МЕТОД CRAMM – КОМПЛЕКСНЫЙ ПОДХОД К ОЦЕНКЕ РИСКОВ

Е.В. Гнедаш
(г. Юрга, Юргинский технологический институт Томского политехнического университета)
E-mail: sunshine9494@rambler.ru

METHOD CRAMM – COMPLEX APPROACH TO RISK ASSESSMENT

E.V. Gnedash
(Jurga, Yurginskiy Technological Institute of the National Research Tomsk Polytechnic University)

Abstract. The article shows the use of the method CRAMM for risk management and research of information security systems.

Keywords: information technology, risk management, IT projects, method CRAMM, information security systems, threat, probability of realization, damage.

Использование информационных технологий (ИТ) является сегодня обязательным условием для эффективного управления промышленным предприятием и повышения его конкурентоспособности. Стремление компаний сохранить достойное место на рынке обуславливает их желание автоматизировать свою деятельность и, таким образом, тратить драгоценное время не на решение рутинных вопросов, а на реализацию новых стратегических планов. Переход на другой качественный уровень работы с информацией и автоматизация деятельности с помощью внедрения информационной системы, представляет собой достаточно трудоемкий и болезненный процесс, сопровождающийся множеством рисков и непредвиденных ситуаций [1].

Процесс управления рисками можно определенно назвать актуальным и необходимым для реализации успешных ИТ-проектов. Под риском проекта понимают потенциальную, численно измеримую возможность неблагоприятных ситуаций и связанных с ними последствий в виде ущерба, убытков, неблагоприятного изменения основных управляемых параметров проекта. Такие ситуации могут возникать в связи с неопределенностью, то есть со случайными изменениями условий экономической деятельности, неблагоприятными, в том числе форс-мажорными, обстоятельствами, а также в связи с возможностью получения непредсказуемого результата в зависимости от предпринятого или не предпринятого действия [4]. Основываясь на перечисленных факторах, управление рисками проектов по внедрению информационных технологий (ИТ-проектов) заключается в том, чтобы заранее выявить все возможные риски и провести комплекс предупреждающих мероприятий для избежания серьезных проблем во время реализации проекта.

ИТ-риски можно условно разделить на две группы: риски, связанные с обеспечением непрерывности работы организации, и риски реализации новых проектов. Первая группа рисков связана с вопросами эксплуатации ИТ-систем, обеспечения коммуникаций, информационной безопасности, сохранности информации, восстановления после аварий и т. д.

Общеизвестным является тот факт, что значительная доля проектов в области ИТ являются неудачными в части соответствия целям, бюджету или срокам – в среднем в мире этот показатель превышает 50 %, а в государственном секторе даже 70 %. Во многом такие проблемы связаны с недостаточно полным и качественным управлением рисками.

Управление рисками проекта, в целом, включает следующие процессы: выявление и идентификацию предполагаемых рисков; анализ и оценку рисков; выбор методов управления риском; применение выбранных методов управления риском; реагирование на наступление рискового события; разработку и реализацию мер по снижению рисков; контроль, анализ и оценку действий по снижению рисков; выработку корректирующих решений [5]. Управление рисками, естественно, охватывает весь цикл проекта – от подготовки до завершения, но наиболее важным (особенно в контрактах с фиксированными сроками и стоимостью) будет правильная оценка будущих рисков на стадии подготовки проекта.

Существует ряд методом способствующих оптимизации прилагаемых к этому усилий. Рассмотрим подробнее один из этих методов – метод CRAMM (CCTA Risk Analysis & Management Method – метод CCTA анализа и контроля рисков). В основе метода CRAMM лежит комплексный подход к оценке рисков, сочетающий количественные и качественные методы анализа.

Целью разработки метода являлось создание формализованной процедуры, позволяющей:

- убедиться, что требования, связанные с безопасностью, полностью проанализированы и документированы;
- избежать расходов на излишние меры безопасности, возможные при субъективной оценке рисков;
- оказывать помощь в планировании и осуществлении защиты на всех стадиях жизненного цикла информационных систем;
- обеспечить проведение работ в сжатые сроки;
- автоматизировать процесс анализа требований безопасности;
- представить обоснование для мер противодействия;
- оценивать эффективность контрмер, сравнивать различные их варианты;
- генерировать отчеты.

Анализ рисков включает идентификацию и вычисление уровней (мер) рисков на основе оценок, присвоенных ресурсам, угрозам и уязвимостям ресурсов. Контроль рисков состоит в идентификации и выборе контрмер, благодаря которым удается снизить риски до приемлемого уровня.

