УДК 004.056

П.В. Плетнев, В.М. Белов

Методика оценки рисков информационной безопасности на предприятиях малого и среднего бизнеса

Приводится описание процесса оценки рисков информационной безопасности, а также рассматривается способ численной оценки рисков информационной безопасности с применением методов оценки рисков экономической безопасности.

Ключевые слова: оценка рисков, информационная безопасность, численная оценка рисков.

Назначение методики

Настоящая методика предназначена для проведения оценки рисков информационной безопасности (ИБ) в рамках построения или совершенствования системы информационной безопасности на предприятиях малого и среднего бизнеса.

Настоящая методика рекомендована для применения путем прямого использования устанавливаемых в ней положений при проведении оценки рисков ИБ и использовании результатов оценки рисков ИБ.

Постановка задачи

Основная задача данной методики заключается в том, чтобы определить численный показатель риска ИБ с целью принятия эффективных мер по защите информации. Предлагаемая методика оценки рисков позволяет выполнить полноценный анализ и оценку рисков без привлечения высококвалифицированных специалистов.

Обобщенный алгоритм проведения оценки рисков ИБ на предприятиях малого и среднего бизнеса (далее МСБ) приведен на рис. 1.

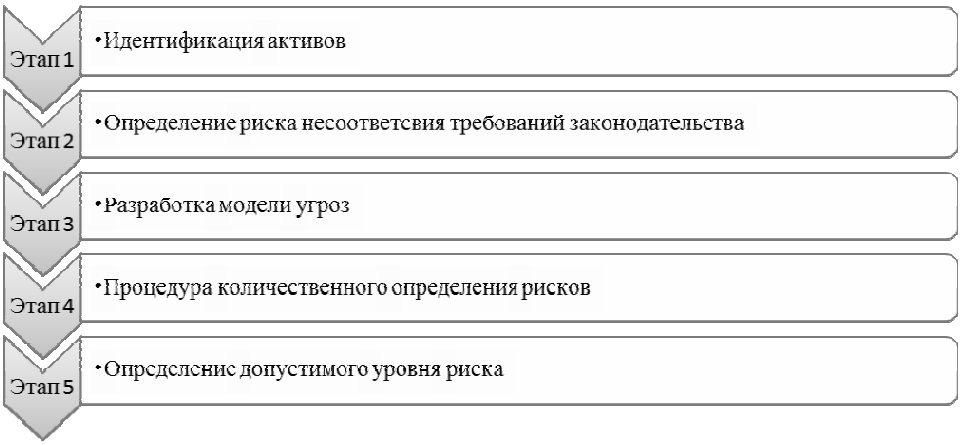


Рис. 1. Алгоритм оценки рисков ИБ

Процедуры оценки рисков ИБ как комплексного подхода выполняются сотрудниками предприятия совместно с руководящим звеном, а также с сотрудниками отделов предприятия.

Этап 1. Идентификация активов. На данном этапе эксперты проводят интервью с персоналом каждого подразделения или отдела с целью выявления используемых активов. Активы системы информационных технологий являются компонентом или частью общей системы, в которую предприятие напрямую вкладывает средства и которые, соответственно, требует защиты со стороны предприятия. При идентификации активов следует иметь в виду, что всякая система информационных технологий включает в себя не только аппаратные средства, но и программное обеспечение. Описание информационных активов проводится путём построения бинарных высказываний (описывалась в более ранних статьях) Могут существовать следующие типы активов:

1. Информация/данные (например, файлы, содержащие информацию о платежах или продукте).
2. Аппаратные средства (например, компьютеры, принтеры).

3. Программное обеспечение, включая прикладные программы (например, программы обработки текстов, программы целевого назначения).

4. Оборудование для обеспечения связи (например, телефоны, медные и оптоволоконные кабели).

5. Программно-аппаратные средства (например, электронные носители информации).

6. Документы (например, контракты).

7. Продукция предприятия.

8. Услуги (например, информационные, вычислительные услуги).

9. Конфиденциальность и доверие при оказании услуг (например, услуг по совершению платежей).

10. Оборудование, обеспечивающее необходимые условия работы.

11. Персонал организации.

12. Престиж (имидж) организации.

Этап 2. Определение риска несоответствия требований законодательства в области ИБ. Любая организация, имеющая информационные системы или работа которой связана с использованием информационных технологий для ведения бизнеса, должна соблюдать федеральные законы в этой отрасли. Невыполнение данных требований может повлечь за собой гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность. Риск невыполнения требований законодательства влияет на общий риск ИБ МСБ. Алгоритм определения риска несоответствия требований законодательства в области ИБ включает в себя проведение всестороннего анализа состояния системы защиты с целью выявления выполнения требований в соответствии с требованиями законодательства. В ходе проведения анализа всем требованиям, которые выполняются, присваивается значение «1», в противном случае – «0». Все значения, которым присвоено значение «1», суммируются, остальные значения не учитываются. В заключение анализа необходимо определить уровень риска несоответствия требований по ИБ, который определяется по табл. 1.

