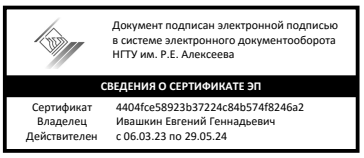
**МИНОБРНАУКИ РОССИИ**
**федеральное государственное бюджетное образовательное учреждение**
**высшего образования**
**«Нижегородский государственный технический университет**
**им. Р.Е. Алексеева» (НГТУ)**

Учебно-научный институт радиоэлектроники и информационных технологий (ИРИТ)
(Полное и сокращенное название института, реализующего данное направление)




УТВЕРЖДАЮ:
Директор института:
_____ Мякиньков А.В.
подпись ФИО
22 апреля 2023г

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.Б.33 Организационное и правовое обеспечение информационной безопасности
(индекс и наименование дисциплины по учебному плану)
для подготовки специалистов

Направление подготовки: 10.05.03 «Информационная безопасность автоматизированных систем»

Направленность: Безопасность открытых информационных систем

Форма обучения: очная
Год начала подготовки 2022

Выпускающая кафедра ИБВСС

Кафедра-разработчик ИБВСС

Объем дисциплины 144/4
часов/з.е
Промежуточная аттестация Экзамен

Разработчик: Капранов С.Н., к.т.н., доцент

Нижний Новгород

2023

Рабочая программа дисциплины: разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования (ФГОС ВО 3++) по направлению подготовки 09.03.02 Информационные системы и технологии, утвержденного приказом МИНОБРНАУКИ РОССИИ от 26 ноября 2020 года № 1457 на основании учебного плана принятого УМС НГТУ

протокол от 20.04.2023г №18.

Рабочая программа одобрена на заседании кафедры протокол от _01.04.2023_ № 4
Зав. кафедрой к.т.н, доцент Ляхманов Д.А. _____
(подпись)

Программа рекомендована к утверждению ученым советом института ИРИТ, Протокол от 21.04.2023г№_4

Рабочая программа зарегистрирована в УМУ, регистрационный № 10.05.03-б-32
Начальник МО _____ Н.Р. Булгакова

Заведующая отделом комплектования НТБ _____ Н.И. Кабанина
(подпись)

**СОДЕРЖАНИЕ**

## 1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

### 1.1 Цель освоения дисциплины

Целью освоения дисциплины является развитие компетенций в области обеспечения информационной безопасности организаций

### 1.2 Задачи освоения дисциплины (модуля)

Дисциплина «Организационное и правовое обеспечение информационной безопасности» способствует подготовке студентов к решению следующих профессиональных задач:

1. Правовое обеспечение организационно-технических мероприятий в организациях.
2. Организация защиты информации на объектах защиты.

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Учебная дисциплина «Организационное и правовое обеспечение информационной безопасности» Б1.Б.33 включена в обязательный перечень дисциплин обязательной части образовательной программы вне зависимости от ее направленности (профиля). Дисциплина реализуется в соответствии с требованиями ФГОС, ОП ВО и УП, по направлению подготовки 10.05.03.

Дисциплина базируется на дисциплине блока защиты информации: «Основы информационной безопасности» и «Правоведение».

Дисциплина «Организационное и правовое обеспечение информационной безопасности» является основополагающей для изучения следующих дисциплин: «Управление информационной безопасностью», также практики: практика по получению профессиональных умений и опыта научно-исследовательской деятельности.

## 3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

Дисциплина «Организационное и правовое обеспечение информационной безопасности» формирует компетенции ОПК-5, ОПК-6 совместно с дисциплинами и практиками, указанными в таблице 3.1.

Таблица 3.1 - Формирование компетенций дисциплинам

| Наименование дисциплин, формирующих компетенцию совместно | Семестры, формирования дисциплины Компетенции берутся из Учебного плана по направлению подготовки бакалавра /специалиста/магистра» | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | *1* | *2* | *3* | *4* | *5* | *6* | *7* | *8* | *9* | *10* | *11* |
| *ОПК-5 (Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации)* | | | | | | | | | | | |
| *Организационное и правовое обеспечение информационной безопасности* | | | | | | | | | | | |
| *Государственный экзамен* | | | | | | | | | | | |

| Наименование дисциплин, формирующих компетенцию совместно | Семестры, формирования дисциплины Компетенции берутся из Учебного плана по направлению подготовки специалиста» | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | *1* | *2* | *3* | *4* | *5* | *6* | *7* | *8* | *9* | *10* | *11* |
| *ОПК-6 (Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю)* | | | | | | | | | | | |
| *Основы информационной безопасности* | | | | | | | | | | | |
| *Организационное и правовое обеспечение информационной безопасности* | | | | | | | | | | | |
| *Подготовка и защита ВКР* | | | | | | | | | | | |

