**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ**

**Федеральное государственное бюджетное образовательное учреждение высшего образования**

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)

УТВЕРЖДАЮ
Проректор по учебной работе
_____ П. Е. Троян
«___» _____ 20__ г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

# Основы информационной безопасности сетей и систем

Уровень образования: **высшее образование - бакалавриат**
Направление подготовки (специальность): **11.03.02 Инфокоммуникационные технологии и системы связи**
Направленность (профиль): **Защищенные системы и сети связи**
Форма обучения: **очная**
Факультет: **РТФ, Радиотехнический факультет**
Кафедра: **РЗИ, Кафедра радиоэлектроники и защиты информации**
Курс: **4**
Семестр: **8**
Учебный план набора 2015 года

Распределение рабочего времени

| № | Виды учебной деятельности | 8 семестр | Всего | Единицы |
|---|---|---|---|---|
| 1 | Лекции | 22 | 22 | часов |
| 2 | Лабораторные работы | 32 | 32 | часов |
| 3 | Всего аудиторных занятий | 54 | 54 | часов |
| 4 | Самостоятельная работа | 54 | 54 | часов |
| 5 | Всего (без экзамена) | 108 | 108 | часов |
| 6 | Подготовка и сдача экзамена | 36 | 36 | часов |
| 7 | Общая трудоемкость | 144 | 144 | часов |
| | | 4.0 | 4.0 | З.Е |

Экзамен: 8 семестр
Курсовая работа (проект): 8 семестр

Томск 2017

Согласована на портале № 19109

Рассмотрена и одобрена на заседании кафедры
протокол № 5 от «28» 3 2017 г.

# ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 11.03.02 Инфокоммуникационные технологии и системы связи, утвержденного 06 марта 2015 года, рассмотрена и утверждена на заседании кафедры «___» _____ 20__ года, протокол №_____.

Разработчик:
доцент каф. РЗИ _____ А. П. Кшнянкин

Заведующий обеспечивающей каф.
РЗИ _____ А. С. Задорин

Рабочая программа согласована с факультетом, профилирующей и выпускающей кафедрами направления подготовки (специальности).

Декан РТФ _____ К. Ю. Попова

Заведующий выпускающей каф.
РЗИ _____ А. С. Задорин

Эксперт:

ведущий инженер каф. РЗИ РТФ _____ Ю. В. Зеленецкая

Согласована на портале № 19109

## 1. Цели и задачи дисциплины

### 1.1. Цели дисциплины

Целью преподавания дисциплины является формирование у студентов устойчивых основ знаний организации информационной безопасности сетей и систем, методов ее управления, а также приобретения при этом необходимых умений и навыков.

### 1.2. Задачи дисциплины

- Основными задачами изучения дисциплины являются:
- • изучение сущности и задач системы защиты информации (СЗИ) сетей и систем (СС);
- • изучение принципов организации и этапов разработки СЗИ СС, факторов, влияющих на организацию СЗИ СС;
- • определение и нормативное закрепление состава защищаемой информации; определение объектов защиты;
- • анализ и оценка угроз безопасности информации: выявление и оценка источников, способов и результатов дестабилизирующего воздействия на информацию;
- • определение потенциальных каналов и методов несанкционированного доступа к информации, определение возможностей несанкционированного доступа к защищаемой информации;
- • определение компонентов и условий функционирования СЗИ СС, разработка модели, технологического и организационного построения СЗИ СС;
- • кадровое, материально-техническое и нормативно-методическое обеспечение функционирования СЗИ СС;
- • назначение, структура и содержание управления СЗИ СС, изучение принципов и методы планирования, сущности и содержание контроля функционирования СЗИ СС;
- • изучение особенностей управления СЗИ СС в условиях чрезвычайных ситуаций;
- • изучение состава методов и моделей оценки эффективности СЗИ СС.
-

## 2. Место дисциплины в структуре ОПОП

Дисциплина «Основы информационной безопасности сетей и систем» (Б1.В.ДВ.10.1) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются следующие дисциплины: Информационные технологии, Техническая защита информации.

## 3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- ПК-13 способностью осуществлять подготовку типовых технических проектов на различные инфокоммуникационные объекты;
- ПК-15 умением разрабатывать и оформлять различную проектную и техническую документацию;

В результате изучения дисциплины студент должен:

- **знать** Основы организации и управления системой защиты информации сетей и систем.
- **уметь** На концептуальном и практическом уровне разрабатывать и внедрять системы защиты информации сетей и систем.
- **владеть** Навыками внедрения систем защиты информации сетей и систем.

## 4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 4.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

| Виды учебной деятельности | Всего часов | Семестры |
|---|---|---|
| | | 8 семестр |
| Аудиторные занятия (всего) | 54 | 54 |

Согласована на портале № 19109

| | | |
|---|---|---|
| Лекции | 22 | 22 |
| Лабораторные работы | 32 | 32 |
| Самостоятельная работа (всего) | 54 | 54 |
| Оформление отчетов по лабораторным работам | 28 | 28 |
| Проработка лекционного материала | 13 | 13 |
| Подготовка к практическим занятиям, семинарам | 13 | 13 |
| Всего (без экзамена) | 108 | 108 |
| Подготовка и сдача экзамена | 36 | 36 |
| Общая трудоемкость ч | 144 | 144 |
| Зачетные Единицы | 4.0 | 4.0 |

## 5. Содержание дисциплины

### 5.1. Разделы дисциплины и виды занятий

Разделы дисциплины и виды занятий приведены в таблице 5.1.

