УДК 004.056
DOI 10.21685/2587-7704-2018-3-2-8

Open Access RESEARCH ARTICLE

Способ риск-ориентированной оценки информационной безопасности организации

А. В. Слепов
Пензенский государственный университет, Россия, 440026 г. Пенза, ул. Красная, 40

С. Л. Зефиров
Пензенский государственный университет, Россия, 440026 г. Пенза, ул. Красная, 40

Аннотация. Анализируются способы оценки информационной безопасности организации и модель риск-ориентированной оценки информационной безопасности.

Ключевые слова: риск-ориентированная оценка, информационная безопасность, менеджмент, процесс, организация.

Method for risk-based assessment of organizational information security

A. V. Slepov
Penza State University, 40 Krasnaya Street, 440026, Penza, Russia

S. L. Zefirov
Penza State University, 40 Krasnaya Street, 440026, Penza, Russia

Abstract. This article analyses methods to assess organizational information security, and the risk-based assessment model of information security.

Keywords: risk-based assessment, information security, management, process, organization.

Процесс проведения оценки информационной безопасности (ИБ) включает следующие элементы проведения оценки:

– контекст оценки, который определяет входные данные: цели и назначение оценки ИБ, вид оценки (независимая оценка, самооценка), объект и области оценки ИБ, ограничения оценки, а также роли и ресурсы;

– критерии оценки;

– модель оценки;

– мероприятия процесса оценки: сбор свидетельств оценки и проверка их достоверности, измерение и оценивание атрибутов объекта оценки;

– выходные данные оценки.

Основные элементы процесса оценки ИБ представлены на рис. 1 в виде процессной модели.

В зависимости от выбранного для оценки ИБ критерия можно разделить способы оценки ИБ организации на оценку по эталону, риск-ориентированную оценку и оценку по экономическим показателям.

Способ оценки ИБ по эталону сводится к сравнению деятельности и мер по обеспечению ИБ организации с требованиями, закрепленными в эталоне. По сути дела, проводится оценка соответствия ИБ организации установленному эталону. Под оценкой соответствия ИБ организации установленным критериям понимается деятельность, связанная с прямым или косвенным определением выполнения или невыполнения соответствующих требований ИБ в организации. С помощью оценки

соответствия ИБ измеряется правильность реализации процессов системы обеспечения ИБ организации и идентифицируются недостатки такой реализации.

Рис. 1. Процесс оценки информационной безопасности объекта

В результате проведения оценки ИБ должна быть сформирована оценка степени соответствия ИБ эталону, в качестве которого могут быть приняты (в совокупности и отдельно):

– требования законодательства Российской Федерации в области ИБ;

– отраслевые требования по обеспечению ИБ;

– требования нормативных, методических и организационно-распорядительных документов по обеспечению ИБ;

– требования национальных и международных стандартов в области ИБ.

Целью риск-ориентированной оценки ИБ является определение, что:

– процессы менеджмента риска ИБ должным образом созданы и внедрены;

– процессы менеджмента риска ИБ действуют надлежащим образом;

– в отношении рисков, подлежащих обработке, действия руководства организации направлены на снижение этих рисков до приемлемого уровня.

Алгоритм проведения риск-ориентированной оценки показан на рис. 2.

При проведении риск-ориентированной оценки ИБ следует:

– оценить инфраструктуру менеджмента риска, например ресурсов, документации, методов;

– оценить риски области оценки;

– оценить возможности процессов менеджмента риска;

– если уровень возможности процессов менеджмента риска недостаточен для снижения рисков до приемлемого уровня, то должны быть сформулированы рекомендации по корректировке процессов менеджмента риска и их реализации для оценки риска области оценки;

– конечный результат оценки должен заключаться в обеспечении уверенности в том, что менеджмент риска осуществляется надлежащим образом и направлен на снижение рисков до приемлемого уровня.