Исследование информационной безопасности системы с помощью метода CRAMM проводится в несколько этапов. На первой стадии производится формализованное описание границ информационной системы, ее основных функций, категорий пользователей, а также персонала, принимающего участие в обследовании.

Оценка производится по десятибалльной шкале, причем критериев оценки может быть несколько – финансовые потери, потери репутации и т. д. В описаниях CRAMM в качестве примера приводится такая шкала оценки по критерию «Финансовые потери, связанные с восстановлением ресурсов» [2]:

Шкала баллов	Величина финансовых потерь
2 балла	менее $1000;
6 баллов	от $1000 до $10 000;
8 баллов	от $10 000 до $100 000;
10 баллов	свыше $100 000.

Для оценки возможного ущерба CRAMM рекомендует использовать следующие параметры: ущерб репутации организации; нарушение действующего законодательства; ущерб для здоровья персонала; ущерб, связанный с разглашением персональных данных отдельных лиц; финансовые потери от разглашения информации; финансовые потери, связанные с восстановлением ресурсов; потери, связанные с невозможностью выполнения обязательств; дезорганизация деятельности [3].

На второй стадии идентифицируются и оцениваются угрозы в сфере информационной безопасности, производится поиск и оценка уязвимостей защищаемой системы. Программное обеспечение CRAMM для каждой группы ресурсов и каждого из 36 типов угроз генерирует список вопросов, допускающих однозначный ответ. Уровень угроз оценивается, в зависимости от ответов, как очень высокий, высокий, средний, низкий и очень низкий. Уровень уязвимости оценивается, в зависимости от ответов, как высокий, средний и низкий. На основе этой информации вычисляется оценка уровня риска по семибалльной шкале. CRAMM

объединяет угрозы и уязвимости в матрице риска. Исходя из оценок стоимости ресурсов защищаемой ИС, оценок угроз и уязвимостей, определяются «ожидаемые годовые потери».

Оценка риска выполняется по двум факторам: вероятность реализации и размер ущерба:

$$\text{Риск} = \text{Р}_{\text{реализации}} * \text{Ущерб}$$

Дальнейшая детализация вероятности реализации:

$$\text{Р}_{\text{реализации}} = \text{Р}_{\text{угрозы}} * \ \text{Р}_{\text{уязвимости}}$$

Где угроза – это действие или событие, способное нанести ущерб безопасности. А уязвимость – слабость в защите ресурса или группы ресурсов, допускающая возможность реализации угрозы.

Третья стадия исследования заключается в поиске адекватных контрмер. По существу, это поиск варианта системы безопасности, наилучшим образом удовлетворяющей требованиям заказчика. На этой стадии CRAMM генерирует несколько вариантов мер противодействия, адекватных выявленным рискам и их уровням.

Таким образом, CRAMM – пример методики расчета, при которой первоначальные оценки даются на качественном уровне, и потом производится переход к количественной оценке (в баллах).

Таблица 1

Достоинства и недостатки метода CRAMM

Достоинства метода	Недостатки метода
Хорошо апробированный метод	Большой объем отчетов,
Удачная система моделирования ИТ	Сравнительно высокая трудоемкость
Обширная база данных для оценки рисков и выбора контрмер	
Возможность использования как средства аудита	

Грамотное использование метода CRAMM позволяет получать очень хорошие результаты, наиболее важным из которых, пожалуй, является возможность экономического обоснования расходов организации на обеспечение информационной безопасности и непрерывности бизнеса. Экономически обоснованная стратегия управления рисками позволяет, в конечном итоге, экономить средства, избегая неоправданных расходов.

Список литературы

1. Успехи современного естествознания // Управление рисками при внедрение ИТ-проектов // [Электронный ресурс] Режим доступа: http://www.econf.rae.ru/pdf/2007/10/Pesotskaya.pdf
2. Интуит Национальный открытый университет // Лекция 4: Методики и программные продукты для оценки рисков // [Электронный ресурс] Режим доступа: http://www.intuit.ru/studies/courses/531/387/lecture/8996?page=1
3. АйТи Управление информационными рисками // [Электронный ресурс] Режим доступа: http://www.it.ru/press_center/publications/3818
4. Чернышева Т.Ю., Удалая Т.В. Оценка риска проекта информатизации на основе продукционных правил // Научное обозрение. 2013. № 5. – С. 169–172.
5. Чернышева Т.Ю., Жуков А.Г. Программный модуль учета рисков проекта на основе дерева решений // Ползуновский вестник. 2012. № 3–2. – С. 70–73.