

ВОПРОСЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

КНИГА 4

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

ТЕХНИЧЕСКИЕ, ОРГАНИЗАЦИОННЫЕ И КАДРОВЫЕ АСПЕКТЫ УПРАВЛЕНИЯ 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» (уровни – бакалавр, 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. Зегжда*; доктор техн. наук, профессор *А. Г. Остапенко*

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

М60 Технические, организационные и кадровые аспекты управления информационной безопасностью. Учебное пособие для вузов. – М.: Горячая линия–Телеком, 2013. – 216 с.: ил. – Серия «Вопросы управления информационной безопасностью. Выпуск 4»
ISBN 978-5-9912-0274-9.

Рассмотрены технические аспекты управления информационной безопасностью (ИБ), включая управление логическим доступом пользователей к активам организации, управление защищенной передачей данных и операционной деятельностью, разработку и обслуживание информационных систем с учетом требований к их ИБ, управление конфигурациями, изменениями и обновлениями в активах организации. Кратко рассмотрены основы физической защиты и защиты от воздействия окружающей среды. Анализируются организационные и кадровые вопросы управления ИБ. Введены четыре основные модели организационного управления ИБ, являющиеся комбинациями централизованных и децентрализованных руководства и администрирования ИБ. Рассмотрена организационная инфраструктура управления ИБ. Перечислены организационные мероприятия по управлению ИБ. Подробно описаны деятельность, функции, состав и варианты создания службы ИБ организации, а также задачи, функции, обязанности, права и ответственность администратора ИБ подразделения организации. Детально анализируются группы компетенций, должности и направления деятельности специалистов в области ИБ. Особое внимание уделено учету вопросов ИБ при найме персонала на работу и при формировании должностных обязанностях персонала.

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

ББК 32.973.2-018.2я73

ISBN 978-5-9912-0274-9

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

ПРЕДИСЛОВИЕ

Учебное пособие «Технические, организационные и кадровые аспекты управления информационной безопасностью» является четвертой частью серии учебных пособий «Вопросы управления информационной безопасностью».

При подготовке данного учебного пособия были поставлены следующие задачи:

- 1) рассмотреть технические аспекты управления информационной безопасностью (ИБ);
- 2) определить взаимосвязь системы управления ИБ (СУИБ) с системой физической защиты объекта и мер по защите от воздействия окружающей среды;
- 3) проанализировать организационные и кадровые вопросы управления ИБ.

Исходя из поставленных задач, была выбрана структура учебного пособия «Технические, организационные и кадровые аспекты управления информационной безопасностью», которое состоит из введения, двух глав, заключения, шести приложений и списка литературы из 35 наименований.

Во введении обоснована актуальность темы учебного пособия.

Первая глава посвящена техническим аспектам управления ИБ организации. Рассматривается управление логическим доступом пользователей к активам организации – приложениям, операционным системам и сетям, основанное на специальной политике и установленных обязанностях пользователей, включая их работу с переносными устройствами и в дистанционном режиме. Исследуются вопросы управления защищенной передачей данных и операционной деятельностью, регламентированного документированными процедурами, подразумевающего разделение полномочий и включающего деятельность по разграничению сред разработки и промышленной эксплуатации, управление системами обработки информации (СОИ) сторонними лицами и/или организациями, планирование нагрузки и приемки систем, защиту от вредоносного программного обеспечения (ПО), управление сетевыми ресурсами, защиту носителей информации, безопасный обмен информацией и ПО и некоторые вспомогательные операции. Обсуждается разработка и обслуживание информационных систем (ИС) с учетом требований к их ИБ, которые должны быть приняты во внимание при обеспечении ИБ (ОИБ) приложений и системных файлов, в том числе с использованием защитных мер, связанных с использованием криптографии. Особое внимание уделено важному вопросу управления конфигурациями, изменениями и обновлениями в активах организации. Кратко рассмотрены основы физической защиты и защиты от воздействия окружающей среды, заклю-

чающиеся в выделении охраняемых зон и обеспечении безопасности оборудования организации.

