

УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМ РИСКОМ БУХГАЛТЕРСКИХ ИНФОРМАЦИОННЫХ СИСТЕМ ПРЕДПРИЯТИЯ

Корнейчук Валерий Иванович,

*канд. физ.-мат. наук, доцент кафедры бухгалтерского учета, налогообложения и таможенного дела,
Московский университет имени С.Ю. Витте,
e-mail: korneichukvi@yandex.ru*

В статье предложена методика расчета информационного риска бухгалтерских информационных систем предприятия на основе индикативного подхода оценки информационных рисков. Определен перечень индикаторов информационного риска бухгалтерских информационных систем предприятия, их характеристики и лица, ответственные за их предоставление. Установлены коэффициенты значимости и уровни оценки индикаторов риска. Описаны способы минимизации информационного риска бухгалтерских информационных систем предприятия на основе предложенной методики.

Ключевые слова: бухгалтерская информационная система, информационный риск, управление информационным риском бухгалтерских информационных систем

DOI 10.21777/2587-9472-2017-4-55-59

Введение

Учет информационного риска [1] и разработка мероприятий по его снижению является актуальной задачей в работе корпоративных информационных систем предприятия [2]. Современные методики расчета информационного риска корпоративных информационных систем предприятия [3–6] громоздки, трудны в реализации и не определяют ответственных за подготовку необходимой информации для последующего расчета риска.

В работе К.Е. Шинакова и О.М. Галембиовской [3] спроецирована зарубежная методика *OCTAVE* на процесс оценки информационных рисков российских предприятий различного уровня и мероприятий по их минимизации. В работе П.В. Плетнева и В.М. Белова [4] приведено описание алгоритма оценки рисков информационной безопасности и способа его численной оценки. В работах И.С. Швалева, Г.Н. Чусавитиной и Л.З. Давлеткиреевой [5, 6] представлена сравнительная оценка автоматизированных инструментальных средств управления информационными рисками зарубежного происхождения, которые требуют значительных затрат на их реализацию.

В настоящей работе предложена компактная методика расчета информационного риска бухгалтерских информационных систем предприятия [7] (далее – БИС) на базе трех групп индикаторов информационного риска, легко реализуемая в работе, свободная от отмеченных выше недостатков.

Выявление и оценка информационных рисков БИС

Для выявления информационного риска БИС предлагается ввести контрольные индикаторы, определяющие текущее состояние информационного риска БИС по следующим основным группам риска:

1 Индикаторы риска по защите БИС от несанкционированного доступа и некомпетентных действий работников предприятия.

2 Индикаторы риска по защите программного обеспечения БИС.

3 Индикаторы риска по повышению эффективности работы и надежности аппаратных средств БИС. Характеристики индикаторов для каждой группы риска представлены в таблицах 1–3.

Ответственными за предоставление значений индикатора 1 данной группы риска являются руководители подразделений предприятия, индикаторов 2, 3 и 4 – руководитель ИТ-отдела.

Ответственными за предоставление значений индикаторов 1–6 данной группы риска является руководитель ИТ-отдела.

Ответственными за предоставление значений индикаторов 1, 3–7 данной группы риска являются руководитель ИТ-отдела, индикатора 2 – руководители подразделений предприятия.

Таблица 1 – Индикаторы группы риска по защите БИС от несанкционированного доступа и некомпетентных действий работников предприятия

№ п/п	Индикатор и его характеристика	Значение индикатора по степеням риска			
		(2)	(1)	(0)	Коэф. знач.
1	Уровень доступа в БИС – устраняет несанкционированный доступ работника в БИС	Доступ пересматривается руководством	Доступ не пересматривается	При установке доступа не учитываются должностные обязанности	3
2	Имя работника для идентификации в локальной сети предприятия и уникальный пароль – устраняет несанкционированный доступ работников в БИС	Да, пароль меняется в соответствии с положением	Да, пароль не меняется	Не все сотрудники	3
3	На предприятии разработано положение по информационной безопасности и назначен администратор по информационной безопасности – позволяет устранить возможность потери информации и т.д.	Да	В стадии разработки или требует доработки	Нет	3
4	На предприятии разработана инструкция и план действий по обеспечению политики информационной безопасности – минимизация информационных рисков	Да	Частично	Нет	3

