

**МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ**  
**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ**  
**УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**  
**«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»**

УТВЕРЖДАЮ:

Директор ИТТСУ



П.Ф. Бестемьянов

26 мая 2020 г.



Кафедра «Управление и защита информации»

Автор Алексеев Виктор Михайлович, д.т.н., профессор

**РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ**

**Модели безопасности компьютерных систем**

|                          |                                                                                        |
|--------------------------|----------------------------------------------------------------------------------------|
| Специальность:           | <u>10.05.01 – Компьютерная безопасность</u>                                            |
| Специализация:           | <u>Информационная безопасность объектов информатизации на базе компьютерных систем</u> |
| Квалификация выпускника: | <u>Специалист по защите информации</u>                                                 |
| Форма обучения:          | <u>очная</u>                                                                           |
| Год начала подготовки    | <u>2020</u>                                                                            |

|                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                       |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p style="text-align: center;">Одобрено на заседании<br/>Учебно-методической комиссии института<br/>Протокол № 10<br/>26 мая 2020 г.<br/>Председатель учебно-методической<br/>комиссии</p>  <p style="text-align: right;">С.В. Володин</p> | <p style="text-align: center;">Одобрено на заседании кафедры</p> <p>Протокол № 16<br/>21 мая 2020 г.<br/>Заведующий кафедрой</p>  <p style="text-align: right;">Л.А. Баранов</p> |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Москва 2020 г.

## 1. ЦЕЛИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Дисциплина «Модели безопасности компьютерных систем» реализует требования федерального государственного образовательного стандарта высшего профессионального образования по направлению подготовки 100501 «Компьютерная безопасность».

Целью изучения дисциплины «Модели безопасности компьютерных систем» является обучение специалистов принципам формального моделирования и анализа безопасности компьютерных систем (КС), реализующих управление доступом и информационными потоками, а также содействие фундаментализации образования, формированию научного мировоззрения и развитию системного мышления.

Дисциплина «Модели безопасности компьютерных систем» относится к числу дисциплин специализации ПСК-8 базовой части профессионального цикла.

Задачами изучения дисциплины являются:

изучение основ устройства и принципов функционирования,

методологии проектирования и построения защищенных,

критериев и методов оценки защищенности КС,

средств и методов защиты от несанкционированного доступа (НСД) к информации.

Основной целью изучения учебной дисциплины «Модели безопасности компьютерных систем» является формирование у обучающегося компетенций для следующих видов деятельности:

- научно-исследовательской;

- специализация № 8.

Дисциплина предназначена для получения знаний для решения следующих профессиональных задач (в соответствии с видами деятельности):

сбор, обработка, анализ и систематизация научно-технической информации,

отечественного и зарубежного опыта по проблемам компьютерной безопасности;

участие в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах;

изучение и обобщение опыта работы других учреждений, организаций и предприятий по способам использования методов и средств обеспечения информационной безопасности с целью повышения эффективности и совершенствования работ по защите информации на конкретном объекте;

разработка математических моделей защищаемых процессов и средств защиты информации и систем, обеспечивающих информационную безопасность объектов;

специализации № 8 "Информационная безопасность объектов информатизации на базе компьютерных систем":

разработка проектных решений и анализ систем обеспечения информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении и процессов их проектирования, создания и модернизации, в том числе разработка модели угроз и формирование требования к обеспечению информационной безопасности.

## **2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО**

Учебная дисциплина "Модели безопасности компьютерных систем" относится к блоку 1 "Дисциплины (модули)" и входит в его базовую часть.

