ПРАКТИЧЕСКАЯ РАБОТА № 7. ОЦЕНКА РИСКОВ

Цель: ознакомиться с принципами управления и оценки рисками.

Теоретические вопросы

Табличный метод оценки рисков.

Оценку проводят на основе рекомендаций по оценке активов данных, которые охватывают:

- личную безопасность;
- персональные данные;
- обязанности соблюдать требования законов и подзаконных актов;
- правовое принуждение;
- коммерческие и экономические интересы;
- финансовые потери/нарушение нормального хода работ;
- общественный порядок;
- политику ведения бизнеса и деловых операций;
- потерю репутации.

Управление и оценка рисками рассматривается на административном уровне ИБ, поскольку только руководство организации способно выделить необходимые ресурсы, инициировать и контролировать выполнение соответствующих программ.

С точки зрения собственника информации и поддерживающей ее инфраструктуры существование некой угрозы или уязвимости может быть не очень критично для него. Вероятность реализации этой угрозы либо использования уязвимости может быть настолько мала, что на факт ее существования можно просто закрыть глаза (например, утечка информации через ПЭМИН для домашнего компьютера). С другой стороны, вероятность реализации угрозы может быть достаточно велика, но стоимость потерь при реализации – столь мала, что нейтрализация данной угрозы потребует большие финансовые затраты, чем возможные потери при реализации.

С точки зрения собственника информации, основными показателями, связанными с угрозами ИБ и влияющими на степень их опасности для ИС, является вероятность их реализации, а также возможный ущерб владельцам или пользователям информации. Комплексный показатель, объединяющий эти два показателя – риск информационной безопасности.

Под **риском информационной безопасности** будем понимать возможные потери собственника или пользователя информации и поддерживающей инфраструктуры связанные с реализацией некоторой угрозы.

Рекомендации облегчают определение значений на числовой шкале (например, от 1 до 4), которая предусмотрена для матрицы, используемой в качестве примера (см. таблицу1.), позволяя, таким образом, использовать там, где возможно, количественные, а там, где невозможно, – логические и качественные оценки, например, при оценивании степени угрозы для жизни людей.

Таблица 1. Табличный метод оценки рисков

Ценность актива	**Уровень угрозы**								
	Низкий			**Средний**			**Высокий**		
	Уровень уязвимости			**Уровень уязвимости**			**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

Ценности активов, а также уровни угроз и уязвимости, соответствующие каждому типу воздействия вводят в матрицу для определения каждого сочетания соответствующих мер риска по шкале от 1 до 8. Значения величин размещают в матрице в структурированной форме в соответствии с таблицей 1.

Для каждого актива рассматривают уязвимые места и соответствующие им угрозы. В Приложении 1 и Приложении 2 перечислены предлагаемые стандартом возможные угрозы и уязвимости. Если имеются уязвимые места без соответствующей угрозы или угрозы без соответствующего уязвимого места, то считают, что в данное время риск отсутствует (необходимо проявлять осторожность на случай возможного изменения ситуации!). Затем идентифицируют соответствующий ряд матрицы по ценности актива, а соответствующую колонку – по степени угрозы и уязвимости. Например, если ценность актива равна 3, угрозу характеризуют как "высокую", а уязвимость – как "низкую", мера риска равна 5. Предположим, что ценность актива равна 2; при оценке, например, угрозы модификации актива, угрозу характеризуют как "низкую", а уязвимость - как "высокую". В этом случае мера риска будет равна 4. Размер матрицы с точки зрения числа категорий, характеризующих степень угрозы, степень уязвимости и ценность актива выбирают в зависимости от потребностей организации. Дополнительные колонки и ряды дают дополнительное число мер риска. Ценность настоящего метода состоит в ранжировании соответствующих рисков.

1. Ранжирование угроз по мерам риска.

Для установления пошаговой взаимозависимости между факторами воздействия (ценность актива) и вероятностью возникновения угрозы (с учетом аспектов уязвимости) может использоваться матрица или таблица (см. таблицу 2.). Первый шаг – оценка воздействия (ценности актива) по заранее определенной шкале, например, от 1 до 5, для каждого подвергаемого угрозе актива (колонка b в таблице 2). Второй шаг – оценка вероятности возникновения угрозы по заранее определенной шкале, например, от 1 до 5, для каждой угрозы (колонка с в таблице 2). Третий шаг – расчет мер риска умножением результатов первых двух шагов (b×c). Теперь можно проранжировать опасности по значению коэффициента "подверженности воздействиям". В таблице 2 цифрой 1 обозначены самое малое воздействие и самая низкая вероятность возникновения угрозы.

