

**МИНОБРНАУКИ РОССИИ**

**Федеральное государственное бюджетное образовательное  
учреждение высшего образования "Пермский  
государственный национальный исследовательский  
университет"**

**Кафедра радиоэлектроники и защиты информации**

Авторы-составители: **Сеник Кирилл Александрович  
Лунегов Игорь Владимирович**

Рабочая программа дисциплины

**АУДИТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СИСТЕМ ОБЕСПЕЧЕНИЯ  
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Код УМК 94427

Утверждено  
Протокол №4  
от «24» июня 2020 г.

Пермь, 2020

## **1. Наименование дисциплины**

Аудит информационных технологий и систем обеспечения информационной безопасности

## **2. Место дисциплины в структуре образовательной программы**

Дисциплина входит в обязательную часть Блока « С.1 » образовательной программы по направлениям подготовки (специальностям):

Специальность: **10.05.03** Информационная безопасность автоматизированных систем  
направленность Безопасность открытых информационных систем

### **3. Планируемые результаты обучения по дисциплине**

В результате освоения дисциплины **Аудит информационных технологий и систем обеспечения информационной безопасности** у обучающегося должны быть сформированы следующие компетенции:

**10.05.03** Информационная безопасность автоматизированных систем (направленность : Безопасность открытых информационных систем)

**ПК.21** способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы

**ПК.24** способность проводить анализ особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите

**ПК.25** способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации

**ПК.26** способность формировать комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной системы

**ПК.30** способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы

**ПК.31** способность управлять информационной безопасностью автоматизированной системы

#### 4. Объем и содержание дисциплины

<b>Направления подготовки</b>	10.05.03 Информационная безопасность автоматизированных систем (направленность: Безопасность открытых информационных систем)
<b>форма обучения</b>	очная
<b>№№ триместров, выделенных для изучения дисциплины</b>	14
<b>Объем дисциплины (з.е.)</b>	3
<b>Объем дисциплины (ак.час.)</b>	108
<b>Контактная работа с преподавателем (ак.час.), в том числе:</b>	42
<b>Проведение лекционных занятий</b>	14
<b>Проведение лабораторных работ, занятий по иностранному языку</b>	28
<b>Самостоятельная работа (ак.час.)</b>	66
<b>Формы текущего контроля</b>	Входное тестирование (1) Итоговое контрольное мероприятие (1) Письменное контрольное мероприятие (3)
<b>Формы промежуточной аттестации</b>	Зачет (14 триместр)

## **5. Аннотированное описание содержания разделов и тем дисциплины**

### **Аудит информационных технологий и систем обеспечения информационной безопасности**

#### **1. Введение. Основы аудита**

Основные понятия, термины и определения. Предмет и задачи дисциплины. Цели и задачи курса и его место в подготовке магистров. Взаимосвязь курса с другими дисциплинами учебного плана. Методические материалы. Периодические издания. Обязательная и дополнительная литература. Определение входных данных оценки. Роли и обязанности по проведению оценивания. Модель оценки процесса. Мероприятия процесса оценивания и выходные данные оценивания. Факторы успешной оценки процесса. Внутренний и внешний аудит. Модели безопасности бизнеса

#### **2. Основы построения систем защиты информации в информационных системах**

Цель и задачи информационной безопасности. Угрозы ИБ и их источники. Модель построения системы информационной безопасности предприятия. Методы и средства построения системы информационной безопасности предприятия

#### **3. Базовые вопросы управления информационной безопасностью. Риски информационной безопасности**

Система управления информационной безопасностью (СУИБ). Понятие аудита безопасности. Методы анализа данных при аудите ИБ.

Цель процесса анализа рисков ИБ. Этапы и участники процесса анализа рисков ИБ. Разработка Методики анализа рисков ИБ.

Инвентаризация активов. Понятие актива. Типы активов. Источники информации об активах организации.

