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)

2-е издание, исправленное

Москва
Горячая линия - Телеком
2014

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. – 2-е изд., испр. – М.: Горячая линия–Телеком, 2014. – 214 с.: ил. – Серия «Вопросы управления информационной безопасностью. Книга 4»

ISBN 978-5-9912-0364-7.

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 978-5-9912-0364-7

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.

ВВЕДЕНИЕ

Управление информационной безопасностью (ИБ) – неотъемлемая часть управления любой современной организацией в целом, независимо от ее размера и сферы деятельности.

Управление ИБ – сложный непрерывный процесс, перед которым стоит множество целей и задач, являющихся обеспечивающими, вспомогательными по отношению к основным бизнес-целям и задачам организации. Они формулируются в различных документах организации: концепциях, стратегиях, политиках, стандартах, инструкциях и т. д.

Процесс управления ИБ распадается на тесно взаимосвязанные подпроцессы, каждый из которых вносит существенный вклад в достижение общих целей управления ИБ. Объектами управления в рамках этих подпроцессов являются активы, риски ИБ, инциденты ИБ, непрерывность бизнеса, изменения, усовершенствования и многое другое. От эффективности и результативности каждого из этих подпроцессов зависят общая эффективность и результативность всей деятельности по управлению ИБ в организации.

Для успешного управления ИБ должна быть создана учитывающая специфику организации и адекватная ее требованиям в отношении обеспечения ИБ (ОИБ) система управления ИБ (СУИБ). Организационный и кадровый аспекты ОИБ организации являются одними из ее важнейших элементов, так как от их реализации в значительной степени зависит эффективность и результативность всей деятельности по управлению ИБ и, следовательно, поддержанию ИБ в организации на должном уровне. Правильные решения вопросов создания организационной инфраструктуры и кадровая политика в области ОИБ способствуют ускорению комплексного внедрения и поддержания целостной системы обеспечения ИБ (СОИБ), увязывающей технические, организационные, административные (включая работу с персоналом) защитные меры.

Рассмотрению этих мер посвящено предлагаемое учебное пособие «Технические, организационные и кадровые аспекты управления информационной безопасностью», являющееся четвертой частью в серии учебных пособий «Вопросы управления информационной безопасностью».