Таблица 5.1 – Разделы дисциплины и виды занятий

| Названия разделов дисциплины | Лекции | Лабораторные работы | Самостоятельная работа | Всего часов (без экзамена) | Формируемые компетенции |
|---|---|---|---|---|---|
| 8 семестр | | | | | |
| 1 Введение. | 1 | 0 | 3 | 4 | ПК-13, ПК-15 |
| 2 Содержание и этапы проведения работ по организации системы защиты информации сетей и систем (СЗИ СС). | 4 | 0 | 3 | 7 | ПК-13, ПК-15 |
| 3 Определение компонентов СЗИ СС. | 3 | 0 | 3 | 6 | ПК-13, ПК-15 |
| 4 Технология определения и классификации состава и защищенности информации. | 2 | 0 | 3 | 5 | ПК-13, ПК-15 |
| 5 Построение системы защиты информации сетей и систем. | 3 | 0 | 4 | 7 | ПК-13, ПК-15 |
| 6 Управление системой защиты информации сетей и систем. | 2 | 0 | 4 | 6 | ПК-13, ПК-15 |
| 7 Служба защиты информации. | 3 | 0 | 2 | 5 | ПК-13, ПК-15 |
| 8 Особенностей управления СЗИ СС в условиях чрезвычайных ситуаций. | 2 | 0 | 2 | 4 | ПК-13, ПК-15 |
| 9 Состав методов и моделей оценки эффективности СЗИ СС. | 2 | 0 | 2 | 4 | ПК-13, ПК-15 |
| 10 Экзамен. | 0 | 32 | 28 | 60 | ПК-13, ПК-15 |
| Итого за семестр | 22 | 32 | 54 | 108 | |
| Итого | 22 | 32 | 54 | 108 | |

Согласована на портале № 19109

**5.2. Содержание разделов дисциплины (по лекциям)**

Содержание разделов дисциплин (по лекциям) приведено в таблице 5.2.

Таблица 5.2 - Содержание разделов дисциплин (по лекциям)

| Названия разделов | Содержание разделов дисциплины по лекциям | Трудоемкость, ч | Формируемые компетенции |
|---|---|---|---|
| 8 семестр | | | |
| 1 Введение. | Цели, структура и задачи курса. Взаимосвязь курса с другими дисциплинами, системный характер научно-технических проблем при решении задач по организации и управлению комплексной системы защиты информации на предприятии. Специфика курса. | 1 | ПК-13, ПК-15 |
| | Итого | 1 | |
| 2 Содержание и этапы проведения работ по организации системы защиты информации сетей и систем (СЗИ СС). | Цели системы защиты информации сетей и систем (СЗИ СС) и способы ее обеспечения. Системный метод при решении задач обеспечения СЗИ СС.Определение возможных каналов утечки информации. Определение объектов и элементов защиты.Оценка угроз технических разведок (ТР) и других источников угроз безопасности защищаемой информации. Выбор методов и средств защиты информации | 4 | ПК-13, ПК-15 |
| | Итого | 4 | |
| 3 Определение компонентов СЗИ СС. | Правовая защита информации. Законодательная база РФ по защите информации (ЗИ). Сертификация и лицензирование. Правовые нормы, методы и средства защиты охраняемой информации в РФ. Система юридической ответственности за нарушение норм защиты государственной, служебной и коммерческой тайны в РФ. Правовые основы выявления и предупреждения утечки охраняемой информации.Техническая защита информации. Виды информации, защищаемой техническими средствами. Демаскирующие признаки объектов защиты и их классификация. Каналы утечки информации (оптический, акустический, радиоэлектронный). Методы защиты от несанкционированного перехвата речевой, визуальной, оптической, радиоэлектронной информации. Радиомониторинг. Криптографическая защита информации. | 3 | ПК-13, ПК-15 |

Согласована на портале № 19109

| | | | |
|---|---|---|---|
| | Средства и методы.Физическая защита информации. Принципы, силы, средства и условия организационной защиты информации. Организация внутриобъектового и пропускного режима предприятия. Организация системы охраны предприятия (физическая охрана, пожарная и охранная сигнализация, охранное телевидение, системы ограничения доступа). Организация аналитической работы по предупреждению перехвата конфиденциальной информации. Направления и методы работы с персоналом, обладающим конфиденциальной информацией. Определение политики защиты информации на предприятии. Особенности организации комплексной защиты информации, отнесенной в установленном порядке к государственной тайне. Определение сил и средств, необходимых для защиты информации. | | |
| | Итого | 3 | |
| 4 Технология определения и классификации состава и защищенности информации. | Охраняемые сведения и объекты защиты.Особенности отнесения сведений, составляющих служебную, конфиденциальную, коммерческую и государственную тайну к различным степеням и категориям доступа. | 2 | ПК-13, ПК-15 |
| | Итого | 2 | |
| 5 Построение системы защиты информации сетей и систем. | Разработка моделей систем защиты информации телекоммуникационных систем. Определение и разработка состава нормативно-технической документации (НТД) по обеспечению защиты информации, материально-техническое и нормативно-методическое обеспечение функционирования СЗИ ТКС.Архитектурное построение системы защиты информации. | 3 | ПК-13, ПК-15 |
| | Итого | 3 | |
| 6 Управление системой защиты информации сетей и систем. | Структура и содержание технологии управления системы защиты информации телекоммуникационных систем. Планирование и оперативное управление системой ЗИ, управление СЗИ ТКС в условиях чрезвычайных ситуаций.Анализ надежности функционирования системы защиты информации телекоммуникационных систем. | 2 | ПК-13, ПК-15 |
| | Итого | 2 | |

Согласована на портале № 19109

| | | | |
|---|---|---|---|
| 7 Служба защиты информации. | Организация службы защиты информации (СлЗИ) и организационное проектирование деятельности СлЗИ. Порядок создания СлЗИ, состав нормативных документов, регламентирующих деятельность служб защиты информации. | 3 | ПК-13, ПК-15 |
| | Итого | 3 | |
| 8 Особенностей управления СЗИ СС в условиях чрезвычайных ситуаций. | Определение и понятие чрезвычайной ситуации. Аспекты обеспечения условий непрерывности в информационной сфере организации. Роль совета директоров и исполнительных органов организации. Идентификация недостатков. Непрерывность сервисов в изменяющейся среде и обеспечение СЗИ ТКС. Реорганизация и ликвидация СЗИ. Определение должностного состава и численности СЗИ. Планирование и отчетность о деятельности СЗИ ТКС.Понимание рисков непрерывности и их влияние на цели деятельности организации и восстановление защитных мер СЗИ ТКС.Восстановление после чрезвычайной ситуации функций и механизмов СЗИ ТКС. организации. Организационная основа процессов восстановления, вопросы системы менеджмента информационной безопасности (ИБ) организации и менеджмента непрерывности бизнеса. Восстановление и обеспечение функционирования процессов системы менеджмента ИБ организации. | 2 | ПК-13, ПК-15 |
| | Итого | 2 | |
| 9 Состав методов и моделей оценки эффективности СЗИ СС. | Основные термины и определения, характеризующие эффективность системы защиты информации. Содержание и особенности методологии оценки эффективности СЗИ ТКС.Основные модели оценки эффективности СЗИ ТКС. | 2 | ПК-13, ПК-15 |
| | Итого | 2 | |
| Итого за семестр | | 22 | |

**5.3. Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами**

Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами представлены в таблице 5.3.