Таблица 3.2 - Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения

| **Код и наименование компетенции** | **Код и наименование индикатора достижения компетенции** | **Планируемые результаты обучения по дисциплине** | | | **Оценочные средства** | |
|---|---|---|---|---|---|---|
| | | | | | **Текущего контроля** | **Промежуточной аттестации** |
| ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации | ИОПК-5.1. Применяет нормативные правовые акты, нормативные и методические документы в различных сферах деятельности<br>ИОПК-5.2. Применяет нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в организации (учреждении, предприятии) | ***Знать:***<br>- правовые акты и нормативные и методические документы, регламентирующие деятельность по защите информации в организации | ***Уметь:***<br>- применять правовые акты, нормативные и методические документы для обеспечения защиты предприятия<br>- разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации | ***Владеть:***<br>- навыками работы с нормативными правовыми актами<br>- методами формирования требований по защите информации | Опрос на практических занятиях по тематике рефератов | Вопросы для устного собеседования – 40 вопросов |
| ОПК-6 Способен при решении профессиональных задач | ИОПК-6.1. Проводит организационные мероприятия по | **Знать:**<br>- нормативные и методические документы, | **Уметь:**<br>- организовать защиту информации ограниченного | **Владеть**:<br>-методами организации и управления | Опрос на практических занятиях по тематике | Вопросы для устного собеседования – 40 вопросов |

| | | | | | | |
|---|---|---|---|---|---|---|
| организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю | управлению информационной безопасности на предприятии в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю<br>ИОПК-6.2. Организовывает систему управления информационной безопасности на предприятии в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной | регламентирующие деятельность по защите информации в организации | доступа в автоматизированных системах в соответствии с нормативными правовыми актами и нормативными и методическими документами | деятельностью служб защиты информации на предприятии - навыками организации и обеспечения режима секретности | рефератов | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю | | | | | |

## 4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

### 4.1 Распределение трудоёмкости дисциплины по видам работ по семестрам

Общая трудоёмкость дисциплины составляет 4 зач. ед. 144 часа, распределение часов по видам работ семестрам представлено в таблице 4.1.

Таблица 4.1 - Распределение трудоёмкости дисциплины по видам работ по семестрам для студентов очного обучения

| **Вид учебной работы** | **Трудоёмкость в час** | |
|---|---|---|
| | **Всего час.** | **В т.ч. по семестрам** |
| | | 3 сем |
| **Формат изучения дисциплины** | с использованием элементов электронного обучения | |
| **Общая трудоёмкость** дисциплины по учебному плану | **144** | **144** |
| **1. Контактная работа:** | **57** | **57** |
| **1.1 Аудиторная работа, в том числе:** | **68** | **51** |
| занятия лекционного типа (Л) | 34 | 34 |
| занятия семинарского типа (ПЗ-семинары, практ. Занятия и др) | 17 | 17 |
| лабораторные работы (ЛР) | | |
| **1.2 Внеаудиторная, в том числе** | 6 | 6 |
| курсовая работа (проект) (КР/КП) (консультация, защита) | | |
| текущий контроль, консультации по дисциплине | 4 | 4 |
| контактная работа на промежуточном контроле (КРА) | 2 | 2 |
| **2. Самостоятельная работа** (СРС) | **51** | **51** |
| реферат/эссе (подготовка) | | |
| расчётно-графическая работа (РГР) (подготовка) | | |
| контрольная работа | | |
| курсовая работа/проект (КР/КП) (подготовка) | | |
| самостоятельное изучение разделов, самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным и практическим занятиям, коллоквиум и т.д.) | 51 | 51 |
| Подготовка к экзамену (контроль) | 36 | 36 |

**4.2 Содержание дисциплины, структурированное по темам**

Таблица 4.1 - Содержание дисциплины, структурированное по темам для студентов очного обучения

| Планируемые (контролируемые) результаты освоения: код УК; ОПК; ПК и индикаторы достижения компетенций | Наименование разделов, тем | Виды учебной работы (час) | | | | | Вид СРС | Наименование используемых активных и интерактивных образовательных технологий | Реализация в рамках Практической подготовки (трудоемкость в часах) | Наименование разработанного Электронного курса (трудоемкость в часах) |
|---|---|---|---|---|---|---|---|---|---|---|
| | | Контактная работа | | | | Самостоятельная работа студентов (час) | | | | |
| | | Лекции (час) | Лабораторные работы (час) | Практические занятия (час) | КСР | | | | | |
| **Раздел 1. Введение** | | | | | | | | | | |
| ОПК-5 - ИОПК-5.1<br>ОПК-6 - ИОПК-6.1<br>ОПК-6 - ИОПК-6.2 | **Тема 1.1** Система обеспечения ИБ | 1 | | | | 2 | Подготовка к лекциям [6.1.1 - 6.1.7] | Разбор конкретных ситуаций | | |
| | **Тема 1.2** Правовые средства обеспечения ИБ | 2 | | | | 2 | Подготовка к лекциям [6.1.1, 6.1.3, 6.1.4] | Разбор конкретных ситуаций | | |
| | **Тема 1.3** Организационные средства обеспечения ИБ | 1 | | | | 2 | Подготовка к лекциям [6.1.1, 6.1.3, 6.1.4] | Разбор конкретных ситуаций | | |
| | **Тема практических занятий:** «Основы организационно-правового обеспечения ЗИ» | | | 3 | | 2 | | | | |
| | **Итого по 1 разделу** | **2** | | **3** | | **8** | | | | |
| **Раздел 2. Правовые основы обеспечения информационной безопасности РФ** | | | | | | | | | | |