Таким образом, модель риск-ориентированной оценки ИБ объекта представляет собой совокупность двух моделей: модель оценки рисков ИБ объекта (области) оценки и модель оценки возможностей процессов менеджмента риска.

Модель оценки рисков ИБ объекта (области) оценки [1] представлена на рис. 3.

В модели показано, что риск реализуется через рисковые события. В свою очередь, рисковые события являются следствием сочетания факторов риска, т.е. любому рисковому событию соответствует некоторый набор факторов риска.

В представленной модели фактор риска используется в качестве измеряемого атрибута. Результаты измерения – это основные меры, производные меры дают оценку рисковых событий. Если областью оценки является процесс, то рисковое событие отражает риски процесса. Дальнейшие преобразования дают возможность получить итоговую оценку ИБ, которая может отражать оценку объекта, например, процессов реализации и функционирования системы менеджмента ИБ.

Модель оценки возможностей процессов менеджмента риска представлена на рис. 4.

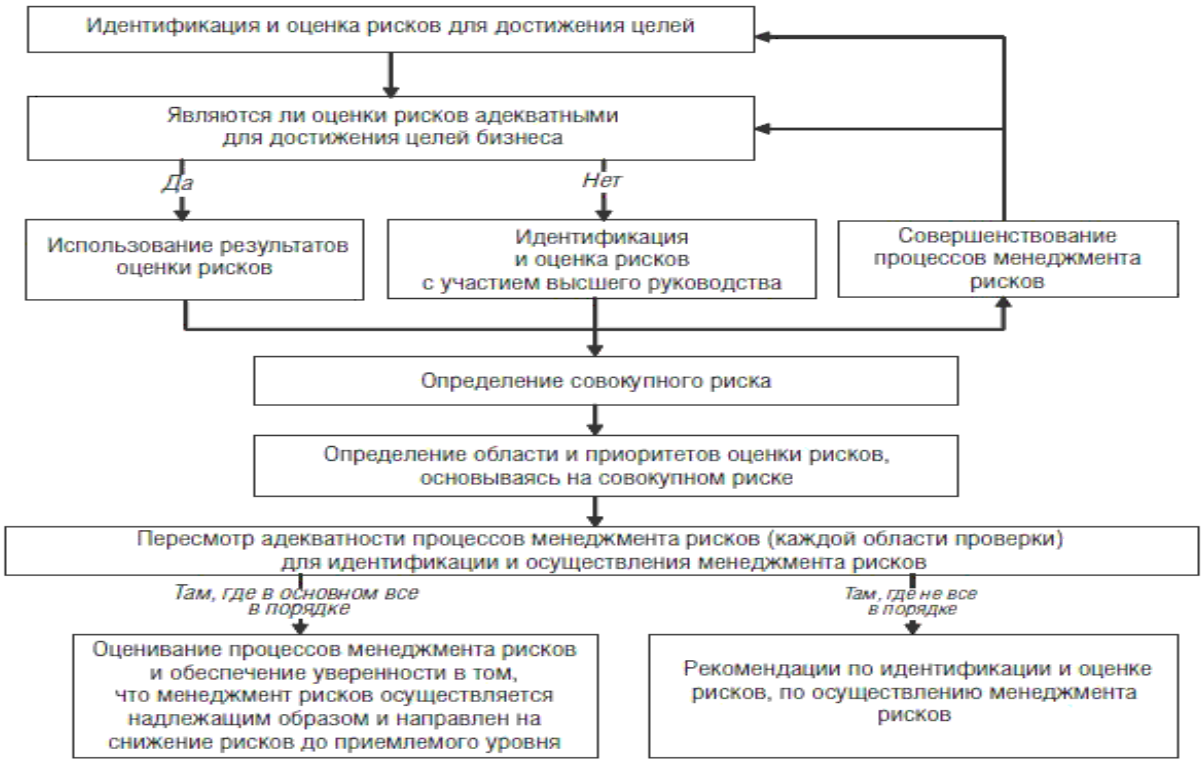

Рис. 2. Алгоритм проведения риск-ориентированной оценки ИБ