Таблица 5.3 - Разделы дисциплины и междисциплинарные связи

| Наименование дисциплин | № разделов данной дисциплины, для которых необходимо изучение обеспечивающих и обеспечиваемых дисциплин |
|---|---|

Согласована на портале № 19109

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| Предшествующие дисциплины | | | | | | | | | | |
| 1 Информационные технологии | | + | + | + | + | | | | | |
| 2 Техническая защита информации | | + | + | + | + | | | | + | |

**5.4. Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий**

Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий представлено в таблице 5.4

Таблица 5.4 – Соответствие компетенций и видов занятий, формируемых при изучении дисциплины

| Компетенции | Виды занятий | | | Формы контроля |
|---|---|---|---|---|
| | Лекции | Лабораторные работы | Самостоятельная работа | |
| ПК-13 | + | + | + | Экзамен, Конспект самоподготовки, Отчет по лабораторной работе, Опрос на занятиях, Защита курсовых проектов (работ), Выступление (доклад) на занятии, Отчет по курсовой работе |
| ПК-15 | + | + | + | Экзамен, Конспект самоподготовки, Отчет по лабораторной работе, Опрос на занятиях, Защита курсовых проектов (работ), Выступление (доклад) на занятии, Отчет по курсовой работе |

## 6. Интерактивные методы и формы организации обучения

Не предусмотрено РУП

## 7. Лабораторные работы

Наименование лабораторных работ приведено в таблице 7.1.

Таблица 7. 1 – Наименование лабораторных работ

| Названия разделов | Наименование лабораторных работ | Трудоемкость, ч | Формируемые компетенции |
|---|---|---|---|
| 8 семестр | | | |
| 10 Экзамен. | Система защиты информации от несанкционированного доступа | 5 | ПК-13, ПК-15 |

Согласована на портале № 19109

| | | | |
|---|---|---|---|
| | SecretNet. | | |
| | Система защиты информации от несанкционированного доступа Dallas Lock. | 5 | |
| | Система защиты информации от несанкционированного доступа Страж NT. | 6 | |
| | DLP-решения по защите информации в информационных системах. | 4 | |
| | Защита информации от программных воздействий на базе антивируса Dr.Web. | 6 | |
| | Защита информации от программных воздействий на базе антивируса KAV. | 6 | |
| | Итого | 32 | |
| Итого за семестр | | 32 | |

## 8. Практические занятия (семинары)

Не предусмотрено РУП

## 9. Самостоятельная работа

Виды самостоятельной работы, трудоемкость и формируемые компетенции представлены в таблице 9.1.

Таблица 9.1 - Виды самостоятельной работы, трудоемкость и формируемые компетенции

| Названия разделов | Виды самостоятельной работы | Трудоемкость, ч | Формируемые компетенции | Формы контроля |
|---|---|---|---|---|
| 8 семестр | | | | |
| 1 Введение. | Подготовка к практическим занятиям, семинарам | 2 | ПК-13, ПК-15 | Выступление (доклад) на занятии, Конспект самоподготовки, Опрос на занятиях, Экзамен |
| | Проработка лекционного материала | 1 | | |
| | Итого | 3 | | |
| 2 Содержание и этапы проведения работ по организации системы защиты информации сетей и систем (СЗИ СС). | Подготовка к практическим занятиям, семинарам | 2 | ПК-13, ПК-15 | Выступление (доклад) на занятии, Конспект самоподготовки, Опрос на занятиях, Экзамен |
| | Проработка лекционного материала | 1 | | |
| | Итого | 3 | | |
| 3 Определение компонентов СЗИ СС. | Подготовка к практическим занятиям, семинарам | 2 | ПК-13, ПК-15 | Выступление (доклад) на занятии, Конспект самоподготовки, Опрос на занятиях, Экзамен |
| | Проработка лекционного материала | 1 | | |

Согласована на портале № 19109

| | | | | |
|---|---|---|---|---|
| | Итого | 3 | | |
| 4 Технология определения и классификации состава и защищенности информации. | Подготовка к практическим занятиям, семинарам | 2 | ПК-13, ПК-15 | Выступление (доклад) на занятии, Конспект самоподготовки, Опрос на занятиях, Экзамен |
| | Проработка лекционного материала | 1 | | |
| | Итого | 3 | | |
| 5 Построение системы защиты информации сетей и систем. | Подготовка к практическим занятиям, семинарам | 2 | ПК-13, ПК-15 | Выступление (доклад) на занятии, Конспект самоподготовки, Опрос на занятиях, Экзамен |
| | Проработка лекционного материала | 2 | | |
| | Итого | 4 | | |
| 6 Управление системой защиты информации сетей и систем. | Подготовка к практическим занятиям, семинарам | 3 | ПК-13, ПК-15 | Выступление (доклад) на занятии, Конспект самоподготовки, Опрос на занятиях, Экзамен |
| | Проработка лекционного материала | 1 | | |
| | Итого | 4 | | |
| 7 Служба защиты информации. | Проработка лекционного материала | 2 | ПК-13, ПК-15 | Конспект самоподготовки, Опрос на занятиях, Экзамен |
| | Итого | 2 | | |
| 8 Особенностей управления СЗИ СС в условиях чрезвычайных ситуаций. | Проработка лекционного материала | 2 | ПК-13, ПК-15 | Конспект самоподготовки, Опрос на занятиях, Экзамен |
| | Итого | 2 | | |
| 9 Состав методов и моделей оценки эффективности СЗИ СС. | Проработка лекционного материала | 2 | ПК-13, ПК-15 | Конспект самоподготовки, Опрос на занятиях, Экзамен |
| | Итого | 2 | | |
| 10 Экзамен. | Оформление отчетов по лабораторным работам | 28 | | Отчет по лабораторной работе, Экзамен |
| | Итого | 28 | | |
| Итого за семестр | | 54 | | |
| | Подготовка и сдача экзамена / зачета | 36 | | Экзамен |
| Итого | | 90 | | |

