

УДК 004.056.5 (075.8)

ББК 32.973Я73

Ш59

*Печатается по решению кафедры информационной безопасности
Института компьютерных технологий и информационной безопасности
Южного федерального университета (протокол №7 от 23 января 2017 г.)*

Рецензенты:

кандидат технических наук, доцент кафедры прикладной математики и
информационных технологий Таганрогского института управления
и экономики, кандидат технических наук *О. И. Овчаренко*

кандидат технических наук, доцент кафедры информационной
безопасности телекоммуникационных систем ЮФУ *С. Л. Балабаев*

Шилов, А. К.

Ш59 Управление информационной безопасностью : учебное пособие /
А. К. Шилов ; Южный федеральный университет. – Ростов-на-Дону ;
Таганрог : Издательство Южного федерального университета, 2018. –
120 с.

ISBN 978-5-9275-2742-7

В учебном пособии дается представление о методологии и нормативном обеспечении процедур управления безопасностью. Рассмотрены современные инструментальные средства, применяемые на практике при оценке безопасности предприятия. Учебное пособие предназначено для подготовки бакалавров, специалистов, магистров и аспирантов по направлениям информационной безопасности.

УДК 004.056.5 (075.8)

ББК 32.973Я73

ISBN 978-5-9275-2742-7

© Южный федеральный университет, 2018

© Шилов А. К., 2018

© Оформление. Макет. Издательство

Южного федерального университета, 2018

СОДЕРЖАНИЕ

Предисловие	4
Введение	7
1. Требования к системам управления безопасностью	9
1.1. Основы управления безопасностью на предприятии	9
1.2. Требования к внедрению стандарта ГОСТ 27001	12
1.3. Работа после внедрения системы управления ИБ	19
2. GRC-системы управления информационной безопасностью	24
2.1. GRC-парадигма управления ИБ	24
2.2. Security GRC-системы управления ИБ	27
2.3. Обзор российских SGRC-продуктов	30
3. Построение СУИБ на основе разработок Positive Technologies	35
3.1. О компании Positive Technologies	35
3.2. Программный продукт MaxPatrol SIEM	35
3.3. Система MaxPatrol для контроля защищенности	39
3.4. Программный продукт MaxPatrol 8 для SAP	42
4. Контроль защищенности автоматизированных систем	45
4.1. Задачи, возникающие в ходе контроля защищенности	45
4.2. Развертывание MaxPatrol	52
5. Инвентаризация информационных активов	64
5.1. Объекты и способы инвентаризации	64
5.2. Инвентаризация с помощью сетевого сканера	65
5.3. Инвентаризация с использованием системных проверок	71
6. Уязвимости и способы их выявления	73
6.1. Понятие уязвимости и категории проверок	73
6.2. Тесты и эксплойты	74
6.3. Выявление уязвимостей по косвенным признакам	76
Контрольные вопросы	78
Заключение	79
Список литературы	81
Приложения	83
Приложение 1. Сайты по теме пособия	83
Приложение 2. Глоссарий терминов по СУИБ	86
Приложение 3. Пакет документов СУИБ по ISO 27001-2013	114