ВОПРОСЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

КНИГА 5

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

ПРОВЕРКА И ОЦЕНКА ДЕЯТЕЛЬНОСТИ ПО УПРАВЛЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

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

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 Проверка и оценка деятельности по управлению информационной безопасностью. Учебное пособие для вузов. – М.: Горячая линия–Телеком, 2013. – 166 с.: ил. – Серия «Вопросы управления информационной безопасностью. Выпуск 5»

ISBN 978-5-9912-0275-6.

Рассмотрены основные процессы анализа системы управления информационной безопасностью (СУИБ): мониторинг информационной безопасности (ИБ), самооценка ИБ, внешний и внутренний аудиты ИБ и анализ СУИБ со стороны руководства организации. Для всех процессов выделены основные цели и задачи, принципы и этапы осуществления, виды проверок, формы отчетности. Анализируется деятельность подразделения внутреннего аудита, контролирующего вопросы ИБ. Исследуется процесс управления программой внешнего аудита ИБ. Затронуты вопросы компетентности аудиторов ИБ и взаимоотношения внешних аудиторов ИБ с проверяемой организацией. Перечислены инструментальные средства, используемые при проведении различных проверок в области ИБ. Также рассмотрены вопросы оценки деятельности по управлению ИБ и функционированию СУИБ организации. Описаны подходы к оценке эффективности и результативности управления ИБ в целом, а также к оценке зрелости процессов СУИБ. На основе международных стандартов анализируются процессы выработки метрик безопасности и показателей функционирования СУИБ.

Для студентов вузов, обучающихся по программе магистратуры направления 090900 – «Информационная безопасность», будет полезно слушателям курсов переподготовки и повышения квалификации, аспирантам, руководителям предприятий и организаций, специалистам в области ИБ.

ББК 32.973.2-018.2я73

ISBN 978-5-9912-0275-6

ПРЕДИСЛОВИЕ

Учебное пособие «Проверка и оценка деятельности по управлению информационной безопасностью» является пятой частью серии учебных пособий «Вопросы управления информационной безопасностью». При подготовке данного учебного пособия были поставлены следующие задачи:

1) подробно рассмотреть основные процессы анализа системы управления информационной безопасностью (СУИБ). К ним относится мониторинг информационной безопасности (ИБ), самооценка ИБ, внутренний и внешний аудит ИБ и анализ СУИБ со стороны руководства организации;

2) оценить возможности инструментальных средств, используемых при проведении различных проверок в области ИБ;

3) проанализировать выработки метрик безопасности и показателей функционирования СУИБ;

4) рассмотреть вопросы оценки деятельности по управлению ИБ и функционированию СУИБ организации и подходы к оценке эффективности и результативности управления ИБ в целом, а также к оценке зрелости процессов СУИБ.

Исходя из поставленных задач, была выбрана структура учебного пособия «Проверка и оценка деятельности по управлению информационной безопасностью», которое состоит из введения, трех глав, заключения, пяти приложений и списка литературы из 53 наименований.

Во введении обоснована актуальность темы данного учебного пособия.

В первой главе анализируется нормативное обеспечение проверки и оценки деятельности по управлению ИБ.

Во второй главе рассматриваются основные процессы анализа СУИБ: мониторинг ИБ, самооценка ИБ, внутренний и внешний аудит ИБ и анализ СУИБ со стороны руководства организации. Для всех процессов выделяются основные цели и задачи, принципы и этапы осуществления, виды проверок, формы отчетности. Анализируется деятельность в организации подразделения внутреннего аудита, контролирующего вопросы ИБ. Исследуется процесс управления программой внешнего аудита ИБ. Затрагиваются вопросы компетентности аудиторов ИБ и взаимоотношения внешних аудиторов ИБ с проверяемой организацией. Перечисляются инструментальные средства, используемые при проведении различных проверок в области ИБ.

В третьей главе рассматриваются вопросы оценки деятельности по управлению ИБ и функционированию СУИБ организации. Описываются подходы к оценке эффективности и результативности управления ИБ в целом, а также к оценке зрелости процессов СУИБ. Вводятся важные в этой области понятия – «измерение», «показатель» и «метрика». На ос-

нове международных стандартов анализируются процессы выработки метрик безопасности и показателей функционирования СУИБ.

В заключении кратко выделяется взаимосвязь изученных понятий, относящихся к проверке и оценке деятельности по управлению ИБ, а также устанавливается связь между материалом учебного пособия и составляющими профессиональных компетенций.

В приложениях приводится информация справочного характера в виде примера возможной программы аудита вопросов управления непрерывностью бизнеса, описаний измерений для оценки СУИБ и модели зрелости для подпроцесса минимизации рисков ИБ в рамках процесса управления рисками ИБ.

Освоение материалов данного учебного пособия лежит в основе формирования у обучающихся следующих профессиональных компетенций:

- способность участвовать в управлении ИБ объекта;
- способность участвовать в проведении контрольных мероприятий по определению эффективности и результативности СУИБ объекта.

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

После изучения учебного пособия «Проверка и оценка деятельности по управлению информационной безопасностью» обучающиеся будут:

Знать:

- современные подходы к проверке и оценке деятельности по управлению ИБ;
- особенности отдельных процессов проверки СУИБ;
- основные международные и российские стандарты, регламентирующие проверку и оценку деятельности по управлению ИБ;
- подходы к оценке деятельности по управлению ИБ;
- принципы создания основных документов, регламентирующих вопросы проверки и оценки деятельности по управлению ИБ.

Уметь:

- формулировать требования к процессам проверки СУИБ;
- формулировать требования к процессам оценки деятельности по управлению ИБ;
- выбирать и использовать инструментальные средства для проверки СУИБ;
- проводить оценку деятельности по управлению ИБ;
- разрабатывать документальное обеспечение для процессов проверки и оценки деятельности по управлению ИБ.

Владеть:

- терминологией, относящейся к проверке и оценке деятельности по управлению ИБ;

ŋqddуeҰ bɆ dəd̶Ɇbүзə d ɛɑɒcɑү Ɉqddүqүè

- навыками анализа эффективности и результативности деятельности по управлению ИБ.

Материалы, вошедшие в учебное пособие «Проверка и оценка деятельности по управлению информационной безопасностью», обеспечивают учебно-методической базой любую учебную дисциплину, относящуюся к управлению ИБ. Однако в полной мере данное учебное пособие может быть востребовано при подготовке 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 «Проверка и оценка деятельности по управлению информационной безопасностью» 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 следующих частей серии учебных пособий «Вопросы управления информационной безопасностью»: «Часть 1. Основы управления информационной безопасностью», «Часть 2. Управление рисками информационной безопасности», «Часть 3. Управление инцидентами информационной безопасности и обеспечение непрерывности бизнеса», «Часть 4. Технические, организационные и кадровые аспекты 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 проблем проверки и оценки деятельности по управлению ИБ, поэтому с благодарностью внимательно изучат и учтут критические замечания и предложения читателей при дальнейшей работе над учебным пособием.

Оглавление

ŋqqdɐǝʎ pƎ dǝqƎbʎɜǝ d ɛɑɑɓɔʎ Ɉqqdʎqɐè