

ВОПРОСЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

КНИГА 3

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

УПРАВЛЕНИЕ ИНЦИДЕНТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И НЕПРЕРЫВНОСТЬЮ БИЗНЕСА

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. Малиюк*); 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 инцидентами информационной безопасности и непрерывностью бизнеса. Учебное пособие для вузов. – М.: Горячая линия–Телеком, 2013. – 170 с.: ил. – Серия «Вопросы управления информационной безопасностью. Выпуск 3»
ISBN 978-5-9912-0273-2.

В учебном пособии изучается процесс управления инцидентами информационной безопасности (ИБ), для чего вводятся понятия события и инцидента ИБ и выделяются цели и задачи управления инцидентами ИБ. Описывается система управления инцидентами ИБ. Анализируются этапы процесса управления инцидентами ИБ. Исследуются подпроцессы обнаружения событий и инцидентов ИБ и оповещения о них; обработка событий и инцидентов ИБ, включая первую оценку и предварительное решение по событию ИБ и вторую оценку и подтверждение инцидента ИБ; реагирования на инциденты ИБ. Описывается документация системы управления инцидентами ИБ, включая политику и программу. Анализируется деятельность группы реагирования на инциденты ИБ. Значительное внимание уделяется сохранению доказательств инцидента ИБ. Далее вводятся определения непрерывности бизнеса, управления ею и системы управления непрерывностью бизнеса (УНБ). Рассматривается применение цикла PDCA к этой системе управления. Детально описывается жизненный цикл УНБ. Определяется состав документации в области непрерывности бизнеса, в частности, политика УНБ и планы управления инцидентом, обеспечения непрерывности и восстановления бизнеса. Анализируются готовность информационных и телекоммуникационных технологий (ИТТ) к обеспечению непрерывности бизнеса (ОНБ) и интеграция процессов готовности ИТТ и ОНБ в рамках цикла PDCA.

ББК 32.973.2-018.2я73

ISBN 978-5-9912-0273-2

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

ПРЕДИСЛОВИЕ

Учебное пособие «Управление инцидентами информационной безопасности и непрерывностью бизнеса» является третьей частью серии учебных пособий «Вопросы управления информационной безопасностью».

При подготовке данного учебного пособия были поставлены следующие задачи:

- 1) описать процесс управления инцидентами информационной безопасности (ИБ);
- 2) определить особенности системы управления инцидентами ИБ и рассмотреть ее основные характеристики;
- 3) дать основные определения, относящиеся к проблеме обеспечения непрерывности бизнеса (ОНБ);
- 4) рассмотреть основные аспекты управления непрерывностью бизнеса (УНБ).

Исходя из поставленных задач, была определена структура учебного пособия «Управление инцидентами информационной безопасности и непрерывностью бизнеса», которое состоит из введения, трех глав, заключения, приложения и списка литературы из 30 наименований.

Во введении обоснована актуальность темы учебного пособия.

В первой главе кратко анализируется нормативное обеспечение вопросов управления инцидентами ИБ и ОНБ.

Во второй главе изучается процесс управления инцидентами ИБ, для чего вводятся понятия события и инцидента ИБ и выделяются цели и задачи управления инцидентами ИБ. Описывается система управления инцидентами ИБ. Анализируются этапы процесса управления инцидентами ИБ, разбиваемого на планирование и подготовку, использование, анализ и улучшение. Отдельно исследуются подпроцессы обнаружения событий и инцидентов ИБ и оповещения о них, а также обработка событий и инцидентов ИБ, включая первую оценку и предварительное решение по событию ИБ и вторую оценку и подтверждение инцидента ИБ. Детально исследуется подпроцесс реагирования на инциденты ИБ и его составляющие: немедленное реагирование, контроль, последующее реагирование, антикризисные действия, правовая экспертиза, передача информации, расширение области принятия решений, регистрация деятельности и контроль за внесением изменений и техническая поддержка реагирования на инциденты ИБ. Описывается документация системы управления инцидентами ИБ, включая политику и программу. Анализируется деятельность группы реагирования на инциденты ИБ. Подчеркивается необходимость обеспечения осведомленности и обучения в области инцидентов ИБ. Значительное внимание уделяется сохранению

доказательств инцидента ИБ и кратко определяются функции инструментальных средств управления событиями ИБ.

В третьей главе вводятся определения, относящиеся к ОНБ, управления ею и системы УНБ. Рассматривается применение циклической модели улучшения процессов PDCA (от англ. *Plan-Do-Check-Act* – планируй–выполни–проверь–действуй) к этой системе управления (сама модель описана в первой части серии учебных пособий). Детально описывается жизненный цикл УНБ, включающий шесть элементов: управление программой УНБ, анализ непрерывности бизнеса (НБ) организации, определение стратегии УНБ, разработка и внедрение в УНБ ответных мер на инциденты, меры по применению, поддержке и анализу УНБ и внедрение УНБ в культуру организации. Определяется состав документации в области НБ, в частности, политика УНБ и планы управления инцидентом, обеспечения непрерывности и восстановления бизнеса. Анализируются готовность информационных и телекоммуникационных технологий (ИТТ) к ОНБ и интеграция процессов готовности ИТТ и ОНБ в рамках цикла PDCA.

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

В приложении приводится информация справочного характера в виде примеров инструментальных средств управления событиями ИБ.

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

- способность участвовать в управлении ИБ объекта (в части управления инцидентами ИБ и НБ);
- способность участвовать в проектировании и разработке системы управления ИБ (СУИБ) объекта (в отношении подсистем управления инцидентами ИБ и НБ);
- способность участвовать в проведении контрольных мероприятий по определению эффективности и результативности СУИБ объекта (в части эффективности и результативности управления инцидентами ИБ и НБ).