| Планируемые (контролируемые) результаты освоения: код УК; ОПК; ПК и индикаторы достижения компетенций | Наименование разделов, тем | Виды учебной работы (час) | | | | | Вид СРС | Наименование используемых активных и интерактивных образовательных технологий | Реализация в рамках Практической подготовки (трудоемкость в часах) | Наименование разработанного Электронного курса (трудоемкость в часах) |
|---|---|---|---|---|---|---|---|---|---|---|
| | | Контактная работа | | | | Самостоятельная работа студентов (час) | | | | |
| | | Лекции (час) | Лабораторные работы (час) | Практические занятия (час) | КСР | | | | | |
| ОПК-5 - ИОПК-5.1<br>ОПК-6 - ИОПК-6.1<br>ОПК-6 - ИОПК-6.2 | **Тема 2.1** Конституция РФ, Указ Президента РФ от 02.07.2021 N 400 «О Стратегии национальной безопасности», Доктрина информационной безопасности, ФЗ «Об информации, информационных технологиях и защите информации | 4 | | | | 2 | Подготовка к лекциям [6.1.1 - 6.1.7] | Разбор конкретных ситуаций | | |
| | **Тема 2.2** Уголовно-правовые и административно-правовые средства обеспечения ИБ | 2 | | | | 2 | Подготовка к лекциям [6.1.1 - 6.1.7] | Разбор конкретных ситуаций | | |
| | **Тема 2.**3 Виды тайн в отечественном законодательстве | 2 | | | | 2 | Подготовка к лекциям [6.1.1 - 6.1.7] | Разбор конкретных ситуаций | | |

| Планируемые (контролируемые) результаты освоения: код УК; ОПК; ПК и индикаторы достижения компетенций | Наименование разделов, тем | Виды учебной работы (час) | | | | | Вид СРС | Наименование используемых активных и интерактивных образовательных технологий | Реализация в рамках Практической подготовки (трудоемкость в часах) | Наименование разработанного Электронного курса (трудоемкость в часах) |
|---|---|---|---|---|---|---|---|---|---|---|
| | | Контактная работа | | | | Самостоятельная работа студентов (час) | | | | |
| | | Лекции (час) | Лабораторные работы (час) | Практические занятия (час) | КСР | | | | | |
| | **Тема 2.4** Закон о персональных данных | 1 | | | | 2 | Подготовка к лекциям [6.1.1 - 6.1.7] | Разбор конкретных ситуаций | | |
| | **Тема 2.5** Ответственность за нарушение ИБ | | | | | 2 | Подготовка к лекциям [6.1.1 - 6.1.7] | Разбор конкретных ситуаций | | |
| | **Тема практических занятий:** Правовые основы обеспечения информационной безопасности | | | 5 | | 2 | | | | |
| | **Итого по 2 разделу** | **10** | | **5** | **1** | **12** | | | | |
| **Раздел 3. Стандарты в области обеспечения ИБ.** | | | | | | | | | | |
| ОПК-5 - ИОПК-5.1<br>ОПК-6 - ИОПК-6.1 | **Тема 3.1** Система стандартов по информационной безопасности (обзор) | 6 | | | | 2 | Подготовка к лекциям [6.1.1 - 6.1.7] | Разбор конкретных ситуаций | | |
| ОПК-6 - ИОПК-6.2 | **Тема практических занятий:** “ Стандарты в области обеспечения ИБ ” | | | 2 | | 2 | | | | |

| Планируемые (контролируемые) результаты освоения: код УК; ОПК; ПК и индикаторы достижения компетенций | Наименование разделов, тем | Виды учебной работы (час) | | | | | Вид СРС | Наименование используемых активных и интерактивных образовательных технологий | Реализация в рамках Практической подготовки (трудоемкость в часах) | Наименование разработанного Электронного курса (трудоемкость в часах) |
|---|---|---|---|---|---|---|---|---|---|---|
| | | Контактная работа | | | | Самостоятельная работа студентов (час) | | | | |
| | | Лекции (час) | Лабораторные работы (час) | Практические занятия (час) | КСР | | | | | |
| | **Итого по 3 разделу** | **6** | | **2** | **1** | **4** | | | | |
| **Раздел 4. Нормативно-методические документы ФСТЭК РФ** | | | | | | | | | | |
| ОПК-5 - ИОПК-5.1<br>ОПК-6 - ИОПК-6.1<br>ОПК-6 - ИОПК-6.2 | **Тема 4.1.** Документы ФСТЭК в области безопасности персональных данных | 2 | | | | **2** | Подготовка к лекциям [6.1.1 - 6.1.7] | Разбор конкретных ситуаций | | |
| | **Тема 4.2.** Руководящие документы ФСТЭК в области ТЗИ | 2 | | | | **2** | Подготовка к лекциям [6.1.1 - 6.1.7] | Разбор конкретных ситуаций | | |
| | **Тема практических занятий:** «Нормативно-методические документы ФСТЭК РФ» | | | **2** | | **2** | | | | |
| | **Итого по 4 разделу** | **4** | | **2** | | **6** | | | | |
| **Раздел 5. Локальные нормативные акты в области ИБ** | | | | | | | | | | |
| ОПК-5 - ИОПК-5.1<br>ОПК-6 - ИОПК-6.1<br>ОПК-6 - ИОПК-6.2. | **Тема 5.1.** Нормативно-правовые документы | 1 | | | | **2** | Подготовка к лекциям [6.1.1 - 6.1.7] | Разбор конкретных ситуаций | | |
| | **Тема 5.2.** Индивидуально-правовые документы | 2 | | | | **2** | Подготовка к лекциям [6.1.1 - 6.1.7] | Разбор конкретных ситуаций | | |

