

ВОПРОСЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

КНИГА 2

Н. Г. Милославская,
М. Ю. Сенаторов, А. И. Толстой

УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Допущено Учебно-методическим объединением высших учебных заведений России по образованию в области информационной безопасности в качестве учебного пособия для студентов высших учебных заведений, обучающихся по направлению подготовки 090900 – «Информационная безопасность» (уровень – магистр)

Москва
Горячая линия - Телеком
2013

УДК 004.732.056(075.8)

ББК 32.973.2-018.2я73

М60

Рецензенты: кафедра защиты информации НИЯУ МИФИ (зав. кафедрой кандидат техн. наук, профессор *А. А. Малюк*); академик РАН *И. А. Соколов*; доктор техн. наук, профессор *П. Д. Зегжeda*; доктор техн. наук, профессор *А. Г. Остапенко*

Милославская Н. Г., Сенаторов М. Ю., Толстой А. И.

М60 Управление рисками информационной безопасности. Учебное пособие для вузов. – М.: Горячая линия–Телеком, 2013. – 130 с.: ил. – Серия «Вопросы управления информационной безопасностью. Выпуск 2»

ISBN 978-5-9912-0272-5.

В учебном пособии вводится понятие риска информационной безопасности (ИБ) и определяются процесс и система управления рисками ИБ. Детально рассмотрены составляющие процесса управления рисками ИБ, а именно: установление контекста управления рисками ИБ с определением базовых критериев принятия решений, области действия и границ управления рисками ИБ; оценка рисков ИБ, состоящая из двух этапов – анализ (с идентификацией активов, угроз ИБ, существующих элементов управления, уязвимостей и последствий) и оценивание (с определением последствий, вероятностей и количественной оценки рисков) рисков ИБ; обработка рисков ИБ, включающая снижение, сохранение, избежание и передачу; принятие риска ИБ; коммуникация рисков ИБ; мониторинг и пересмотр рисков ИБ. Также сравниваются различные подходы к анализу (базовый, неформальный, детальный, комбинированный) и оценке (высокоуровневая и детальная) рисков ИБ. В заключении кратко описываются документальное обеспечение и инструментальные средства управления рисками ИБ.

Для студентов высших учебных заведений, обучающихся по программам магистратуры направления 090900 – «Информационная безопасность», будет полезно слушателям курсов переподготовки и повышения квалификации и специалистам.

ББК 32.973.2-018.2я73

Учебное издание

**Милославская Наталья Георгиевна,
Сенаторов Михаил Юрьевич, Толстой Александр Иванович**

Управление рисками информационной безопасности

Учебное пособие для вузов

Обложка художника *О. Г. Карповой*
Компьютерная верстка *Н. В. Дмитриевой*

Подписано в печать 30.06.2012. Формат 60×90/16. Усл. печ. л. 8,25. Тираж 500 экз. Изд. № 12271

ISBN 978-5-9912-0272-5

© Н. Г. Милославская,
М. Ю. Сенаторов, А. И. Толстой, 2012
© Издательство «Горячая линия–Телеком», 2012

ПРЕДИСЛОВИЕ

Учебное пособие «Управление рисками информационной безопасности» является второй частью серии учебных пособий «Вопросы управления информационной безопасностью».

При подготовке данного учебного пособия были поставлены следующие задачи:

- 1) определить основные понятия, относящиеся к управлению рисками информационной безопасности (ИБ);
- 2) детально рассмотреть составляющие процесса управления рисками ИБ;
- 3) описать различные подходы к анализу и оценке рисков ИБ;
- 4) проанализировать систему управления рисками ИБ (СУРИБ);
- 5) рассмотреть необходимое документальное обеспечение и применяемые в настоящее время инструментальные средства управления рисками ИБ.

Исходя из поставленных задач, была определена структура учебного пособия «Управление рисками информационной безопасности», которое состоит из введения, 6 глав, трех приложений и списка литературы из 41 наименования.

Во введении обоснована актуальность темы учебного пособия.

Далее кратко анализируется нормативное обеспечение управления рисками ИБ, последовательно вводится понятие риска ИБ и определяются процесс и система управления рисками ИБ.