### **2.1. Наименования предшествующих дисциплин**

Для изучения данной дисциплины необходимы следующие знания, умения и навыки, формируемые предшествующими дисциплинами:

#### **2.1.1. Дискретная математика:**

Знания: методы ДМ

Умения: применять методы ДМ

Навыки: основными методами оценки состояния объекта

### **2.2. Наименование последующих дисциплин**

Результаты освоения дисциплины используются при изучении последующих учебных дисциплин:

2.2.1. Защита информации в интернет и интранет системах

2.2.2. Защита информации в телекоммуникационных системах железнодорожного транспорта

2.2.3. Криптографические протоколы

### 3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫЕ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

В результате освоения дисциплины студент должен:

| №<br>п/п | Код и название компетенции                                                                                                                                                                                 | Ожидаемые результаты                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1        | ОПК-3 Способен на основании совокупности существующих математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач защиты информации                                         | ОПК-3.1 Применяет систему фундаментальных знаний? (математических, естественнонаучных и инженерных) для формулирования и решения проблем задач защиты информации.<br>ОПК-3.2 Применяет методы математического моделирования для формализации содержательно отчетливо сформулированных проблем.                                                                                                                                                                                                                                                                                 |
| 2        | ОПК-9 Способен разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации                 | ОПК-9.1 Владеет методами и средствами моделирования политик безопасности, политик управления доступом и информационными потоками в компьютерных системах, угроз безопасности информации.<br>ОПК-9.2 Знает типовые модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах, угроз безопасности информации.<br>ОПК-9.3 Умеет адаптировать типовые и строить оригинальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации. |
| 3        | ПКО-2 Способен применять математические методы в области компьютерной безопасности                                                                                                                         | ПКО-2.1 Проводит анализ и разрабатывает под руководством квалифицированного специалиста математические модели безопасности компьютерных систем.<br>ПКО-2.2 Применяет специальные математические методы, включая криптографические, для анализа и разработки защищенных компьютерных систем.<br>ПКО-2.3 Применяет решения на основе специальных математических методов для обеспечения защищенной передачи данных в современных компьютерных сетях.                                                                                                                             |
| 4        | ПКО-5 Способен участвовать в работах по проектированию и реализации комплексного подхода к обеспечению информационной безопасности объекта защиты                                                          | ПКО-5.1 Принимает участие в формировании политики информационной безопасности, ее реализации и контроле выполнения.<br>ПКО-5.2 Формирует, организует и поддерживает комплекс мер по обеспечению информационной безопасности.                                                                                                                                                                                                                                                                                                                                                   |
| 5        | ПКР-1 Способен строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов               | ПКР-1.1 Строит математические модели для оценки безопасности компьютерных систем.<br>ПКР-1.2 Анализирует компоненты системы безопасности с использованием современных математических методов.                                                                                                                                                                                                                                                                                                                                                                                  |
| 6        | ПКС-1 Способен разрабатывать модели угроз, формировать требования по защите информации в объектах информатизации на базе компьютерных систем, а также процессов их проектирования, создания и модернизации | ПКС-1.1 Знать основные формальные модели изолированной программной среды и безопасности информационных потоков.<br>ПКС-1.2 Уметь разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем.                                                                                                                                                                                                                                                                                                                                                              |

#### 4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) В ЗАЧЕТНЫХ ЕДИНИЦАХ И АКАДЕМИЧЕСКИХ ЧАСАХ

##### 4.1. Общая трудоемкость дисциплины составляет:

4 зачетных единиц (144 ак. ч.).

##### 4.2. Распределение объема учебной дисциплины на контактную работу с преподавателем и самостоятельную работу обучающихся

| Вид учебной работы                                                 | Количество часов        |           |
|--------------------------------------------------------------------|-------------------------|-----------|
|                                                                    | Всего по учебному плану | Семестр 6 |
| Контактная работа                                                  | 68                      | 68,15     |
| Аудиторные занятия (всего):                                        | 68                      | 68        |
| В том числе:                                                       |                         |           |
| лекции (Л)                                                         | 34                      | 34        |
| практические (ПЗ) и семинарские (С)                                | 34                      | 34        |
| Самостоятельная работа (всего)                                     | 76                      | 76        |
| ОБЩАЯ трудоемкость дисциплины, часы:                               | 144                     | 144       |
| ОБЩАЯ трудоемкость дисциплины, зач.ед.:                            | 4.0                     | 4.0       |
| Текущий контроль успеваемости (количество и вид текущего контроля) | ПК1, ПК2                | ПК1, ПК2  |
| Виды промежуточной аттестации (экзамен, зачет)                     | ЗаО                     | ЗаО       |