Таблица 2 – Индикаторы группы риска по защите программного обеспечения БИС

№ п/п	Индикатор и его характеристика	Значение индикатора по степеням риска			
		(2)	(1)	(0)	Коэф. знач.
1	Программное обеспечение для деятельности предприятия поддерживается производителем и своевременно обновляется – минимизирует риск несоответствия используемого программного обеспечения требованиям финансово-хозяйственной деятельности	Да	Не полностью	Нет	3
2	Некорректная работа либо умышленные действия пользователей не могут привести к искажению или утрате данных и/или программных модулей в БИС – минимизирует риск отказов, сбоев и некорректной работы программного обеспечения БИС	Да	Существует опасность повреждения некоторых модулей	Существует опасность повреждения критически важного программного обеспечения	3
3	Сбои в работе оборудования (выключение электропитания, критические сбои операционных систем и т.п.) не могут явиться причиной искажения программных модулей и содержания БИС – минимизирует риск отказов программного обеспечения, риск потери или искажения информации в хранилищах данных	Да	Работа отдельных модулей может быть нарушена	Может быть нарушена работа важного программного обеспечения	3
4	Ежедневно создается резервная копия БИС – минимизирует риск потери актуальной информации в хранилищах данных	Да, ведется журнал учета сделанных копий	Да, журнал учета не ведется	Нет	3
5	Существует несгораемый сейф для хранения резервных копий – минимизирует риск потери актуальной информации в хранилищах данных	Да, хранятся все копии	Да хранятся не все копии	Нет	3
6	Проверка БИС на наличие компьютерных вирусов – минимизирует риск повреждения, потери или кражи конфиденциальной информации	Да	Да, не каждый компьютер или несвоевременно обновляется	Нет	3

Оценка возможности возникновения информационного риска БИС осуществляется по балльно-весовому методу, предложенному в работе В.И. Корнейчука [8], который основан на относительной значимости индикаторов в общей оценке риска с точки зрения потенциальных потерь (негативных последствий) от их невыполнения. Применение балльно-весового метода позволяет выявить слабые и сильные стороны в управлении информационным риском БИС.

Таблица 3 – Индикаторы группы риска по повышению эффективности работы и надежности аппаратных средств БИС

№ п/п	Индикатор и его характеристика	Значение индикатора по степеням риска			
		(2)	(1)	(0)	Коэф. знач.
1	Количество произошедших продолжительных сбоев оборудования и систем в БИС – показывает текущее состояние отказоустойчивости БИС	до 1	1–3	свыше 3	3
2	Конфигурация технических средств соответствует требованиям бизнес- процессов предприятия – минимизирует риск сбоев аппаратного обеспечения, риск возникновения задержек в работе работников предприятия, вызванных неэффективным функционированием оборудования и каналов связи	Да	Отдельные блоки требуют замены	Большая часть оборудования не соответствует	3
3	Аппаратные средства обновляются своевременно, согласно срокам службы на различные виды техники аналогично 2 индикатору	Да, существуют утвержденные сроки	Да, по мере возникающей необходимости	Нет, значительная часть оборудования требует замены	3
4	На серверах и рабочих станциях, работоспособность которых является критически важной для функционирования предприятия, предусмотрена автономная система электропитания – минимизирует риск выхода из строя оборудования БИС и потери актуальной информации в хранилищах данных	Да	После выхода из строя	Нет	3
5	Помещения, в которых расположены серверы БИС, оборудована система климат-контроля – аналогично 4 индикатору	Да	Не всегда	Нет	2
6	ИТ-подразделением разработан план действий в случае отказа важных аппаратных средств и каналов связи и меры по восстановлению их работоспособности – план содержит алгоритм действий работников в критических случаях, позволяет быстро восстанавливать работоспособность оборудования	Да	Только на локальные сбои	Нет	3
7	На предприятии предусмотрены дополнительные каналы связи на случай потери работоспособности основных каналов – обеспечивает непрерывность производственного процесса в случае выхода из строя основных каналов связи	Да	Да, не все	Нет	2

Оценка состояния индикаторов проводится ежеквартально на основании сведений, предоставляемых ответственными за текущее состояние каждого индикатора должностными лицами. Для оценки состояния индикатора вводятся три значения:

0 – плохо. Требования данного индикатора не выполнены.

1 – удовлетворительно. Требования данного индикатора выполняются частично. Варианты: не на должном уровне; требуют совершенствований либо находятся в стадии разработки; соответствуют не в полной мере.

2 – хорошо. Требования данного индикатора выполняются.

По экономическому содержанию значения индикатора могут быть оценены по степени удовлетворения индикатора требуемым нормам: 0 – низкая, 1 – средняя, 2 – высокая.

Для оценки значимости, то есть степени важности выполнения каждого индикатора с точки зрения потенциальных потерь (негативных последствий), вводится коэффициент значимости, который может принимать три значения:

1 – низкий. Требования выполнения данного индикатора желательны, но не являются критическими.

