МЕТОД СТРУКТУРИРОВАННОЙ ОЦЕНКИ ИНФОРМАЦИОННЫХ РИСКОВ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

Замула А.А., Черныш В. И., Иванов К.И.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Ленина,14, каф. БИТ, тел. (057) 702-14-25)
E-mail: vlad.chernish@gmail.com, тел. (063) 208-44-30

The method of analytical work in structuring risk of IS. A seven components described method steps.

Информационная безопасность (ИБ) в настоящее время становится необходимым условием успешного развития хозяйствующего субъекта. Риск компрометации информации влияет на материальные и нематериальные активы организации и, в конечном счёте, на результаты её производственно-экономической деятельности. В связи с широким спектром возможных информационных рисков, значительным разбросом значений ущерба при их реализации и ограниченностью бюджета на информационную безопасность возникает задача рационального финансирования затрат на защиту информации. Возможна и другая постановка задачи: при фиксированном объеме финансовых вложений необходимо снизить уровень риска компрометации информации до минимального значения.

Оценка информационных рисков (ИР) проводится с использованием методов, требующих статистических данных по инцидентам, либо использующих некоторые категории значимости ИР. Недостатком таких методов является тот факт, что величина ИР имеет (чаще всего) субъективные значения, что вносит существенную погрешность в результаты их оценки. С другой стороны, оценка рисков с помощью экспертных методов вносит помеху в виде неточности оценки.

Цель процесса оценивания рисков состоит в определении характеристик рисков в информационной системе (ИС) и ее ресурсах. На основе таких данных выбираются необходимые средства управления ИБ.

В докладе предлагается метод выполнения аналитических работ по структурированию рисков ИБ. Метод включает в себя 7 шагов. Приводится характеристика шагов предлагаемого метода.

Шаг 1: Описание системы. На этом шаге проводится сбор сведений для определения границ и описания системы на различных иерархических уровнях с целью выявления уязвимостей и оценки достаточности принятых мер защиты.

Шаг 2: Идентификация источников угроз. Целью данного шага является определение потенциальных источников угроз для оцениваемой ИТ-системы и составление списка актуальных источников угроз для данной информационной системы.

Шаг 3: Идентификация уязвимостей. Целью данного шага является создание списка уязвимостей (недостатков или упущений), которыми могут воспользоваться потенциальные источники угроз.

Шаг 4: Анализ контроля безопасности. Цель данного шага – анализ средств контроля, уже внедренных компанией или планируемых для внедрения для уменьшения или устранения вероятности использования уязвимости системы.

Шаг 5: Определение вероятности. На данном шаге вычисляется значение вероятности успешной атаки, которое зависит от потенциала угрозы, создаваемой активным источником угрозы в поле уязвимости (табл. 1).

Шаг 6: Определение риска. Цель данного этапа заключается в определении максимального уровня риска при успешной реализации атаки от i-го источника по j-й уязвимости.

Простой способ получения оценок ИР для каждой пары угроза/уязвимость, который можно заложить в механизм оценки ИР, заключается в перемножении вероятности реализации угрозы и ущерба от реализации угрозы с последующим ранжированием полученных значений.

Таблица 1. Показатели веса вероятности успешной атаки

Эффективность защиты *Z(i,j)*	Потенциал угрозы *U(i,j)*				
	1	2	3	4	5
0 (защита отсутствует)	1	2	3	4	5
1	0	1	2	3	4
2	0	0	1	2	3
3	0	0	0	1	2
4	0	0	0	0	1
5	0	0	0	0	0

Табличные данные отражают пороговый эффект, связанный с преодолением защиты и получены на основе операции алгебраической разности. Распределение числовых значений показателя уровня вероятности приведено в таблице 2.

Таблица 2. Шкала значений уровня вероятности реализации угрозы

Уровень вероятности		Описание уровня
1	Очень низкий	Используемые средства защиты и методы их применения гарантируют защиту по отношению к данному типу угроз в пределах заданной уязвимости (используются сертифицированные профили защиты).
2	Низкий	У источника угрозы недостаточно мотиваций или возможностей, либо существующие средства контроля способны предотвратить или, по крайней мере, значительно помешать использованию уязвимости.
3	Средний	Источник угрозы мотивирован и обладает возможностями, но существующие средства контроля могут препятствовать успешному использованию уязвимости.
4	Высокий	Источник угрозы имеет высокие мотивации и достаточные возможности, а методы контроля для предотвращения проявления уязвимости не гарантируют защиту.
5	Очень высокий	Уровень мотивации, технические и организационные возможности источника угроз превышают соответствующие параметры защиты.

Шаг 7: Рекомендации по контролю и оформление итоговых документов. Данный шаг обеспечивает средства контроля, которые могут снизить или устранить идентифицированные риски и которые являются подходящими для данной компании. Целью рекомендуемых методов контроля является снижение уровня рисков для ИТ-системы и ее данных до приемлемого уровня.

После завершения оценки ИР (идентифицированы угрозы и уязвимости, оценены риски, рекомендованы средства контроля) следует оформить документацию в виде официального отчета или кратких инструкций.

В предложенном методе структурирования появляется возможность получения качественных и количественных оценок величин риска с максимальной возможностью учета априорных данных и результатов предварительных исследований характеристик и свойств ИР. Полученные оценки ИР могут быть использованы при разработке концепции обеспечения ИБ на этапе создания ИС, и для поддержания установленного уровня риска на этапе эксплуатации ИС.