### 4.3. Содержание дисциплины (модуля), структурированное по темам (разделам)

| № п/п | Семестр | Тема (раздел) учебной дисциплины                                                                                                                                                                                                                                                                                                                                  | Виды учебной деятельности в часах/<br>в том числе интерактивной форме |    |    |     |    |       | Формы текущего контроля успеваемости и промежуточной аттестации |
|-------|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|----|----|-----|----|-------|-----------------------------------------------------------------|
|       |         |                                                                                                                                                                                                                                                                                                                                                                   | Л                                                                     | ЛР | ПЗ | КСР | СР | Всего |                                                                 |
| 1     | 2       | 3                                                                                                                                                                                                                                                                                                                                                                 | 4                                                                     | 5  | 6  | 7   | 8  | 9     | 10                                                              |
| 1     | 6       | Раздел 1<br>Введение.<br>Основные понятия и определения<br>Основные элементы теории компьютерной безопасности.<br>Модели ценности информации.<br>Угрозы безопасности информации.<br>Политика безопасности.                                                                                                                                                        | 4                                                                     |    | 6  |     | 10 | 20    |                                                                 |
| 2     | 6       | Раздел 2<br>Модели компьютерных систем с дискреционным управлением доступа<br>Модель матрицы доступов Харрисона-Рузсо-Ульмана (ХРУ).<br>Модель типизированной матрицы доступов (ТМД).<br>Классическая модель распространения прав доступа Take-Grant.<br>Расширенная модель Take-Grant.<br>Алгоритм построения замыкания графа доступов и информационных потоков. | 6                                                                     |    | 8  |     | 10 | 24    |                                                                 |
| 3     | 6       | Раздел 3<br>Модели компьютерных систем с мандатным управлением                                                                                                                                                                                                                                                                                                    | 6                                                                     |    | 10 |     | 16 | 32    | ПК1,<br>Устный опрос                                            |

| № п/п | Семестр | Тема (раздел) учебной дисциплины                                                                                                                                                                                                                                                     | Виды учебной деятельности в часах/<br>в том числе интерактивной форме |    |    |     |    |       | Формы текущего контроля успеваемости и промежуточной аттестации |
|-------|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|----|----|-----|----|-------|-----------------------------------------------------------------|
|       |         |                                                                                                                                                                                                                                                                                      | Л                                                                     | ЛР | ПЗ | КСР | СР | Всего |                                                                 |
| 1     | 2       | 3                                                                                                                                                                                                                                                                                    | 4                                                                     | 5  | 6  | 7   | 8  | 9     | 10                                                              |
|       |         | доступа<br>Классическая модель Белла-Ла Падулы.<br>Модель мандатной политики целостности информации Биба.<br>Интерпретации модели Белла-Ла Падулы.                                                                                                                                   |                                                                       |    |    |     |    |       |                                                                 |
| 4     | 6       | Раздел 4<br>Модели безопасности информационных потоков и изолированной программной среды<br>Автоматная, программная и вероятностная модели безопасности информационных потоков.<br>Субъективно-ориентированная модель изолированной программной среды (ИПС).<br>Базовая теорема ИПС. | 6                                                                     |    | 4  |     | 10 | 20    |                                                                 |
| 5     | 6       | Раздел 5<br>Модели компьютерных систем с ролевым управлением доступа<br>Базовая модель ролевого управления доступом. Модель административного ролевого управления доступом.<br>Субъектно-ориентированная модель изолированной программной                                            | 6                                                                     |    |    |     | 14 | 20    |                                                                 |