2 – средний. Невыполнение данного требования может повлечь определенные негативные последствия для работы предприятия в будущем.

3 – высокий. Невыполнение требований данного индикатора несет высокий риск возникновения возможных потерь.

Коэффициенты значимости каждого индикатора определяются руководителем ИТ-подразделения и, в случае необходимости, могут быть пересмотрены.

Индикаторы информационного риска БИС и коэффициенты значимости утверждаются руководителем ИТ-подразделения.

Для оценки риска по каждому индикатору определяется весовой коэффициент индикатора по формуле:

*Весовой коэффициент = Состояние индикатора * Коэффициент значимости индикатора*

В случае наименьшего риска по индикатору весовой коэффициент индикатора будет иметь максимально возможное значение. В случае минимального риска, сумма весовых коэффициентов по виду риска должна быть максимальна:

Весовой коэффициент риска по виду (объекту) $\max = \sum_{i=1}^n \text{Весовой коэффициент индикатора } \max(i)$,

где n – количество индикаторов.

После определения состояния каждого индикатора ответственными лицами, общий риск по объекту рассчитывается по следующей формуле:

$$\text{Риск по объекту (\%)} = \left(1 - \frac{\sum_{i=1}^n \text{Весовой коэффициент индикатора } (i)}{\text{Весовой коэффициент группы } (\max)} * 100 \right).$$

Предельные значения информационного риска БИС представлены в таблице 4.

Таблица 4 – Предельные значения информационного риска БИС

Уровень риска	Значения (%)
Низкий	От 0 до 25
Средний	От 26 до 50
Высокий	От 51 до 100

Минимизации информационного риска БИС

Минимизация информационного риска БИС заключается в анализе состояния индикаторов риска, выявления их наиболее худших значений и выработке рекомендаций по устранению имеющихся недостатков. На основе итоговых значений риска по группам индикаторов риска и общего значения информационного риска БИС определяется динамика изменения информационного риска БИС по отчетным периодам.

Подразделение предприятия, ответственное за эксплуатацию БИС, анализирует причины, повлиявшие на значение риска, в том числе в разрезе всех иных подразделений предприятия, и выносит мотивированное суждение об общем уровне информационного риска БИС, сложившегося на отчетную дату.

На основании мотивированного суждения принимаются меры по минимизации возникающих информационных рисков БИС.

Разработанная методика может быть использована для расчета информационного риска бухгалтерских информационных систем предприятия и иных корпоративных информационных систем.

Список литературы

1. Скородумов Б.И. Информационные риски: проблемы и тенденции // Вестник РНУ. – 2012. – № 4. – С. 101–105.
2. Градусов Д.А., Шутков А.В., Градусов А.Б. Корпоративные информационные системы: учебное пособие; в 2 ч. – Владимир: Изд-во ВГУ им. А.Г. и Н.Г. Столетовых, 2014.
3. Шинаков К.Е., Галембиевская О.М. Формализация процесса оценки рисков информационной безопасности на основе методики OCTAVE // Вестник БГТУ. – 2015. – № 3. – С. 175–179.
4. Плетнев П.В., Белов В.М. Методика оценки рисков информационной безопасности на предприятиях малого и среднего бизнеса // Доклады ТУСУРа. – 2012. – № 1. – С. 83–86.
5. Швалев И.С., Чусавитина Г.Н., Давлеткиреева Л.З. Сравнительная характеристика автоматизированных инструментальных средств управления информационными рисками // Современные научные исследования и инновации. – 2012. – №11. – С. 5–11.
6. Парфентьев А. Методики оценки рисков для информационных систем [Электронный ресурс]. URL: <https://www.anti-malware.ru/practice/methods/risk-assessment-methods-for-information-systems>

7. Адуева Т.В. Бухгалтерские информационные системы: учебное пособие. – Томск: Эль Контент, 2012.
8. Корнейчук В.И. Организация управления операционным риском в кредитной организации // Финансовая аналитика: проблемы и решения. – 2011. – № 8. – С. 19–33.

**MANAGEMENT OF INFORMATION RISK OF ACCOUNTING INFORMATION SYSTEMS OF
THE ENTITY**

Korneychuk V.I.,

*candidate of physical and mathematical sciences,
the associate professor “Accounting, the taxation and customs affairs”,
the Moscow university of S.Yu. Witte,
e-mail: korneichukvi@yandex.ru*

In work indicators of information risk of accounting information systems of the enterprise are offered. The methodology of management of information risk of accounting information systems on the basis of the offered indicators is described.

Keywords: accounting information system, information risk, management of information risk of accounting information systems