| Планируемые (контролируемые) результаты освоения: код УК; ОПК; ПК и индикаторы достижения компетенций | Наименование разделов, тем | Виды учебной работы (час) | | | | | Вид СРС | Наименование используемых активных и интерактивных образовательных технологий | Реализация в рамках Практической подготовки (трудоемкость в часах) | Наименование разработанного Электронного курса (трудоемкость в часах) |
|---|---|---|---|---|---|---|---|---|---|---|
| | | Контактная работа | | | | Самостоятельная работа студентов (час) | | | | |
| | | Лекции (час) | Лабораторные работы (час) | Практические занятия (час) | КСР | | | | | |
| | **Тема практических занятий:** Локальные нормативные акты в области ИБ | | | **2** | | **2** | | | | |
| | **Итого по 5 разделу** | **3** | | **2** | **1** | **6** | | | | |
| **Раздел 6. Организационные основы ИБ** | | | | | | | | | | |
| ОПК-5 - ИОПК-5.1<br>ОПК-6 - ИОПК-6.1<br>ОПК-6 - ИОПК-6.2 | **Тема 6.1.** Структура обеспечения ИБ в РФ | 1 | | | **1** | **2** | Подготовка к лекциям [6.1.1 - 6.1.7] | Разбор конкретных ситуаций | | |
| | **Тема 6.2.** Структура системы ИБ в организации | 1 | | | | **2** | Подготовка к лекциям [6.1.1 - 6.1.7] | Разбор конкретных ситуаций | | |
| | **Тема 6.3.** Основные организационные мероприятия в области ИБ | 2 | | | | **3** | Подготовка к лекциям [6.1.1 - 6.1.7] | Разбор конкретных ситуаций | | |
| | **Тема 6.4.** Документальное обеспечения ИБ | 2 | | | | **4** | Подготовка к лекциям [6.1.1 - 6.1.7] | Разбор конкретных ситуаций | | |
| | **Тема практических занятий:** Организационные основы ИБ | | | **3** | | **4** | | | | |
| | **Итого по 6 разделу** | **4** | | **3** | **1** | **15** | | | | |

| Планируемые (контролируемые) результаты освоения: код УК; ОПК; ПК и индикаторы достижения компетенций | Наименование разделов, тем | Виды учебной работы (час) | | | | | Вид СРС | Наименование используемых активных и интерактивных образовательных технологий | Реализация в рамках Практической подготовки (трудоемкость в часах) | Наименование разработанного Электронного курса (трудоемкость в часах) |
|---|---|---|---|---|---|---|---|---|---|---|
| | | Контактная работа | | | | Самостоятельная работа студентов (час) | | | | |
| | | Лекции (час) | Лабораторные работы (час) | Практические занятия (час) | КСР | | | | | |
| | Подготовка к экзамену | | | | **2** | **36** | | | | |
| | **Итого за семестр** | **34** | | **17** | **6** | **51** | | | | |

## 5. ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ.

### 5.1 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности

1) Перечень вопросов, выносимых на промежуточную аттестацию (экзамен)

1. Конституция Российской Федерации: аспекты обеспечения ИБ
2. Стратегия национальной безопасности РФ до 2020 г: аспекты обеспечения ИБ
3. Доктрина информационной безопасности
4. Уголовный кодекс Российской Федерации (за исключением главы 28 и ст. 183 УК РФ)
5. Статья 183 УК РФ Незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну.
6. Компьютерные преступления (глава 28 УК РФ)
7. Виды тайн по гражданскому кодексу РФ.
8. Обеспечение ИБ в трудовом кодексе РФ.
9. Обеспечение ИБ в кодексе об административных правонарушениях РФ.
10. Законы о государственной тайне и о служебной тайне

Для выполнения процедур оценивания составлен паспорт оценочных средств.

Комплект оценочных средств является неотъемлемой частью ФОС и хранится на кафедре «Информационная безопасность вычислительных систем и сетей».

### 5.2 Описание показателей и критериев контроля успеваемости, описание шкал оценивания

Таблица 5.4 - При текущем контроле (контрольные недели) и оценке выполнения лабораторных работ

| **Шкала оценивания** | **Экзамен (зачет с оценкой)** |
|---|---|
| 40<R<=50 | Отлично |
| 30<R<=40 | Хорошо |
| 20<R<=30 | Удовлетворительно |
| O<R<=20 | Неудовлетворительно |

При промежуточном контроле успеваемость студентов оценивается по четырехбалльной системе «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Таблица 5.4 – Критерии оценивания результата обучения по дисциплине и шкала оценивания

| **Код и наименование компетенции** | **Код и наименование индикатора достижения компетенции** | **Критерии оценивания результатов обучения** | | | |
|---|---|---|---|---|---|
| | | Оценка **«неудовлетворительно»** / «не зачтено» 0-59% от max рейтинговой оценки контроля | Оценка **«удовлетворительно»** / «зачтено» 60-74% от max рейтинговой оценки контроля | Оценка **«хорошо» /** «зачтено» 75-89% от max рейтинговой оценки контроля | Оценка **«отлично» /** «зачтено» 90-100% от max рейтинговой оценки контроля |
| ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации | ИОПК-5.1. Применяет нормативные правовые акты, нормативные и методические документы в различных сферах деятельности<br><br>ИОПК -5.2. Применяет нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в организации (учреждении, предприятии) | Изложение учебного материала бессистемное, неполное, не освоены базовые понятия дисциплины. Не знает основы правового регулирования отношений в области обеспечения информационной безопасности; организационные основы обеспечения информационной безопасности; ответственность за нарушения в сфере обеспечения информационной безопасности | Фрагментарные, поверхностные знания базовых понятий. Имеет представление о разработке организационно-нормативной документации в области обеспечения информационной безопасности. Владеет некоторыми основами организационно-правового обеспечения ИБ | Знает базовые понятия дисциплины. Умеет разрабатывать организационно-нормативную документацию в области обеспечения информационной безопасности. Владеет основами организационно-правового обеспечения ИБ. | Имеет глубокие знания всего материала дисциплины. Владеет навыками организации защиты информации и правового обеспечения. |

