The article analyzes the content of the information objects in the information field. It describes the characteristics of the information field. The article analyzes the nature of information objects. Article typifies information objects. It describes the qualitative heterogeneity used concepts. The paper recommends the narrow definition of the term «information object» by adding the attribute characteristics. This will bring the concept into one category and ensure the comparability of this term in the subject areas.

Keywords: information, information resources, information objects, categories, analysis, systematization, typing

УДК 519.876.5

МЕТОДИКИ АНАЛИЗА И ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

***Елена Константиновна Баранова**, доцент кафедры информационной безопасности,*
E-mail: ekbaranova@hse.ru,
Национальный исследовательский университет,
Высшая школа экономики,
http://www.hse.ru

В общем случае под риском понимают возможность наступления некоторого неблагоприятного события, влекущего за собой различного рода потери. В соответствии с ГОСТ Р 51897–2002 «Менеджмент риска. Термины и определения» и международным стандартом ISO 27001 «Система управления информационной безопасностью» – процесс управления рисками представляет собой скоординированные действия по управлению и контролю организации в отношении риска информационной безопасности (ИБ). Управление рисками включает в себя оценку риска, обработку риска, принятие риска и сообщение о риске.

Ключевые слова: информационная безопасность, аудит информационной безопасности, риски информационной безопасности, защита информации, управление рисками.


Е.К. Баранова

Цель процесса оценивания рисков состоит в определении характеристик рисков по отношению к информационной системе (ИС) и ее ресурсам (активам). На основе полученных данных могут быть выбраны необходимые средства защиты. При оценивании рисков учитываются многие факторы: ценность ресурсов, оценки значимости угроз и уязвимостей, эффективность существующих и планируемых средств защиты и многое другое.

Базовый уровень безопасности (*baseline security*) – обязательный минимальный уровень защищенности для ИС. В ряде стран существуют критерии для определения этого уровня. В качестве примера приведем критерии Великобритании – *CCTA Baseline Security Survey*, определяющие минимальные требования в области ИБ для государственных учреждений этой страны. В Германии эти критерии изложены в стандарте *BSI*. Существуют критерии ряда организаций – *NASA, X/Open, ISACA* и другие. В нашей стране это может быть класс защищенности в соответствии с требованиями ФСТЭК России, профиль защиты, разработанный в соответствии со стандартом *ISO-15408*, или какой-либо другой набор требований. Тогда критерий достижения базового уровня безопасности – это выполнение заданного набора требований.

Базовый (baseline) анализ рисков – анализ рисков, проводимый в соответствии с требованиями базового уровня защищенности. Прикладные методы анализа рисков, ориентированные на данный уровень, обычно не рассматривают ценность ресурсов и не оценивают эффективность контрмер. Методы данного класса применяются в случаях, когда к информационной системе не предъявляется повышенных требований в области ИБ.

Полный (full) анализ рисков – анализ рисков для информационных систем, предъявляющих повышенные требования в области ИБ. Включает в себя определение ценности информационных ресурсов, оценку угроз и уязвимостей, выбор адекватных контрмер, оценку их эффективности.

При анализе рисков, ожидаемый ущерб в случае реализации угроз, сравнивается с затратами на меры и средства защиты, после чего принимается решение в отношении оцениваемого риска, который может быть:

– *снижен,* например, за счет внедрения средств и механизмов защиты, уменьшающих вероятность реализации угрозы или коэффициент разрушительности;

– *устранен* за счет отказа от использования подверженного угрозе ресурса;

– *перенесен*, например, застрахован, в результате чего в случае реализации угрозы безопасности, потери будет нести страховая компания, а не владелец ресурса;

– *принят*.

Наиболее трудоемким является процесс оценки рисков, который условно можно разделить на следующие этапы: идентификация риска; анализ риска; оценивание риска[1].

На рисунке 1 схематично изображен процесс оценки рисков информационной безопасности.

