

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

**СОГЛАСОВАНО**

Декан ФИТ

А.С. Авдеев

## **Рабочая программа дисциплины**

Код и наименование дисциплины: **Б1.О.40 «Организация и проведение аудита защищенности объекта информатизации»**

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>
Разработал	старший преподаватель доцент	Л.Д. Алфёрова Е.В. Шарлаев
Согласовал	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-2.4	Способен проводить аудит защищенности объекта информатизации в соответствии с нормативными документами	ОПК-2.4.1	Демонстрирует знание нормативных документов по проведению аудита защищенности объекта информатизации
		ОПК-2.4.2	Способен применять методики проведения аудита защищенности объекта информатизации

## 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, Методы и средства криптографической защиты информации, Моделирование и анализ процессов, систем и объектов защиты информации, Организационное и правовое обеспечение информационной безопасности, Программно-аппаратные средства защиты информации, Сети и системы передачи информации, Технологии защиты информации в вычислительных сетях
Дисциплины (практики), для которых результаты освоения данной дисциплины будут необходимы, как входные знания, умения и владения для их изучения.	Комплексная защита объектов информатизации, Подготовка к процедуре защиты и защита выпускной квалификационной работы, Преддипломная практика, Проектирование компонентов системы защиты объектов информатизации, Разработка организационно-распорядительной документации по защите 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: Зачет

Форма обучения	Виды занятий, их трудоемкость (час.)				Объем контактной работы обучающегося с преподавателем (час)
	Лекции	Лабораторные работы	Практические занятия	Самостоятельная работа	
очная	32	0	48	64	90

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

**Форма обучения: очная**

**Семестр: 7**

**Лекционные занятия (32ч.)**

- 1. Введение. Организация и проведение аудита защищенности объекта информатизации. {лекция с разбором конкретных ситуаций} (4ч.)[1,2,3,4,5,6,7,8,9]** Постановка проблемы. Задачи. Формы и цели аудита. Общие понятия и определения.
- 2. Аудит информационной безопасности компании {с элементами электронного обучения и дистанционных образовательных технологий} (6ч.)[1,2,3,4,5,6,7,8,9]** Профессиональная квалификация аудитора. Этика аудитора ИТ-инфраструктуры. Критерии аудита. Законодательная и нормативная база аудита.
- 3. Стандарты и критерии проведения аудита информационной безопасности. {дискуссия} (4ч.)[1,2,3,4,5,6,7,8,9]** Общие критерии. Отечественные и международные стандарты. Управление и аудит ИТ.
- 4. Практики и методики оценки информационной защищенности объекта информатизации {лекция с разбором конкретных ситуаций} (4ч.)[1,2,3,4,5,6,7,8,9]** Особенности оценки информационной безопасности организаций банковской системы. Аудит управления непрерывностью бизнеса и восстановления после сбоев. Особенности аудита информационной безопасности организаций, использующих аутсорсинг. Текущий и регулярный аудит
- 5. Инструментальные средства аудита безопасности компании. {лекция с разбором конкретных ситуаций} (6ч.)[1,2,3,4,5,6,7,8,9]** Методы и инструментальные средства аудита безопасности.
- 6. Применение методик проведения аудита защищенности объекта информации. {лекция с разбором конкретных ситуаций} (2ч.)[1,2,3,4,5,6,7,8,9]** Особенности применения методик проведения аудита в органах государственной власти.
- 7. Методология аудита информационной безопасности. Организация процесса аудита. {лекция с разбором конкретных ситуаций} (6ч.)[1,2,3,4,5,6,7,8,9]** Основные этапы и методы работ по проведению аудита безопасности. Сбор исходной информации Цели сбора, методы, общие исходные данные. Порядок планирования аудита. Анализ значимости информационных ресурсов. Анализ процесса обработки информации. Отчетные материалы. Требования к документированию результатов.

### **Практические занятия (48ч.)**

- 1. Организация процесса аудита информационной безопасности. {имитация} (6ч.)[1,2,3,4,5,6,7,8,9]** Сбор данных, сбор дополнительных исходных данных, постановка цели и задач. Анализ значимости информационных ресурсов. Применение методологии аудита информационной безопасности.
- 2. Применение практик и методик оценки информационной защищенности объекта информатизации на соответствие нормативных документов {работа в малых группах} (8ч.)[1,2,3,4,5,6,7,8,9]**
- 3. Проведение аудита информационной безопасности ИТ-инфраструктуры с помощью инструментальных средств. {работа в малых группах} (6ч.)[1,2,3,4,5,6,8,9]**
- 4. Проведение аудита информационной безопасности ИТ-инфраструктуры с применением программных средств управления рисками {работа в малых группах} (6ч.)[1,2,3,4,5,6,8,9]**
- 5. Проведение тестовых испытаний программных средств защиты. {работа в малых группах} (8ч.)[1,2,3,4,5,6,8,9]** Проведение тестовых испытаний программных средств защиты (испытание функций защиты от НСД). Моделирование действий злоумышленника. Особенности тестовых испытаний рабочих станций (АРМ), серверного оборудования, VPN-устройств.
- 6. Проведение анализа организационно-распорядительных документов и выполнения организационно-технических требований по защите информации. {с элементами электронного обучения и дистанционных образовательных технологий} (4ч.)[1,2,3,4,5,6,7,8,9]**
- 7. Демонстрация знаний нормативных документов по проведению аудита защищенности объекта информатизации {творческое задание} (6ч.)[1,2,3,4,5,6,7,8,9]**
- 8. Подготовка отчетных материалов. Документирование результатов и подведение итогов проведения аудита защищенности объекта информатизации. {работа в малых группах} (4ч.)[1,2,3,4,5,6,7,8,9]**

### **Курсовые работы (24ч.)**

- 1. Защита курсовых работ {разработка проекта} (24ч.)[1,2,3,4,5,6,7,8,9]**

### **Самостоятельная работа (64ч.)**

- 1. Подготовка к текущим занятиям, к контрольной работе, самостоятельное изучение материала {с элементами электронного обучения и дистанционных образовательных технологий} (58ч.)[1,2,3,4,5,6,7,8,9]**
- 2. Подготовка к зачету {с элементами электронного обучения и дистанционных образовательных технологий} (6ч.)[1,2,3,4,5,6,7,8,9]**

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

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

1. 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>

## **6. Перечень учебной литературы**

### **6.1. Основная литература**

2. Аверченков, В.И. Аудит информационной безопасности : учебное пособие для вузов / В.И. Аверченков. - 2-е изд., стер. - М. : Флинта, 2011. - 269 с. - ISBN 978-5-9765-1256-6 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=93245> (12.04.2017)

3. 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. - Библ. 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**

4. 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>

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», 2008.-320с. ( 25 экз. Гриф УМО)

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

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

www.fstec.ru

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

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

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

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

Содержание промежуточной аттестации раскрывается в комплекте контролируемых 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.

<b>№пп</b>	<b>Используемое программное обеспечение</b>
1	Acrobat Reader
1	LibreOffice
2	Chrome
2	Windows
3	Debian
3	Антивирус Kaspersky
5	Linux
8	Гарант

<b>№пп</b>	<b>Используемые профессиональные базы данных и информационные справочные системы</b>
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».