УДК 004.056

К.Е. Шинаков, О.М. Голембиовская

ФОРМАЛИЗАЦИЯ ПРОЦЕССА ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ МЕТОДИКИ OCTAVE

Рассмотрен процесс оценки рисков информационной безопасности на основе методики OCTAVE.

Ключевые слова: риски информационной безопасности, методика OCTAVE, ценность информационных ресурсов.

На сегодняшний день вопрос оценки рисков информационной безопасности является актуальным для многих предприятий. Связано это в первую очередь с модернизированной нормативно-правовой базой, позволяющей четко определять наказания и штрафы для операторов систем защиты конфиденциальной информации, не обеспечивающих принципы конфиденциальности, целостности и доступности последней.

Вместе с этим сформулированные понятия уровня исходной защищенности и вероятности реализации угрозы не позволяют оператору получить полное представление о защищенности ценных ресурсов и спрогнозировать возможный ущерб при их разглашении, удалении или изменении. Существующие методики оценки рисков информационной безопасности (CRAMM, FRAP, RiskWatch, OCTAVE и др.) позволяют спрогнозировать возможный ущерб. Наиболее интересной и многосторонней является методика OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation, в переводе с англ. – «оперативная оценка критических угроз, активов и уязвимостей»).

В основе ее работы лежит дерево, имеющее вершины «Ресурс», «Уязвимость», «Угроза», «Ущерб», «Риск». В данной статье предпринята попытка проецирования данной методики на процесс оценки рисков предприятий разного профиля на территории Российской Федерации. Алгоритм оценки рисков информационной безопасности (ИБ) на предприятии в соответствии с методикой OCTAVE состоит из нескольких этапов (рисунок):

1. Определение ценности активов организации (S_i).
2. Определение угроз и соответствующих им уязвимостей, оценка вероятности реализации угроз (V_{ry}).
3. Определение риска информационной безопасности (R).
4. Формирование планов по снижению риска ИБ [1].