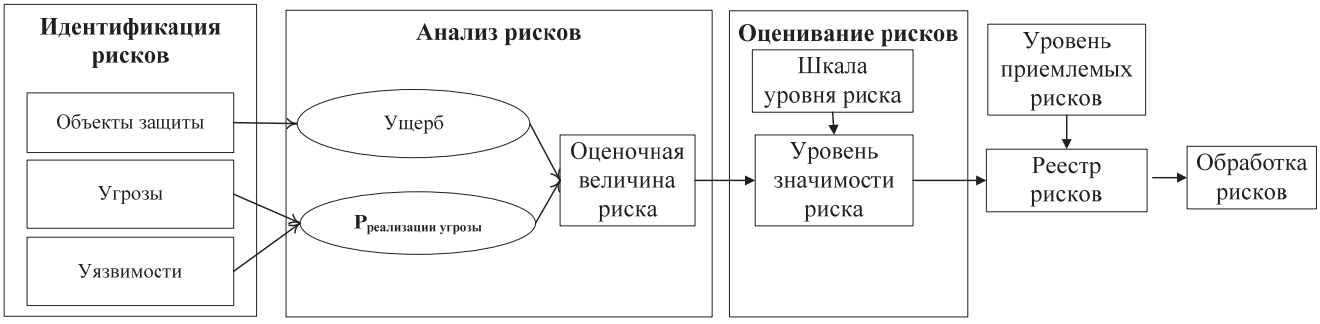

Рисунок 1 – Процесс оценки рисков информационной безопасности

Идентификация риска заключается в составлении перечня и описании элементов риска: объектов защиты, угроз, уязвимостей.

Принято выделять следующие типы объектов защиты: информационные активы; программное обеспечение; физические активы; сервисы; люди, а также их квалификации, навыки и опыт; нематериальные ресурсы, такие как репутация и имидж организации.

Как правило, на практике рассматривают первые три группы. Остальные объекты защиты не рассматриваются в силу сложности их оценки.

На этапе идентификации рисков так же выполняется идентификация угроз и уязвимостей. В качестве исходных данных для этого используются результаты аудитов; данные об инцидентах информационной безопасности; экспертные оценки пользователей, специалистов по информационной безопасности, ИТ-специалистов и внешних консультантов.

[1] *ГОСТ Р ИСО/МЭК 13335-1-2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий».*

Информация, полученная на этапе идентификации рисков, используется в процессе анализа рисков для определения:

– возможного ущерба, наносимого организации в результате нарушений безопасности активов;

– вероятности наступления такого нарушения;

– величины риска.

Величина возможного ущерба формируется с учетом стоимости активов и тяжести последствий нарушения их безопасности.

Второй составляющей, формирующей значение возможного ущерба, является тяжесть последствий нарушения безопасности активов. Учитываются все возможные последствия и степень их негативного влияния на организацию, ее партнеров и сотрудников.

Необходимо определить степень тяжести последствий от нарушения конфиденциальности, целостности, доступности и других важных свойств информационного актива, а затем найти общую оценку.

