

Документ подписан простой электронной подписью  
Информация о владельце:  
ФИО: Локтионова Оксана Геннадьевна  
Должность: проректор по учебной работе  
Дата подписания: 23.03.2023 13:58:35  
Уникальный программный ключ:  
0b817ca911e6668abb13a5d426d39e5f1c11eabbf73e943df4a4851ba56d080

МИНОБРАЗОВАНИЯ И НАУКИ РОССИИ

Федеральное государственное бюджетное образовательное  
учреждения высшего образования  
«Юго-Западный государственный университет»  
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ  
Проректор по учебной работе  
О.Г. Локтионова  
« 1 » 02 (ЮЗГУ) 2018 г.



## ЗАЩИЩЁННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

Методические указания к самостоятельной  
для студентов укрупненной группы специальностей и  
направлений подготовки 10.00.00 «Информационная безопасность»

Курск 2018

УДК 004

Составитель: М.О. Таныгин

Рецензент

Кандидат технических наук, доцент кафедры  
«Информационная безопасность» А.Л. Марухленко

**Защищённые информационные системы** [Текст]:  
методические указания к самостоятельной работе по дисциплине  
«Защищенные информационные системы»/ Юго-Зап. гос. ун-т;  
сост.: М.О. Таныгин. – Курск, 2018. – 9 с. – Библиогр.: с. 9.

Содержат сведения по вопросам самостоятельной работы на протяжении изучения дисциплины. Указывается порядок выполнения самостоятельных работ, содержание работы.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по специальности.

Предназначены для студентов укрупненной группы специальностей и направлений подготовки 10.00.00 «Информационная безопасность».

Текст печатается в авторской редакции

Подписано в печать *1.02.18*. Формат 60x84 1/16.  
Усл.печ. л. 0,52. Уч.-изд. л. 0,47. Тираж 100 экз. Заказ. Бесплатно. *234*  
Юго-Западный государственный университет.  
305040, г. Курск, ул. 50 лет Октября, 94.

## СОДЕРЖАНИЕ

Введение.....	4
Цель работы .....	4
Основные определения.....	4
Содержание работы .....	5
Тема самостоятельной работы 1: «Основные аспекты построения системы информационной безопасности» .....	5
Тема самостоятельной работы 2: «Мероприятия по защите информации» .....	5
Тема самостоятельной работы 3: «Требования к архитектуре ИС для обеспечения безопасности ее функционирования».....	5
Тема самостоятельной работы 4: «Оценочные стандарты и технические спецификации. » .....	5
Тема самостоятельной работы 5: «Критерии оценки безопасности информационных технологий.» .....	5
Тема самостоятельной работы 6: «Руководящие документы ФСТЭК России.» .....	5
Методические указания для обучающихся по освоению дисциплины .....	6
Вопросы для самопроверки .....	7
Список информационных источников .....	9

## **ВВЕДЕНИЕ**

Самостоятельная работа важна для каждой дисциплины, так как позволяет на более глубоком уровне усвоить студентам основы мониторинга безопасности информационных систем.

## **ЦЕЛЬ РАБОТЫ**

Цель самостоятельно работы – получить более полные знания по изучаемой дисциплине.

## **ОСНОВНЫЕ ОПРЕДЕЛЕНИЯ**

Информация – сведения о каких-либо событиях, процессах, фактах или предметах;

Защита информации – это комплекс мероприятий, направленных на обеспечение информационной безопасности.

Информационная система - система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы (человеческие, технические, финансовые и т. д.), которые обеспечивают и распространяют информацию;

# СОДЕРЖАНИЕ РАБОТЫ

## **Тема самостоятельной работы 1:**

### **«Основные аспекты построения системы информационной безопасности»**

Регулирование ответственности нарушений информационной безопасности. Программа информационной безопасности. Контроль деятельности в области безопасности. Модели представления информационной защиты. Формирование требований к системе информационной безопасности. Этапы обеспечения информационной безопасности.

## **Тема самостоятельной работы 2:**

### **«Мероприятия по защите информации»**

Нормативно-законодательный аспект. Процедурный аспект. Программно-технический аспект.

## **Тема самостоятельной работы 3:**

### **«Требования к архитектуре ИС для обеспечения безопасности ее функционирования»**

Структурирование ЗИС. Анализ безопасности ИС. Критерии адекватности средств защиты. Структура профиля защиты ИТ-продукта. Соотношение эффективности и рентабельности систем информационной безопасности. Зависимость эффективности защиты от величины ущерба.