| №<br>п/п | Семестр | Тема (раздел)<br>учебной<br>дисциплины                                                                                                                                                                                                                                                                                                                                                               | Виды учебной деятельности в часах/<br>в том числе интерактивной форме |    |    |     |    |       | Формы<br>текущего<br>контроля<br>успеваемости и<br>промежу-<br>точной<br>аттестации |
|----------|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|----|----|-----|----|-------|-------------------------------------------------------------------------------------|
|          |         |                                                                                                                                                                                                                                                                                                                                                                                                      | Л                                                                     | ЛР | ПЗ | КСР | СР | Всего |                                                                                     |
| 1        | 2       | 3                                                                                                                                                                                                                                                                                                                                                                                                    | 4                                                                     | 5  | 6  | 7   | 8  | 9     | 10                                                                                  |
|          |         | среды.<br>Безопасность<br>информационных<br>потоков.                                                                                                                                                                                                                                                                                                                                                 |                                                                       |    |    |     |    |       |                                                                                     |
| 6        | 6       | Раздел 6<br>Развитие<br>формальных<br>моделей<br>безопасности<br>компьютерных<br>систем<br>Взаимосвязь<br>положений<br>классических<br>формальных<br>моделей<br>безопасности КС.<br>Проблема<br>адекватности<br>реализации модели<br>безопасности в<br>реальной КС.<br>Семейство моделей<br>безопасности<br>логического<br>управления<br>доступом и<br>информационными<br>потоками (ДП-<br>моделей). | 6                                                                     |    | 6  |     | 16 | 28    | ПК2,<br>Устный опрос                                                                |
| 7        | 6       | Раздел 7<br>Зачет с оценкой                                                                                                                                                                                                                                                                                                                                                                          |                                                                       |    |    |     |    | 0     | ЗаО                                                                                 |
| 8        |         | Всего:                                                                                                                                                                                                                                                                                                                                                                                               | 34                                                                    |    | 34 |     | 76 | 144   |                                                                                     |



#### 4.4. Лабораторные работы / практические занятия

Лабораторные работы учебным планом не предусмотрены.

Практические занятия предусмотрены в объеме 34 ак. ч.

| № п/п | № семестра | Тема (раздел) учебной дисциплины                                                         | Наименование занятий                                             | Всего часов/ из них часов в интерактивной форме |
|-------|------------|------------------------------------------------------------------------------------------|------------------------------------------------------------------|-------------------------------------------------|
| 1     | 2          | 3                                                                                        | 4                                                                | 5                                               |
| 1     | 6          | РАЗДЕЛ 1<br>Введение. Основные понятия и определения                                     | Решетка многоуровневой безопасности                              | 2                                               |
| 2     | 6          | РАЗДЕЛ 1<br>Введение. Основные понятия и определения                                     | Применение теорем о передаче прав доступа                        | 4                                               |
| 3     | 6          | РАЗДЕЛ 2<br>Модели компьютерных систем с дискреционным управлением доступа               | Применение теоремы об условиях реализации информационного потока | 4                                               |
| 4     | 6          | РАЗДЕЛ 2<br>Модели компьютерных систем с дискреционным управлением доступа               | Построение замыкания графа доступов                              | 4                                               |
| 5     | 6          | РАЗДЕЛ 3<br>Модели компьютерных систем с мандатным управлением доступа                   | Модель ХРУ                                                       | 4                                               |
| 6     | 6          | РАЗДЕЛ 3<br>Модели компьютерных систем с мандатным управлением доступа                   | Сведение модели ХРУ к модели ТМД и наоборот                      | 4                                               |
| 7     | 6          | РАЗДЕЛ 3<br>Модели компьютерных систем с мандатным управлением доступа                   | ПК1 - текущ. контроль по разделам 1,2,3                          | 2                                               |
| 8     | 6          | РАЗДЕЛ 4<br>Модели безопасности информационных потоков и изолированной программной среды | Безопасность переходов                                           | 2                                               |
| 9     | 6          | РАЗДЕЛ 4<br>Модели безопасности информационных потоков и изолированной программной среды | Потенциальная модификация сущности                               | 2                                               |
| 10    | 6          | РАЗДЕЛ 6<br>Развитие формальных моделей безопасности компьютерных систем                 | Модель мандатного ролевого управления доступом                   | 4                                               |

