М. К. Янчин

УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМИ РИСКАМИ НА ОСНОВЕ МЕТОДОЛОГИИ MEHARI

Введение

Оценка и управление рисками представляют собой одну из важных и постоянно развивающихся задач в сфере управления. По мнению специалистов, пренебрежение оценкой финансовых рисков привело к серьезным последствиям во время экономического кризиса [1]. Важность оценки рисков в сфере информационной безопасности демонстрируют появление новых угроз и рост числа преступлений, связанных с информационными технологиями. Одной из серьезных проблем в нашей стране является утечка конфиденциальной информации. В качестве примера может служить утечка персональных данных из сети оператора мобильной связи «МегаФон», произошедшая в июле этого года.

Об осознании наличия данной проблемы и важности процесса оценки и управления информационными рисками свидетельствует то, что создаются разработки стандартов оценки рисков в сфере информационной безопасности.

На данный момент на рынке представлен ряд программных количественных методов оценки рисков в сфере информационной безопасности, таких как CRAMM, Risk Watch или OCTAVE, однако они обладают некоторыми следующими недостатками:

1. Недостаточная совместимость с международными стандартами;
2. Неполный охват активов (сосредоточение внимания только на активах информационных технологий);
3. Сложность использования;
4. Проблемы с отображением русского языка (в связи с тем, что продукты являются импортными).

Наконец, пожалуй, самым важным недостатком программных методов является скрытость процесса расчета рисков от пользователя [1].

Ввиду вышесказанного интерес представляет методология оценки рисков в сфере информационной безопасности MEHARI (Méthode Harmonisée d'Analyse de Risques — Harmonised Risk Analysis Method), разработанная французской организацией CLUSIF (CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS).

Методология представлена в 1996 г. и поддерживается в актуальном состоянии относительно развития сферы информационной безопасности (последняя редакция базы знаний датируется апрелем 2011 г.); успешно опробована на практике в странах Европы, например во Франции, Польше (компания Systemics) и Румынии (Managementul riscurilor).

1. Состав и задачи методологии

Основной задачей MEHARI является предоставление метода оценки и управления рисками в сфере информационной безопасности, совместимого с требованиями ISO/IEC 27005, а также инструментов, необходимых для его внедрения [2].

Кроме того, задача MEHARI — предоставить индивидуальный анализ рискованных ситуаций (risk situations), описываемых сценариями. Сценарий определяется в методологии как описание всех характеристик риска, включая затронутые активы, их внутреннюю уязвимость и угрозу, приводящую к возникновению риска [3].

В состав методологии входят следующие документы:

1. MEHARI: Общие представления и функциональные требования (Concepts and functional specifications);

2. MEHARI: Руководство по процессу управления и анализу рисков (Processing guide for risk analysis and management);

3. MEHARI: Руководство по анализу и классификации ставок безопасности (Security stakes analysis and classification guide);

4. MEHARI: Руководство по анализу рисков (Risk analysis and treatment guide);

5. База знаний MEHARI (Knowledge base).

Назначение первого документа — помочь определить принципы, которым должна отвечать вводимая в организации методология управления рисками, а также выделить функциональные требования, возникающие из этих принципов.

Руководство по процессу управления описывает общую технологию управления рисками методологии MEHARI и составляющие ее этапы. В описании каждого этапа указаны его цели, начальные условия, участники этапа, итоги этапа и процессы, происходящие на данном этапе.

Руководство по анализу и классификации ставок безопасности (security stakes) описывает процесс создания градации уровней неисправностей или нарушений (malfunction value scale), а также классификации активов компании. Под ставкой безопасности в MEHARI подразумеваются последствия, представляющие собой результат воздействия инцидента безопасности на цели организации.

В руководстве по анализу рисков описано применение базы знаний MEHARI в процессе оценки рисков.

База знаний содержит заготовки опросников для аудита, списков угроз, активов, сценариев и других элементов, используемых в методологии, а также встроенные функции расчета текущего значения уровня риска на основе заполненных форм, представленных в базе.

2. Процесс оценки рисков в методологии MEHARI

Процесс оценки рисков по методологии MEHARI состоит из трех этапов: опознания риска, анализа риска и оценки [4].

Опознание рисков состоит в определении сценариев, которым подвержена организация.

Для каждого сценария указаны:

1. Основные затронутые активы;

2. Тип уязвимости, включающий тип наносимого вреда (исчезновение, изменение и др.) и критерии безопасности (конфиденциальность, целостность, доступность, а также эффективность (для процессов управления по отношению к выполнению требований заказчиков и нормативных документов));

3. Тип угрозы, включающий тип события, приводящего к угрозе, его последствия и участвующих лиц (actor) (в случае наличия человеческого фактора);

4. Текстовое описание сценария.