Таблица 1

Сумма выполненных требований	Риск несоответствия требованиям законодательства (R_n)
1	**2**
40–51	0,01
27–39	0,25
Менее 26	0,5
Не выполняются	0,9

Этап 3. Разработка модели угроз.

В методике с целью максимально точного определения риска ИБ необходимо разработать частную модель угроз ИБ предприятию. В модели угроз предлагается использовать уже разработанный и описанный в более ранних статьях метод оценки угроз с использованием алгоритма логического вывода Сорит. Определение вероятности наступления неблагоприятных событий определяется экспертом или группой экспертов, занимающихся разработкой модели угроз. Экспертным методом определяется и актуальность угроз ИБ.

После завершения оценки угроз составляют перечень актуальных идентифицированных угроз на каждый идентифицированный актив или групп активов, подверженных этим угрозам, а также определяют вероятность реализации угроз. Весь процесс составления перечня актуальных угроз проводится с использованием теории графов, с помощью которой описывается методика актуализации угроз.

Этап 4. Процедура количественной оценки рисков ИБ. Основным этапом в процессе оценки рисков является процедура количественного определения рисков ИБ. Пошаговый алгоритм количественного определения риска ИБ представлен на рис. 2.

Процедура количественной оценки рисков ИБ включает в себя следующие шаги:

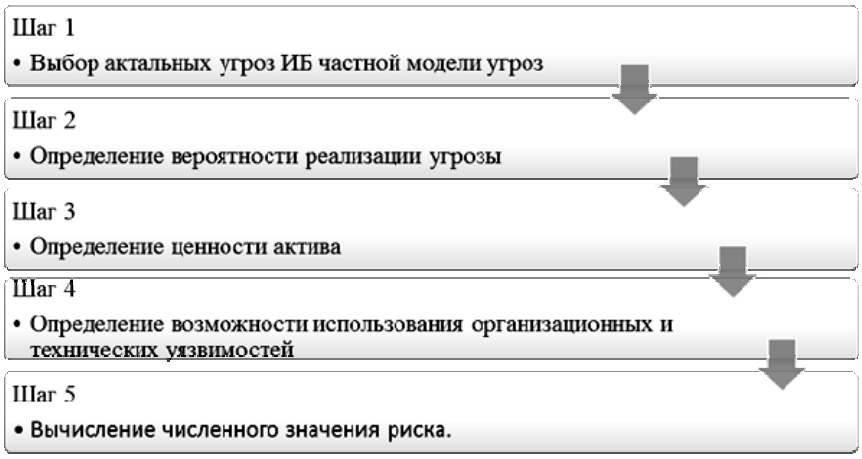
Шаг 1. Выбор актуальных угроз частной модели угроз. На данном шаге, используя частную модель угроз, формируется перечень актуальных угроз ИБ активов предприятия. На данном шаге количественного оценивания рисков сопоставляются идентифицированные активы с направленными на них угрозами. Для этого используется перечень активов предприятия и каждому из них сопоставляются актуальные угрозы из модели угроз.

Шаг 2. Определение вероятности наступления угрозы. В связи с тем, что на один актив могут воздействовать одновременно несколько угроз, необходимо определить вероятность того, что хотя бы одна угроза реализуется по отношению к выбранному активу.

Определение вероятности наступления неблагоприятных событий в связи с реализацией хотя бы одной угрозы из перечня актуальных угроз на рассматриваемый актив. Вероятность реализации хотя бы одной угрозы из совокупности вероятностей угроз y_1, y_2, ..., y_n, где n – количество угроз,

равна разности между единицей и произведением вероятностей противоположных событий. Вероятность противоположных событий определяется как разность между единицей и вероятностью угроз.

Шаг 3. Определение ценности актива. Ценность актива определяется стоимостью информационного актива. В связи с тем, что зачастую невозможно определить точные стоимости активов и предприятия в целом, рекомендуется ценность актива задавать в диапазоне от 0 до 1, которая будет показывать отношение цены актива к стоимости всего бизнеса.



Так как универсальной методики оценки активов нет, то в данной методике оценка актива определяется владельцем предприятия совместно с экспертом по оценке рисков.

Рис. 2. Алгоритм количественного оценивания риска ИБ

Шаг 4. Определение возможности использования организационных и технических уязвимостей.

Возможность использования организационных уязвимостей проводится экспертным методом, анализируя применяемые организационные меры защиты информации. В ходе проведения анализа, всем организационным мерам, которые выполняются, присваивается значение «1», в противном случае – «0». Все значения, которым присвоено значение «1», суммируются, остальные значения не учитываются. В табл. 2 представлены соответствие выполняемых организационных мер защиты информации и коэффициент уязвимости организационных мер защиты информации.