| № п/п  | № семестра | Тема (раздел) учебной дисциплины                                         | Наименование занятий                       | Всего часов/ из них часов в интерактивной форме |
|--------|------------|--------------------------------------------------------------------------|--------------------------------------------|-------------------------------------------------|
| 1      | 2          | 3                                                                        | 4                                          | 5                                               |
| 11     | 6          | РАЗДЕЛ 6<br>Развитие формальных моделей безопасности компьютерных систем | ПК2 - текущ. контроль по разделам 4, 5, 6. | 2                                               |
| ВСЕГО: |            |                                                                          |                                            | 34 / 0                                          |

#### 4.5. Примерная тематика курсовых проектов (работ)

Курсовые работы (проекты) не предусмотрены.

## 5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Преподавание дисциплины «Модели безопасности компьютерных систем» осуществляется в форме лекций, лабораторных работ и практических занятий. Лекции проводятся в традиционной классно-урочной организационной форме, по типу управления познавательной деятельностью на 30 % являются традиционными классически-лекционными (объяснительно-иллюстративные), и на 70 % с использованием интерактивных (диалоговых) технологий, в том числе мультимедиа лекция.

Практические занятия и лабораторные работы организованы с использованием технологий развивающего обучения. Часть практического курса выполняется в виде традиционных практических занятий (объяснительно-иллюстративное решение задач). Остальная часть практического курса проводится с использованием интерактивных (диалоговые) технологий, в том числе электронный практикум (решение проблемных поставленных задач с помощью современной вычислительной техники и исследование моделей); технологий, основанных на коллективных способах обучения, а так же использованием компьютерной тестирующей системы.

В ходе выполнения курсовой работы реализуются проектные и исследовательские методы обучения. Это позволяет развивать индивидуальные творческие способности обучающихся, более осознанно подходить к профессиональному и социальному самоопределению, самостоятельно пополнять свои знания, глубоко вникать в изучаемую проблему и предполагать пути ее решения, что важно при формировании мировоззрения. Это важно для определения индивидуальной траектории развития каждого обучающегося. Самостоятельная работа студента организована с использованием традиционных видов работы и интерактивных технологий. К традиционным видам работы относятся отработка лекционного материала и отработка отдельных тем по учебным пособиям. К интерактивным (диалоговым) технологиям относятся отработка отдельных тем по электронным пособиям, подготовка к промежуточным контролям в интерактивном режиме, интерактивные консультации в режиме реального времени по специальным разделам и технологиям, основанным на коллективных способах самостоятельной работы студентов.

Оценка полученных знаний, умений и навыков основана на модульно-рейтинговой технологии. Весь курс разбит на 6 разделов, представляющих собой логически завершённый объём учебной информации. Фонды оценочных средств освоенных компетенций включают как вопросы теоретического характера для оценки знаний, так и задания практического содержания (решение конкретных задач, работа с данными) для оценки умений и навыков. Теоретические знания проверяются путём применения таких организационных форм, как индивидуальные и групповые опросы, решение тестов с использованием компьютеров или на бумажных носителях.