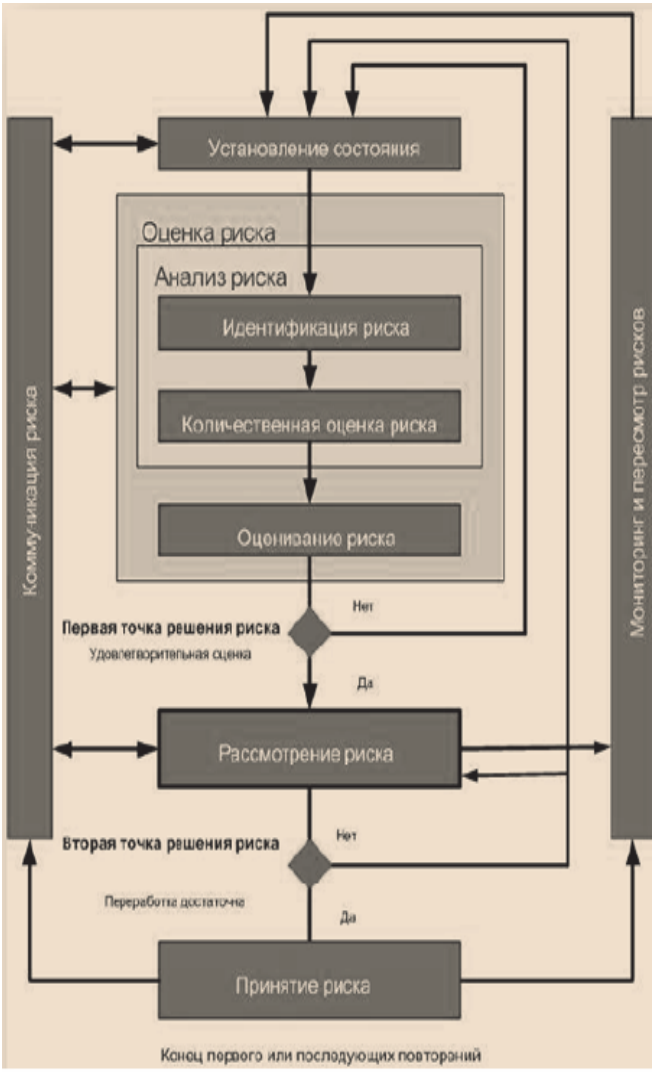

Рисунок 2 – Процесс управления риском ИБ

Следующим этапом анализа рисков является оценка вероятности реализации угроз.

После того, как были определены величина возможного ущерба и вероятность реализации угроз, определяется величина риска. Вычисление рисков производится путем комбинирования возможного ущерба, выражающего вероятные последствия нарушения безопасности активов, и вероятности реализации угроз. Такое комбинирование часто осуществляется при помощи матрицы, где в строках размещаются возможные значения ущерба, а в столбцах – вероятности реализации угрозы, на пересечение – величина риска.

Далее производится сравнение вычисленных уровней риска со шкалой уровня риска. Это необходимо для того, чтобы реалистично оценивать влияние, которое вычисленные риски оказывают на бизнес организации, и доносить смысл уровней риска до руководства. Оценивание рисков должно также идентифицировать приемлемые уровни риска, при которых дальнейшие действия не требуются. Все остальные риски требуют принятия дополнительных мер.

Результаты оценки рисков используются для определения экономической целесообразности и приоритетности проведения мероприятий по обработке рисков,

позволяют обоснованно принять решение по выбору защитных мер, снижающих уровни рисков.

На рисунке 2 приведен процесс управления риском ИБ согласно ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности».

Существует множество методик анализа рисков. Некоторые из них основаны на достаточно простых табличных методах и не предполагают применения специализированного программного инструментария, другие наоборот, активно его используют. Несмотря на повышение интереса к управлению рисками, используемые в настоящее время методики относительно неэффективны, поскольку этот процесс во многих компаниях осуществляется каждым подразделением независимо. Централизованный контроль над их действиями зачастую отсутствует, что исключает возможность реализации единого и целостного подхода к управлению рисками во всей организации.

Для решения задачи оценки рисков информационной безопасности в настоящее время наиболее часто используются следующие программные комплексы: *CRAMM, FRAP, RiskWatch*, *Microsoft Security Assessment Tool (MSAT), ГРИФ, CORAS* и ряд других. Все известные методики можно разделить на:

- методики, использующие оценку риска на качественном уровне (например, по шкале «высокий», «средний», «низкий»), к таким методикам, в частности, относится *FRAP*;
- количественные методики (риск оценивается через числовое значение, например, размер ожидаемых годовых потерь), к этому классу относится методика *RiskWatch*;
- методики, использующие смешанные оценки (такой подход используется в *CRAMM,* методике *MSAT*).

До принятия решения о внедрении той или иной методики управления рисками ИБ следует убедиться, что она достаточно полно учитывает бизнес-потребности компании, ее масштабы, а также соответствует лучшим мировым практикам и имеет достаточно подробное описание процессов и требуемых действий.

В таблице 1 представлен сравнительный анализ наиболее популярных в настоящее время методик (*CRAMM, ГРИФ, RiskWatch, CORAS, MSAT*).