## 10. Курсовая работа (проект)

### 10.1 Темы курсовых работ

Примерная тематика курсовых работ (проектов):

– Разработка подсистемы технической защиты выделенного помещения предприятий сетей и систем.

– Разработка подсистемы технической защиты объекта вычислительной техники.

– Разработка подсистемы технической защиты персональных данных, обрабатываемых в информационной системе предприятия.

Согласована на портале № 19109

## 11. Рейтинговая система для оценки успеваемости студентов

### 11.1. Балльные оценки для элементов контроля

Таблица 11.1 – Балльные оценки для элементов контроля

| Элементы учебной деятельности | Максимальный балл на 1-ую КТ с начала семестра | Максимальный балл за период между 1КТ и 2КТ | Максимальный балл за период между 2КТ и на конец семестра | Всего за семестр |
|---|---|---|---|---|
| 8 семестр | | | | |
| Выступление (доклад) на занятии | 5 | 5 | 10 | 20 |
| Конспект самоподготовки | 3 | 5 | 7 | 15 |
| Опрос на занятиях | 3 | 5 | 7 | 15 |
| Отчет по лабораторной работе | 5 | 5 | 10 | 20 |
| Итого максимум за период | 16 | 20 | 34 | 70 |
| Экзамен | | | | 30 |
| Нарастающим итогом | 16 | 36 | 70 | 100 |

### 11.2. Пересчет баллов в оценки за контрольные точки

Пересчет баллов в оценки за контрольные точки представлен в таблице 11.2.

Таблица 11. 2 – Пересчет баллов в оценки за контрольные точки

| Баллы на дату контрольной точки | Оценка |
|---|---|
| ≥ 90% от максимальной суммы баллов на дату КТ | 5 |
| От 70% до 89% от максимальной суммы баллов на дату КТ | 4 |
| От 60% до 69% от максимальной суммы баллов на дату КТ | 3 |
| < 60% от максимальной суммы баллов на дату КТ | 2 |

### 11.3. Пересчет суммы баллов в традиционную и международную оценку

Пересчет суммы баллов в традиционную и международную оценку представлен в таблице 11.3.

Таблица 11. 3 – Пересчет суммы баллов в традиционную и международную оценку

| Оценка (ГОС) | Итоговая сумма баллов, учитывает успешно сданный экзамен | Оценка (ECTS) |
|---|---|---|
| 5 (отлично) (зачтено) | 90 - 100 | A (отлично) |
| 4 (хорошо) (зачтено) | 85 - 89 | B (очень хорошо) |
| | 75 - 84 | C (хорошо) |
| | 70 - 74 | D (удовлетворительно) |
| 3 (удовлетворительно) (зачтено) | 65 - 69 | |
| | 60 - 64 | E (посредственно) |
| 2 (неудовлетворительно) (не зачтено) | Ниже 60 баллов | F (неудовлетворительно) |

Согласована на портале № 19109

## 12. Учебно-методическое и информационное обеспечение дисциплины

### 12.1. Основная литература

1. Защита информации в инфокоммуникационных системах и сетях: Учебное пособие / Голиков А. М. - 2015. 284 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/5262, дата обращения: 27.04.2017.

### 12.2. Дополнительная литература

1. Защита информации от утечки по техническим каналам: Учебное пособие / Голиков А. М. - 2015. 256 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/5263, дата обращения: 27.04.2017.

### 12.3 Учебно-методические пособия

#### 12.3.1. Обязательные учебно-методические пособия

1. Защита информации в инфокоммуникационных системых и сетях: Учебное пособие для практических и семинарских занятий (Часть 1) / Голиков А. М. - 2015. 103 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/5330, дата обращения: 27.04.2017.
2. Защита информации в инфокоммуникационных системах и сетях: Сборник лабораторных работ / Голиков А. М. - 2015. 373 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/5378, дата обращения: 27.04.2017.
3. Информационные технологии в управлении качеством и защита информации: Методические рекомендации к курсовым работам и организации самостоятельной работы студентов / Годенова Е. Г. - 2011. 35 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/290, дата обращения: 27.04.2017.

#### 12.3.2 Учебно-методические пособия для лиц с ограниченными возможностями здоровья

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся из числа инвалидов предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации.

**Для лиц с нарушениями зрения:**

- в форме электронного документа;
- в печатной форме увеличенным шрифтом.

**Для лиц с нарушениями слуха:**

- в форме электронного документа;
- в печатной форме.

**Для лиц с нарушениями опорно-двигательного аппарата:**

- в форме электронного документа;
- в печатной форме.

### 12.4. Базы данных, информационно-справочные, поисковые системы и требуемое программное обеспечение

1. 1. Базовые законодательные и нормативно-правовые документы РФ в области защиты
2. информации. [Электронный ресурс]. - Режим доступа: http://www.consultant.ru, (дата обращения 25.03.2017);
3. 2. Научно-образовательный портал ТУСУРа, https://edu.tusur.ru

## 13. Материально-техническое обеспечение дисциплины

### 13.1. Общие требования к материально-техническому обеспечению дисциплины

#### 13.1.1. Материально-техническое обеспечение для лекционных занятий

Лекционные, практические и лабораторные занятия проводятся в специализированных аудиториях кафедры РЗИ. Для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используется учебная аудитория, с количеством посадочных мест не менее 22-24, оборудованная доской и стандартной учебной мебелью. Имеются наглядные пособия в виде презентаций по лекционным разделам дисциплины.