В основных главах учебного пособия детально рассматриваются составляющие процесса управления рисками ИБ, а именно:

- установление контекста управления рисками ИБ с определением базовых критериев принятия решений и определения области действия и границ управления рисками ИБ;
- оценка рисков ИБ, состоящая из двух этапов – анализ (с идентификацией активов, угроз ИБ, существующих элементов управления, уязвимостей и последствий) и оценивание (с определением последствий, вероятностей и количественной оценки рисков) рисков ИБ;
- обработка рисков ИБ, включающая снижение, сохранение, избежание и передачу;
- принятие, коммуникация, мониторинг и пересмотр рисков ИБ.

Также анализируются различные подходы к анализу (базовый, неформальный, детальный, комбинированный) и оценке (высокоуровневая и детальная) рисков ИБ. В завершении основной части учебного пособия кратко описываются документальное обеспечение и инструментальные средства управления рисками ИБ.

В заключении кратко выделяется взаимосвязь изученных понятий, относящихся к управлению рисками ИБ, а также устанавливается связь

между материалом учебного пособия и составляющими профессиональных компетенций.

В приложениях приводится информация справочного характера в виде описания угроз ИБ и уязвимостей, а также инструментальных средств управления рисками ИБ.

Освоение материалов данного учебного пособия формирует у обучающихся следующие профессиональные компетенции:

- способность участвовать в управлении ИБ объекта в части оценки рисков ИБ;
- способность участвовать в проектировании и разработке системы управления ИБ объекта в части применения методов оценки рисков ИБ, т. е. СУРИБ.

Эти профессиональные компетенции необходимы для решения задач, относящихся к таким видам профессиональной деятельности в сфере управления ИБ, как проектная и организационно-управленческая.

После изучения учебного пособия «Управление рисками информационной безопасности» обучающиеся будут

Знать:

- современные подходы к управлению рисками ИБ и направления их развития;
- особенности отдельных процессов управления рисками ИБ в рамках СУИБ;
- основные международные и российские стандарты, регламентирующие управление рисками ИБ.

Уметь:

- анализировать текущее состояние ИБ на предприятии с целью разработки требований к разрабатываемым процессам управления рисками ИБ;
- определять цели и задачи, решаемые разрабатываемыми процессами управления рисками ИБ;
- разрабатывать процессы управления рисками ИБ, учитывающие особенности функционирования предприятия и решаемых им задач;
- практически решать задачи формализации разрабатываемых процессов управления рисками ИБ;
- проектировать СУРИБ.

Владеть:

- терминологией в области управления рисками ИБ;
- навыками анализа активов организации, их угроз ИБ и уязвимостей в рамках управления рисками ИБ.

Материалы, вошедшие в учебное пособие «Управление рисками информационной безопасности» обеспечивают учебно-методической базой любую учебную дисциплину, относящуюся к управлению ИБ. Однако в полной мере данное учебное пособие может быть востребовано при

подготовки профессионалов в области управления ИБ. Поэтому оно может быть рекомендовано студентам высших учебных заведений, обучающимся по программам магистратуры направления 090900 – «Информационная безопасность».

Кроме этого учебное пособие из серии «Вопросы управления информационной безопасностью» может быть полезным при реализации программ дополнительного образования (курсы повышения квалификации или переподготовки кадров).

Важно подчеркнуть, что для приступающих к ознакомлению с данным учебным пособием есть определенные требования по предварительной подготовке. Например, следует знать основы теории ИБ и комплексный подход к обеспечению ИБ (ОИБ), уязвимости и угрозы ИБ в информационной среде. Следует рекомендовать предварительное ознакомление с материалом первой части серии учебных пособий «Основы управления информационной безопасностью».

Авторы признательны коллегам по факультету «Кибернетика и информационная безопасность» НИЯУ МИФИ, а также всем рецензентам.

Авторы, естественно, не претендуют на исчерпывающее изложение всех названных в работе аспектов проблемы управления ИБ организации, поэтому с благодарностью внимательно изучат и учтут критические замечания и предложения читателей при дальнейшей работе над учебным пособием.