## **Тема самостоятельной работы 4:**

### **«Оценочные стандарты и технические спецификации. »**

"Оранжевая книга" как оценочный стандарт. Стандарты информационной безопасности распределенных систем. Механизмы реализации сервисов (функций) безопасности. Администрирование средств безопасности

## **Тема самостоятельной работы 5:**

### **«Критерии оценки безопасности информационных технологий.»**

Основные понятия. Стандарт "Критерии оценки безопасности информационных технологий" . Иерархия класс-семейство-компонент-элемент. Требования доверия безопасности.

## **Тема самостоятельной работы 6:**

### **«Руководящие документы ФСТЭК России.»**

Требования к защищенности автоматизированных систем. Классы защищённости информационных систем. Аспекты защищённых ИС, фигурирующие в требованиях ФСТЭК. Классификация защищённых информационных систем.

## **Методические указания для обучающихся по освоению дисциплины**

Основными видами аудиторной работы студента при изучении дисциплины «Защищённые информационные системы» являются лекции, лабораторные занятия. Студент не имеет права пропускать занятия без уважительных причин.

На лекциях излагаются и разъясняются основные понятия темы, связанные с ней теоретические и практические проблемы, даются рекомендации для самостоятельной работы. В ходе лекции студент должен внимательно слушать и конспектировать материал.

Изучение наиболее важных тем или разделов дисциплины завершают лабораторные и практические занятия, которые обеспечивают: контроль подготовленности студента; закрепление учебного материала; приобретение опыта устных публичных выступлений, ведения дискуссии, в том числе аргументации и защиты выдвигаемых положений и тезисов.

Лабораторному занятию предшествует самостоятельная работа студента, связанная с освоением материала, полученного на лекциях, и материалов, изложенных в учебниках и учебных пособиях, а также литературе, рекомендованной преподавателем.

Качество учебной работы студентов преподаватель оценивает по результатам тестирования, собеседования, защиты отчетов по лабораторным и практическим работам.

Преподаватель уже на первых занятиях объясняет студентам, какие формы обучения следует использовать при самостоятельном изучении дисциплины «Защищённые информационные системы»: конспектирование учебной литературы и лекции, составление словарей понятий и терминов и т. п.

В процессе обучения преподаватели используют активные формы работы со студентами: чтение лекций, привлечение студентов к творческому процессу на лекциях, промежуточный контроль путем отработки студентами пропущенных лекций, участие в групповых и индивидуальных консультациях (собеседовании). Эти формы способствуют выработке у студентов умения работать с учебником и литературой. Изучение литературы и справочной документации составляет значительную часть самостоятельной работы студента. Это большой труд, требующий усилий и желания студента. В самом начале работы над книгой важно определить цель и направление этой работы. Прочитанное следует закрепить в памяти. Одним из приемов закрепления освоенного материала является конспектирование, без которого немыслима серьезная работа над литературой. Систематическое конспектирование помогает научиться правильно, кратко и четко излагать своими словами прочитанный материал.

Самостоятельную работу следует начинать с первых занятий. От занятия к занятию нужно регулярно прочитывать конспект лекций,

знакомится с соответствующими разделами учебника, читать и конспектировать литературу по каждой теме дисциплины. Самостоятельная работа дает студентам возможность равномерно распределить нагрузку, способствует более глубокому и качественному усвоению учебного материала. В случае необходимости студенты обращаются за консультацией к преподавателю по вопросам дисциплины «Защищенные информационные системы» с целью усвоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины «Защищенные информационные системы» - закрепить теоретические знания, полученные в процессе лекционных занятий, а также сформировать практические навыки самостоятельного анализа особенностей дисциплины.

### **Вопросы для самоконтроля**

Тема 1. Основные аспекты построения системы информационной безопасности.

1. Чем регулируется ответственность нарушений информационной безопасности во внешней среде?
2. Что такое программа информационной безопасности?
3. Опишите структуру модели информационной безопасности.
4. Какие параметры СЗИ можно оценить с помощью системы количественных метрик?
5. Какие существуют модели и алгоритмы классификации СЗИ?
6. Опишите требования к системе информационной безопасности.
7. Назовите этапы обеспечения информационной безопасности.

Тема 2. Мероприятия по защите информации.

