стратегических позиций:

1. Область с низким потенциалом (три верхних квадранта) Это системы, имеющие низкие или средние по сравнению с остальными значения факторов привлекательности системы для реализации на них потенциальных угроз.

2. Область с высоким потенциалом (три нижних квадранта). Это системы, обладающие по крайней мере, одним из низших и не обладают ни одним из высших параметров, откладываемых по осям.

3. Средняя область или пограничная (три средних квадранта). Это системы, которые при определенных условиях могут либо расти и превращаться в системы с «высоким потенциалом», либо сокращаться и становиться системами с «низким потенциалом».

Основной задачей данного метода является увеличение защиты слабозащищенных систем, в отстающих областях, или наоборот поддержание системы с высоким потенциалом защищенности.

Для позиции, которая условно названа «низкий потенциал», характерны наивысшая степень уязвимости системы и относительно сильную подверженность угрозам. Система, скорее всего, будет являться самой слабозащищенной, поэтому находясь в такой позиции, должна быть защищена с помощью допол-

нительных средств защиты. Стратегической задачей для такой системы является, прежде всего, определение своих слабых и сильных сторон, а затем осуществление необходимого усиления защиты с целью извлечения максимальной выгоды из своих сильных сторон и устранения слабых.

Системы, попадающие в три клетки в нижнем правом углу матрицы, условно можно назвать «победителями». В данной позиции, они обладают по крайней мере одним из низших и не обладают ни одним из высших параметров, откладываемых на осях. Такого рода системы, как правило, не нуждаются в дополнительной защите.

Для системы, попавшей в квадрат с названием «высокий потенциал», характерна низкая степень уязвимости и низкая подверженность угрозам. В данной позиции целесообразно отыскать те области, в которых система имеет явно высокий уровень риска, стремиться по возможности превращать отдельные слабые стороны в сильные. В данной позиции систему скорее можно назвать непривлекательной для потенциальных угроз. В таком положении риски реализации угроз сводятся к минимальным, следовательно, можно не беспокоиться за безопасность системы.

Заключение. Предложенный подход к оценке состояния системы имеет свои преимущества и недостатки. К преимуществам можно отнести то, что модель позволяет рассматривать привлекательность стратегии выбранной для защиты системы на начальном этапе построения комплексной защиты информационной системы. Также, имеется значительно расширенный выбор критериев для оценки.

К основным недостаткам модели можно отнести:

1. При наличии большого количества критериев могут возникнуть трудности подсчета.
2. Присутствует субъективная оценка факторов.
3. Модель имеет статичный характер.
4. Рекомендации имеют слишком общий характер, отсутствуют конкретные стратегии решения проблем систем.

Список используемых источников:

1. Фрига Пол, Итан Расиел. Инструменты McKinsey. Лучшая практика решения бизнес-проблем. М.: Корпоративная культура, 2007. 224 с.