Таблица 2. Ранжирование рисков

Дескриптор угроз *a*	**Оценка воздействия (ценности актива) *b***	**Вероятность возникновения угрозы *c***	**Мера риска *d***	**Ранг угрозы *e***
Угроза A	5	2	10	2
Угроза B	2	4	8	3
Угроза C	3	5	15	1
Угроза D	1	3	3	5
Угроза E	4	1	4	4
Угроза F	2	4	8	3

Как показано выше, такой метод позволяет сравнивать и ранжировать по приоритетности разные угрозы с различными воздействиями и вероятности возникновения угрозы. В некоторых случаях необходимо соотнести используемые в этой процедуре эмпирические шкалы с денежными единицами.

2. Оценка частоты появления и возможного ущерба, связанного с рисками.

В настоящем примере основное внимание уделяется воздействию нежелательных инцидентов и определению систем, которым следует предоставить приоритет. Для этого оценивают по два значения для каждого актива и риска, которые в разных комбинациях определяют оценку каждого актива. Вычисляют сумму оценок всех активов данной системы и определяют меру риска для данной системы информационных технологий.

Прежде всего, определяют ценность каждого актива. Ценность актива связана с возможным повреждением актива, которому угрожают, и назначается для каждой угрозы, которой может подвергнуться данный актив.

Затем определяют значение частоты. Частоту оценивают по сочетанию вероятности возникновения угрозы и легкости возникновения угроз в уязвимых местах (см. таблицу 3.).

Таблица 3. Частота появления ущерба

Частота	Уровень угрозы (Вероятность)								
	"Низкий"			"Средний"			"Высокий"		
	Уровень уязвимости			Уровень уязвимости			Уровень уязвимости		
	Н	С	В	Н	С	В	Н	С	В
	0	1	2	1	2	3	2	3	4

Затем по таблице 4. определяют оценки по активам/угрозам, находя пересечение колонки ценности актива и строки частоты. Оценки по активам/угрозам суммируют и определяют общую оценку актива. Эта оценка может быть использована для определения различий между активами, образующими часть системы.

Таблица 4. Общая оценка актива

Частота	Ценность актива				
	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8

Последний шаг состоит в вычислении суммы оценок всех активов системы для определения оценки системы. Эта оценка может быть использована для определения различий между системами, а также для определения средств защиты системы, которые следует использовать в первую очередь.

В приведенных ниже примерах все значения величин выбраны случайным образом. Предположим, что в системе S имеется три актива: A1, A2 и A3. Предположим также, что данная система может подвергаться двум угрозам: T1 и T2. Пусть ценность актива A1 будет равна 3, ценность актива A2 - 2 и ценность актива A3 - 4. Если для сочетания актива A1 и угрозы T1 вероятность возникновения угрозы мала, а легкость возникновения угрозы в уязвимых местах имеет среднее значение, то частота будет равна 1 (см. таблицу 3.).

Оценка сочетания актива A1 и угрозы T1 может быть взята по таблице 4 на пересечении колонки "ценность актива", равной 3, и строки "частота", равной 1. В данном случае эта оценка будет равна 4. Аналогично принимают для оценки сочетания актива A1 и угрозы T2 среднюю вероятность возникновения угрозы и высокую легкость возникновения угрозы в уязвимых местах. Тогда оценка сочетания актива A1 и угрозы T2 будет равна 6.

Затем вычисляют значение общей оценки A1T, которая будет равна 10. Общую оценку активов рассчитывают для каждого актива и применимой угрозы. Общую оценку системы ST определяют по сумме A1T+A2T+A3T.

Теперь можно сопоставить различные системы и различные активы внутри одной системы и установить приоритеты.

3. Разграничение между допустимыми и недопустимыми рисками

Другой способ измерения рисков состоит только в разграничении допустимых и недопустимых рисков. Предпосылка заключается в том, что меры рисков используют лишь для ранжирования областей по срочности принятия необходимых мер, что может быть достигнуто с затратой меньших усилий.

В соответствии с таким подходом применяемая матрица уже не содержит числовых значений, а только буквы T (для допустимых рисков) и N (для недопустимых рисков). Так, например, матрица, используемая для метода 3, может быть преобразована в матрицу по таблице 5.

Таблица 5. Оценка допустимости риска

Частота	Ценность актива				
	0	1	2	3	4
0	T	T	T	T	N
1	T	T	T	N	N
2	T	T	N	N	N
3	T	N	N	N	N
4	N	N	N	N	N

Задание. На примере конкретной АС (ИС), провести оценку рисков в соответствии свыше описанным методом.

Пример АС (ИС) (староста распределяет темы)

1. ИС Сбербанка
2. ИС Поликлиники
3. ИС Больницы
4. ИС Библиотеки
5. ИС Школы
6. ИС Университета
7. ИС Детского сада
8. ИС интернет магазина
9. ИС супермаркет Перекресток
10. ИС супермаркет Пятерочка
11. ИС супермаркет Лента
12. ИС Военной части
13. ИС Монастыря
14. ИС Аэропорта
15. ИС Железнодорожного вокзала
16. ИС Кинотеатра
17. ИС Зоопарка
18. ИС Метрополитена
19. ИС Мосбиржа
20. ИС Управление делами президента