ВОПРОСЫ УПРАВЛЕНИЯ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

КНИГА 1

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

ОСНОВЫ 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 направлениям подготовки (специальностям) укрупненной группы специальностей 090000 – «Информационная безопасность»

Москва
Горячая линия - Телеком
2013

УДК 004.732.056(075.8)
ББК 32.973.2-018.2я73
О-75

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*

А в т о р ы : А. П. Курило, Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой

О-75 **Основы** управления информационной безопасностью. Учебное пособие для вузов. – М.: Горячая линия–Телеком, 2013. – 244 с.: ил. – Серия «Вопросы управления информационной безопасностью. Выпуск 1»

ISBN 978-5-9912-0271-8.

Изложены основы управления информационной безопасностью (ИБ). Вводятся основные определения и понятия: ИБ, политика ИБ, управление ИБ и другие. Описываются процесс управления ИБ и его составляющие. Определяются система управления (СУИБ) организации, ее область действия и документальное обеспечение, включая политику СУИБ. Подробно рассматриваются этапы планирования, реализации, проверки и совершенствования СУИБ. Анализируется текущая ситуация в области стандартизации управления ИБ, в частности международные и российские стандарты, устанавливающие требования к СУИБ и отдельным процессам управления ИБ.

Для студентов высших учебных заведений, обучающихся по программам бакалавриата, магистратуры и специалитета укрупненного направления 090000 – «Информационная безопасность», будет полезно слушателям курсов переподготовки и повышения квалификации и специалистам.

ББК 32.973.2-018.2я73

Учебное издание

Курило Андрей Петрович, **Милославская** Наталья Георгиевна,
Сенаторов Михаил Юрьевич, **Толстой** Александр Иванович

Основы управления информационной безопасностью

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. 15,25. Тираж 500 экз. Изд. № 12271

ISBN 978-5-9912-0271-8

ПРЕДИСЛОВИЕ

Учебное пособие «Основы управления информационной безопасностью» является первой частью серии учебных пособий «Вопросы управления информационной безопасностью». При подготовке данного учебного пособия были поставлены следующие задачи:

1) определить основные понятия, относящиеся к управлению информационной безопасностью (ИБ);

2) описать процесс управления ИБ и его составляющие;

3) определить особенности системы управления ИБ (СУИБ) организации, ее область действия и документальное обеспечение, включая политику СУИБ;

4) подробно рассмотреть этапы планирования, реализации, проверки и совершенствования СУИБ;

5) дать подробный анализ текущей ситуации в области стандартизации управления ИБ.

Исходя из поставленных задач, была определена структура учебного пособия «Основы управления информационной безопасностью», которое состоит из введения, четырех глав, приложения и списка литературы из 98 наименований.

Во введении обоснована актуальность темы учебного пособия.

Глава 1 посвящена определению круга понятий, которые будут использоваться в последующих разделах и на всех этапах, относящихся к разработке, эксплуатации и контролю эффективности. В частности, напоминаются основные определения из теории систем («система», «системный подход», «системный подход к управлению организацией») и теории управления («процесс», «процессный подход», «процессный подход к управлению организацией», «циклическая модель улучшения процессов» – цикл PDCA, «управление»), которые будут использоваться во всех последующих главах учебного пособия, и термин «информационная безопасность».

В главе 2 проанализирована текущая ситуация в области стандартизации управления ИБ. Рассматриваются международные и российские стандарты, выдвигающие требования как к СУИБ, так и к отдельным процессам управления ИБ (серия стандартов ИСО/МЭК 27000, немецкие стандарты BSI, стандарты Банка России в области обеспечения ИБ (ОИБ) для организаций банковской системы Российской Федерации и т. д.).

В главе 3 вводятся понятия политик ОИБ вообще и ПолИБ организации. Излагаются причины выработки политик для организации, основные требования к ней и принципы ее разработки и внедрения. Подробно рассматриваются содержания корпоративной и частных ПолИБ. Описываются основные шаги, необходимые для выполнения на различных стадиях жизненного цикла политики.

Глава 4 рассматривает вопросы, связанные с управлением ИБ и построением СУИБ. Обосновывается необходимость управления деятельностью по ОИБ, которая описывается как процесс. Вводится понятие «управление ИБ организации». Рассматривается процесс управления ИБ информационно-телекоммуникационными технологиями (ИТТ), который интегрируется в общий процесс управления ИТТ организации. Определяется СУИБ организации, ее область действия и документальное обеспечение, включая политику СУИБ. В рамках управления ИБ описывается применение процессного подхода с этапами «планирование – реализация – проверка – совершенствование» ко всем процессам СУИБ. Анализируется работа с процессами СУИБ, включающая задание процесса, его идентификацию, документирование и описание, мониторинг и измерение. Рассматриваются две стратегии построения и внедрения СУИБ – в целом и по отдельным процессам управления ИБ.

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

В приложении приводится информация справочного характера в виде примеров частных ПолИБ.

Освоение материалов данного учебного пособия формирует у обучающихся обозначенные выше профессиональные компетенции:

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

После изучения учебного пособия «Основы управления информационной безопасностью» обучающиеся будут

Знать

- принципы построения СУИБ объекта;
- современные подходы к управлению ИБ объекта и направления их развития;
- особенности отдельных процессов управления ИБ в рамках СУИБ;
- основные международные и российские стандарты, регламентирующие управление ИБ;
- принципы разработки процессов управления ИБ.

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;
- применять процессный подход к управлению ИБ в различных сферах деятельности.

ŋqddɐʎеʎ рƎ dədƎрʎзә р ɐɔɐбɔʎ Ɉqddʎqɐè

Владеть терминологией и процессным подходом построения СУИБ.

Материалы, вошедшие в учебное пособие «Основы управления информационной безопасностью», обеспечивают учебно-методической базой любую учебную дисциплину, относящуюся к управлению ИБ. Поэтому данное учебное пособие может быть рекомендовано студентам высших учебных заведений, обучающимся по программам бакалавриата, магистратуры и специалитета укрупненного направления 090000 – «Информационная безопасность».

Учебное пособие может быть также полезно слушателям курсов повышения квалификации.

Кроме этого, представляемое учебное пособие «Основы управления информационной безопасностью» из серии «Вопросы управления информационной безопасностью» может быть полезным при реализации программ дополнительного образования (курсы повышения квалификации или переподготовки кадров).

Оглавление