| | | | | | |
|---|---|---|---|---|---|
| ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю | ИОПК-6.1. Проводит организационные мероприятия по управлению информационной безопасности на предприятии в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю<br>ИОПК-6.2. Организовывает систему управления информационной безопасности на предприятии в соответствии с нормативными | Изложение учебного материала бессистемное, неполное, не освоены базовые понятия дисциплины. Не знает основы правового регулирования отношений в области обеспечения информационной безопасности; организационные основы обеспечения информационной безопасности; ответственность за нарушения в сфере обеспечения информационной безопасности | Фрагментарные, поверхностные знания базовых понятий. Имеет представление о разработке организационно-нормативной документации в области обеспечения информационной безопасности. Владеет некоторыми основами организационно-правового обеспечения ИБ | Знает базовые понятия дисциплины. Умеет разрабатывать организационно-нормативную документацию в области обеспечения информационной безопасности. Владеет основами организационно-правового обеспечения ИБ. | Имеет глубокие знания всего материала дисциплины. Владеет навыками организации защиты информации и правового обеспечения. |

| | | | | | |
|---|---|---|---|---|---|
| | правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю | | | | |

Таблица 5.5 - Критерии оценивания

| Оценка | Критерии оценивания |
|---|---|
| Высокий уровень «5» (отлично) | оценку **«отлично»** заслуживает студент, освоивший знания, умения, компетенции и теоретический материал без пробелов; выполнивший все задания, предусмотренные учебным планом на высоком качественном уровне; практические навыки профессионального применения освоенных знаний сформированы. |
| Средний уровень «4» (хорошо) | оценку **«хорошо»** заслуживает студент, практически полностью освоивший знания, умения, компетенции и теоретический материал, учебные задания не оценены максимальным числом баллов, в основном сформировал практические навыки. |
| Пороговый уровень «3» (удовлетворительно) | оценку **«удовлетворительно»** заслуживает студент, частично с пробелами освоивший знания, умения, компетенции и теоретический материал, многие учебные задания либо не выполнил, либо они оценены числом баллов близким к минимальному, некоторые практические навыки не сформированы. |
| Минимальный уровень «2» (неудовлетворительно) | оценку «неудовлетворительно» заслуживает студент, не освоивший знания, умения, компетенции и теоретический материал, учебные задания не выполнил, практические навыки не сформированы. |

## 6. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

### 6.1 Учебная литература


6.1.1. Гафарова, Е.А. Организационно-правовое обеспечение информационной безопасности : учеб. пособие / Е.А. Гафарова. Челябинск: «Библиотека А. Миллера», 2019. 153 с.

6.1.2. Организационное и правовое обеспечение информационной безопасности: учебник и практикум / Т.А. Полякова [и др.]. – М.: Юрайт, 2018. 325 с.

6.1.3. Кармановский, Н.С. Организационно-правовое и методическое обеспечение информационной безопасности: учеб. пособие / Н.С. Кармановский, О.В. Михайличенко, Н.Н/ Прохожев. СПб.: Университет ИТМО, 2016. 168 с.

6.1.4. Трещев, И.А. Организационное и правовое обеспечение информационной безопасности: для студентов и специалистов / И.А. Трещев. Екатеринбург: Издательские решения, 2019. 760 с.

6.1.5. Организационное и правовое обеспечение информационной безопасности / под ред. М.П. Сычева. М.: МГТУ им. Н.Э. Баумана, 2018. 292 с.

6.1.6. Жигулин Г.П. Организационное и правовое обеспечение информационной безопасности / Г.П. Жигулин. – СПб.: СПбНИУИТМО, 2014. – 173 с.

6.1.7. Карпычев В.Ю. Защита информации: организационно-правовые основы: учеб. пособие / В.Ю. Карпычев; Нижегород. гос. техн. ун-т. им. Р.Е. Алексеева. – Нижний Новгород, 2021. 119 с.


### 6.2 Перечень журналов по профилю дисциплины:

Журнал «Информационное право» (http://lawinfo.ru/catalog/contents/informacionnoe-pravo/1/)

### 6.3 Методические указания, рекомендации и другие материалы к занятиям

Методические указания по выполнению лабораторных работ по дисциплине «Организационное и правовое обеспечение информационной безопасности» в электронном варианте находятся на кафедре «Информационная безопасность вычислительных систем и сетей». Электронные варианты методических указаний по выполнению лабораторных работ отправляются

на электронные адреса групп.

6.3.1 Методические указания к лабораторным работам по дисциплине «Организационное и правовое обеспечение информационной безопасности» [Электронные текстовые данные]: метод. указания к лаб. работе по дисциплине «Организационное и правовое обеспечение информационной безопасности» для студентов направления подготовки 10.05.03 «Информационная безопасность автоматизированных систем» дневной формы обучения / НГТУ; Сост.: С.Н. Капранов. Н. Новгород, 2021, 76 с.

## 7. ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Учебный процесс по дисциплине обеспечен необходимым комплектом свободно распространяемого программного обеспечения (состав по дисциплине определен в настоящей РПД и подлежит обновлению при необходимости).