## 6. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

| № п/п | № семестра | Тема (раздел) учебной дисциплины                                                         | Вид самостоятельной работы студента. Перечень учебно-методического обеспечения для самостоятельной работы                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Всего часов |
|-------|------------|------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| 1     | 2          | 3                                                                                        | 4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 5           |
| 1     | 6          | РАЗДЕЛ 1<br>Введение. Основные понятия и определения                                     | <p>Модели ценности информации</p> <ol style="list-style-type: none"> <li>1. Подготовка к практическому занятию.</li> <li>2. Повторение лекционного материала.</li> <li>3. Изучение учебной литературы из приведенных источников: [2, с.11-52], [доп. 2, стр.4-17].</li> <li>4. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины.</li> <li>5. Конспектирование изученного материала по темам:</li> </ol> <p>Модели ценности информации</p>                                                                            | 10          |
| 2     | 6          | РАЗДЕЛ 2<br>Модели компьютерных систем с дискреционным управлением доступа               | <p>Модели ХРУ и ТМД.</p> <ol style="list-style-type: none"> <li>1. Подготовка к практическому занятию.</li> <li>2. Повторение лекционного материала.</li> <li>3. Изучение учебной литературы из приведенных источников: [1 с.7-298,], [доп 2, с. с.19-72] .</li> <li>4. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины.</li> <li>5. Конспектирование изученного материала по темам:</li> </ol> <p>Модели ХРУ и ТМД.<br/>Классическая и расширенная модели Take-Grant</p>                                           | 10          |
| 3     | 6          | РАЗДЕЛ 3<br>Модели компьютерных систем с мандатным управлением доступа                   | <p>Модели решетки многоуровневой безопасности</p> <ol style="list-style-type: none"> <li>1. Подготовка к практическому занятию.</li> <li>2. Повторение лекционного материала.</li> <li>3. Подготовка к текущему контролю.</li> <li>4. Изучение учебной литературы из приведенных источников:, [1 с.7-298], [2 доп. с.69-103]</li> <li>5. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины.</li> <li>6. Конспектирование изученного материала по темам:</li> </ol> <p>Модели решетки многоуровневой безопасности.</p> | 16          |
| 4     | 6          | РАЗДЕЛ 4<br>Модели безопасности информационных потоков и изолированной программной среды | <p>Классическая модель Белла-Ла Падулы</p> <ol style="list-style-type: none"> <li>1. Подготовка к практическому занятию.</li> <li>2. Повторение лекционного материала.</li> <li>3. Изучение учебной литературы из приведенных источников: [1 с.7-298], [2 доп. с.157-170].</li> <li>4. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины.</li> <li>5. Конспектирование изученного материала</li> </ol>                                                                                                                | 10          |

|        |   |                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |    |
|--------|---|--------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
|        |   |                                                                          | по темам:<br>Классическая модель Белла-Ла Падулы                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |    |
| 5      | 6 | РАЗДЕЛ 5<br>Модели компьютерных систем с ролевым управлением доступа     | Модель ролевого управления доступом.<br>Иерархия ролей в модели мандатного ролевого управления доступом.<br>1. Подготовка к практическому занятию.<br>2. Повторение лекционного материала.<br>3. Изучение учебной литературы из приведенных источников: [1 с.7-298], [2 доп. с.234-253].<br>4. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины.<br>5. Конспектирование изученного материала по темам:<br>Модель ролевого управления доступом.<br>Иерархия ролей в модели мандатного ролевого управления доступом. | 14 |
| 6      | 6 | РАЗДЕЛ 6<br>Развитие формальных моделей безопасности компьютерных систем | Анализ в рамках ДП-моделей информационных потоков по памяти или по времени<br>1. Подготовка к практическому занятию.<br>2. Повторение лекционного материала.<br>3. Подготовка к текущему контролю.<br>4. Изучение учебной литературы из приведенных источников: [1 с.7-298], [2 доп. с. 199-230]<br>5. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины.<br>6. Конспектирование изученного материала по темам:<br>Анализ в рамках ДП-моделей информационных потоков по памяти или по времени.                      | 16 |
| ВСЕГО: |   |                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 76 |

