

Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«Алтайский государственный технический университет им. И.И. Ползунова»

**СОГЛАСОВАНО**

Декан ФИТ  
Авдеев

А.С.

## **Рабочая программа дисциплины**

**Код и наименование дисциплины: Б1.О.39 «Моделирование и анализ процессов, систем и объектов защиты информации»**

**Код и наименование направления подготовки (специальности): 10.03.01  
Информационная безопасность**

**Направленность (профиль, специализация): Организация и технологии защиты информации (в сфере техники и технологий, связанных с обеспечением защищенности объектов информатизации)**

**Статус дисциплины: обязательная часть**

**Форма обучения: очная**

| <b>Статус</b>     | <b>Должность</b>                                | <b>И.О. Фамилия</b> |
|-------------------|---|---------------------|
| <b>Разработал</b> | старший преподаватель                           | Л.Д. Алфёрова       |
|                   | доцент  | Е.В. Шарлаев        |
| <b>Согласовал</b> | Зав. кафедрой «ИВТиИБ»                          | А.Г. Якунин         |
|                   | руководитель направленности (профиля) программы | Е.В. Шарлаев        |

г. Барнаул

## 1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

| Компетенция | Содержание компетенции   | Индикатор | Содержание индикатора   |
|-------------|--|-----------|---|
| ОПК-2.1     | Способен проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба | ОПК-2.1.1 | Анализирует процессы, системы и объекты защиты информации                               |
|             |  | ОПК-2.1.2 | Способен выявлять источники информационных угроз и определять уязвимости объекта защиты |
|             |  | ОПК-2.1.3 | Способен моделировать объекты защиты и их информационные составляющие                   |

## 2. Место дисциплины в структуре образовательной программы

|   |   |
|---|---|
| Дисциплины (практики), предшествующие изучению дисциплины, результаты освоения которых необходимы для освоения данной дисциплины.                 | Защита информации от утечки по техническим каналам, Информационные процессы и системы, Методы принятия организационно-технических решений, Организационное и правовое обеспечение информационной безопасности, Основы информационной безопасности, Основы управления проектами, Программно-аппаратные средства защиты информации, Технология проведения исследования защищенности объектов и средств защиты   |
| Дисциплины (практики), для которых результаты освоения данной дисциплины будут необходимы, как входные знания, умения и владения для их изучения. | Организация и проведение аудита защищенности объекта информатизации, Организация и технологии защиты данных в информационных системах, Подготовка к процедуре защиты и защита выпускной квалификационной работы, Преддипломная практика, Применение интеллектуальных технологий при проектировании элементов систем защиты информации, Разработка организационно-распорядительной документации по защите информации, Современные средства проектирования и разработки программных компонентов системы защиты информации |

## 3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающегося с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающегося

Общий объем дисциплины в з.е. /час: 4 / 144

Форма промежуточной аттестации: Экзамен

| Форма обучения | Виды занятий, их трудоемкость (час.) |                     |                      |                        | Объем контактной работы обучающегося с преподавателем (час) |
|----------------|--------------------------------------|---------------------|----------------------|------------------------|---|
|                | Лекции                               | Лабораторные работы | Практические занятия | Самостоятельная работа |   |
| очная          | 32                                   | 32                  | 0                    | 80                     | 71  |

