

УДК 004.056.5 (075.8)  
ББК 32.973 я73  
П 24

Печатается по решению  
редакционно-издательского совета  
Северо-Кавказского федерального  
университета

**Пелешенко В. С., Говорова С. В., Лапина М. А.**

П 24 **Менеджмент инцидентов информационной безопасности  
защищенных автоматизированных систем управления:**  
учебное пособие. – Ставрополь: Изд-во СКФУ, 2017. – 86 с.

Пособие составлено в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования, учебным планом и программой дисциплины. Содержит курс лекций, включающих основные теоретические положения курса, вопросы для самопроверки, литературу.

Предназначено для студентов, обучающихся по направлениям подготовки бакалавриата 10.03.01 – Информационная безопасность; магистратуры 10.04.01 – Информационная безопасность (Комплексная защита объектов информатизации) и по специальностям 10.05.01 – Компьютерная безопасность; 10.05.03 – Информационная безопасность автоматизированных систем, кроме того, может быть полезно специалистам, интересующимся вопросами менеджмента инцидентов информационной безопасности защищенных автоматизированных систем управления.

УДК 004.056.5 (075.8)  
ББК 32.973 я73

**Рецензенты:**

д-р техн. наук, профессор *И. А. Калмыков*,  
д-р техн. наук, доцент *Г. И. Линец*

© ФГАОУ ВО «Северо-Кавказский  
федеральный университет», 2017

# Содержание

Предисловие .....	4
1. Введение в дисциплину «Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления». Основные понятия .	5
2. Общие положения менеджмента инцидентов информационной безопасности .....	8
3. Преимущества структурного подхода и ключевые вопросы менеджмента инцидентов информационной безопасности автоматизированных систем управления .....	10
4. Причины инцидентов информационной безопасности и их примеры .....	21
5. Планирование и подготовка менеджмента инцидентов информационной безопасности защищенных автоматизированных систем управления .....	26
6. Планирование и подготовка менеджмента инцидентов. Этап «Использование» .....	39
7. Планирование и подготовка менеджмента инцидентов. Этап «Анализ» .....	60
8. Планирование и подготовка менеджмента инцидентов. Этап «Улучшение» .....	63
9. Принципы и условия обработки персональных данных ...	65
10. Защита от несанкционированного доступа .....	78
Литература .....	85

## Предисловие

Пособие представляет собой курс из 10 лекций, целью которых является выработка навыков по обнаружению, оповещению об инцидентах информационной безопасности и их оценке, а также обучение правилам реагирования на инциденты информационной безопасности, включая активизацию соответствующих защитных мер для предотвращения, уменьшения последствий и восстановления после негативных воздействий.

*Первая лекция посвящена введению в дисциплину и знакомству с основными понятиями. Во второй лекции рассматриваются общие положения менеджмента инцидентов информационной безопасности. Третья лекция рассматривает ключевые вопросы структурного подхода и менеджмента инцидентов информационной безопасности автоматизированных систем управления. В четвертой лекции показаны причины инцидентов информационной безопасности и их примеры. Пятая лекция посвящена планированию и подготовки менеджмента инцидентов информационной безопасности защищенных автоматизированных систем управления. В шестой лекции рассматривается планирование и подготовка менеджмента инцидентов, а также этап «Использование». Седьмая лекция рассматривает криптографические средства защиты систем баз данных. В восьмой лекции показано планирование и подготовка менеджмента инцидентов, а также этап «Улучшение». Девятая лекция разъясняет принципы и условия обработки персональных данных, а также описывает особенности обработки персональных данных в государственных или муниципальных информационных системах персональных данных. Десятая лекция посвящена вопросам защиты от несанкционированного доступа.*