Таблица 2

Сумма выполняемых мер защиты	Коэффициент уязвимости (K_o)
14–17	0,01
8–13	0,25
Менее 8	0,5
Не выполняются	0,9

Возможность использования технических уязвимостей проводится экспертным методом, анализируя применяемые технические меры защиты информации. В ходе проведения анализа всем техническим мерам, которые выполняются, присваивается значение «1», в противном случае – «0». Все значения, которым присвоено значение «1», суммируются, остальные значения не учитываются. В табл. 3 представлено соответствие выполняемых технических мер защиты информации и коэффициент уязвимости технических мер защиты информации.

Таблица 3

Сумма выполняемых мер защиты	Коэффициент уязвимости (K_t)
15–19	0,01
9–14	0,25
Менее 9	0,5
Не выполняются	0,9

Шаг 5. Вычисление численного значения риска. В разрабатываемой методике процедура оценки рисков реализации хотя бы одной угрозы основывается на взаимности нескольких факторов – вероятности происшествия, а именно вероятности реализации хотя бы одной актуальной угрозы, коэффициента ценности актива, среднеарифметического значения коэффициентов возможности использования организационных уязвимостей и возможности использования технических уязвимостей и риска несоответствия требованиям законодательства. Под коэффициентом ценности актива понимают ценность или критичность актива по отношению ко всему бизнесу.

В настоящей методике процедура количественной оценки рисков реализации хотя бы одной угрозы из всего перечня актуальных угроз по отношению к конкурентному активу определяется относительно каждого типа актива, на который воздействует совокупность угроз ИБ, что позволяет дискретно определить риск наступления неблагоприятных событий на каждый тип актива.

Общая формула (1) определения риска реализации хотя бы одной угрозы из всего перечня актуальных угроз с учетом наличия уязвимостей по отношению к конкурентному активу:

$$R = P_{\text{угр}} R_n C \frac{K_o + K_t}{2} 100\%, \quad (1)$$

где R – численная величина риска реализации угроз ИБ; $P_{\text{угр}}$ – вероятность реализации хотя бы одной угрозы из всего перечня актуальных угроз; R_n – риск несоответствия требованиям законодательства; C – ценность актива; K_o – вероятность использования организационных уязвимостей; K_t – вероятность использования технических уязвимостей.

Этап 5. Определение допустимого уровня риска.

Допустимый риск принято считать риск, который в данной ситуации считают приемлемым при существующих общественных ценностях. Для предприятия МСБ рекомендованное значение риска не должно превышать 5%. Это обусловливается в первую очередь тем, что максимальная выручка предприятий МСБ за отчетный период, например 1 год, может составлять до 400 млн рублей, это из расчета того, что в случае реализации одной из актуальных угроз, может повлечь убыток в размере более 5% выручки, является недопустимым и требующим принятия эффективных мер.

Заключение

Выполнение всех этапов проведения оценки рисков ИБ на предприятиях МСБ повторяется для каждого типа актива.

Полученное значение рисков ИБ необходимо для выработки рекомендаций по снижению уровня риска, а также принятия эффективных мер по обеспечению ИБ предприятия. В случае если итоговое значение риска менее 5%, то делается вывод о том, что на предприятии выполнены требования по ИБ в полной необходимости, а также что риск ИБ оцениваемого типа актива допустимый. Но необходимо периодически проводить переоценку рисков ИБ. В случае если итоговое значение риска более или равно 5%, то делается вывод о том, что на предприятии не выполняются требования по ИБ, а также что риск ИБ оцениваемого типа актива повышенный и требует немедленного принятия решений.

Литература

1. Кудрявцева Р.Т. Управление информационными рисками с использованием технологий когнитивного моделирования : автореф. дис. … канд. техн. наук. – Уфа, 2008. – 17 с.

2. Кустов Г.А. Управление информационными рисками организации на основе логико-вероятностного метода: автореф. дис. ... канд. тех. наук. – Уфа, 2008. – 18 с.

3. Симонов С. Технологии и инструментарий для управления рисками // Jet Info. – 2003. – № 2 (117). – С. 3–32.

4. Digital Security [Электронный ресурс]. – Режим доступа: http://www.dsec.ru/about/articles/ar_compare/, свободный (дата обращения: 29.04.2012).

Плетнев Павел Валерьевич
Аспирант каф. «Безопасность и управление в телекоммуникациях» Сибирского государственного университета телекоммуникаций и информатики (СибГУТИ), г. Новосибирск
Тел.: 8-923-655-03-00
Эл. почта: pavel-pletnev@rambler.ru

Белов Виктор Матвеевич
Д-р техн. наук, профессор кафедры «Безопасность и управление в телекоммуникациях» СибГУТИ
Тел.: (383) 269-82-45
Эл. почта: vmbelov@mail.ru

Pletnev P.V., Belov V.M.

Methods of assessing information security risks in small and medium businesses

This article describes the process of risk assessment of information security, and examines how the numerical evaluation of information security risks with the use of risk assessment methods of economic security.

Keywords: risk assessment, information security, a numerical estimate of risk.