УДК 65.012.27, 004.056.5

АНАЛИЗ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ СТАНДАРТА ISO/IEC 31010

Е. А. Еременко, к. т. н. А. С. Сафронов

Одесский национальный политехнический университет
Украина, г. Одесса
AlexanderSafronov@rambler.ru

В работе анализируются методы оценки рисков, представленные в стандарте ISO/IEC 31010, с целью выявления их применимости для оценки рисков информационной безопасности (ИБ). В результате исследований были сформулированы критерии выбора оптимальных методов для оценки рисков ИБ. Согласно предложенным критериям, было выбрано 6 методов и проведен их сравнительный анализ.

Ключевые слова: методы оценки рисков, информационная безопасность.

Основная цель систем защиты информации (ЗИ) состоит в обеспечении необходимого уровня защищенности информационных ресурсов организации. При этом важными задачами являются выявление угроз и уязвимостей информационных ресурсов и противодействие данным событиям. Известные методики построения систем ЗИ предполагают выполнять учет и анализ угроз ИБ, но при этом они не предоставляют практически применимых и достоверных методов измерения и оценки параметров данных угроз. Поэтому представляется интересным применить методы теории управления рисками для анализа угроз ИБ, которые фактически являются рисками [1].

Процесс управления рисками (УР) состоит из последовательных этапов выявления, оценки и обработки рисков. А этап оценки разделяется на идентификацию и анализ рисков.

Международный стандарт ISO/IEC 31010 определяет 31 общий метод оценки риска. Предложенные методы можно (в некоторых случаях — необходимо) комбинировать и применять на разных этапах процесса управления рисками [2].

В стандарте рассматриваемые методы разделены на пять следующих групп: методы наблюдения, вспомогательные методы, анализ сценариев, функциональный анализ и статистические методы. Однако, после подробного исследования данных методов, становится очевидным, что далеко не все из них применимы для оценки рисков в области информационной безопасности.

Принимая во внимание основные положения стандарта ISO/IEC 31010 и требования задач ИБ, был сформулирован ряд критериев для выбора наиболее подходящих методов из стандарта: область применения метода, соответствие рассматриваемым ситуациям, информативность результата, обеспечение доступности информации, практичность метода (в конкретной области), временные затраты, сложность применения.

С учетом вышеперечисленных критериев, из каждой группы было выбрано по одному/два наиболее подходящих методов оценки риска в области ИБ: предварительный анализ опасностей, метод Дельфи, анализ дерева событий, исследование опасности и работоспособности, матрица последствий и вероятностей, а также марковский анализ. Далее была составлена таблица применимости, с помощью которой можно определить целесообразность использования того или иного метода на различных этапах оценки риска (идентификация риска, анализ риска: последствие, вероятностные характеристики, уровень риска). В таблице методы упорядочены по уровню применимости для задач ИБ, кроме того, можно определить, какие методы возможно использовать на каких этапах оценки рисков.

Применимость методов оценки риска

Наименование метода	Процесс оценки риска			
	Идентификация риска	Анализ риска		
		Последствие	Вероятностные характеристики	Уровень риска
Матрица последствий и вероятностей	**+!**	**+!**	**+!**	**+!**
Анализ дерева событий	+	**+!**	+	+
HAZOP	**+!**	**+!**	+	+
Марковский анализ	+	**+!**	–	–
Предварительный анализ опасностей	**+!**	–	–	–
Метод Дельфи	**+!**	–	–	–

Обозначения: «+!» — строго применим, «+» — применим, «–» — не применим

Подведя итог вышеперечисленным методам оценки рисков информационной безопасности, произведем сравнительный анализ данных методов и составим рейтинговый список, оценив возможность и удобство использования каждого из них в области информационной безопасности.

Сравнительный анализ методов оценки рисков ИБ

Методы оценки рисков ИБ	Количественная оценка	Качественная оценка	Ресурсы: временные/информационные	Сложность	Возможность оценки в динамике	Неопределённость
Метод Дельфи	-	+	Средние	Средняя	+	Средняя
Анализ дерева событий	+	+	Средние	Средняя	-	Средняя
Матрица последствий и вероятностей	+	+	Средние	Средняя	-	Средняя
Марковский анализ	+	-	Высокие	Высокая	+	Низкая
HAZOP	-	+	Средние	Высокая	+	Высокая
Предварительный анализ опасностей	-	+	Низкие	Средняя	-	Высокая

Таким образом, в результате анализа существующих методов оценки рисков были сформулированы критерии применимости данных методов для задач ИБ. На основе данных критериев было выбрано 6 методов, наиболее подходящих для оценки рисков ИБ. Был выполнен детальный сравнительный анализ выбранных методов, составлен их рейтинг применимости. Также сделан вывод, что комбинированное использование нескольких методов дает более точную оценку, что достигается взаимной компенсацией недостатков различных методов.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Сафронов А. С., Барабанов Н. А., Венедиктов Ю. И. Анализ процессов развития систем информационной безопасности организации // Труды XIV Международной научно-практической конференции «СИЭТ—2013».— Украина, г. Одесса.— 2013.— Т. 1.— С. 201—203.

2. ISO/IEC 31010. Risk assessment techniques.

———

E. A. Eremenko, A. S. Safronov

Analysis of risks of information security based on standard ISO/IEC 31010.

This paper analyzes the methods of risk assessment of the standard ISO / IEC 31010, in order to identify their applicability to assess the risk of information security (IS). As a result of researches the criteria of choice of the optimal methods were set forth for the estimation of risks of IS. According to criteria, 6 methods were chosen and their comparative analysis was conducted.

Keywords: *risk assessment techniques, information security management.*