Определение величины риска

написано Александр Астахов | 10 июня, 2023

Ценность активов, вероятности угроз и уровни уязвимостей сопоставляются в следующей таблице.

Таблица С.6 Матрица с величиной рисков

Стоимость ресурса	Уровень угрозы								
	Низкий			Средний			Высокий		
	Уровень уязвимости								
	Н	С	В	Н	С	В	Н	С	В
0	0	1	2	1	2	3	2	3	4
1	1	2	3	2	3	4	3	4	5
2	2	3	4	3	4	5	4	5	6
3	3	4	5	4	5	6	5	6	7
4	4	5	6	5	6	7	6	7	8

При объединении ценности активов с угрозами и уязвимостями необходимо рассмотреть возможность создания комбинацией угроза/уязвимость проблем для конфиденциальности, целостности и/или доступности этих активов. В зависимости от результатов этих рассмотрений должны быть выбраны подходящие значения ценности активов, т.е. значения, которые выражают последствия нарушения конфиденциальности, или целостности, или доступности.

Использование этого метода может привести к рассмотрению одного, двух или трех рисков для одного актива, в зависимости от конкретной рассматриваемой комбинации «угроза/уязвимость». Если используются дополнительные свойства (такие, например, как аутентичность или неотказуемость), тогда для каждого актива и каждой комбинации «угроза/уязвимость» может вычисляться даже более трех рисков. В этом примере величина рисков определяется по шкале от **0** до **8**:

- Величина риска в диапазоне от **0** до **2** соответствует относительно низкому уровню риска, который, как правило, может быть принят без дальнейшей обработки.
- Величина риска в диапазоне от **3** до **5** соответствует

среднему уровню риска, который может требовать определенной обработки.

- Величина риска в диапазоне от **6** до **8** соответствует высокому уровню риска, который должен быть обработан в первую очередь.

Для многих организаций такой шкалы вполне достаточно. Однако ничто не мешает эту шкалу расширить, введя дополнительные уровни угроз, уязвимостей или ущерба (ценности актива).

Реестр информационных рисков – основной документ, описывающий текущую ситуацию с рисками в организации. Он формируется путем объединения таблицы ценности активов, таблицы оценки угроз и уязвимостей и таблицы величины рисков.

Реестр информационных рисков

№	Группы угроз	Уязвимости	Активы	Вероятность угроз	Уровень уязвимости	Ценность актива	Уровень риска	Механизмы контроля
			Риски офисной сети					
			Физические риски					
1	Кража компьютерного оборудования и носителей информации инсайдерами Физический НСД в помещения организации, в кабинеты и серверные комнаты, к оборудованию, бумажным документам, запоминающим устройствам, носителям информации и т.п.	Не производится регистрация оборудования и информационных носителей, выносимых за пределы территории организации. Отсутствуют правила работы в зонах безопасности. При приеме на работу не производится проверка истории кандидатов.	Корпоративный веб сайт	М	М	0	2	Средний уровень лояльности сотрудников. Существует политика безопасности в отношении мобильных носителей информации и использования внешних устройств. Существует политика возврата оборудования, носителей информации и документации при увольнении сотрудников. Для доступа на территорию организации используются смарт-карты Территория охраняется службой безопасности Офисное оборудование и документация находятся строго в зонах безопасности.
			Отчеты по мероприятиям			1	3	
			Электронные сообщения			2	4	
			Проектная документация			2	4	
			Договора соглашения			1	3	
			Бухгалтерская база данных			3	5	
			Первичная бухгалтерская документация			3	5	
			Финансовые			3	5	