Выбор угроз ИБ и уязвимостей для выделенных на этапе инвентаризации активов. Оценка рисков ИБ. Планирование мер по обработке выявленных рисков ИБ. Утверждение результатов анализа рисков ИБ у высшего руководства. Использование результатов анализа рисков ИБ

#### **4. Аудит информационной безопасности и методы его проведения**

Планирование программы аудита информационной безопасности. Реализация программы аудита информационной безопасности. Контроль и совершенствование программы аудита информационной безопасности. Методы оценивания информационной безопасности. Оценивание информационной безопасности на основе показателей информационной безопасности. Исследование полученных оценок информационной безопасности. Оценивание результатов аудита и самооценки информационной безопасности. Оценивание процессов проведения аудита и самооценки информационной безопасности. Риск-ориентированная интерпретация полученных оценок информационной безопасности. Выработка рекомендаций и подготовка отчетных документов. Экономическая оценка обеспечения ИБ

#### **5. Средства проведения аудита информационной безопасности информационных систем**

Анкетирование. Вопросные листы. Интервью. Опросы. Программные средства аудита. Сетевые сканеры. Средства тестирования доступа к ресурсам. Средства контроля целостности. Средства инвентаризации ресурсов. Средства встроенные в DLP-системы. Средства встроенные в средства защиты от несанкционированного доступа. Средства встроенные в ERP- системы. Средства операционных систем и сетей. Средства оценки утечки по техническим каналам. Аппаратные средства тестирования сетей. Поисковое оборудование специальных проверок и специальных исследований. Измерительное оборудование оценки технических каналов утечки. Программы оценки рисков информационной безопасности

#### **6. Стандарты в области информационной безопасности**

Предпосылки создания стандартов ИБ. Стандарт COBIT. Стандарты семейств ГОСТ Р ИСО/МЭК 27001,

ISO/IEC 18044, ISO/IEC 25999, ГОСТ Р ИСО/МЭК 27001. Американские стандарты NIST, британские стандарты BS, немецкие стандарты BSI в области информационной безопасности

Предпосылки введения международного стандарта ISO 15408. Основные понятия общих критериев. Методология оценки безопасности информационных технологий по общим критериям. Оценка уровня доверия функциональной безопасности ИТ. Обзор классов и семейств общих критериев.

Нормативные документы ФСТЭК РФ и ФСБ РФ как критерии аудита ИБ и ИТ. Стандарты ЦБ РФ в области информационной безопасности в банковской сфере

## **7. Стандарт управления информационной безопасностью ГОСТ Р ИСО 17799**

Назначение стандарта ISO 17799 для управления информационной безопасностью.

Практика прохождения аудита и получения сертификата ИСО 17799. Политика безопасности.

Организационные меры по обеспечению информационной безопасности. Классификация ресурсов и их контроль. Безопасность персонала. Физическая безопасность. Администрирование компьютерных систем и вычислительных сетей. Управление доступом к системам. Разработка и сопровождение информационных систем. Планирование бесперебойной работы организации. Соответствие системы основным требованиям

## **8. Оценка безопасности информационных технологий на основе международных стандартов.**

### **Методика проведения аудита информационной безопасности на предприятии**

Методика проведения аудита информационной безопасности на предприятии в соответствии с требованиями международных стандартов. Сертификация по ISO/IEC 27001 или ГОСТ Р ИСО/МЭК 27001. Период эксплуатации СУИБ перед сертификацией. Органы по сертификации, работающие в РФ (их различия и требования). Этапы сертификационного аудита. Решение о сертификации

## **9. Особенности аудита информационной безопасности организаций банковской системы РФ.**

### **Стандарты Центрального банка России.**

Направления обеспечения и оценки информационной безопасности. Размерность и значимость объектов оценки при проведении аудита информационной безопасности. Работы по созданию системы оценки информационной безопасности организаций банковской системы Российской Федерации. Аудит в области информационной безопасности Центрального банка России. Отчетность по результатам аудита

## **10. Аудит управления непрерывностью бизнеса и восстановления после сбоев**

Методологии, стандарты и нормативные требования в области управления непрерывностью бизнеса.

Основные цели аудита в области непрерывности бизнеса. Основные вопросы, рассматриваемые при аудите управления непрерывностью бизнеса и восстановления после сбоев. Реализация аудита.

Заключительные процедуры аудита. Особенности аудита информационной безопасности организаций, использующих аутсорсинг

## **11. Особенности аудита безопасности в области поиска средств негласного съема информации**

проверки технических средств и помещений на наличие средств негласного съема информации.

