

**УЧЕБНОЕ
ПОСОБИЕ**

ПИТЕР®

СТАНДАРТ ТРЕТЬЕГО ПОКОЛЕНИЯ

Ю. А. Родичев

Нормативная база и стандарты в области информационной безопасности

**РЕКОМЕНДОВАНО ДЛЯ СТУДЕНТОВ, ОБУЧАЮЩИХСЯ
ПО НАПРАВЛЕНИЮ ПОДГОТОВКИ 10.00.00
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»**



СТАНДАРТ ТРЕТЬЕГО ПОКОЛЕНИЯ

Ю. А. Родичев

Нормативная база и стандарты в области информационной безопасности

Рекомендовано к изданию редакционно-издательским советом федерального государственного автономного образовательного учреждения высшего образования «Самарский национальный исследовательский университет имени академика С. П. Королева» в качестве учебного пособия для студентов, обучающихся по программам высшего образования укрупненной группы специальностей и направлений подготовки 10.00.00 «Информационная безопасность»



Санкт-Петербург · Москва · Екатеринбург · Воронеж
Нижний Новгород · Ростов-на-Дону
Самара · Минск

2017

ББК 67.621.162я7
УДК 351.864.1(075)
Р60

Рецензенты:

доктор педагогических наук, профессор кафедры прикладной математики
и информационной безопасности Самарского государственного
экономического университета *А. Г. Абросимов*;
доктор технических наук, профессор Самарского национального
исследовательского университета имени академика С. П. Королева *В. С. Кузьмичев*.

Родичев Ю. А.
Р60 Нормативная база и стандарты в области информационной безопасности. Учебное пособие. — СПб.: Питер, 2017. — 256 с.: ил. — (Серия «Учебник для вузов»).

ISBN 978-5-496-02434-1

В учебном пособии рассмотрены наиболее важные нормативные документы ФСТЭК, а также международные и национальные стандарты Российской Федерации в области информационной безопасности.

Предназначено для студентов высших учебных заведений, обучающихся по специальностям в области информационной безопасности, слушателей курсов повышения квалификации по проблемам защиты информации. Рассмотренные вопросы будут полезны руководителям учреждений, а также специалистам в области ИТ, занимающимся разработкой и эксплуатацией аппаратно-программных средств и обеспечением их безопасности.

Рекомендовано к изданию редакционно-издательским советом федерального государственного автономного образовательного учреждения высшего образования «Самарский национальный исследовательский университет имени академика С.П. Королева» в качестве учебного пособия для студентов, обучающихся по программам высшего образования укрупненной группы специальностей и направлений подготовки 10.00.00 «Информационная безопасность».

12+ (В соответствии с Федеральным законом от 29 декабря 2010 г. № 436-ФЗ.)

ББК 67.621.162я7
УДК 351.864.1(075)

Все права защищены. Никакая часть данной книги не может быть воспроизведена в какой бы то ни было форме без письменного разрешения владельцев авторских прав.

ISBN 978-5-496-02434-1

© ООО Издательство «Питер», 2017
© Серия «Учебник для вузов», 2017

Содержание

| | |
|---|-----------|
| Перечень сокращений | 7 |
| Введение | 8 |
| Глава 1. Основы технического регулирования и стандартизации в Российской Федерации | 17 |
| 1.1. Общие замечания | 17 |
| 1.2. Федеральный закон Российской Федерации № 184-ФЗ «О техническом регулировании» | 20 |
| 1.3. Основы стандартизации в Российской Федерации | 27 |
| 1.3.1. Основные положения системы стандартизации в Российской Федерации (ГОСТ Р 1.0–2012) | 27 |
| 1.3.2. Правила разработки национальных стандартов (ГОСТ Р 1.2–2014) ... | 30 |
| 1.3.3. Стандарты организаций (ГОСТ Р 1.4–2004) | 30 |
| 1.4. Основы стандартизации в области защиты информации | 31 |
| 1.4.1. Основные термины в сфере защиты информации (ГОСТ Р 50922–2006) | 31 |
| 1.4.2. Защита информации в организации (ГОСТ Р 53114–2008) | 33 |
| 1.4.3. Система стандартов по защите информации (ГОСТ Р 52069.0–2013) | 35 |
| 1.4.4. Факторы, воздействующие на информацию (ГОСТ Р 51275–2006) .. | 38 |
| 1.4.5. Оценка соответствия (ГОСТ 17000–2012) | 39 |
| Контрольные вопросы и задания к главе 1 | 44 |
| Глава 2. Нормативные документы ФСТЭК России | 46 |
| 2.1. Основные нормативные документы в области защиты информации | 46 |
| 2.2. Защита от несанкционированного доступа к информации. Термины и определения | 53 |
| 2.3. Концепция защиты СВТ и АС от НСД к информации | 55 |
| 2.4. Показатели защищенности СВТ от НСД к информации | 58 |
| 2.5. Классификация автоматизированных систем и требования по защите информации | 61 |
| 2.6. Межсетевые экраны. Показатели защищенности от НСД | 65 |