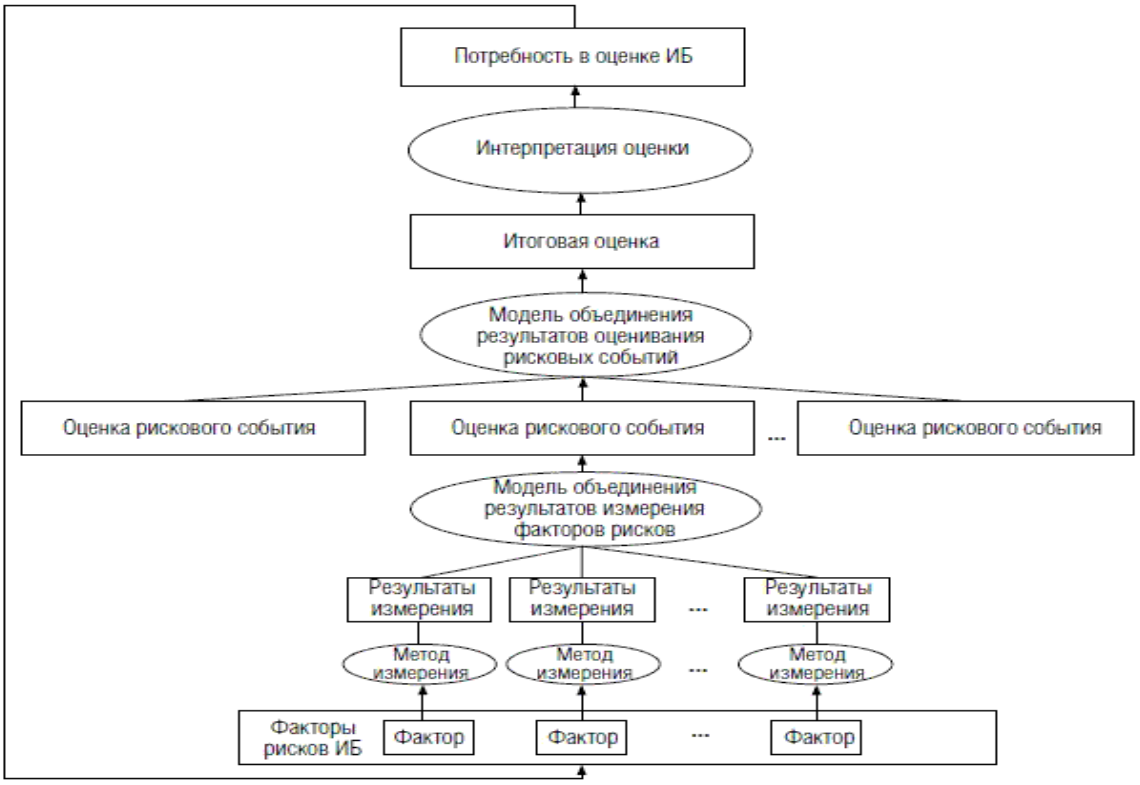

Рис. 3. Модель оценки ИБ объекта

В модели для определения уровней возможностей процессов выделяются девять измеряемых атрибутов [2]:

– функционирование процесса – процесс выполняется и формирует определенные результаты;

– менеджмент функционирования – процесс управляем в контексте его назначения и целей;

– менеджмент результата процесса – осуществляется управление результатами процесса в части их содержания и использования;

– формализация процесса – имеется полная формальная модель процесса и его реализация осуществляется в соответствии с моделью;

– развертывание процесса – реализацией процесса охвачены все вовлеченные стороны;

– количественная оценка процесса – определены и используются количественные оценки процесса;

– контроль процесса – процесс контролируется во всех операциях;

– инновация процесса – разрабатываются и внедряются лучшие практики и передовые технологии для операций процесса;

– оптимизация процесса – осуществляются меры по улучшению процесса, результаты которых оцениваемы в количественном или качественном выражении.