Технические средства аудита и проверок. Порядок и особенности проверок. Средства сигнализации использования закладных устройств

## **12. Аттестация объектов информатизации как аудит информационной безопасности объектов информатизации**

Виды объектов информатизации. Особенности аттестации объектов информатизации обрабатывающих государственную тайну, коммерческую тайну, служебную информацию ограниченного распространения, государственные информационные системы. Документация подготавливаемая заказчиком к аттестации. Виды и содержание аттестационных мероприятий и проверок.



## **6. Методические указания для обучающихся по освоению дисциплины**

Освоение дисциплины требует систематического изучения всех тем в той последовательности, в какой они указаны в рабочей программе.

Основными видами учебной работы являются аудиторные занятия. Их цель - расширить базовые знания обучающихся по осваиваемой дисциплине и систему теоретических ориентиров для последующего более глубокого освоения программного материала в ходе самостоятельной работы. Обучающемуся важно помнить, что контактная работа с преподавателем эффективно помогает ему овладеть программным материалом благодаря расстановке необходимых акцентов и удержанию внимания интонационными модуляциями голоса, а также подключением аудио-визуального механизма восприятия информации.

Самостоятельная работа преследует следующие цели:

- закрепление и совершенствование теоретических знаний, полученных на лекционных занятиях;
- формирование навыков подготовки текстовой составляющей информации учебного и научного назначения для размещения в различных информационных системах;
- совершенствование навыков поиска научных публикаций и образовательных ресурсов, размещенных в сети Интернет;
- самоконтроль освоения программного материала.

Обучающемуся необходимо помнить, что результаты самостоятельной работы контролируются преподавателем во время проведения мероприятий текущего контроля и учитываются при промежуточной аттестации.

Обучающимся с ОВЗ и инвалидов предоставляется возможность выбора форм проведения мероприятий текущего контроля, альтернативных формам, предусмотренным рабочей программой дисциплины. Предусматривается возможность увеличения в пределах 1 академического часа времени, отводимого на выполнение контрольных мероприятий.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации.

При проведении текущего контроля применяются оценочные средства, обеспечивающие передачу информации, от обучающегося к преподавателю, с учетом психофизиологических особенностей здоровья обучающихся.

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

При самостоятельной работе обучающимся следует использовать:

- конспекты лекций;
- литературу из перечня основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля);
- текст лекций на электронных носителях;
- ресурсы информационно-телекоммуникационной сети "Интернет", необходимые для освоения дисциплины;
- лицензионное и свободно распространяемое программное обеспечение из перечня информационных технологий, используемых при осуществлении образовательного процесса по дисциплине;
- методические указания для обучающихся по освоению дисциплины.



## **8. Перечень основной и дополнительной учебной литературы**

### **Основная:**

1. Миргородская Т. В. Аудит: учебное пособие / Т. В. Миргородская. - Москва: КНОРУС, 2016, ISBN 978-5-406-02669-4. - 3071. - Библиогр.: с. 271-274
2. Аверченков В. И. Аудит информационной безопасности: Учебное пособие для вузов / Аверченков В. И.. - Брянск: Брянский государственный технический университет, 2012, ISBN 978-89838-487-6. - 268. <http://www.iprbookshop.ru/6991>
3. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для бакалавриата и магистратуры / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2019. — 325 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-03600-8. — Текст : электронный // ЭБС Юрайт [сайт]. <https://www.urait.ru/bcode/432966>

### **Дополнительная:**

1. Информационное право. Информационная безопасность и защита информации: сб. нормативно - правовых актов / Перм. гос. ин-т искусства и культуры. - Пермь: [б. и.], 2004. - 328.
2. Аверченков В. И. Аудит информационной безопасности органов исполнительной власти: Учебное пособие / Аверченков В. И.. - Брянск: Брянский государственный технический университет, 2012, ISBN 978-89838-491-3. - 100. <http://www.iprbookshop.ru/6992>
3. Петренко В. И. Защита персональных данных в информационных системах: Учебное пособие / Петренко В. И.. - Ставрополь: Северо-Кавказский федеральный университет, 2016. - 201. <http://www.iprbookshop.ru/66023.html>