### 7.1 Перечень информационных справочных систем

Таблица 7.1 - Перечень электронных библиотечных систем

| № | Наименование ЭБС | Ссылка к ЭБС |
|---|---|---|
| 1 | «Консультант студента - Электронная библиотека технического вуза» | http://www.studentlibrary.ru/ |
| 2 | Лань | https://e.lanbook.com/ |
| 3 | «Юрайт» (коллекция «Легендарные книги») | https://urait.ru/ |
| 4 | «Техэксперт» - «Нормы, правила, стандарты и законодательство России» | https://www.nntu.ru/frontend/web/ngtu/files/org_structura/library/resurvsy/tehekspert.pdf |

### 7.2 Перечень свободно распространяемого программного обеспечения

Таблица 7.2 – Программное обеспечение, используемое студентами очного обучения

| Программное обеспечение, используемое в университете на договорной основе | Программное обеспечение свободного распространения |
|---|---|
| 1. Windows 7 32 bit корпоративная VL 49477S2<br>2. Microsoft Office Professional Plus 2007 (лицензия № 42470655);<br>3. Dr.Web (с/н GMN9-DSLH-G4U1-LW6H от 11.05.23<br>4. Microsoft Windows 7 MSDN ( подписка DreamSpark Premium, договор № Tr113003 от 25.09.14) | Adobe Acrobat Reader DC-Russian (беспл.)<br>Браузер Google Chrome, Браузер Mozilla Firefox, McAfee Security Scan |

### 7.3 Перечень современных профессиональных баз данных и информационных справочных систем

В таблице 7.4 указан перечень профессиональных баз данных и информационных справочных систем, к которым обеспечен доступ (удаленный доступ). Данный перечень подлежит обновлению в соответствии с требованиями ФГОС ВО.

В данном разделе могут быть приведены ресурсы (ссылки на сайты), на которых можно найти полезную для курса информацию, в т.ч. статистические или справочные данные, учебные материалы, онлайн курсы и т.д.

Таблица 7.4 – Перечень современных профессиональных баз данных и информационных справочных систем

| № | Наименование профессиональной базы данных, информационно-справочной системы | Доступ к ресурсу (удаленный доступ с указанием ссылки/доступ из локальной сети университета) |
|---|---|---|
| 1 | 2 | 3 |
| 1 | База данных издательства Wiley | https://onlinelibrary.wiley.com/ |
| 2 | База данных Polpred | http://www.polpred.com |
| 3 | Научная электронная библиотека ELIBRARY.RU | http://elibrary.ru |
| 4 | База данных стандартов и регламентов РОССТАНДАРТ | https://www.rst.gov.ru/portal/gost/home/standarts |
| 5 | Перечень профессиональных баз данных и информационных справочных систем | https://cyberpedia.su/21x47c0.html |
| 6 | Каталог паттернов проектирования | https://refactoring.guru/ru/design-patterns/catalog |

## 8. ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОВЗ

В таблице 8.1 указан перечень образовательных ресурсов, имеющих формы, адаптированные к ограничениям их здоровья, а также сведения о наличии специальных технических средств обучения коллективного и индивидуального пользования. При заполнении таблицы может быть использована информация, размещенная в подразделе «Доступная среда» специализированного раздела сайта НГТУ «Сведения об образовательной организации» https://www.nntu.ru/sveden/ovz/.

Таблица 8.1 - Образовательные ресурсы для инвалидов и лиц с ОВЗ

| № | Перечень образовательных ресурсов, приспособленных для использования инвалидами и лицами с ОВЗ | Сведения о наличии специальных технических средств обучения коллективного и индивидуального пользования |
|---|---|---|
| 1 | ЭБС «Консультант студента» | Версия для слабовидящих, прослушивание с помощью синтезатора речи |
| 2 | ЭБС «Лань» | Версия для слабовидящих, прослушивание с помощью синтезатора речи |
| 3 | «Юрайт» (коллекция «Легендарные книги») | Версия для слабовидящих |

## 9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ, НЕОБХОДИМОЕ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Учебные аудитории для проведения занятий по дисциплине, оснащены оборудованием и техническими средствами обучения

В таблице 9.1 перечислены:

- учебные аудитории для проведения учебных занятий, оснащенные оборудованием и техническими средствами обучения;
- помещения для самостоятельной работы обучающихся, которые должны оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду НГТУ.

Таблица 9.1 - Оснащенность аудиторий и помещений для самостоятельной работы студентов по дисциплине

| № | Наименование аудиторий и помещений для самостоятельной работы | Оснащенность аудиторий помещений и помещений для самостоятельной работы | Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа |
|---|---|---|---|
| 1 | 1 | 2 | 3 |
| 1 | Учебная аудитория № 6421 учебно-лабораторного корпуса № 6 для проведения учебных занятий. 603163, Нижегородская область, г. Нижний Новгород, Казанское шоссе, д.12 | 1. Доска меловая – 1 шт. 3. Экран – 1 шт. 4. Мультимедийный проектор Epson X12 – 1 шт. 5. Компьютер PC MB Asus на чипсете Nvidia/AMDAthlonXII CPU 2.8Ggz/ RAM 4 Ggb/SVGAStandartGraphics +Ge-FORCE Nvidia GT210/HDD 250Ggb,SATAinterface, монитор 19”, с выходом на проектор. 6. Рабочее место студента - 74 7. Рабочее место для преподавателя – 1 шт. | 1. Windows 7 32 bit корпоративная; VL 49477S2 2. Adobe Acrobat Reader DC-Russian (беспл.) 3. Microsoft Office Professional Plus 2007 (лицензия № 42470655); 4. Dr.Web (с/н GMN9-DSLH-G4U1-LW6H от 11.05.23 до 28.05.24) |
| 2 | Помещение для самостоятельной работы обучающихся № 6545 учебно-лабораторного корпуса № 6 для проведения научно-исследовательской работы обучающихся, курсового и дипломного проектирования. 603163, Нижегородская область, г. Нижний Новгород, Казанское шоссе, д.12 | 1. Рабочие места, оснащенные ПК на базеCore 2 Duo с мониторами – 5 шт. 2. Рабочее место преподавателя, оснащенное ПК на базе Intel Core i5 с монитором – 1 шт. 3. Доска интерактивная ScreenMedia-M. ПК подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду университета. 4. Посадочных мест - 12, шесть оснащены ПК. 5. Принтер Xerox Phaser 3300 MFP | 1. Microsoft Windows 7 MSDN реквизиты договора - подписка (подписка DreamSpark Premium, договор № 0509/КМР от 15.10.18), 2. Бесплатное ПО: Пакет программ Open Office, True Conf, Браузер Google Chrome, Браузер Mozilla Firefox, Браузер Opera, McAfee Security Scan, Adobe Acrobat Reader DC |