**4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий**

**Форма обучения: очная**

**Семестр: 6**

**Лекционные занятия (32ч.)**

- 1. Основные принципы и технологии моделирования процессов и систем защиты информации. {лекция с разбором конкретных ситуаций} (4ч.) [1,2,3,4,5,6,7,8,9,10] Структура и свойства оценки процессов и систем. Модели управления качеством процессов и систем. Основы системного подхода при моделировании процессов и систем СИ**
- 2. Принципы организации и этапы разработки модели системы защиты информации {лекция с разбором конкретных ситуаций} (4ч.) [1,2,3,4,5,6,7,8,9,10] Методологические основы организации СЗИ. Цели, задачи и принципы построения системы обеспечения безопасности информации. Требования, предъявляемые к системе обеспечения безопасности информации. Этапы разработки системы обеспечения безопасности информации**
- 3. Факторы, влияющие на организацию системы защиты информации. Перечень факторов влияющих на организацию СОИБ {лекция с разбором конкретных ситуаций} (6ч.) [1,2,3,4,5,6,7,8,9,10] Факторы, определяющие особенности защиты информации ограниченного доступа. Факторы, оказывающие влияние на построение СОИБ. Факторы определяющие особенности для ГИС и ИСПДн**
- 4. Моделирование технологических процессов. {лекция с разбором конкретных ситуаций} (6ч.) [1,2,3,4,5,6,7,8,9,10] Методы математического моделирования процессов в системах СИ. Построение эмпирических регрессионных моделей**
- 5. Методы имитационного моделирования процессов в системах СИ. Использование компьютерных пакетов для моделирования систем СИ {лекция с разбором конкретных ситуаций} (4ч.) [1,2,3,4,5,6,7,8,9,10] Математический пакет Matchad как основа формирования цифровых процессов и систем СИ**
- 6. Моделирование объектов информатизации для оценки рисков. {лекция с разбором конкретных ситуаций} (4ч.) [1,2,3,4,5,6,7,8,9,10] Применение теории**

нечетких множеств при анализе рисков информационной безопасности. Оценка уязвимостей

7. Анализ функционального процесса защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, путей реализации, предполагаемого ущерба. {лекция с разбором конкретных ситуаций} (4ч.)[1,2,3,4,5,6,7,8,9,10] Процессы и системы при проверке информационной защищенности. Методика оценки угроз безопасности информации.

#### Лабораторные работы (32ч.)

1. Поиск и анализ программного обеспечения для оценки рисков организации. Риск-ориентированный подход. {работа в малых группах} (4ч.)[1,2,3,4,5,6,7,8,9,10]

2. Использование компьютерных пакетов для моделирования системЗИ {работа в малых группах} (8ч.)[1,2,3,4,5,6,7,8,9,10] Построению системы защиты информационных систем данных в организации

3. Модели системы обеспечения информационной безопасности и ее информационных составляющих. {работа в малых группах} (6ч.)[1,2,3,4,5,6,7,8,9,10]

4. Исследование оценок при проверке информационной защищенности на соответствие нормативных документов {работа в малых группах} (4ч.)[1,2,3,4,5,6,7,8,9,10]

5. Моделирование системы управления инцидентами информационной безопасности {работа в малых группах} (6ч.)[1,2,3,4,5,6,7,8,9,10]

6. Применение оценки информационных рисков на основе когнитивных карт для типового объекта информатизации {работа в малых группах} (4ч.)[1,2,3,4,5,6,7,8,9,10]

#### Самостоятельная работа (80ч.)

1. Подготовка к текущим занятиям, самостоятельное изучение материала {с элементами электронного обучения и дистанционных образовательных технологий} (44ч.)[1,2,3,4,5,6,7,8,9,10]

2. Подготовка к экзамену {с элементами электронного обучения и дистанционных образовательных технологий} (36ч.)[1,2,3,4,5,6,7,8,9,10]

5. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

Для каждого обучающегося обеспечен индивидуальный неограниченный доступ к электронной информационно-образовательной среде АлтГТУ:

1. Методические указания по выполнению практических работ по

дисциплине «Нормативные акты и стандарты по информационной безопасности»/Л.Д. Алферова; АлтГТУ им. И.И. Ползунова.- Барнаул, 2015.- 21 с. -  
<http://elib.altstu.ru/eum/download/ivtib/uploads/alferova-l-d-ivtiib-563b0b4c3de4a.pdf>