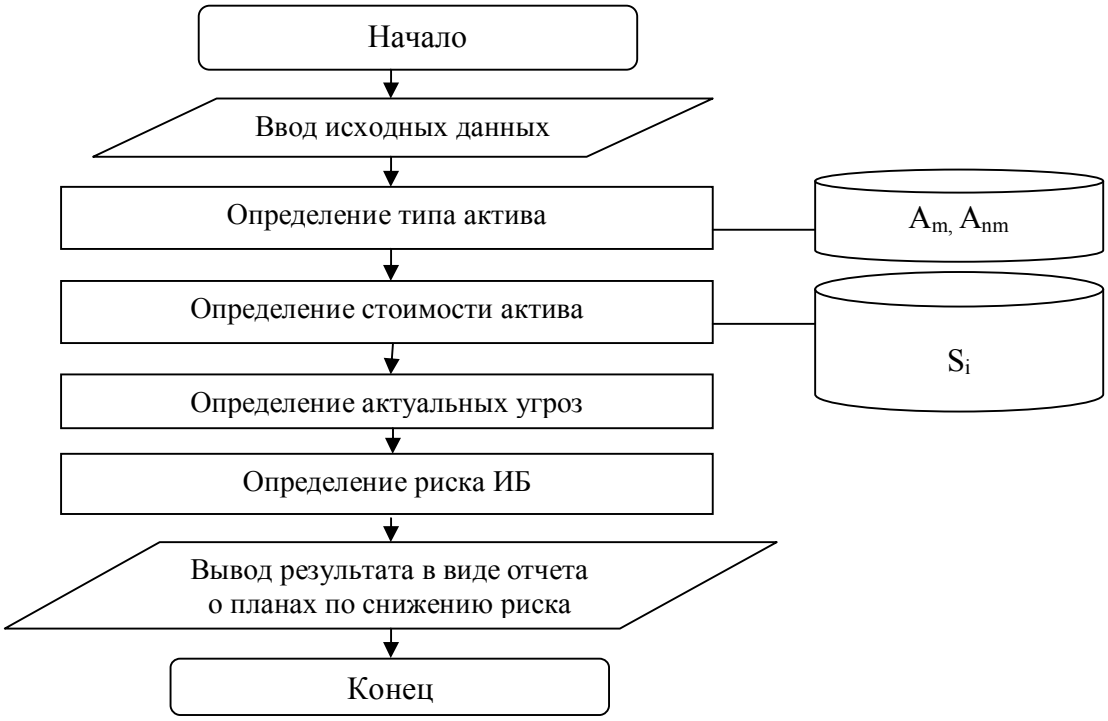

Рис. Блок-схема алгоритма оценки рисков ИБ в соответствии с методикой OCTAVE

Для определения ценности активов организации целесообразно разделить их на материальные (A_m) и нематериальные (A_{nm}) (табл. 1).

Таблица 1

Определение активов организации

№ п/п	Материальные активы (A_m)	№ п/п	Нематериальные активы (A_{nm})
1.1	Производственное оборудование	2.1	Персональные данные (личные дела сотрудников, медицинские карты)
1.2	Электронно-вычислительные машины	2.2	Коммерческая тайна (бизнес-план, секрет производства)

На первом этапе для обозначенных активов необходимо определить их возможную стоимость или тот денежный ущерб, который может быть нанесен вследствие разглашения, удаления или изменения данного актива.

Для удобства оценки рисков информационной безопасности используем балльную систему. Для оценки стоимости активов введем соответствующие баллы (табл. 2).

Таблица 2

Определение ценности активов организации

№ актива	Основание для оценки актива	Стоимость актива (S_i)	№ актива	Основание для оценки актива	Стоимость актива (S_i)
1.1	Производственное оборудование	10 баллов (≥ 1 000 000 руб.)	2.1	Персональные данные	6 баллов (500 000 т.руб.)
1.2	Электронно-вычислительные машины	2 балла (> 10 000 т.руб.)	2.2	Коммерческая тайна	6 баллов (120 000 т.руб.)
1.3	Комплектующие изделия	6 баллов (> 100 000 т.руб.)	2.3	Иная конфиденциальная информация	2 балла (50 000 т.руб.)

Вторым этапом оценки рисков ИБ является определение угроз и соответствующих им уязвимостей (табл. 3) [2].

Таблица 3

Перечень угроз и соответствующих им уязвимостей

№ п/п	Угрозы	Уязвимости
1	Утечка видовой информации	Отсутствие жалюзи на окнах
		Расположение ПК мониторами к окнам
2	Утечка акустической информации	Отсутствие шумогенератора
3	Кража носителей информации	Хранение носителей информации за пределами сейфа
		Отсутствие системы контроля доступа
		Отсутствие системы видеонаблюдения
		Отсутствие системы сигнализации
4	Утечка информации по каналам ПЭМИН	Отсутствие экранирования кабельных коммуникаций
5	Преднамеренное уничтожение информации	Отсутствие утвержденного «Положения о разграничении доступа»

Окончание табл. 3

№ п/п	Угрозы	Уязвимости
		Отсутствие программной системы разграничения доступа типа Secret Net
		Отсутствие системы контроля доступа, КПП
		Отсутствие утвержденного «Положения о защите конфиденциальной информации, обрабатываемой в организации»
6	Непреднамеренное уничтожение информации	Отсутствие системы резервного копирования
7	Действия вредоносных программ	Не установлено сертифицированное антивирусное ПО
8	Удаленный запуск приложений	Отсутствие средств межсетевого экранирования
9	Стихийное бедствие	Отсутствие противопожарной системы
		Отсутствие источников бесперебойного питания

Также на данном этапе целесообразно определить вероятность реализации угроз - V_{ry} (табл. 4).