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 инцидентами информационной безопасности и непрерывностью бизнеса» обучающиеся будут:

Знать:

- принципы построения СУИБ объекта в части систем управления инцидентами ИБ и НБ;

- современные подходы к управлению инцидентами ИБ и НБ объекта и направления их развития;
- особенности отдельных процессов управления инцидентами ИБ в рамках СУИБ и УНБ;
- основные международные и российские стандарты, регламентирующие управление инцидентами ИБ и НБ;
- принципы разработки процессов управления инцидентами ИБ и НБ;
- принципы создания основных документов, регламентирующих вопросы управления инцидентами ИБ и НБ.

Уметь:

- анализировать текущее состояние ИБ на предприятии с целью разработки требований к разрабатываемым процессам управления инцидентами ИБ и НБ;
- определять цели и задачи, решаемые разрабатываемыми процессами управления инцидентами ИБ и НБ;
- применять процессный подход к управлению инцидентами ИБ и НБ;
- используя современные методы и средства, разрабатывать процессы управления инцидентами ИБ и НБ, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность;
- практически решать задачи формализации разрабатываемых процессов управления инцидентами ИБ и НБ;
- разрабатывать документальное обеспечение для процессов управления инцидентами ИБ и НБ, включая различные политики и применять его на практике.

Владеть:

- терминологией и процессным подходом построения систем управления инцидентами ИБ и систем управления НБ;
- навыками построения как отдельных процессов управления инцидентами ИБ и НБ, так и систем процессов в целом.

Материалы, вошедшие в учебное пособие «Управление инцидентами информационной безопасности и непрерывностью бизнеса» 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 «Управление инцидентами информационной безопасности и непрерывностью бизнеса» из серии «Вопросы управления информационной безопасностью» может быть полезным при реализации программ дополнительного образования (курсы повышения квалификации или переподготовки кадров).

ОГЛАВЛЕНИЕ

Предисловие	3
Введение	7
1. Нормативная база управления инцидентами ИБ и обеспечение непрерывности бизнеса.....	9
1.1. ISO/IEC 27035:2011 – управление инцидентами ИБ.....	10
1.2. ISO/IEC 27037 – руководство по идентификации, сбору и/или получению и обеспечению сохранности свидетельств, представленных в электронной форме	12
1.3. ISO/IEC 27031:2011 – руководство по готовности информационных и телекоммуникационных технологий для обеспечения непрерывности бизнеса	14
1.4. BS 25999 и ГОСТ Р 53647 – управление непрерывностью бизнеса	17
Выводы	18
Вопросы для самоконтроля	19
2. Управление инцидентами ИБ	20
2.1. Событие и инцидент ИБ.....	21
2.2. Цели и задачи управления инцидентами ИБ.....	26
2.3. Система управления инцидентами ИБ	31
2.4. Этапы процесса управления инцидентами ИБ	39
2.4.1. Планирование и подготовка процесса управления инцидентами ИБ	40
2.4.2. Использование системы управления инцидентами ИБ.....	41
2.4.3. Анализ процесса управления инцидентами ИБ	43
2.4.4. Улучшение процесса управления инцидентами ИБ	45
2.5. Обнаружение событий ИБ и инцидентов ИБ и оповещение о них	46
2.6. Обработка событий ИБ и инцидентов ИБ	48
2.6.1. Первая оценка и предварительное решение по событию ИБ.....	49
2.6.2. Вторая оценка и подтверждение инцидента ИБ	53
2.7. Реагирование на инциденты ИБ.....	55
2.7.1. Немедленное реагирование на инцидент ИБ	56
2.7.2. Контролируемость инцидента ИБ	59
2.7.3. Последующее реагирование на инцидент ИБ	59
2.7.4. Антикризисные действия	60
2.7.5. Правовая экспертиза инцидентов ИБ.....	61
2.7.6. Передача информации.....	66
2.7.7. Расширение области принятия решений	67

2.7.8. Регистрация деятельности и контроль за внесением изменений	67
2.7.9. Техническая поддержка реагирования на инциденты ИБ	67
2.8. Документация системы управления инцидентами ИБ	69
2.8.1. Политика управления инцидентами ИБ	71
2.8.2. Программа управления инцидентами ИБ	72
2.9. Группа реагирования на инциденты ИБ	77
2.10. Обеспечение осведомленности и обучение в области инцидентов ИБ	83
2.11. Сохранение доказательств инцидента ИБ	84
2.12. Средства управления событиями ИБ	90
Выводы	92
Вопросы для самоконтроля	93
3. Управление непрерывностью бизнеса организации	96
3.1. Определения непрерывности бизнеса и управления ею	99
3.2. Система управления непрерывностью бизнеса	103
3.3. Жизненный цикл управления непрерывностью бизнеса	105
3.3.1. Управление программой УНБ	107
3.3.2. Анализ непрерывности бизнеса организации	110
3.3.3. Определение стратегии УНБ	116
3.3.4. Разработка и внедрение в УНБ ответных мер на инциденты	121
3.3.5. Меры по применению, поддержке и анализу УНБ	125
3.3.6. Внедрение УНБ в культуру организации	134
3.4. Документация и записи в области непрерывности бизнеса	136
3.4.1. Политика УНБ	137
3.4.2. Планы управления инцидентом, ОНБ и восстановления бизнеса	139
3.5. Готовность ИТТ к ОНБ	151
3.6. Средства управления непрерывностью бизнеса	157
Выводы	158
Вопросы для самоконтроля	158
Заключение	160
Приложения	163
Примеры систем управления событиями ИБ	163
Принятые сокращения	163
Список литературы	165