Оглавление

Предисловие	3
Введение	6
1. Нормативное обеспечение управления рисками информационной безопасности	8
1.1. ISO/IEC 27005:2011 и ГОСТ Р ИСО/МЭК 27005–2010 – управление рисками ИБ	9
1.2. BS 7799–3:2006 – руководство по управлению рисками ИБ	11
Вопросы для самоконтроля	12
2. Основные определения	13
2.1. Риск ИБ	13
2.2. Управление рисками ИБ	17
2.3. Составляющие процесса управления рисками ИБ	20
2.4. Системный подход к управлению рисками ИБ	27
2.5. Установление контекста управления рисками ИБ	32
2.5.1. Базовые критерии принятия решений по управлению рисками ИБ	33
2.5.2. Область действия и границы управления рисками ИБ	34
2.5.3. Учет требований по ОИБ при управлении рисками ИБ	35
Вопросы для самоконтроля	37
3. Оценка рисков ИБ	38
3.1. Этап 1 – анализ рисков ИБ	41
3.1.1. Подэтап 1 анализа рисков ИБ – идентификация рисков ИБ	42
3.1.2. Шаг 1 подэтапа 1 – идентификация активов	43
3.1.3. Шаг 2 подэтапа 1 – идентификация угроз ИБ	47
3.1.4. Шаг 3 подэтапа 1 – идентификация существующих средств управления рисками ИБ	49
3.1.5. Шаг 4 подэтапа 1 – идентификация уязвимостей	50
3.1.6. Шаг 5 подэтапа 1 – идентификация последствий	52
3.1.7. Подэтап 2 анализа рисков ИБ – количественная оценка рисков ИБ	53
3.1.8. Шаг 1 подэтапа 2 – оценка последствий	55
3.1.9. Шаг 2 подэтапа 2 – оценка вероятностей	60
3.1.10. Шаг 3 подэтапа 2 – определение уровня (величины) рисков ИБ	63
3.2. Этап 2 – оценивание рисков ИБ	66
3.3. Подходы к оценке рисков ИБ	67

3.3.1. Базовый анализ рисков ИБ	70
3.3.2. Неформальный анализ рисков ИБ	72
3.3.3. Детальный анализ рисков ИБ	73
3.3.4. Комбинированный анализ рисков ИБ	75
3.3.5. Высокоуровневая оценка рисков ИБ	75
3.3.6. Детальная оценка рисков ИБ.....	77
3.3.7. Общий подход к оценке рисков ИБ РС БР ИББС-2.2–2009	84
Вопросы для самоконтроля	89
4. Обработка рисков ИБ	90
4.1. Снижение риска ИБ.....	93
4.2. Сохранение риска ИБ	95
4.3. Избежание риска ИБ.....	96
4.4. Передача риска ИБ	96
Вопросы для самоконтроля	98
5. Принятие, коммуникация, мониторинг и пересмотр рисков ИБ	99
5.1. Принятие рисков ИБ.....	99
5.2. Коммуникация рисков ИБ.....	100
5.3. Мониторинг и пересмотр рисков ИБ	102
5.3.1. Мониторинг и пересмотр показателей риска ИБ	102
5.3.2. Мониторинг, пересмотр и усовершенствование процесса управления рисками ИБ	103
Вопросы для самоконтроля	104
6. Обеспечение управления рисками ИБ	105
6.1. Документальное обеспечение управления рисками ИБ.....	105
6.2. Инструментальные средства управления рисками ИБ.....	107
Вопросы для самоконтроля	109
Заключение	110
Приложения.....	112
П1. Примеры угроз ИБ.....	112
П1.1. Физическая безопасность и безопасность окружающей среды	112
П1.2. Управление коммуникациями и операциями	113
П1.3. Аспекты ИБ в управлении непрерывностью бизнеса ..	114
П1.4. Соответствие	114
П2. Примеры уязвимостей.....	120
П3. Инструментальные средства управления рисками ИБ.....	123
Принятые сокращения.....	125
Список литературы	126