## 9. Перечень ресурсов сети Интернет, необходимых для освоения дисциплины

<https://www.securitycode.ru/> сайт компании код безопасности

<https://searchinform.ru/informatsionnaya-bezopasnost/> сайт компании SearchInform

<https://www.croc.ru/> Сайт компании Крок

## 10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

Образовательный процесс по дисциплине **Аудит информационных технологий и систем обеспечения информационной безопасности** предполагает использование следующего программного обеспечения и информационных справочных систем:

Образовательный процесс по дисциплине предполагает использование следующего информационных технологий, программного обеспечения и информационных справочных систем:

- презентационные материалы (слайды по темам лекционных и практических занятий);
- доступ в режиме on-line в Электронную библиотечную систему (ЭБС);
- доступ в электронную информационно-образовательную среду университета (ЕТИС ПГНИУ);
- интернет-сервисы и электронные ресурсы (поисковые системы, электронная почта, профессиональные тематические чаты и форумы, системы аудио и видео конференций, онлайн энциклопедии и т.д.).

Перечень используемого программного обеспечения:

- открытая система "ALT Linux"
- офисный пакет приложений "Libre office";
- приложение позволяющее просматривать и воспроизводить медиа контент PDF-файлов "Adobe Acrobat Reader DC";
- программы демонстрации видео материалов (проигрыватель) "Windows Media Player";
- программа просмотра интернет контента (браузер) "Google Chrome"

Дополнительно при проведении практических занятий используется следующее программное обеспечение:

- Средство Microsoft Baseline Security Analyzer (MBSA) версии 1.2.1 свободно распространяемая версия
- ПО "Гриф", "Кондор" компании Digital Security академическая лицензия
- ПО SIEM Splunk свободно распространяемая версия
- ПО "Wingdocs"свободно распространяемая версия
- ПО оценки рисков "RA 2A" свободно распространяемая версия.

Справочная система "Консультант плюс", "Гарант" онлайн версия

При освоении материала и выполнения заданий по дисциплине рекомендуется использование материалов, размещенных в Личных кабинетах обучающихся ЕТИС ПГНИУ (**student.psu.ru**).

При организации дистанционной работы и проведении занятий в режиме онлайн могут использоваться:

система видеоконференцсвязи на основе платформы BigBlueButton (<https://bigbluebutton.org/>).

система LMS Moodle (<http://e-learn.psu.ru/>), которая поддерживает возможность использования текстовых материалов и презентаций, аудио- и видеоконтент, а так же тесты, проверяемые задания, задания для совместной работы.

система тестирования Indigo (<https://indigotech.ru/>).

## 11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Лекционные занятия, групповые (индивидуальные) консультации, мероприятия текущего контроля и промежуточной аттестации проводятся в аудитории, оснащенной презентационной техникой (проектор,

экран для проектора, компьютер/ноутбук), а также меловой (и) или маркерной доской

Аудитория для лабораторных занятий, оснащенная презентационной техникой (проектор, экран для проектора, компьютер/ноутбук), а также меловой (и) или маркерной доской.

Аудитория для самостоятельной работы, в том числе помещения Научной библиотеки ПГНИУ, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет», обеспеченные доступом в электронную информационно-образовательную среду университета

Помещения научной библиотеки ПГНИУ для обеспечения самостоятельной работы обучающихся:

1. Научно-библиографический отдел, корп.1, ауд. 142. Оборудован 3 персональными компьютера с доступом к локальной и глобальной компьютерным сетям.

2. Читальный зал гуманитарной литературы, корп. 2, ауд. 418. Оборудован 7 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

3. Читальный зал естественной литературы, корп.6, ауд. 107а. Оборудован 5 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

4. Отдел иностранной литературы, корп.2 ауд. 207. Оборудован 1 персональным компьютером с доступом к локальной и глобальной компьютерным сетям.

5. Библиотека юридического факультета, корп.9, ауд. 4. Оборудована 11 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

6. Читальный зал географического факультета, корп.8, ауд. 419. Оборудован 6 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

Все компьютеры, установленные в помещениях научной библиотеки, оснащены следующим программным обеспечением:

Операционная система ALT Linux;

Офисный пакет Libreoffice.