| | |
|---|-----|
| 2.7. Контроль отсутствия НДС в программном обеспечении | 67 |
| 2.8. Требования к защите персональных данных | 71 |
| 2.9. Требования о защите информации в государственных информационных системах | 76 |
| 2.10. Требования о защите информации в ИС общего пользования | 80 |
| 2.11. Требования к обеспечению защиты информации в АСУ ТП | 84 |
| 2.12. Новое поколение нормативных документов ФСТЭК | 89 |
| 2.12.1. Общие замечания | 89 |
| 2.12.2. Пакет документов по профилям защиты | 90 |
| 2.12.3. Требования к средствам антивирусной защиты | 93 |
| 2.12.4. Требования к средствам обнаружения вторжений | 97 |
| 2.12.5. Требования к средствам контроля съемных машинных носителей | 100 |
| 2.12.6. Требования к средствам доверенной загрузки | 104 |
| 2.13. Заключительные замечания | 106 |
| Контрольные вопросы и задания к главе 2 | 108 |

Глава 3. Национальные и международные стандарты в области информационной безопасности 110

| | |
|--|-----|
| 3.1. Государственный стандарт по защите информации от НСД ГОСТ Р 50739–95 | 110 |
| 3.2. Национальный стандарт по менеджменту инцидентов ИБ ГОСТ Р ИСО/МЭК ТО 18044–2007 | 112 |
| 3.3. Национальный стандарт по менеджменту безопасности ИТТ ГОСТ Р ИСО/МЭК 13335-1–2006 | 115 |
| 3.4. Национальный стандарт по менеджменту безопасности сетей ГОСТ Р ИСО/МЭК 13335-5–2006 | 122 |
| 3.5. Стандарты серии 27000 по менеджменту ИБ | 123 |
| 3.5.1. История создания стандартов серии 27000 | 123 |
| 3.5.2. Национальный стандарт ГОСТ Р ИСО/МЭК 27000–2012 — термины по СМИБ | 128 |
| 3.5.3. Национальный стандарт ГОСТ Р ИСО/МЭК 27001–2006 — требования к СМИБ | 130 |
| 3.5.4. Национальный стандарт ГОСТ Р ИСО/МЭК 27002–2012 — свод норм и правил СМИБ | 132 |
| 3.5.5. Национальный стандарт ГОСТ Р ИСО/МЭК 27003–2012 — реализация СМИБ | 136 |
| 3.5.6. Национальный стандарт ГОСТ Р ИСО/МЭК 27004–2011 — измерения в СМИБ | 141 |
| 3.5.7. Национальный стандарт ГОСТ Р ИСО/МЭК 27005–2010 — менеджмент риска ИБ | 143 |
| 3.5.8. Национальные стандарты в области аудита СМИБ (ГОСТ 27006–2008, ГОСТ 27007–2014) | 146 |

| | |
|---|-----|
| 3.5.9. Национальный стандарт по СМИБ в телекоммуникационных организациях (ГОСТ 27011–2014) | 148 |
| 3.6. Стандарты серии 27033 по безопасности сетей | 150 |
| 3.6.1. Общие замечания | 150 |
| 3.6.2. Национальный стандарт ГОСТ Р ИСО/МЭК 27033-1–2011 — обзор и концепции безопасности сетей | 153 |
| 3.6.3. Национальный стандарт ГОСТ Р ИСО/МЭК 27033-3–2014 — эталонные сетевые сценарии | 160 |
| 3.7. Стандарты по безопасности сетей электросвязи (ГОСТ Р 52448–2005, ГОСТ Р 53110–2008) | 166 |
| 3.8. Защита от угроз, реализуемых через скрытые каналы (ГОСТ Р 53113.1, ГОСТ Р 53113.2) | 171 |
| 3.9. Стандарты по уязвимостям ИС (ГОСТ Р 56545, ГОСТ Р 56546) | 175 |
| 3.10. Комплекс стандартов по информационной безопасности Банка России (ИББС) | 178 |
| Контрольные вопросы и задания к главе 3 | 182 |

Глава 4. Национальные стандарты Российской Федерации на основе «Общих критериев»

| | |
|---|-----|
| 4.1. История создания «Общих критериев» и национальных стандартов на их основе | 184 |
| 4.2. Национальный стандарт ГОСТ Р ИСО/МЭК 15408-1–2012 | 189 |
| 4.3. Национальный стандарт ГОСТ Р ИСО/МЭК 15408-2–2013 | 196 |
| 4.4. Национальный стандарт ГОСТ Р ИСО/МЭК 15408-3–2013 | 200 |
| 4.5. Национальный стандарт ГОСТ Р ИСО/МЭК 18045–2013 | 209 |
| 4.6. Национальный стандарт ГОСТ Р ИСО/МЭК 51583–2014 | 213 |
| 4.7. Национальный стандарт ГОСТ Р ИСО/МЭК 19791–2008 | 219 |
| 4.8. Национальный стандарт ГОСТ Р ИСО/МЭК 15446–2008 | 227 |
| 4.9. Национальные стандарты по биометрической аутентификации серии ГОСТ Р 52633 | 231 |
| 4.10. Краткий обзор некоторых стандартов | 234 |
| Контрольные вопросы и задания к главе 4 | 239 |

Список литературы

Список документов ФСТЭК

Список национальных стандартов

Список стандартов Банка России