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

Электронный архив библиотеки МГТУ им. Н.Э. Баумана

УДК 004.732.056(075.8)
ББК 32.973.2-018.2я73
М60

Р е ц е н з е н т ы : 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. Зегжда*; 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

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