Справочно-правовая система «КонсультантПлюс»

**Фонды оценочных средств для аттестации по дисциплине**  
**Аудит информационных технологий и систем обеспечения информационной безопасности**

**Планируемые результаты обучения по дисциплине для формирования компетенции.**  
**Индикаторы и критерии их оценивания**

**ПК.30**

**способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы**

<b>Компетенция (индикатор)</b>	<b>Планируемые результаты обучения</b>	<b>Критерии оценивания результатов обучения</b>
<p><b>ПК.30</b>  способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы</p>	<p>знать:  основные методы управления информационной безопасностью организаций, объектов и систем.  • основные стандарты, регламентирующие управление ИБ;  • принципы построения СУИБ;  • принципы разработки процессов управления ИБ;  • взаимосвязи отдельных процессов управления ИБ в рамках общей СУИБ;  • подходы к интеграции СУИБ в общую систему управления предприятие  Уметь находить современные подходы к управлению ИБ.</p>	<p style="text-align: center;"><b>Неудовлетворител</b>  Не знает комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной системы.  Не умеет проверять наличие и эффективность мер и средств защиты информации в автоматизированных системах предприятия</p> <p style="text-align: center;"><b>Удовлетворительн</b>  Общие, но не структурированные знания комплекса мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной системы.  Частично сформированное умение проверять наличие и эффективность мер и средств защиты информации в автоматизированных системах предприятия.</p> <p style="text-align: center;"><b>Хорошо</b>  Сформированные, но содержащие отдельные пробелы знания комплекса мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной системы.  Умение проверять наличие и эффективность мер и средств защиты информации в автоматизированных системах предприятия.</p> <p style="text-align: center;"><b>Отлично</b>  Сформированные знания комплекса мер</p>

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p><b>Отлично</b></p> <p>(правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной системы.</p> <p>Умение проверять наличие и эффективность мер и средств защиты информации в автоматизированных системах предприятия.</p>

#### ПК.24

**способность проводить анализ особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите**

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p><b>ПК.24</b></p> <p>способность проводить анализ особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите</p>	<p>Знать основные понятия аудита информационной безопасности; методы оценивания информационной безопасности ; основы контроля и проверки процессов и систем. Уметь оценивать информационную безопасность на основе показателей информационной безопасности. Владеть навыками разработки и исследования процессов защиты информации и ее компонентов по результатам аудита информационной безопасности</p>	<p><b>Неудовлетворител</b></p> <p>Отсутствие знаний основных понятий аудита информационной безопасности; методов оценивания информационной безопасности ; основ контроля и проверки процессов и систем.</p> <p>Отсутствие умений оценивать информационную безопасность на основе показателей информационной безопасности.</p> <p>Отсутствие навыков разработки и исследования процессов защиты информации и ее компонентов по результатам аудита информационной безопасности</p> <p><b>Удовлетворительн</b></p> <p>Общие, но не структурированные знания основных понятий аудита информационной безопасности; методов оценивания информационной безопасности ;</p> <p>Частично сформированное умение оценивать информационную безопасность на основе показателей информационной безопасности.</p> <p>Фрагментарное применение навыков разработки и исследования процессов защиты информации и ее компонентов по результатам аудита информационной</p>

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p><b>Удовлетворительн</b> безопасности</p> <p><b>Хорошо</b> Сформированные, но содержащие отдельные пробелы знания основных понятий аудита информационной безопасности; методов оценивания информационной безопасности ;</p> <p>В целом успешные, но содержащие отдельные пробелы умения оценивать информационную безопасность на основе показателей информационной безопасности. В целом успешное, но содержащее отдельные пробелы применение навыков разработки и исследования процессов защиты информации и ее компонентов по результатам аудита информационной безопасности</p> <p><b>Отлично</b> Сформированные систематические знания основных понятий аудита информационной безопасности; методов оценивания информационной безопасности ; Сформированное умение оценивать информационную безопасность на основе показателей информационной безопасности Успешное и систематическое применение навыков разработки и исследования процессов защиты информации и ее компонентов по результатам аудита информационной безопасности</p>

#### ПК.21

**способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы**

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
<b>ПК.21</b> способность разрабатывать предложения по совершенствованию	Знать и уметь находить сновные подходы к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем	<p><b>Неудовлетворител</b> Отсутствие знаний и умения находить сновные подходы к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления</p>