## 6. Перечень учебной литературы

### 6.1. Основная литература

2. Аверченков, В.И. Аудит информационной безопасности : учебное пособие для вузов / В.И. Аверченков. - 3-е изд., стер. - Москва : Издательство «Флинта», 2016. - 269 с. - Библиогр. в кн. - ISBN 978-5-9765-1256-6 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=93245>

3. Загинайлов, Ю.Н. Организационно-правовое обеспечение информационной безопасности. В 2-х частях. Правовое обеспечение информационной безопасности: Учебное пособие. Ч. 1 /Ю. Н. Загинайлов.- Барнаул : Изд-во АлтГТУ , 2012 - 172 с. -Режим доступа:

<http://new.elib.altstu.ru/eum/download/vsib/zaginajlov-opobespet.pdf>

4. Ширялкин, А.Ф. Стандартизация и техническое регулирование : учебно-практическое пособие / А.Ф. Ширялкин ; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования "Ульяновский государственный технический университет", д.и. Институт. - Ульяновск : УлГТУ, 2013. - 196 с. : ил., табл., схем. - Библиогр. в кн. - ISBN 978-5-9795-1153-5 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=363509>.

### 6.2. Дополнительная литература

5. Грибунин В.Г. Комплексная система защиты информации на предприятии: учебник для студ. высш. учеб. заведений./ В.Г.Грибунин, В.В. Чудовский.- М.: Издательский центр «Академия», 2009.-412с. ( 25 экз. Гриф УМО)

6. Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю.Н. Загинайлов. - М. ; Берлин : Директ-Медиа, 2015. - 253 с. : ил. - Библиогр. в кн. - ISBN 978-5-4475-3946-7 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=276557>

**7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины**

7. Официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК) России [электронный ресурс]:- режим доступа: <http://www.fstec.ru>.

8. Правовая справочная система «Гарант» [электронный ресурс] <http://www.garant.ru>

9. Официальный сайт Совета Безопасности Российской Федерации <http://www.scrf.gov.ru/>

10. Официальный сайт федерального агентства по техническому регулированию и метрологии [электронный ресурс]: режим доступа: <http://protect.gost.ru//>

**8. Фонд оценочных материалов для проведения текущего контроля успеваемости и промежуточной аттестации**

Содержание промежуточной аттестации раскрывается в комплекте контролирующих материалов, предназначенных для проверки соответствия уровня подготовки по дисциплине требованиям ФГОС, которые хранятся на кафедре-разработчике РПД в печатном виде и в ЭИОС.

**9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем**

Для успешного освоения дисциплины используются ресурсы электронной информационно-образовательной среды, образовательные интернет-порталы, глобальная компьютерная сеть Интернет. В процессе изучения дисциплины происходит интерактивное взаимодействие обучающегося с преподавателем через личный кабинет студента.

| №пп | Используемое программное обеспечение |
|-----|--------------------------------------|
| 1   | Acrobat Reader                       |
| 1   | LibreOffice                          |
| 2   | Windows                              |
| 3   | Linux                                |
| 3   | Антивирус Kaspersky                  |

| №пп | Используемые профессиональные базы данных и информационные справочные системы  |
|-----|--|
| 1   | Национальная электронная библиотека (НЭБ) – свободный доступ читателей к фондам российских библиотек. Содержит коллекции оцифрованных документов (как открытого доступа, так и ограниченных авторским правом), а также каталог изданий, хранящихся в библиотеках России. ( <a href="http://нэб.рф/">http://нэб.рф/</a> ) |

**10. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине**

|  |
|--|
| <b>Наименование специальных помещений и помещений для самостоятельной работы</b> |
| учебные аудитории для проведения учебных занятий                                 |
| помещения для самостоятельной работы   |

Материально-техническое обеспечение и организация образовательного процесса по дисциплине для инвалидов и лиц с ограниченными возможностями здоровья осуществляется в соответствии с «Положением об обучении инвалидов и лиц с ограниченными возможностями здоровья».