## 7. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

### 7.1. Основная литература

| № п/п | Наименование                                                                                      | Автор (ы)                                     | Год и место издания<br>Место доступа                                                   | Используется при изучении разделов, номера страниц |
|-------|---------------------------------------------------------------------------------------------------|-----------------------------------------------|----------------------------------------------------------------------------------------|----------------------------------------------------|
| 1     | Информационная безопасность и защита информации                                                   | В.П. Мельников, С.А. Клейменов, А.М. Петраков | Издательский центр "Академия", 2012<br>ИТБ УЛУПС (Абонемент ЮИ);<br>ИТБ УЛУПС (ЧЗ1 ЮИ) | Все разделы                                        |
| 2     | Модели безопасности компьютерных систем                                                           | П.Н. Девянин                                  | Академия, 2005<br>НТБ (фб.)                                                            | Все разделы                                        |
| 3     | Информационная безопасность и защита информации в корпоративных сетях железнодорожного транспорта | В.В. Яковлев, А.А. Корниенко                  | УМК МПС России, 2002<br>НТБ (уч.4); НТБ (фб.); НТБ (чз.1)                              | Все разделы                                        |

### 7.2. Дополнительная литература

| № п/п | Наименование                                                                                                                                                           | Автор (ы)             | Год и место издания<br>Место доступа            | Используется при изучении разделов, номера страниц |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|-------------------------------------------------|----------------------------------------------------|
| 4     | Модели безопасности компьютерных систем. Управление доступом и информационными потоками                                                                                | Девянин П.Н.          | М: Горячая линия-Телеком - 2011, 0<br>НТБ (фб.) | Все разделы                                        |
| 5     | Применение объектно-ориентированных моделей разграничения доступа к анализу безопасности ряда компьютерных систем (Математические структуры и моделирование №2, 2016). | С.В. БЕЛИМ, С.В. УСОВ | Лань, 2016<br>ЭБС Лань; elibrary.ru             | Все разделы                                        |

## 8. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ "ИНТЕРНЕТ", НЕОБХОДИМЫЕ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

<http://library.miit.ru/> - электронно-библиотечная система Научно-технической библиотеки МИИТ.

<http://elibrary.ru/> - научно-электронная библиотека.

<http://robotosha.ru/>

[www.chipinfo.ru](http://www.chipinfo.ru).

<http://siblec.ru/>

<http://autex.ru/>

<http://www.intuit.ru>

<http://twirpx.com>

<http://habrahabr.ru>

<http://semestr.ru>

<http://www.cisco.ru>

Поисковые системы: Yandex, Google, Mail, база научно-технической информации ВИНТИ РАН.

## **9. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)**

Для проведения лекционных занятий необходима специализированная лекционная аудитория с мультимедиа аппаратурой и интерактивной доской.

Для проведения практических занятий необходимы компьютеры с рабочими местами в компьютерном классе. Компьютеры должны быть обеспечены лицензионными программными продуктами:

Microsoft Office или Work 9,

среда разработки программного обеспечения HTML5 и PHP.

Для проведения практических занятий и необходимо иметь комплекс программ для ПЭВМ, обеспечивающих возможность выполнения работ:

в области построения программных и аппаратных средств защиты информации в телекоммуникационных сетях (iOS15 Cisco и выше);

программные продукты Mac OS server, XSan.

## **10. ОПИСАНИЕ МАТЕРИАЛЬНО ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)**

Для проведения аудиторных занятий и самостоятельной работы требуется:

1. Рабочее место преподавателя с персональным компьютером, подключённым к сетям INTERNET и INTRANET.

2. Специализированная лекционная аудитория с мультимедиа аппаратурой и интерактивной доской.

3. Компьютерный класс. Рабочие места студентов в компьютерном классе, подключённые к сетям INTERNET и INTRANET

4. Для проведения практических занятий: компьютерный класс; компьютеры с минимальными требованиями – Core 5, ОЗУ 4 ГБ, HDD 300 ГБ, wifi, USB 2.0.

## **11. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)**

Обучающимся необходимо помнить, что качество полученного образования в немалой степени зависит от активной роли самого обучающегося в учебном процессе.

Обучающийся должен быть нацелен на максимальное усвоение подаваемого лектором материала, после лекции и во время специально организуемых индивидуальных встреч он может задать лектору интересующие его вопросы.