<b>Компетенция (индикатор)</b>	<b>Планируемые результаты обучения</b>	<b>Критерии оценивания результатов обучения</b>
системы управления информационной безопасностью автоматизированной системы	управления информационной безопасностью автоматизированной системы	<p><b>Неудовлетворител</b> информационной безопасностью автоматизированной системы</p> <p><b>Удовлетворительн</b> Общие, но не структурированные знания и частично сформированное умение находить сновные подходы к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью автоматизированной системы</p> <p><b>Хорошо</b> Сформированные, но содержащие отдельные пробелы знания и умения находить сновные подходы к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью автоматизированной системы</p> <p><b>Отлично</b> Хорошо сформированные знания и умения находить сновные подходы к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью автоматизированной системы</p>

### **ПК.31**

#### **способность управлять информационной безопасностью автоматизированной системы**

<b>Компетенция (индикатор)</b>	<b>Планируемые результаты обучения</b>	<b>Критерии оценивания результатов обучения</b>
<b>ПК.31</b> способность управлять информационной безопасностью автоматизированной системы	Знать основные методы и средства управления информационной безопасностью (ИБ) автоматизированной системы; базовые вопросы управления информационной безопасности. риски информационной безопасности Ас; содержание процесса комплексного	<p><b>Неудовлетворител</b> Отсутствие знаний основных методов и средств управления информационной безопасностью (ИБ) автоматизированной системы; содержание процесса комплексного обследования информационной безопасности; направления обеспечения и оценки информационной безопасности; риски информационной безопасности АС. Не знает основ управления ИБ АС, контроля</p>

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
	<p>обследования информационной безопасности; основы контроля и проверки процессов и систем; направления обеспечения и оценки информационной безопасности.</p> <p>Уметь исследовать полученные оценки информационной безопасности АС;</p> <p>Уметь владеть навыками разработки и исследования процессов защиты информации и ее компонентов по результатам аудита информационной безопасности</p>	<p><b>Неудовлетворител</b> и проверки процессов и систем. Отсутствие умения исследовать полученные оценки информационной безопасности АС ; Отсутствие владения навыками разработки и исследования процессов защиты информации и ее компонентов по результатам аудита информационной безопасности</p> <p><b>Удовлетворительн</b> Общие, но не структурированные знания основных методов и средств управления информационной безопасностью (ИБ) автоматизированной системы; содержания процесса комплексного обследования информационной безопасности; направления обеспечения и оценки информационной безопасности; рисков информационной безопасности АС. Общие знания основ управления ИБ АС, контроля и проверки процессов и систем Частично сформированное умение исследовать полученные оценки информационной безопасности АС ; Частично сформированное владение навыками разработки и исследования процессов защиты информации и ее компонентов по результатам аудита информационной безопасности</p> <p><b>Хорошо</b> Сформированные, но содержащие отдельные пробелы знания основ управления ИБ АС, контроля и проверки процессов и систем; основных методов и средств управления информационной безопасностью (ИБ) автоматизированной системы; содержания процесса комплексного обследования информационной безопасности; направления обеспечения и оценки информационной безопасности; рисков информационной безопасности АС. В целом успешные, но содержащие отдельные пробелы умения</p>



Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p><b>Хорошо</b></p> <p>исследовать полученные оценки информационной безопасности АС ; В целом успешные, но содержащие отдельные пробелы применение навыков разработки и исследования процессов защиты информации и ее компонентов по результатам аудита информационной безопасности</p> <p><b>Отлично</b></p> <p>Хорошо сформированные систематические знания основ управления ИБ АС, контроля и проверки процессов и систем; основных методов и средств управления информационной безопасностью (ИБ) автоматизированной системы; содержания процесса комплексного обследования информационной безопасности; направления обеспечения и оценки информационной безопасности; рисков информационной безопасности АС. Сформированное умение исследовать полученные оценки информационной безопасности АС ; Успешное и систематическое применение навыков разработки и исследования процессов защиты информации и ее компонентов по результатам аудита информационной безопасности</p>