Вторая глава анализирует организационные и кадровые вопросы управления ИБ. Вводятся четыре основные модели организационного управления ИБ, являющиеся комбинациями централизованных и децентрализованных руководства и администрирования ИБ. Рассматривается организационная инфраструктура управления ИБ, базирующаяся на поддержке со стороны руководства организации и опирающаяся на комитет по управлению вопросами ИБ, координационный комитет и службу ИБ. Перечисляются организационные мероприятия по управлению ИБ, классифицируемые как разовые, постоянно и периодические проводимые и проводимые по мере необходимости. Подробно описывается деятельность и функции Службы ИБ организации, опирающейся на предоставляемые ей полномочия. Также определяются различные варианты создания этой службы, ее состав, функции руководителя. Отдельно рассматриваются задачи, функции, обязанности, права и ответственность администратора ИБ подразделения организации. Детально анализируются группы компетенций, должности и направления деятельности специалистов в области ИБ. Особое внимание уделяется учету вопросов ИБ при найме персонала на работу и в должностных обязанностях персонала. Кратко затрагивается сотрудничество между организациями и консультации со специалистами в области ИБ.

В заключении кратко выделяется взаимосвязь изученных понятий, относящихся к техническим, организационным и кадровым аспектам управления ИБ, а также устанавливается связь между материалом учебного пособия и составляющими профессиональных компетенций.

В приложениях приводится информация справочного характера в виде примерных положений об Управляющем совете по вопросам ИБ, Координационном комитете по вопросам управления ИБ и Службе ИБ.

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

- способность участвовать в управлении ИБ объекта;
- способность участвовать в проектировании и разработке СУИБ объекта.

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

После изучения данного учебного пособия обучающиеся будут:

Знать:

- современные подходы к управлению ИБ объекта и направления их развития;
- особенности отдельных процессов управления ИБ в рамках СУИБ;
- подходы к интеграции СУИБ в общую систему управления организации.

Уметь:

- анализировать текущее состояние ИБ на предприятии с целью разработки требований к разрабатываемым процессам управления ИБ;
- определять цели и задачи, решаемые разрабатываемыми процессами управления ИБ.

Владеть:

- терминологией в области технических, организационных и кадровых аспектов управления ИБ;
- навыками построения отдельных процессов управления ИБ, относящихся к области технических, организационных и кадровых аспектов управления ИБ.

Материалы, вошедшие в учебное пособие «Технические, организационные и кадровые аспекты управления 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 бакалавриата и магистратуры направления 090900 – «Информационная безопасность».

Кроме этого учебное пособие «Технические, организационные и кадровые аспекты управления 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 ОИБ, уязвимости и угрозы ИБ в информационной среде. Следует рекомендовать предварительное ознакомление с материалом первой части серии учебных пособий «Вопросы управления информационной безопасностью»: «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 проблем, поэтому с благодарностью внимательно изучат и учтут критические замечания и предложения читателей при дальнейшей работе над учебным пособием.