Таблица 4

Фрагмент опросной таблицы «Оценка вероятности реализации угроз»

№ п/п	Угроза	Средство нейтрализации угрозы	Имеется ли на объекте данное средство защиты?	
			Да	Нет
1	Утечка видовой информации	Жалюзи на окнах	+	
2	Утечка акустической информации	Шумогенератор		+
3	Кража носителей информации	Сейфы для хранения носителей информации	+	
		Система контроля доступа		+
		Система видеонаблюдения	+	
		Сигнализация	+	
4	Утечка информации по каналам ПЭМИН	Экранирование кабельных коммуникаций		+
5	Преднамеренное уничтожение информации	Система видеонаблюдения	+	
		Сигнализация	+	
		Решетки на окнах		+
		КПП		+
6	Непреднамеренное уничтожение информации	Учет доступа сотрудников к конфиденциальной информации		+
7	Действия вредоносных программ	Антивирусное сертифицированное ПО на ПК сотрудников		+

Окончание табл. 4

№ п/п	Угроза	Средство нейтрализации угрозы	Имеется ли на объекте данное средство защиты?	
			Да	Нет
8	Удаленный запуск приложений	Средства межсетевого экранирования	+	
9	Стихийное бедствие	Противопожарная система	+	

В случае наличия на объекте всех средств защиты $V_{гу}$=0, при наличии 50 % средств защиты $V_{гу}$=5, в случае отсутствия более 80 % средств защиты $V_{гу}$=10.

В приведенном фрагменте опросной таблицы (табл. 4) на объекте отсутствует 57% средств защиты, следовательно, $V_{гу}$=5.

Для определения риска информационной безопасности воспользуемся формулой

$$R= S_i V_{гу},$$

где S_i – ценность актива; $V_{гу}$ – вероятность реализации угрозы; R- риск ИБ.

Определив значение риска, мы можем сформировать план по его снижению (табл. 5).

Таблица 5

Определение значений риска ИБ

$V_{гу}$	S_i	R	Величина риска	План по снижению риска
1	2	2	Низкая	Долговременный
	6	6	Средняя	
	10	10	Высокая	
5	2	10	Низкая	На среднюю перспективу
	6	30	Средняя	
	10	50	Высокая	
10	2	20	Низкая	Списки задач на ближайшее время
	6	60	Средняя	
	10	100	Высокая	

На основании данных табл. 5 можно сделать вывод о том, что план по снижению риска индивидуален для каждой вероятности реализации угроз.

Можно проиллюстрировать процесс оценки риска ИБ по методике OCTAVE на примере условной организации – ООО «Олимп» (табл. 6).

Таблица 6

Процесс оценки риска ИБ

План развития предприятия	Ценность актива	Вероятность реализации угрозы	Риск ИБ	План по снижению риска	Меры по снижению риска
Коммерческая тайна	S_1= 6	$V_{гу}$= 5	R=30	На среднюю перспективу	Использование шумогенератора при проведении совещаний
					Обеспечение контроля доступа
					Экранирование кабельных коммуникаций
					Установка решеток на окнах
					Организация системы контроля доступа, КПП
					Обеспечение учета доступа сотрудников к конфиденциальной информации

Таким образом, с помощью использования основ методики OCTAVE можно однозначно определить как риск информационной безопасности, так и меры, необходимые для его снижения.

СПИСОК ЛИТЕРАТУРЫ

1. Голембиовская, О.М. Оценка рисков безопасности информационных систем персональных данных/О.М.Голембиовская, В.И.Аверченков, М.Ю.Рытов//Информация и безопасность. – Воронеж, 2012. – №3. – С. 321 – 328.
2. Формализация подходов к обеспечению защиты персональных данных, обрабатываемых в информационных системах: монография/ О.М.Голембиовская, М.Ю.Рытов, К.Е.Шинаков. – Брянск: БГТУ, 2014. – 189 с.

Материал поступил в редколлегию 12.05.15.