М. И. ТЕНЕТКО, О. Ю. ПЕСКОВА, ТТИ ЮФУ

ОБЗОР МЕТОДОВ АНАЛИЗА И ОЦЕНКИ ИНФОРМАЦИОННЫХ РИСКОВ

The article reviews some methods of risk analysis and vulnerability assessment of information systems. Main principles of work are descripted shortly, and the analysis of weaknesses is given. The approach for improvement of risk analysis and vulnerability assessment is offered.

Одним из важных аспектов обеспечения безопасности предприятия является проведение аудита информационной безопасности. При аудите большое значение имеет анализ и оценка информационных рисков компании.

Цель мероприятий по анализу и оценке рисков состоит в определении характеристик рисков информационной системы и её ресурсов. В результате становится возможным выбрать средства, обеспечивающие желаемый уровень защищённости информационных ресурсов компании.

При анализе и оценке рисков традиционно используются математические методы поддержки принятия решений: табличный метод, метод анализа иерархий, метод экспертных оценок. Рассмотрим вкратце эти методы и определим их основные недостатки.

Табличный метод – етод, опирающийся на таблицу, которая является схемой связей между угрозами, уязвимостями и ресурсами. Количественные и качественные показатели оцениваются при помощи балльных шкал. Качественные оценки используются в случаях, когда количественные оценки по ряду причин затруднены [1].

Относящиеся к каждому типу негативных воздействий уровни рисков, соответствующих показателям ценности ресурсов, а также показателям угроз и уязвимостей, оцениваются при помощи таблицы. Количественный показатель риска определяется в фиксированной шкале. Для каждого ресурса рассматриваются относящиеся к нему уязвимые места и соответствующие им угрозы. Каждая строка в таблице определяется показателем ресурса, а каждый столбец –степенью опасности угрозы и уязвимости.

Как правило, значения риска находятся в определённой линейной зависимости от показателей ценности ресурса, угроз и уязвимостей. Шкалы качественных показателей при этом легко конвертируются в шкалы с численными значениями.

Описанный метод позволяет провести классификацию рассматриваемых рисков. Кроме того, метод даёт возможность наглядно отразить в таблице связь между угрозами, негативными воздействиям и возможностями реализации. Для этого необходимо умножить показатель негативного воздействия каждой угрозы на реальность её реализации. Оба эти показателя предварительно оцениваются по фиксированной шкале. По итогам вычисления проводится ранжирование угроз.

Метод анализа иерархий – тод, применение которого сводит исследование практически любых сложных систем к последовательности попарных сравнений компонент данных систем [2]. Иерархия в данном случае — система наслаиваемых уровней, каждый из которых состоит из многих элементов, или факторов. Иначе говоря, иерархия — структура, копирующая естественный ход человеческого мышления, при котором разум объединяет множество элементов, отражающих сложную ситуацию, в группы в соответствии с распределением некоторых свойств между элементами.

Центральным вопросом на языке иерархии является следующий: насколько сильно влияют отдельные факторы самого низкого уровня иерархии на вершину –общую цель? Неравномерность влияния по всем факторам приводит к необходимости определения интенсивности влияния, или приоритетов факторов.

Модель должна включать в себя и позволять измерять все важные количественные и качественные факторы. Однако метод работает лишь в том случае, когда практически все эти факторы измерены объективно и в полном объёме, значения показателей непротиворечивы, результаты задач принятия решений однозначны и соответствуют мнению эксперта. Иначе можно ожидать появления систематических и случайных ошибок в оценках [3].

Метод экспертных оценок –метод, в центре которого лежит декомпозиция сложной трудноформализуемой задачи на последовательность более простых подзадач, соответствующих определённому числу элементарных экспертиз. Оценка параметров входит в число наиболее распространённых элементарных экспертиз. Как правило, под оценкой нечисловой информации понимается приписывание нечисловым характеристикам количественных или качественных значений по выбранной шкале измерений.

В общем случае оценка заключается в назначении вероятностей совершения событий, реализации угрозы, дат событий или весов. Определение весовых коэффициентов рисков используется для их упорядочения и определения первоочередных действий по защите. Затем для определения степени безопасности системы на основании

уже определённых параметров используется линейный метод взвешивания и подсчёта [1, 4].

У описанных методов есть ряд недостатков, в целом, не являющихся критическими. Их устранение могло бы повысить эффективность оценивания. Перечислим недостатки подробнее.

Во-первых, методы, особенно метод анализа иерархий, требуют предоставления исчерпывающей исходной информации об объекте оценки. Однако для этого необходимо проанализировать большое количество разнородных параметров состояния. Исчерпывающее количественное описание состояния исследуемой системы в этом случае получить невозможно, поскольку за время, необходимое для его получения, обстановка внутри и вне системы может значительно измениться. Кроме того, даже в случае получения такого описания оно будет представлять собой огромный объём информации, требующий для своей обработки большого количества времени и вычислительных ресурсов.

Далее, оценки даются относительно дискретной шкалы и являются, как правило, численными. Это утверждение в какой-то степени относится и к качественным оценкам. Такая схема представления данных не учитывает особенностей представления сложных знаний в человеческом мозге. В результате математическая модель объекта оценки, служащая основой для принятия решений, обедняется, упрощается и, возможно, даже искажается.

Например, объект оценки может обладать частью характерных признаков определённой категории, а другой частью в то же время не обладать. Иными словами, принадлежность объекта к определённому классу может быть размыта. Соответственно, в таком случае принципиально меняется логика взаимосвязи входных и выходных данных.

Оценка всегда зависит от субъективных суждений эксперта, его знаний и опыта. В целом, влияние субъективности при обработке субъективных данных неизбежно и даже полезно. Однако возможны случаи отрицательного влияния субъективности, и в таких случаях должны быть надёжные механизмы для коррекции субъективности.

Наконец, для проведения аудита при помощи указанных методов и реализующих их средств эксперт должен обладать достаточно большим опытом аудита и навыками работы с системой. Средства, реализующие описанные методы, являются средствами поддержки принятия решений. К самостоятельным действиям, направленным на накопление собственного опыта, коррекцию субъективности при оценивании и поиск оптимального решения поставленной задачи они не способны.

Таким образом, для повышения качества оценки рисков необходимо исследовать и реализовать, во-первых, механизмы представления нечётких и неполных данных (нечёткие механизмы), во-вторых, механизмы устранения субъективности нечётких и неполных данных и поиска оптимального решения задачи (эволюционные механизмы). На сегодняшний день несколькими исследователями независимо друг от друга исследуются вопросы применения нечётких механизмов для указанных целей. Однако вопросы применения эволюционных механизмов при аудите информационной безопасности в настоящее время остаются неисследованными.

Библиография:

1. Петренко, С. А. Аудит безопасности Intranet. / С. А. Петренко, А. А. Петренко. — М.: ДМК Пресс, 2002. — 416 с.: ил.
2. Саати, Т. Г. Принятие решений. Метод анализа иерархий. / Т. Г. Саати; пер. с англ. Р. Г. Вачнадзе. — М.: «Радио и связь», 1993. — 320 с.: ил.
3. Харитонов, Е. В. Согласование исходной субъективной информации в методах анализа иерархий. / Е. В. Харитонов // Математическая морфология. т. 3, выпуск 2. — 1999. — с. 41 – 51.
4. Корченко, А. Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения. / А. Г. Корченко — К.: "МК-Пресс", 2006. — 320 с.: ил.