#### 13.1.2. Материально-техническое обеспечение для лабораторных работ

Для проведения лабораторных занятий используется учебно-исследовательская вычисли-

Согласована на портале № 19109

тельная лаборатория, расположенная по адресу 634034, Томская область, г. Томск, Вершинина улица, д. 47, 4 этаж, ауд. 407, 412, 416. Состав оборудования: Учебная мебель; Экран с электроприводом DRAPER BARONET – 1 шт.; Мультимедийный проектор TOSHIBA – 1 шт.; Компьютеры класса не ниже Intel Pentium G3220 (3.0GHz/4Mb)/4GB RAM/ 500GB с широкополосным доступом в Internet, с мониторами типа Samsung 18.5" S19C200N– 18 шт.; Используется лицензионное программное обеспечение, пакеты версией не ниже: Microsoft Windows XP Professional with SP3; Visual Studio 2008 EE with SP1; Microsoft Office Visio 2010; Microsoft SQL-Server 2005; Matlab v6.5

**13.1.3. Материально-техническое обеспечение для самостоятельной работы**

Для самостоятельной работы используется учебная аудитория (компьютерный класс), расположенная по адресу 634034, г. Томск, ул. Вершинина, 47, 4 этаж, ауд. 407,412, 416. Состав оборудования: учебная мебель; компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8ГГц. - 4 шт.; компьютеры подключены к сети ИНТЕРНЕТ и обеспечивают доступ в электронную информационно-образовательную среду университета.

**13.2. Материально-техническое обеспечение дисциплины для лиц с ограниченными возможностями здоровья**

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения.

При обучении студентов **с нарушениями слуха** предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах для студентов с нарушениями слуха, мобильной системы обучения для студентов с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой обучаются студенты с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При обучении студентов **с нарушениями зрениями** предусмотрено использование в лекционных и учебных аудиториях возможности просмотра удаленных объектов (например, текста на доске или слайда на экране) при помощи видеоувеличителей для удаленного просмотра.

При обучении студентов **с нарушениями опорно-двигательного аппарата** используются альтернативные устройства ввода информации и другие технические средства приема/передачи учебной информации в доступных формах для студентов с нарушениями опорно-двигательного аппарата, мобильной системы обучения для людей с инвалидностью.

**14. Фонд оценочных средств**

**14.1. Основные требования к фонду оценочных средств и методические рекомендации**

Фонд оценочных средств и типовые контрольные задания, используемые для оценки сформированности и освоения закрепленных за дисциплиной компетенций при проведении текущей, промежуточной аттестации по дисциплине приведен в приложении к рабочей программе.

**14.2 Требования к фонду оценочных средств для лиц с ограниченными возможностями здоровья**

Для студентов с инвалидностью предусмотрены дополнительные оценочные средства, перечень которых указан в таблице.

**Таблица 14 – Дополнительные средства оценивания для студентов с инвалидностью**

| Категории студентов | Виды дополнительных оценочных средств | Формы контроля и оценки результатов обучения |
|---|---|---|
| С нарушениями слуха | Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы | Преимущественно письменная проверка |
| С нарушениями зрения | Собеседование по вопросам к зачету, опрос по терминам | Преимущественно устная проверка (индивидуально) |
| С нарушениями опорно-двигательного | Решение дистанционных тестов, контрольные работы, письменные самостоятельные работы, вопросы к | Преимущественно дистанционными методами |

Согласована на портале № 19109

| | | |
|---|---|---|
| аппарата | зачету | |
| С ограничениями по общемедицинским показаниям | Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы, устные ответы | Преимущественно проверка методами, исходя из состояния обучающегося на момент проверки |

### 14.3 Методические рекомендации по оценочным средствам для лиц с ограниченными возможностями здоровья

Для студентов с ОВЗ предусматривается доступная форма предоставления заданий оценочных средств, а именно:

- в печатной форме;
- в печатной форме с увеличенным шрифтом;
- в форме электронного документа;
- методом чтения ассистентом задания вслух;
- предоставление задания с использованием сурдоперевода.

Студентам с инвалидностью увеличивается время на подготовку ответов на контрольные вопросы. Для таких студентов предусматривается доступная форма предоставления ответов на задания, а именно:

- письменно на бумаге;
- набор ответов на компьютере;
- набор ответов с использованием услуг ассистента;
- представление ответов устно.

Процедура оценивания результатов обучения инвалидов по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

**Для лиц с нарушениями зрения:**

- в форме электронного документа;
- в печатной форме увеличенным шрифтом.

**Для лиц с нарушениями слуха:**

- в форме электронного документа;
- в печатной форме.

**Для лиц с нарушениями опорно-двигательного аппарата:**

- в форме электронного документа;
- в печатной форме.

При необходимости для обучающихся с инвалидностью процедура оценивания результатов обучения может проводиться в несколько этапов.

Согласована на портале № 19109

**Приложение 1**

**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ**

**Федеральное государственное бюджетное образовательное учреждение высшего образования**

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)

УТВЕРЖДАЮ
Проректор по учебной работе
_____ П. Е. Троян
«___» _____ 20__ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

# Основы информационной безопасности сетей и систем

Уровень образования: **высшее образование - бакалавриат**
Направление подготовки (специальность): **11.03.02 Инфокоммуникационные технологии и системы связи**
Направленность (профиль): **Защищенные системы и сети связи**
Форма обучения: **очная**
Факультет: **РТФ, Радиотехнический факультет**
Кафедра: **РЗИ, Кафедра радиоэлектроники и защиты информации**
Курс: **4**
Семестр: **8**

Учебный план набора 2015 года

Разработчик:
- доцент каф. РЗИ А. П. Кшнянкин

Экзамен: 8 семестр
Курсовая работа (проект): 8 семестр

Томск 2017

Согласована на портале № 19109

## 1. Введение

Фонд оценочных средств (ФОС) является приложением к рабочей программе дисциплины (практики) и представляет собой совокупность контрольно-измерительных материалов (типовые задачи (задания), контрольные работы, тесты и др.) и методов их использования, предназначенных для измерения уровня достижения студентом установленных результатов обучения.