В ходе анализа для каждого сценария определяются степень воздействия (impact) и вероятность реализации сценария (likelihood), однако происходит это не напрямую, а через промежуточные характеристики: внутреннее воздействие в отсутствие защитных мер (intrinsic impact), внутренняя вероятность реализации в отсутствие защитных мер (intrinsic likelihood), влияние защитных мер на вышеупомянутые параметры. Оценка воздействия и вероятности в отсутствие защитных мер производится в связи с тем, что она проще, а также потому, что проводящие оценку сотрудники недооценивают риск, переоценив возможности внедренных механизмов безопасности.

Защитные меры, оказывающие влияние на вероятность реализации сценария, разделяют на два типа — отпугивающие (dissuasive) и превентивные (preventive). Отпугивающие меры направлены на участвующих в сценарии людей — злоумышленников или рядовых сотрудников организаций. Превентивные включают в себя технические меры защиты и мониторинг механизмов, эффективность и прочность которых можно оценить.

Защитные меры, влияющие на воздействие, делятся на ограничивающие (confinement) и смягчающие (palliative). Ограничивающие меры подразумевают механизмы, способные сдержать распространение последствий нарушения работы одного компонента системы на другие. Смягчающие меры не сдерживают последствия нарушения напрямую, но предназначены для снижения воздействий на другие компоненты системы. В базе знаний эффективность мер обозначается соответственно EFF-DISS, EFF-PREV, EFF-CONF, EFF-PALL. Для каждого сценария базы эти показатели определяются либо напрямую от конкретного типа мер защиты, либо от нескольких, если на параметр сценария оказывают влияние несколько типов мер защиты.

Например:

EFF-PREV = 03D01,

где 03D01 — это уровень качества противопожарной безопасности;

EFF-PREV = MAX(02C03; 02D02),

где 02C03 — это уровень качества управления авторизацией доступа в защищенную часть офиса, 02D02 — уровень качества защиты документов и сменных носителей информации [5].

На основе указанных выше параметров вычисляются значения вероятности реализации сценария STATUS-P и его воздействия STATUS-I, используемые при расчете конечного уровня риска.

В случае, если для какой-либо организации существуют специфические сценарии, документация методологии позволяет добавить их к уже созданным и использовать при оценке.

Таким образом, представленные в методологии база знаний и метод оценки рисков могут использоваться в качестве основы или быть адаптированы для оценки рисков информационной безопасности в отечественных организациях.

3. Меры по снижению уровня риска

Помимо оценки рисков по ряду параметров методология MEHARI предоставляет помощь в организации работ по снижению уровня рисков.

На основе анализа сценария риска может быть использовано одно из следующих решений: принять риск; снизить уровень риска, предпринять меры по снижению вероятности реализации сценария и его воздействия; перенести риск, например через страхование.

Работу по данным направлениям в методологии рекомендуется организовать за счет разграничения семейств сценариев. Иначе говоря, сценарии, затрагивающие одинаковые типы активов, группируются. Для каждого семейства затем предлагается план действий (action plan). Каждый план включает в себя сервисы безопасности, относящиеся к семейству, и их целевой уровень по завершении внедрения плана.

В базе знаний реализованы механизмы выбора планов действий на основе семейств сценариев, а также итоговые представления, отображающие список сервисов безопасности и задачи, которые необходимо выполнить для повышения эффективности тех или иных сервисов, если в ходе оценки были выявлены какие-либо слабости в их реализации.

После проведения работ по доработке сервисов безопасности процесс оценки рисков может быть проведен повторно для проверки их эффективности. Таким образом, методология MEHARI позволяет осуществлять полный процесс управления информационными рисками в соответствии со стандартами ISO/IEC 27000. Кроме того, в базу знаний методологии включена оценка

комплектации средствами защиты по стандарту ISO/IEC 27002:2005, что позволяет организации подготовиться к прохождению аудита на соответствие стандарту.

СПИСОК ЛИТЕРАТУРЫ:

1. *Астахов А. М.* Искусство управления информационными рисками. М.: ДМК Пресс, 2010.
2. *CLUSIF* MEHARI 2010 Overview. URL: http://www.clusif.asso.fr/fr/production/ouvrages/pdf/MEHARI-2010-Overview.pdf.
3. *CLUSIF* MEHARI 2010 Fundamental concepts and functional specifications. URL: http://www.clusif.asso.fr/fr/production/ouvrages/pdf/MEHARI-2010-Principles-Specifications.pdf.
4. *CLUSIF* MEHARI 2010 Risk analysis and treatment guide. URL: http://www.clusif.asso.fr/fr/production/ouvrages/pdf/MEHARI-2010-Risk-Analysis-and-Treatment-Guide.pdf.
5. *CLUSIF* MEHARI 2010 knowledge base. URL: http://www.clusif.asso.fr/en/production/mehari/download.asp.