XXXI Неделя науки СПбГПУ. Материалы межвузовской научной конференции. Ч. VI: С.162-163, 2003.
© Санкт-Петербургский государственный политехнический университет, 2003.

УДК 681.324.067: 658.5.011.56

А.В. Уланов (5 курс каф. САиУ).

АНАЛИЗ РИСКОВ В СФЕРЕ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Меры по обеспечении безопасности информационной системы, какими бы серьёзными они ни были, не могут гарантировать 100% защиту от всех угроз. Поэтому анализ рисков – оценка уязвимостей и угроз системы – является основной частью любого проекта по обеспечению безопасности. Управление рисками – это процесс введения и поддержания контрмер, которые снижают размер рисков до приемлемого уровня. Анализ рисков – это фактически извлечение данных, необходимых для управления информационной системой, чтобы сделать обоснованные выводы о защищённости информации. При этом: определяются существующие средства защиты, подсчитываются уязвимости и оцениваются последствия угроз в каждой уязвимой области системы.

В настоящее время существует множество методик анализа рисков. Большинство из них имеет программную реализацию и входят в пакеты программ, направленных на аудит информационной безопасности. Среди них: CRAMM, COBRA, RiskWatch, OCTAVE, Buddy Systems. Все они построены по схожим схемам. Однако результаты, получаемые по окончанию анализа информационной системы, существенно различаются.

В данной работе производится анализ перечисленных методик, приводятся их алгоритмы, определяются достоинства и недостатки, а также типы предприятий, где эти методики применимы. На основе рассмотренных методик выводится общая схема построения методики анализа рисков. Даются рекомендации по разработке новых методик, учитывая то, какая имеется информация о безопасности системы, и где они будут применяться.

В большой степени похожесть методик анализа рисков связана с использованием следующего критерия: стоимость контролирования любого из рисков не должна превышать максимальных потерь с ним связанных. Исходя из этого, анализ рисков сводится к нахождению разумного (с экономической точки зрения) баланса между потерями в результате рисков и стоимостью средств защиты, ими управляющими. В процессе анализа используются как количественные, так и качественные оценки рисков. По завершению анализа рисков системы сообщается, какие меры по обеспечению безопасности необходимо применить для достижения приемлемого уровня рисков и к чему это приведёт. На основе этой информации можно принять решение о введении тех или иных средств защиты, а также организационных или технологических мер.

Анализируя рассмотренные методики, можно выявить общую схему построения методики анализа рисков:

1. Определение и оценка ресурсов информационной системы (ИС);
2. Определение соответствующих данным ресурсам угроз;
3. Определение и описание уязвимостей ИС;
4. Нахождение мер противодействия угрозам (контрмеры);
5. Определение остаточного риска;

Определение дополнительных контрмер (рекомендации);
Подготовка отчёта по анализу рисков.

Основываясь на том, как хорошо в данной конкретной методике освещён каждый из вышеперечисленных пунктов, выявляются достоинства и недостатки этой методики. Также, в качестве достоинства методики, можно рассматривать удобство её программной реализации. Кроме того, необходимо определить, для каких типов предприятий наиболее применима эта методика.

Применение зарубежных методик в наших условиях, затруднено из-за отсутствия достоверных статистических данных об инцидентах в сфере безопасности в отечественных ком-

паниях. Поэтому для проведения анализа рисков, необходимо на базе имеющихся (по предложенной схеме) разработать новые методики, учитывающие наши особенности. Предполагается дальнейшее развитие тематики данной работы. В настоящий момент автором ведётся разработка методики анализа рисков в сфере информационной безопасности. Предлагаемый подход основывается на методах получения и корректировки экспертных оценок, а также на математических моделях конфликтных ситуаций, разработанных в теории игр.