ФОС по дисциплине (практике) используется при проведении текущего контроля успеваемости и промежуточной аттестации студентов.

Перечень закрепленных за дисциплиной (практикой) компетенций приведен в таблице 1.

Таблица 1 – Перечень закрепленных за дисциплиной компетенций

| Код | Формулировка компетенции | Этапы формирования компетенций |
|---|---|---|
| ПК-15 | умением разрабатывать и оформлять различную проектную и техническую документацию | Должен знать Основы организации и управления системой защиты информации сетей и систем.;<br>Должен уметь На концептуальном и практическом уровне разрабатывать и внедрять системы защиты информации сетей и систем. ;<br>Должен владеть Навыками внедрения систем защиты информации сетей и систем. ; |
| ПК-13 | способностью осуществлять подготовку типовых технических проектов на различные инфокоммуникационные объекты | |

Общие характеристики показателей и критериев оценивания компетенций на всех этапах приведены в таблице 2.

Таблица 2 – Общие характеристики показателей и критериев оценивания компетенций по этапам

| Показатели и критерии | Знать | Уметь | Владеть |
|---|---|---|---|
| Отлично (высокий уровень) | Обладает фактическими и теоретическими знаниями в пределах изучаемой области с пониманием границ применимости | Обладает диапазоном практических умений, требуемых для развития творческих решений, абстрагирования проблем | Контролирует работу, проводит оценку, совершенствует действия работы |
| Хорошо (базовый уровень) | Знает факты, принципы, процессы, общие понятия в пределах изучаемой области | Обладает диапазоном практических умений, требуемых для решения определенных проблем в области исследования | Берет ответственность за завершение задач в исследовании, приспосабливает свое поведение к обстоятельствам в решении проблем |
| Удовлетворительно (пороговый уровень) | Обладает базовыми общими знаниями | Обладает основными умениями, требуемыми для выполнения простых задач | Работает при прямом наблюдении |

## 2 Реализация компетенций

### 2.1 Компетенция ПК-15

ПК-15: умением разрабатывать и оформлять различную проектную и техническую документацию.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 3.

Таблица 3 – Этапы формирования компетенции и используемые средства оценивания

| Состав | Знать | Уметь | Владеть |
|---|---|---|---|
| Содержание эта- | Основы организации и | На концептуальном и | Навыками внедрения си- |

Согласована на портале № 19109

| | | | |
|---|---|---|---|
| пов | управления системой защиты информации сетей и систем. | практическом уровне разрабатывать и внедрять системы защиты информации сетей и систем. | стем защиты информации сетей и систем. |
| Виды занятий | • Лабораторные работы;<br>• Лекции;<br>• Самостоятельная работа; | • Лабораторные работы;<br>• Лекции;<br>• Самостоятельная работа; | • Лабораторные работы;<br>• Самостоятельная работа; |
| Используемые средства оценивания | • Конспект самоподготовки;<br>• Отчет по лабораторной работе;<br>• Опрос на занятиях;<br>• Выступление (доклад) на занятии;<br>• Отчет по курсовой работе;<br>• Экзамен;<br>• Курсовая работа (проект); | • Конспект самоподготовки;<br>• Отчет по лабораторной работе;<br>• Опрос на занятиях;<br>• Защита курсовых проектов (работ);<br>• Выступление (доклад) на занятии;<br>• Отчет по курсовой работе;<br>• Экзамен;<br>• Курсовая работа (проект); | • Отчет по лабораторной работе;<br>• Защита курсовых проектов (работ);<br>• Выступление (доклад) на занятии;<br>• Отчет по курсовой работе;<br>• Экзамен;<br>• Курсовая работа (проект); |

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 4.

Таблица 4 – Показатели и критерии оценивания компетенции на этапах

| Состав | Знать | Уметь | Владеть |
|---|---|---|---|
| Отлично (высокий уровень) | • Обладает фактическими и теоретическими знаниями в пределах изучаемой области с пониманием границ применимости.; | • Обладает диапазоном практических умений, требуемых для развития творческих решений, абстрагирования проблем.; | • Контролирует работу, проводит оценку, совершенствует действия работы.; |
| Хорошо (базовый уровень) | • Знает факты, принципы, процессы, общие понятия в пределах изучаемой области.; | • Обладает диапазоном практических умений, требуемых для решения определенных проблем в области исследования .; | • Берет ответственность за завершение задач в исследовании, приспосабливает свое поведение к обстоятельствам в решении проблем. ; |
| Удовлетворительно (пороговый уровень) | • Обладает базовыми общими знаниями.; | • Обладает основными умениями, требуемыми для выполнения простых задач.; | • Работает при прямом наблюдении.; |

**2.2 Компетенция ПК-13**

ПК-13: способностью осуществлять подготовку типовых технических проектов на различные инфокоммуникационные объекты.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания пред-

Согласована на портале № 19109

ставлены в таблице 5.

Таблица 5 – Этапы формирования компетенции и используемые средства оценивания

| Состав | Знать | Уметь | Владеть |
|---|---|---|---|
| Содержание этапов | Основы организации и управления системой защиты информации сетей и систем. | На концептуальном и практическом уровне разрабатывать и внедрять системы защиты информации сетей и систем. | Навыками внедрения систем защиты информации сетей и систем. |
| Виды занятий | • Лабораторные работы;<br>• Лекции;<br>• Самостоятельная работа; | • Лабораторные работы;<br>• Лекции;<br>• Самостоятельная работа; | • Лабораторные работы;<br>• Самостоятельная работа; |
| Используемые средства оценивания | • Конспект самоподготовки;<br>• Отчет по лабораторной работе;<br>• Опрос на занятиях;<br>• Выступление (доклад) на занятии;<br>• Отчет по курсовой работе;<br>• Экзамен;<br>• Курсовая работа (проект); | • Конспект самоподготовки;<br>• Отчет по лабораторной работе;<br>• Опрос на занятиях;<br>• Защита курсовых проектов (работ);<br>• Выступление (доклад) на занятии;<br>• Отчет по курсовой работе;<br>• Экзамен;<br>• Курсовая работа (проект); | • Отчет по лабораторной работе;<br>• Защита курсовых проектов (работ);<br>• Выступление (доклад) на занятии;<br>• Отчет по курсовой работе;<br>• Экзамен;<br>• Курсовая работа (проект); |

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 6.