## 10. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ОБУЧАЮЩИМСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

### 10.1 Общие методические рекомендации для обучающихся по освоению дисциплины, образовательные технологии

Дисциплина реализуется посредством проведения контактной работы с обучающимися (включая проведение текущего контроля успеваемости), самостоятельной работы обучающихся и промежуточной аттестации.

При преподавании дисциплины «Организационное и правовое обеспечение информационной безопасности», используются современные образовательные технологии, позволяющие повысить активность студентов при освоении материала курса и предоставить им возможность эффективно реализовать часы самостоятельной работы.

Весь лекционный материал курса сопровождается компьютерными презентациями, в которых наглядно преподносятся материал различных разделов курса и что дает возможность обсудить материал со студентами во время чтения лекций, активировать их деятельность при освоении материала. Электронные материалы лекций в период дистанционного обучения отправляются по электронной почте на адреса групп и могут быть получены до чтения лекций и

проработаны студентами в ходе самостоятельной работы.

На лекциях, лабораторных занятиях реализуются интерактивные технологии, приветствуются вопросы и обсуждения, используется личностно-ориентированный подход, технология работы в малых группах, что позволяет студентам проявить себя, получить навыки самостоятельного изучения материала, выровнять уровень знаний в группе.

Все вопросы, возникшие при самостоятельной работе над домашним заданием подробно разбираются на лабораторных занятиях и лекциях. Проводятся индивидуальные и групповые консультации с использованием современных информационных технологий: электронная почта, мессенджеры, Zoom, Discord.

Инициируется активность студентов, поощряется задание любых вопросов по материалу, практикуется индивидуальный ответ на вопросы студента, рекомендуются методы успешного самостоятельного усвоения материала в зависимости от уровня его базовой подготовки.

Для оценки знаний, умений, навыков и уровня сформированности компетенции применяется балльно-рейтинговая система контроля и оценки успеваемости студентов в процессе текущего контроля.

Промежуточная аттестация проводится в форме экзамена с учетом текущей успеваемости.

**10.2 Методические указания для занятий лекционного типа**

Лекционный курс предполагает систематизированное изложение основных вопросов тематического плана. В ходе лекционных занятий раскрываются базовые вопросы в рамках каждой темы дисциплины (Таблицы 4.4, 4.5, 4.6) . Обозначаются ключевые аспекты тем, а также делаются акценты на наиболее сложные и важные положения изучаемого материала. Материалы лекций являются опорной основой для подготовки обучающихся к лабораторным работам и выполнения заданий самостоятельной работы, а также к мероприятиям текущего контроля успеваемости и промежуточной аттестации по дисциплине.

**10.3 Методические указания по освоению дисциплины на практических занятиях**

Практические (семинарские) занятия представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают все основные разделы. Основной формой проведения семинаров и практических занятий является обсуждение наиболее проблемных и сложных вопросов по отдельным темам, а также решение задач и разбор примеров и ситуаций в аудиторных условиях.

Практические (семинарские) занятия обучающихся обеспечивают:

- проверку и уточнение знаний, полученных на лекциях;
- получение умений и навыков составления докладов и сообщений, обсуждения вопросов по учебному материалу дисциплины;
- подведение итогов занятий по рейтинговой системе, согласно технологической карте дисциплины.

Приводятся конкретные методические указания для обучающихся по выполнению реферата или эссе, требования к их оформлению, порядок сдачи

Примерная тематика рефератов

1. Доктрина информационной безопасности. Закон «Об информации, информационных технологиях и защите информации» № 149-ФЗ.
2. Уголовный кодекс Российской Федерации (обеспечение ИБ) в т.ч. ст. 183 УК РФ Незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну; глава 28 УК РФ Компьютерные преступления;
3. Обеспечение ИБ в трудовом кодексе РФ. Обеспечение ИБ в Кодексе об административных правонарушениях РФ. Ответственность за нарушение информационной безопасности
4. Виды тайн: Законы «О государственной тайне» , «О коммерческой тайне», «О персональных данных»
5. Правовое регулирование технической защиты информации, в том числе Положение «О

государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам».

6. Правовое регулирование Лицензирования в области ИБ, в том числе "Перечень технической документации, национальных стандартов и методических документов, необходимых для выполнения работ и оказания услуг, установленных положением о лицензировании деятельности по технической защите конфиденциальной информации, утвержденным постановлением Правительства Российской Федерации от 3 февраля 2012 г. N 79" (утв. ФСТЭК России 24.07.2017).