Оглавление

Предисловие	3
Введение	6
1. Технические аспекты управления ИБ	7
1.1. Управление логическим доступом к активам организации	7
1.1.1. Политика в отношении логического доступа	10
1.1.2. Управление доступом пользователей	11
1.1.3. Обязанности пользователя при доступе к активам	15
1.1.4. Управление сетевым доступом	17
1.1.5. Управление доступом к операционной системе	21
1.1.6. Управление доступом к приложениям	25
1.1.7. Работа с мобильными устройствами и в дистанционном режиме.....	27
1.2. Управление защищенной передачей данных и операционной деятельностью.....	30
1.2.1. Документированные процедуры	32
1.2.2. Разделение полномочий.....	34
1.2.3. Разграничение сред разработки и промышленной эксплуатации	35
1.2.4. Доступ к средствам обработки информации сторонних лиц и/или организаций	36
1.2.5. Планирование нагрузки и приемка систем	39
1.2.6. Защита от вредоносного ПО.....	41
1.2.7. Управление сетевыми ресурсами.....	42
1.2.8. Защита носителей информации.....	45
1.2.9. Обмен информацией и ПО.....	47
1.2.10. Вспомогательные операции.....	51
1.3. Разработка и обслуживание информационных систем	53
1.3.1. Выработка требований по обеспечению ИБ систем.....	53
1.3.2. ИБ приложений.....	59
1.3.3. ИБ исходных текстов ПО, исполняемых и системных файлов	61
1.3.4. ИБ данных и учетных записей	63
1.3.5. ИБ в процессах разработки и сопровождения ИС	65
1.3.6. Защитные меры, связанные с использованием криптографии.....	67
1.4. Управление конфигурациями, изменениями и обновлениями.....	72
1.4.1. Управление конфигурациями.....	72
1.4.2. Управление изменениями	75
1.4.3. Управление обновлениями ИБ.....	78
1.5. Физическая защита и защита от воздействия окружающей среды	82

1.5.1. Охраняемые зоны	83
1.5.2. Безопасность оборудования.....	88
Выводы	91
Вопросы для самоконтроля.....	91
2. Организационные и кадровые вопросы управления ИБ	93
2.1. Модели организационного управления ИБ	93
2.1.1. Централизованное руководство/централизованное администрирование ИБ.....	98
2.1.2. Централизованное руководство/децентрализованное администрирование ИБ.....	99
2.1.3. Децентрализованное руководство/централизованное администрирование ИБ.....	100
2.1.4. Децентрализованное руководство/децентрализованное администрирование ИБ.....	101
2.2. Организационная инфраструктура управления ИБ	101
2.2.1. Обязанности руководства	103
2.2.2. Комитет по управлению вопросами ИБ	103
2.2.3. Координационный комитет по вопросам управления ИБ	104
2.3. Организационные мероприятия по управлению ИБ.....	105
2.3.1. Разовые мероприятия	105
2.3.2. Постоянно проводимые мероприятия	107
2.3.3. Периодически проводимые мероприятия	107
2.3.4. Мероприятия, проводимые по мере необходимости.....	108
2.4. Служба ИБ организации.....	108
2.4.1. Полномочия службы ИБ	110
2.4.2. Основные функции службы ИБ	112
2.4.3. Варианты создания службы ИБ.....	115
2.4.4. Состав службы ИБ.....	119
2.4.5. Руководитель службы ИБ	121
2.5. Компетентностные уровни профессионалов в области ИБ	122
2.5.1. Квалификационные характеристики должностей руководителей и специалистов по ОБИ	123
2.5.2. Квалификационные характеристики из ФГОС.....	127
2.5.3. Квалификационные характеристики профессионалов в области ИБ: вариант для негосударственной организации	132
2.6. Учет вопросов ИБ при работе с персоналом	145
2.6.1. Учет вопросов ИБ в должностных обязанностях	147
2.6.2. Учет вопросов ИБ при найме персонала	148
2.7. Сотрудничество между организациями и консультации со специалистами в области ИБ.....	150
Выводы	151
Вопросы для самоконтроля.....	152
Заключение	153

Приложения.....	155
П1. Примерное положение об управляющем совете по вопросам ИБ в банке.....	155
П2. Примерное положение о координационном комитете по вопросам управления ИБ в банке	158
П3. Примерное положение о службе ИБ в банке.....	160
П4. Квалификационные характеристики должностей руководителей и специалистов по ОБИ в КСИИ, ПТР и ТЗИ	167
П5. Задачи, функции, обязанности, права и ответственность администратора ИБ подразделения организации.....	180
П6. Квалификационные характеристики профессионалов в области информационной безопасности.....	184
Принятые сокращения.....	207
Список литературы	209