## ПК.25

**способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации**

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
<b>ПК.25</b> способность участвовать в формировании политики информационной безопасности	знать требования для формирования политик информационной безопасности организации и уметь контролировать эффективность ее реализации	<p><b>Неудовлетворител</b></p> <p>не знает требований формирования политики информационной безопасности организации и не умеет контролировать эффективность ее реализации</p> <p><b>Удовлетворительн</b></p> <p>Частично сформированные знания</p>

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
организации и контролировать эффективность ее реализации		<p><b>Удовлетворительн</b> требований формирования политики информационной безопасности организации. Частично сформированные умения контролировать эффективность реализации политики информационной безопасности организации</p> <p><b>Хорошо</b> Сформированные, но содержащие определенные пробелы знания требований формирования политики информационной безопасности организации. Сформированные, но содержащие определенные пробелы умения контролировать эффективность реализации политики информационной безопасности организации</p> <p><b>Отлично</b> Полностью сформированные знания требований формирования политики информационной безопасности организации. Полностью сформированные умения контролировать эффективность реализации политики информационной безопасности организации</p>

## ПК.26

**способность формировать комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной системы**

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
<b>ПК.26</b> способность формировать комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной	Знать основные понятия аудита информационной безопасности АС; правила, процедуры, практические приемы, методы, средства для обеспечения информационной безопасности АС; правовые и методологические основы аудита информационной безопасности. Уметь исследовать полученные оценки информационной безопасности;	<p><b>Неудовлетворител</b> Знать основные понятия аудита информационной безопасности АС; правила, процедуры, практические приемы, руководящие принципы, методы, средства для обеспечения информационной безопасности АС; правовые и методологические основы аудита информационной безопасности. Уметь исследовать полученные оценки информационной безопасности; оценивать результаты аудита и самооценки информационной безопасности АС.</p>

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
системы	<p>оценивать результаты аудита и самооценки информационной безопасности АС.</p> <p>Формирование навыков использования методологии, стандартов и нормативных требования в области аудита информационной безопасности АС.</p>	<p><b>Неудовлетворительн</b></p> <p>Формирование навыков использования методологии, стандартов и нормативных требования в области аудита информационной безопасности АС.</p> <p><b>Удовлетворительн</b></p> <p>Общие, но не структурированные знания основных понятий аудита информационной безопасности АС; правил, процедур, практических приемов, руководящих принципов, методов, средств для обеспечения информационной безопасности АС; правовых и методологических основ аудита информационной безопасности.</p> <p>Частично сформированное умение исследовать полученные оценки информационной безопасности; оценивать результаты аудита и самооценки информационной безопасности АС.</p> <p>Фрагментарное применение навыков использования методологии, стандартов и нормативных требования в области аудита информационной безопасности АС.</p> <p><b>Хорошо</b></p> <p>Сформированные, но содержащие отдельные пробелы знания основных понятий аудита информационной безопасности АС; правил, процедур, практических приемов, руководящих принципов, методов, средств для обеспечения информационной безопасности АС; правовых и методологических основ аудита информационной безопасности.</p> <p>В целом успешные, но содержащие отдельные пробелы умения исследовать полученные оценки информационной безопасности; оценивать результаты аудита и самооценки информационной безопасности АС.</p> <p>В целом успешное, но содержащее отдельные пробелы применение навыков использования методологии, стандартов и нормативных требования в области аудита информационной безопасности АС.</p> <p><b>Отлично</b></p>

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p style="text-align: center;"><b>Отлично</b></p> <p>Сформированные систематические знания основных понятий аудита информационной безопасности АС; правил, процедур, практических приемов, руководящих принципов, методов, средств для обеспечения информационной безопасности АС; правовых и методологических основ аудита информационной безопасности. Сформированное умение исследовать полученные оценки информационной безопасности; оценивать результаты аудита и самооценки информационной безопасности АС.</p> <p>Успешное и систематическое применение навыков использования методологии, стандартов и нормативных требования в области аудита информационной безопасности АС</p>

## Оценочные средства текущего контроля и промежуточной аттестации

Схема доставки : Базовая

**Вид мероприятия промежуточной аттестации : Зачет**

**Способ проведения мероприятия промежуточной аттестации :** Оценка по дисциплине в рамках промежуточной аттестации определяется на основе баллов, набранных обучающимся на контрольных мероприятиях, проводимых в течение учебного периода.