Лекционные занятия составляют основу теоретического обучения и должны давать систематизированные основы знаний по дисциплине, раскрывать состояние и перспективы развития соответствующей области науки, концентрировать внимание обучающихся на наиболее сложных и узловых вопросах, стимулировать их активную познавательную деятельность и способствовать формированию творческого мышления. Главная задача лекционного курса – сформировать у обучающихся системное представление об изучаемом предмете, обеспечить усвоение будущими специалистами основополагающего учебного материала, принципов и закономерностей развития соответствующей научно-практической области, а также методов применения полученных знаний, умений и навыков.

Основные функции лекций: 1. Познавательная-обучающая; 2. Развивающая; 3. Ориентирующе-направляющая; 4. Активизирующая; 5. Воспитательная; 6.

Организирующая; 7. информационная.

Выполнение практических заданий и лабораторных работ служит важным связующим звеном между теоретическим освоением данной дисциплины и применением ее положений на практике. Они способствуют развитию самостоятельности обучающихся, более активному освоению учебного материала, являются важной предпосылкой формирования профессиональных качеств будущих специалистов.

Проведение практических занятий и лабораторных работ не сводится только к органическому дополнению лекционных курсов и самостоятельной работы обучающихся. Их вместе с тем следует рассматривать как важное средство проверки усвоения обучающимися тех или иных положений, даваемых на лекции, а также рекомендуемой для изучения литературы; как форма текущего контроля за отношением обучающихся к учебе, за уровнем их знаний, а следовательно, и как один из важных каналов для своевременного подтягивания отстающих обучающихся.

При подготовке специалиста важны не только серьезная теоретическая подготовка, но и умение ориентироваться в разнообразных практических ситуациях, ежедневно возникающих в его деятельности. Этому способствует форма обучения в виде практических занятий и лабораторных работ. Задачи практических занятий и лабораторных работ: закрепление и углубление знаний, полученных на лекциях и приобретенных в процессе самостоятельной работы с учебной литературой, формирование у обучающихся умений и навыков работы с исходными данными, научной литературой и специальными документами. Практическому занятию и лабораторной работе должно предшествовать ознакомление с лекцией на соответствующую тему и литературой, указанной в плане этих занятий.

Самостоятельная работа может быть успешной при определенных условиях, которые необходимо организовать. Ее правильная организация, включающая технологии отбора целей, содержания, конструирования заданий и организацию контроля, систематичность самостоятельных учебных занятий, целесообразное планирование рабочего времени позволяет привить студентам умения и навыки в овладении, изучении, усвоении и систематизации приобретаемых знаний в процессе обучения, привить навыки повышения профессионального уровня в течение всей трудовой деятельности.

Каждому студенту следует составлять еженедельный и семестровый планы работы, а также план на каждый рабочий день. С вечера всегда надо распределять работу на завтра. В конце каждого дня целесообразно подводить итог работы: тщательно проверить, все ли выполнено по намеченному плану, не было ли каких-либо отступлений, а если были, по какой причине это произошло. Нужно осуществлять самоконтроль, который является необходимым условием успешной учебы. Если что-то осталось невыполненным, необходимо изыскать время для завершения этой части работы, не уменьшая объема недельного плана.

Компетенции обучающегося, формируемые в результате освоения учебной дисциплины, рассмотрены через соответствующие знания, умения и владения. Для проверки уровня освоения дисциплины предлагаются вопросы к экзамену и тестовые материалы, где каждый вариант содержит задания, разработанные в рамках основных тем учебной дисциплины и включающие терминологические задания.

Фонд оценочных средств является составной частью учебно-методического обеспечения процедуры оценки качества освоения образовательной программы и обеспечивает повышение качества образовательного процесса и входит, как приложение, в состав рабочей программы дисциплины.

Основные методические указания для обучающихся по дисциплине указаны в разделе основная и дополнительная литература.