Таблица 6 – Показатели и критерии оценивания компетенции на этапах

| Состав | Знать | Уметь | Владеть |
|---|---|---|---|
| Отлично (высокий уровень) | • Обладает фактическими и теоретическими знаниями в пределах изучаемой области с пониманием границ применимости.; | • Обладает диапазоном практических умений, требуемых для развития творческих решений, абстрагирования проблем.; | • Контролирует работу, проводит оценку, совершенствует действия работы.; |
| Хорошо (базовый уровень) | • Знает факты, принципы, процессы, общие понятия в пределах изучаемой области.; | • Обладает диапазоном практических умений, требуемых для решения определенных проблем в области исследования. ; | • Берет ответственность за завершение задач в исследовании, приспосабливает свое поведение к обстоятельствам в решении проблем. ; |
| Удовлетворительно (пороговый уровень) | • Обладает базовыми общими знаниями.; | • Обладает основными умениями, требуемыми для выполнения простых задач.; | • Работает при прямом наблюдении.; |

Согласована на портале № 19109

## 3 Типовые контрольные задания

Для реализации вышеперечисленных задач обучения используются типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы, в следующем составе.

### 3.1 Вопросы на самоподготовку

- 1. Системный подход. Определение и понятие.
- 2. Система обеспечения информационной безопасности организации. Определение и понятие.
- 3. Система защиты информации организации. Определение и понятие.
- 4. Объект защиты информации. Определение и понятие.
- 5. Защищаемая информация. Определение и понятие.
- 6. Защита информации. Определение и понятие.
- 7. Организация защиты информации. Определение и понятие.
- 8. Техника защиты информации. Определение и понятие.
- 9. Контроль защиты информации. Цели и понятие.
- 10. Контролируемая зона. Определение и понятие.
- 11. Технический канал утечки информации (ТКУИ), виды ТКУИ. Определение, физический смысл.
- 12.Подсистема технической защиты информации объектов информатизации, предназначенных для
- ведения конфиденциальных переговоров. Модель и понятие.
- 13. Подсистема технической защиты информации объектов информатизации, реализующих
- информационные технологии с использованием технических средств и систем. Модель и
- понятие.
- 14. Модель угроз подсистемы технической защиты информации объектов информатизации,
- реализующих информационные технологии с использованием технических средств и систем.
- 15. Модель угроз подсистемы технической защиты информации объектов информатизации,
- предназначенных для ведения конфиденциальных переговоров.
- 16. Уязвимости системы обеспечения ИБ организации. Определение и понятие.
- 17. Нарушитель ИБ организации. Определение и понятие.
- 18. Модель технической реализации ПТЗИ ОИ.
- 19. Защита информации от несанкционированного доступа (НСД). Определение и понятие.
- 20. Основа концепции защиты СВТ и АС от НСД к информации.
- 21. Классификация АС. Цели и основные понятия.
- 22. Аттестация объектов информатизации. Понятие.
- 23. Алгоритм приобретения ПЭВМ в защищенном исполнении.
- 24. Доктрина ИБ РФ. Общие положения.

### 3.2 Темы опросов на занятиях

- Цели, структура и задачи курса. Взаимосвязь курса с другими дисциплинами, системный характер научно-технических проблем при решении задач по организации и управлению комплексной системы защиты информации на предприятии. Специфика курса.
- Цели системы защиты информации сетей и систем (СЗИ СС) и способы ее обеспечения. Системный метод при решении задач обеспечения СЗИ СС.
- Определение возможных каналов утечки информации. Определение объектов и элементов защиты.

Согласована на портале № 19109

– Оценка угроз технических разведок (ТР) и других источников угроз безопасности защищаемой информации.

– Выбор методов и средств защиты информации

– Правовая защита информации. Законодательная база РФ по защите информации (ЗИ). Сертификация и лицензирование. Правовые нормы, методы и средства защиты охраняемой информации в РФ. Система юридической ответственности за нарушение норм защиты государственной, служебной и коммерческой тайны в РФ. Правовые основы выявления и предупреждения утечки охраняемой информации.

– Техническая защита информации.

– Виды информации, защищаемой техническими средствами. Демаскирующие признаки объектов защиты и их классификация. Каналы утечки информации (оптический, акустический, радиоэлектронный). Методы защиты от несанкционированного перехвата речевой, визуальной, оптической, радиоэлектронной информации. Радиомониторинг.

– Криптографическая защита информации. Средства и методы.

– Физическая защита информации. Принципы, силы, средства и условия организационной защиты информации. Организация внутриобъектового и пропускного режима предприятия. Организация системы охраны предприятия (физическая охрана, пожарная и охранная сигнализация, охранное телевидение, системы ограничения доступа).

– Организация аналитической работы по предупреждению перехвата конфиденциальной информации. Направления и методы работы с персоналом, обладающим конфиденциальной информацией. Определение политики защиты информации на предприятии.

– Особенности организации комплексной защиты информации, отнесенной в установленном порядке к государственной тайне. Определение сил и средств, необходимых для защиты информации.

– Охраняемые сведения и объекты защиты.

– Особенности отнесения сведений, составляющих служебную, конфиденциальную, коммерческую и государственную тайну к различным степеням и категориям доступа.

– Разработка моделей систем защиты информации телекоммуникационных систем. Определение и разработка состава нормативно-технической документации (НТД) по обеспечению защиты информации, материально-техническое и нормативно-методическое обеспечение функционирования СЗИ ТКС.

– Архитектурное построение системы защиты информации.