Таблица 1

Сравнение программного инструментария для управления рисками ИБ

Критерии сравнения	**GRAMM**	**ГРИФ**	**RiskWatch**	**CORAS**	**MSAT**
Риски					
Использование категорий рисков	+	+	+	+	+
Использование понятия максимально допустимого риска	+	+	+	+	+
Подготовка плана мероприятий по снижению рисков	+	+	+	–	+
Управление					
Информирование руководителя	+	+	+	+	+
План работ по снижению рисов	–	+	+	–	+
Включает проведение тренингов, семинаров, собраний	–	+	+	–	+
Оценка бизнес-рисков/операционных рисков/ИТ-рисков	–	+	+	+	–
Оценка рисков на организационном уровне	+	+	–	+	+
Оценка рисков на техническом уровне	+	+	+	+	+
Предлагаемые способы снижения рисков					
Обход (исключение) риска	–	+	+	–	–
Снижение риска	+	+	+	+	+
Принятие риска	–	+	–	+	+

Процессы					
Использование элементов риска					
Материальные активы	+	+	+	+	+
Нематериальные активы	+	+	+	+	+
Угрозы	+	+	+	+	+
Ценность активов	+	+	+	+	+
Уязвимости	+	+	+	+	+
Меры безопасности	+	+	+	–	+
Потенциальный ущерб	+	+	+	+	+
Вероятность реализации угроз	+	+	+	+	+
Рассматриваемые типы рисков					
Бизнес-риски	–	+	+	+	–
Риски, связанные с нарушением законодательных актов	–	+	–	–	+
Риски, связанные с использованием технологий	–	+	–	+	+
Коммерческие риски	+	+	+	+	+
Риски, связанные с привлечением третьих лиц	+	+	+	+	+
Риски, связанные с привлечением персонала	+	+	–	+	+
Повторные оценки рисков	–	+	+	–	+
Определение правил принятия рисков	–	+	–	–	+
Способы измерения величин рисков					
Качественная оценка	+	+	+	+	+
Количественная оценка	–	+	+	–	–
Способы управления					
Качественное ранжирование рисков	+	+	+	+	+
Количественное ранжирование рисков	–	+	+	–	–
Использование независимой оценки	–	+	–	+	+
Расчет возврата инвестиций	–	+	–	–	–
Расчет оптимального баланса между различными типами мер безопасности, такими как:					
Меры предотвращения	–	+	+	–	+
Меры выявления	–	+	+	–	+
Меры по исправлению	–	+	+	–	+
Меры по восстановлению	–	+	+	–	+
Интеграция способов управления	–	+	–	–	–
Описание назначения способов управления	–	+	+	+	+
Процедура принятие остаточных рисков	+	+	–	–	+
Управление остаточными рисками	–	+	–	–	+
Мониторинг рисков					
Применение мониторинга эффективности мер ИБ	–	+	+	–	–
Проведение мероприятий по снижению рисков	–	+	+	–	+
Использование процесса реагирования на инциденты в области ИБ	–	+	–	–	+
Структурированное документирование результатов оценок рисков	–	+	+	–	+

Примечание: Таблица сравнения программного инструментария для анализа и оценки рисков приводится по материалам доклада Барановой Е.К., Черновой М.В. на II Международной конференции «Управление информационной безопасностью в современной обществе», 3–4 июня 2014 г., НИУ ВШЭ, г. Москва.

Оценка CRAMM

Данная методика не учитывает сопроводительной документации, такой как описание бизнес-процессов или отчетов по проведенным оценкам рисков. В отношении стратегии работы с рисками *CRAMM* предполагает использование только методов их снижения. Такие способы управления рисками, как обход или принятие, не рассматриваются. В методике отсутствуют: процесс интеграции способов управления и описание

назначения того или иного способа; мониторинг эффективности используемых способов управления и способов управления остаточными рисками; перерасчет максимально допустимых величин рисков; процесс реагирования на инциденты.

Практическое применение *CRAMM* сопряжено с необходимостью привлечения специалистов высокой квалификации; трудоемкостью и длительностью процесса оценки рисков. Кроме того, следует отметить высокую стоимость лицензии.

Оценка ГРИФ

Методика *ГРИФ* использует количественные и качественные способы оценки рисков, а также определяет условия, при которых последние могут быть приняты компанией, включает в себя расчет возврата инвестиций на внедрение мер безопасности. В отличие от других методик анализа рисков, *ГРИФ* предлагает все способы снижения рисков (обход, снижение и принятие). Данная методика учитывает сопроводительную документацию, такую как описание бизнес-процессов или отчетов по проведенным оценкам рисков ИБ.