**Максимальное количество баллов : 100**

### Конвертация баллов в отметки

«отлично» - от 81 до 100

«хорошо» - от 61 до 80

«удовлетворительно» - от 44 до 60

«неудовлетворительно» / «незачтено» менее 44 балла

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
<b>Входной контроль</b>	1. Введение. Основы аудита <b>Входное тестирование</b>	Проверяются остаточные знания студентов по дисциплинам:- основы информационной безопасности;- программно-аппаратные средства обеспечения информационной безопасности;- технические средства защиты информации;- безопасность операционных систем.
<b>ПК.30</b> способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы	3. Базовые вопросы управления информационной безопасности. Риски информационной безопасности <b>Письменное контрольное мероприятие</b>	Понимание комплексного подхода к обследованию информационной безопасности АС

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
<p><b>ПК.24</b> способность проводить анализ особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите</p> <p><b>ПК.26</b> способность формировать комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной системы</p>	<p>8. Оценка безопасности информационных технологий на основе международных стандартов. Методика проведения аудита информационной б</p> <p><b>Письменное контрольное мероприятие</b></p>	<p>Понимание основ аудита информационной безопасности и методы его проведения</p>
<p><b>ПК.30</b> способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы</p> <p><b>ПК.31</b> способность управлять информационной безопасностью автоматизированной системы</p>	<p>10. Аудит управления непрерывностью бизнеса и восстановления после сбоев</p> <p><b>Письменное контрольное мероприятие</b></p>	<p>Особенности аудита информационной безопасности организаций</p>

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
<p><b>ПК.21</b> способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы</p> <p><b>ПК.24</b> способность проводить анализ особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите</p> <p><b>ПК.25</b> способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации</p> <p><b>ПК.26</b> способность формировать комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной системы</p> <p><b>ПК.30</b> способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы</p> <p><b>ПК.31</b> способность управлять информационной безопасностью автоматизированной системы</p>	<p>12. Аттестация объектов информатизации как аудит информационной безопасности объектов информатизации</p> <p><b>Итоговое контрольное мероприятие</b></p>	<p>Понимание методов и средств управления информационной безопасностью (ИБ) на объекте, а также на изучение основных подходов к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью определенного объекта</p>

## Спецификация мероприятий текущего контроля

### 1. Введение. Основы аудита

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**

Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **0**

Проходной балл: **0**

Показатели оценивания	Баллы
Отсутствие ошибок при входном контроле	100
Одна ошибка при входном контроле	81
Две ошибки при входном контроле	61
Три ошибки при входном контроле	41

### 3. Базовые вопросы управления информационной безопасности. Риски информационной безопасности

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**

Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **20**

Проходной балл: **9**

Показатели оценивания	Баллы
Базовые вопросы управления информационной безопасности. Риски информационной безопасности	10
Основы построения систем защиты информации в информационных системах	10

### 8. Оценка безопасности информационных технологий на основе международных стандартов. Методика проведения аудита информационной б

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**

Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **20**

Проходной балл: **9**

Показатели оценивания	Баллы
Основы построения систем защиты информации в информационных системах	10
Нормативные документы ФСТЭК РФ и ФСБ РФ как критерии аудита ИБ. Стандарт управления информационной безопасностью	10

### 10. Аудит управления непрерывностью бизнеса и восстановления после сбоев

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**

Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **20**

Проходной балл: **9**

Показатели оценивания	Баллы
Система оценки информационной безопасности организаций банковской системы	10



Российской Федерации. Пример аудита банка на соответствие требованиям ЦБ РФ	
Аудит управления непрерывностью бизнеса и восстановления после сбоев	10

## **12. Аттестация объектов информатизации как аудит информационной безопасности объектов информатизации**

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**

Условия проведения мероприятия: **в часы самостоятельной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **40**

Проходной балл: **17**

<b>Показатели оценивания</b>	<b>Баллы</b>
Полный, исчерпывающий ответ на второй вопрос билета	12
Полный, исчерпывающий ответ на первый вопрос билета	12
Полный ответ на дополнительный вопрос	8
Полный ответ на дополнительный вопрос	8