1. Перечислите мероприятия по ЗИ в нормативно-законодательном аспекте.
2. Перечислите мероприятия по ЗИ в процедурном аспекте.
3. Перечислите мероприятия по ЗИ в организационном аспекте.
4. Перечислите мероприятия по ЗИ в программно-техническом аспекте.
5. Понятие «политика информационной безопасности».
6. Особенности реализации политики ИБ при разработке СЗИ.
7. Опишите системное содержание политики информационной безопасности.
8. Этапы реализации политики ИБ.
9. Уровни политики ИБ

Тема 3. Требования к архитектуре ИС для обеспечения безопасности ее функционирования.

1. Что нужно учитывать при выборе компонент СЗИ и связей между ними?
2. Назовите основные принципы разработки СЗИ.
3. Как влияет простота структуры ЗИС на качество выполняемых ею функций?
4. Для чего нужна стандартизация подходов при разработке СЗИ?

5. Перечислите основные стандарты, в которых изложены требования к защищённым информационным системам.
6. Опишите структуру и содержание стандарта ISO 13335.
7. Опишите структуру профиля защиты ИТ-продукта.
8. Критерии рентабельности защищённой информационной системы.
9. Как зависит эффективность и рентабельность защиты от величины максимального ущерба?
10. Как зависит эффективность и рентабельность системы защиты от величины общих ресурсов?

Тема 4. Требования к архитектуре ИС для обеспечения безопасности ее функционирования.

1. Понятие оценочного стандарта
2. Назовите основные термины «Оранжевой книги»
3. Назовите характеристики монитора информационной безопасности.
4. Для чего нужен механизм подотчётности при реализации политики информационной безопасности?
5. Что такое операционная гарантированность и что она в себя включает?
6. Понятие класса безопасности и критерии отнесения ЗИС к определённому классу.
7. Механизмы информационной безопасности, описываемые в оценочных критериях

Тема 5. Критерии оценки безопасности информационных технологий.

1. Опишите иерархию сущностей в "Критериях оценки безопасности информационных технологий".
2. Назовите основные термины, описанные в "Критериях оценки безопасности информационных технологий".
3. Опишите структуру класса «приватность».
4. Опишите структуру класса «использование ресурсов».
5. Что такое требования доверия безопасности и для чего они нужны?
6. Что такое уровни доверия?
7. Какие существуют механизмы обеспечения безопасности в распределённых системах?

Тема 6. Руководящие документы ФСТЭК России.

1. Назовите основные документы, которыми руководствуются разработчики ЗИС?
2. Назовите основные классы безопасности, фигурирующие в документах ФСТЭК, и критерии отнесения систем к каждому из них.

## Список информационных источников

- 1) Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства. Москва: ДМК Пресс, 2010.- 544 с. (полнотекстовый доступ в базе Iqlib.ru)
- 2) Грибунин В.Г., Чудовский В.В. Комплексная система защиты информации на предприятии: учеб. пособие для студ. высш. учеб. заведений. – М.: Издательский дом «Академия», 2009. – 416 с.
- 3) Мельников В.П., Клейменов С.А., Петракова А.М. Информационная безопасность и защита информации: учеб. пособие для студ. учреждений высш. проф. образования. – 6-е изд., стер. – М.: Издательский центр «Академия», 2012. – 336 с.
- 4) Барабанова М.И., Кияев В.И. Информационные технологии: открытые системы, сети, безопасность в системах и сетях: Учебное пособие.– СПб.: Изд-во СПбГУЭФ, 2010.– 267 с.
- 5) Макаренко С.И. Информационная безопасность: учебное пособие для студентов вузов. – Ставрополь: СФ МГГУ им. М.А. Шолохова, 2009. – 372с.:ил.
- 6) Грушо А.А., Применко Э.А., Тимонина Е.Е. Теоретические основы компьютерной безопасности: учеб. Пособие для студентов высш. учеб. заведений – М.: Издательский центр «Академия», 2009 – 272 с.
- 7) Норткат Стивен, Новак Джуди. Обнаружение нарушений безопасности, 3-е издание,: Пер. с англ. – М.: Издательский дом «Вильямс», 2003. – 448 с.:ил.
- 8) Андрончик А.Н., Богданов В.В., Домуховский Н.А., Коллеров А.С., Синадский Н.И., Хорьков Д.А., Щербаков М.Ю. Защита информации в компьютерных сетях. Практический курс: учебное пособие. – Екатеринбург: УГТУ-УПИ, 2008. – 248 с..