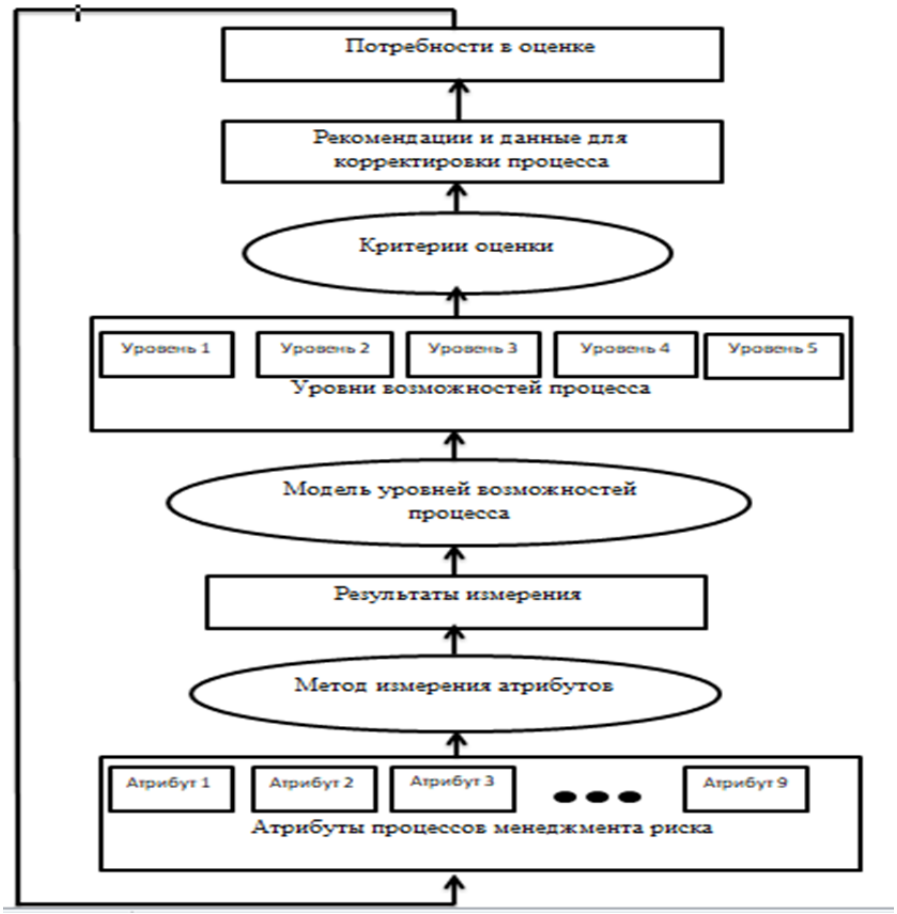

Рис. 4. Модель оценки возможностей процессов менеджмента риска

Модель уровней возможностей процесса [2] сформирована на основе степени достижения определенных значений оцениваемых атрибутов процесса.

Формирование оценки ИБ на основе риск-ориентированного подхода с использованием представленных моделей позволит получить не только оценку ИБ в момент проведения оценки, но и прогноз ИБ в будущем.

Библиографический список

1. Андрианов, В. В. Обеспечение информационной безопасности бизнеса / В. В. Андрианов. – URL: https://econ.wikireading.ru/25722 (дата обращения: 01.10. 2018).
2. ГОСТ Р. ИСО/МЭК 15504-3-2009 Информационная технология (ИТ). Оценка процесса. Часть 3. Руководство по проведению оценки

Слепов, А. В.
Способ риск-ориентированной оценки информационной безопасности организации / А. В. Слепов, С. Л. Зефиров// Инжиниринг и технологии. – 2018. – Vol. 3(2). – DOI 10.21685/2587-7704-2018-3-2-8.