7. Правовое регулирование аттестации объектов информатизации

8. Правовое регулирование сертификации средств защиты информации

9. Критическая информационная инфраструктура

9.1. Закон 187-ФЗ 2017 «О безопасности критической информационной инфраструктуры Российской Федерации».

9.2. Приказ ФСТЭК от 14 марта 2014 г. N 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»

9.3. Приказ ФСТЭК от 25 декабря 2017 г. N 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»,

9.4. Приказ от 21 декабря 2017 г. N 235 Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования,

10. Документы ФСТЭК по персональным данным

10.1. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008 год

10.2. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2008 год

10.3. Приказ ФСТЭК России № 21 от 18 февраля 2013 г. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

10.4. Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" (2 человека)

11. Документы ФСТЭК по ГИС

11.1. «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», Приказ ФСТЭК России от 11.02.2013г. N 17 (Зарегистрировано в Минюсте России 31.05.2013г. N 28608);

11.2. Методический документ. Меры защиты информации в государственных информационных системах», Приказ ФСТЭК России от 11 февраля 2014г.

### 10.4 Методические указания по самостоятельной работе обучающихся

Самостоятельная работа обеспечивает подготовку обучающегося к аудиторным занятиям и мероприятиям текущего контроля и промежуточной аттестации по изучаемой дисциплине. Результаты этой подготовки проявляются в активности обучающегося на занятиях и в качестве выполненных практических заданий и других форм текущего контроля.

При выполнении заданий для самостоятельной работы рекомендуется проработка материалов лекций по каждой пройденной теме, а также изучение рекомендуемой литературы, представленной в Разделе 6.

В процессе самостоятельной работы при изучении дисциплины студенты могут работать на компьютере в специализированных аудиториях для самостоятельной работы, указанных в Разделе

9. В аудиториях имеется доступ через информационно-телекоммуникационную сеть «Интернет» к электронной информационно-образовательной среде университета (ЭИОС) и электронной библиотечной системе (ЭБС), где в электронном виде располагаются учебные и учебно-методические материалы, которые могут быть использованы для самостоятельной работы при изучении дисциплины.

## 11. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

**11.1 Типовые контрольные задания или иные +материалы, необходимые для оценки знаний, умений, навыков и (или) опыта в ходе текущего контроля успеваемости**

Для текущего контроля знаний студентов по дисциплине проводится комплексная оценка знаний, включающая

- выполнение и защита рефератов для студентов всех форм обучения

Перечень тем рефератов – 18 шт.

- 11.1.1 Типовые задания для практических работ

Типовые задания для практических работ приведены в учебно-методических пособиях по проведению практических занятий.

**11.2 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта в ходе промежуточной аттестации по дисциплине**

11.2.2. Экзамен для студентов очной формы обучения в 3 семестре.

Типовые вопросы для промежуточной аттестации в форме экзамена для студентов очной формы обучения

Вопросы, направленные на проверку компетенции ОПК-5:

1. Конституция Российской Федерации: аспекты обеспечения ИБ
2. Стратегия национальной безопасности РФ до 2020 г: аспекты обеспечения ИБ
3. Доктрина информационной безопасности
4. Уголовный кодекс Российской Федерации (за исключением главы 28 и ст. 183 УК РФ)
5. Статья 183 УК РФ Незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну.
6. Компьютерные преступления (глава 28 УК РФ)
7. Виды тайн по гражданскому кодексу РФ.
8. Обеспечение ИБ в трудовом кодексе РФ.
9. Обеспечение ИБ в кодексе об административных правонарушениях РФ.
10. Законы о государственной тайне и о служебной тайне
11. Иные виды тайн (по федеральным законам).
12. Закон об информации, информационных технологиях и защите информации № 149-ФЗ
13. Ответственность за нарушение информационной безопасности

Вопросы, направленные на проверку компетенции ОПК-6:

14. Система стандартов по информационной безопасности
15. Стандарты ГОСТ Р ИСО/МЭК 1333х-х-200х (4 стандарта). Информационная технология. Методы и средства обеспечения безопасности.
16. ГОСТ Р ИСО/МЭК 15408-х-2008 (3 стандарта). Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.17. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Прчактические правила управления информационной безопасностью.
17. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Прчактические правила управления информационной безопасностью.
18. ГОСТ Р ИСО/МЭК ТО 19791-2008. Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем.

19. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

20. Р 50.1.056 Техническая защита информации. Основные термины и определения.

21. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования.

22. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения.

23. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

24. ГОСТ Р 52069.0-2003. Защита информации. Система стандартов. Основные положения.

25. ГОСТ Р 53113.х-200х. (2 стандарта)Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов.

26. ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения.

27. Отраслевые стандарты информационной безопасности

28 Стандарты Банка России

29 Нормативные документы ФСТЭК России

30. "Концепция защиты СВТ и АС от НСД к информации";

31. "Автоматизированные системы. Защита от НСД к информации. Классификация АС и требования по защите информации"

32. "Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности СВТ"

33. "Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации"

34. "Средства антивирусной защиты. Показатели защищенности и требования по защите от вирусов"

35. РД 19.06 2002. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий

36. РД. 04.06.1999. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей

37. РД. 25.07 1997 Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации

38. РД.30.03.1992. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации

39. РД.30.03.1992. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации

40. РД.30.03.1992. Защита от несанкционированного доступа к информации. Термины и определения

41. РД.30.03.1992. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации

В полном объеме оценочные средства имеются на кафедре «Информационная безопасность вычислительных систем и сетей». Оценочные средства могут быть получены по требованию.