Оценка RiskWatch

Эта методика использует количественные и качественные способы оценки рисков. Трудоемкость работ по анализу рисков с использованием этого метода сравнительно невелика. Такой метод подходит, если требуется провести анализ рисков на программно-техническом уровне защиты без учета организационных и административных факторов. Существенным достоинством *RiskWatch* является интуитивно понятный интерфейс и большая гибкость метода, обеспечиваемая возможностью введения новых категорий, описаний, вопросов и т. д.

Оценка CORAS

CORAS не предусматривает такой эффективной меры по управлению рисками, как «Программа повышения информированности сотрудников в области информационной безопасности». Такая программа позволяет снизить риски ИБ, связанные с нарушениями режима информационной безопасности сотрудниками компании по причине их неосведомленности в отношении корпоративных требований в этой области и правил безопасного использования информационных систем. Также в *CORAS* не предусмотрена периодичность проведения оценки рисков и обновление их величин, что свидетельствует о том, что методика пригодна для выполнения разовых оценок и не годится для регулярного использования.

Положительной стороной *CORAS* является то, что программный продукт, реализующий эту методику, распространяется бесплатно и не требует значительных ресурсов для установки и применения.

Оценка MSAT

Ключевыми показателями для данного программного продукта являются: профиль риска для бизнеса (величина изменения риска в зависимости от бизнес-среды, действительно, важный параметр, который не всегда учитывается при оценки уровня защищенности системы в организациях разных сфер деятельности) и индекс эшелонированной защиты (сводная величина уровня защищенности). *MSAT* не дает количественной оценки уровня рисков, однако, качественные оценки могут быть привязаны к ранговой шкале.

MSAT позволяет оценить эффективность инвестиций, вложенных во внедрение мер безопасности, но не дает возможности найти оптимальный баланс между мерами, направленными на предотвращение, выявление, исправление или восстановление информационных активов.

Заключение

Рассмотренные методики хорошо соответствуют требованиям групп «Риски» и «Процессы (Использование элементов риска)», но некоторые из них (*CRAMM, CORAS*)

имеют недостатки в соответствии с разделами «Мониторинг» и «Управление», а также со многими подразделами «Процессы». Немногие (*ГРИФ, RiskWatch, MSAT*) дают подробные рекомендации по поводу составления расписания проведения повторных оценок рисков.

В тех случаях, когда требуется выполнить только разовую оценку уровня рисков в компании среднего размера, целесообразно рекомендовать использование методики *CORAS*. Для управления рисками на базе периодических оценок на техническом уровне лучше всего подходит *CRAMM*. Методики *Microsoft Security Assessment Tool* и *RiskWatch* предпочтительны для использования в крупных компаниях, где предполагается внедрение управления рисками ИБ на базе регулярных оценок, на уровне не ниже организационного и требуется разработка обоснованного плана мероприятий по их снижению.

Литература

1. *Баранова Е.К., Бабаш А.В.* Информационная безопасность и защита информации. – М.: ИНФРА-М_РИОР, 2014.

2. *Баранова Е.К.* Методики и программное обеспечение для оценки рисков в сфере информационной безопасности // Управление риском. 2009. № 1(49). С. 15–26.

3. *Петренко С.А.* Управление информационными рисками. Экономически оправданная безопасность / Петренко С.А., Симонов С.В. М.: Компания АйТи; ДМК Пресс, 2004.

4. Международный стандарт ISO/IEC 27005:2008. Информационная технология – Методы защиты – Менеджмент рисков информационной безопасности BS ISO/IEC 27005:2008.

5. *Левченко В.Н.* Этапы анализа рисков. URL: http://www.cfin.ru/finanalysis/risk/ stages.shtml

6. Средство оценки безопасности Microsoft Security Assessment Tool (MSAT). http://technet.microsoft.com/ru-ru/security/cc185712.aspx

Methods of analysis and risk assessment Information security

***Elena Konstantinovna Baranova**, Associate professor of the Information Security Department Higer school of economics National reserch university.*

In General, risk understand the possibility of the occurrence of certain adverse events, which leads to a different kind of loss. In accordance with GOST R 51897-2002 «Management of risk. Terms and definitions» and the international standard ISO 27001 management System information security – risk management process is a coordinated action to manage and control an organization's information security risk (IB). Risk management includes risk assessment, treatment of risk, assumption of risk and the message about the risk.

Keywords: information security; information security audit; the risks of information security; information security; risk management.