– Структура и содержание технологии управления системы защиты информации телекоммуникационных систем. Планирование и оперативное управление системой ЗИ, управление СЗИ ТКС в условиях чрезвычайных ситуаций.

– Анализ надежности функционирования системы защиты информации телекоммуникационных систем.

– Организация службы защиты информации (СлЗИ) и организационное проектирование деятельности СлЗИ.

– Порядок создания СлЗИ, состав нормативных документов, регламентирующих деятельность служб защиты информации.

– Определение и понятие чрезвычайной ситуации. Аспекты обеспечения условий непрерывности в информационной сфере организации. Роль совета директоров и исполнительных органов организации. Идентификация недостатков. Непрерывность сервисов в изменяющейся среде и обеспечение СЗИ ТКС. Реорганизация и ликвидация СЗИ. Определение должностного состава и численности СЗИ. Планирование и отчетность о деятельности СЗИ ТКС.

– Понимание рисков непрерывности и их влияние на цели деятельности организации и восстановление защитных мер СЗИ ТКС.

– Восстановление после чрезвычайной ситуации функций и механизмов СЗИ ТКС. организации. Организационная основа процессов восстановления, вопросы системы менеджмента информационной безопасности (ИБ) организации и менеджмента непрерывности бизнеса. Восстановление и обеспечение функционирования процессов системы менеджмента ИБ организации.

– Основные термины и определения, характеризующие эффективность системы защиты

Согласована на портале № 19109

информации. Содержание и особенности методологии оценки эффективности СЗИ ТКС.

– Основные модели оценки эффективности СЗИ ТКС.

### 3.3 Темы докладов

– 1. Особенности разработки подсистемы технической защиты объекта вычислительной техники организации.

– 2. Особенности разработки подсистемы технической защиты защищаемого помещения организации.

– 3. Особенности разработки подсистемы технической защиты персональных данных, обрабатываемых в информационной системе организации.

### 3.4 Экзаменационные вопросы

– 1. Системный подход. Определение и понятие.

– 2. Система обеспечения информационной безопасности организации. Определение и понятие.

– 3. Система защиты информации организации. Определение и понятие.

– 4. Объект защиты информации. Определение и понятие.

– 5. Защищаемая информация. Определение и понятие.

– 6. Защита информации. Определение и понятие.

– 7. Организация защиты информации. Определение и понятие.

– 8. Техника защиты информации. Определение и понятие.

– 9. Контроль защиты информации. Цели и понятие.

– 10. Контролируемая зона. Определение и понятие.

– 11. Технический канал утечки информации (ТКУИ), виды ТКУИ. Определение, физический смысл.

– 12.Подсистема технической защиты информации объектов информатизации, предназначенных для ведения конфиденциальных переговоров. Модель и понятие. 13. Подсистема технической защиты информации объектов информатизации, реализующих информационные технологии с использованием технических средств и систем. Модель и понятие.

– 14. Модель угроз подсистемы технической защиты информации объектов информатизации, реализующих информационные технологии с использованием технических средств и систем.

– 15. Модель угроз подсистемы технической защиты информации объектов информатизации, предназначенных для ведения конфиденциальных переговоров. 16. Уязвимости системы обеспечения ИБ организации. Определение и понятие.

– 17. Нарушитель ИБ организации. Определение и понятие.

– 18. Модель технической реализации ПТЗИ ОИ.

– 19. Защита информации от несанкционированного доступа (НСД). Определение и понятие.

– 20. Основа концепции защиты СВТ и АС от НСД к информации.

– 21. Классификация АС. Цели и основные понятия.

– 22. Аттестация объектов информатизации. Понятие.

– 23. Алгоритм приобретения ПЭВМ в защищенном исполнении.

– 24. Доктрина ИБ РФ. Общие положения.

### 3.5 Темы лабораторных работ

– Система защиты информации от несанкционированного доступа SecretNet.

– Система защиты информации от несанкционированного доступа Dallas Lock.

– Система защиты информации от несанкционированного доступа Страж NT.

– DLP-решения по защите информации в информационных системах.

– Защита информации от программных воздействий на базе антивируса Dr.Web.

– Защита информации от программных воздействий на базе антивируса KAV.

### 3.6 Темы курсовых проектов (работ)

– ˜ Разработка подсистемы технической защиты выделенного помещения предприятия се-

Согласована на портале № 19109

тей и систем.

– Разработка подсистемы технической защиты объекта вычислительной техники.

– Разработка подсистемы технической защиты персональных данных, обрабатываемых в информационной системе предприятия.

## 4 Методические материалы

Для обеспечения процесса обучения и решения задач обучения используются следующие материалы:

– методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы фор-мирования компетенций, согласно п. 12 рабочей программы.

### 4.1. Основная литература

1. Защита информации в инфокоммуникационных системах и сетях: Учебное пособие / Голиков А. М. - 2015. 284 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/5262, свободный.

### 4.2. Дополнительная литература

1. Защита информации от утечки по техническим каналам: Учебное пособие / Голиков А. М. - 2015. 256 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/5263, свободный.

### 4.3. Обязательные учебно-методические пособия

1. Защита информации в инфокоммуникационных системых и сетях: Учебное пособие для практических и семинарских занятий (Часть 1) / Голиков А. М. - 2015. 103 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/5330, свободный.
2. Защита информации в инфокоммуникационных системах и сетях: Сборник лабораторных работ / Голиков А. М. - 2015. 373 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/5378, свободный.
3. Информационные технологии в управлении качеством и защита информации: Методические рекомендации к курсовым работам и организации самостоятельной работы студентов / Годенова Е. Г. - 2011. 35 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/290, свободный.

### 4.4. Базы данных, информационно справочные и поисковые системы

1. 1. Базовые законодательные и нормативно-правовые документы РФ в области защиты
2. информации. [Электронный ресурс]. - Режим доступа: http://www.consultant.ru, (дата обращения 25.03.2017);
3. 2. Научно-образовательный портал ТУСУРа, https://edu.tusur.ru

Согласована на портале № 19109