

**МИНОБРНАУКИ РОССИИ**

**Федеральное государственное автономное 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 2021 г.

Пермь, 2021

## **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)

**ОПК.13** Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений

#### **Индикаторы**

**ОПК.13.1** Определяет структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов

**ОПК.13.2** Оценивает эффективность и надежность средств защиты информации программного обеспечения автоматизированных систем

**ОПК.14** Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем

#### **Индикаторы**

**ОПК.14.1** Контролирует эффективность принятых мер по реализации политик безопасности информации автоматизированных систем

**ОПК.14.2** Анализирует программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации

**ПК.3** Способен управлять функционированием и защищенностью автоматизированных систем

#### **Индикаторы**

**ПК.3.3** Проводит мероприятия по аттестации на предмет соответствия требованиям по защите сооружений и автоматизированных систем от НСД

**ПК.5** Способен анализировать уязвимости внедряемой системы защиты информации

#### **Индикаторы**

**ПК.5.3** Строит модели угроз безопасности информации автоматизированной системы

**ПК.6** Способен проводить контроль защищенности информации от утечки по техническим каналам

#### **Индикаторы**

**ПК.6.2** Подготавливает отчетные материалы по результатам специальных исследований

**ПК.6.3** Проводит контроль защищенности информации от несанкционированного доступа и специальных воздействий

**ОПСК.1** Способен разрабатывать и реализовывать политику информационной безопасности открытых информационных систем

#### **Индикаторы**

**ОПСК.1.2** Проводит сбор, систематизацию и оценку сведений об угрозах безопасности информации, оценивает необходимость защиты информации, формулирует требования к защите информации

#### 4. Объем и содержание дисциплины

|   |  |
|---|--|
| <b>Специальность</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)<br>Итоговое контрольное мероприятие (1)<br>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 аудиторские 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 вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2021. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. <https://www.urait.ru/bcode/469235>

### 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 Plaer";
- 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**

**ОПК.14**

**Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем**

| <b>Компетенция<br/>(индикатор)</b>  | <b>Планируемые результаты<br/>обучения</b>  | <b>Критерии оценивания результатов<br/>обучения</b>   |
|---|---|---|
| <p><b>ОПК.14.2</b><br/>Анализирует программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации</p> | <p>Анализирует программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации</p> | <p align="center"><b>Неудовлетворител</b></p> <p>Не знает программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации. Не умеет анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации.</p> <p align="center"><b>Удовлетворительн</b></p> <p>Общие, но не структурированные знания программных, архитектурно-технических и схемотехнических решений компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации. Частично сформированное умение анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации.</p> <p align="center"><b>Хорошо</b></p> <p>Сформированные, но содержащие отдельные пробелы знания программных, архитектурно-технических и схемотехнических решений компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации. Умение с небольшими пробелами анализировать программные, архитектурно-</p> |

| Компетенция<br>(индикатор)   | Планируемые результаты<br>обучения   | Критерии оценивания результатов<br>обучения  |
|--|--|--|
|  |  | <p style="text-align: center;"><b>Хорошо</b></p> <p>технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации.</p> <p style="text-align: center;"><b>Отлично</b></p> <p>Сформированные знания программных, архитектурно-технических и схемотехнических решений компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации.</p> <p>Умение анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации.</p>   |
| <p><b>ОПК.14.1</b><br/>Контролирует эффективность принятых мер по реализации политик безопасности информации автоматизированных систем</p> | <p>Контролирует эффективность принятых мер по реализации политик безопасности информации автоматизированных систем</p> | <p style="text-align: center;"><b>Неудовлетворител</b></p> <p>Отсутствие знаний о мерах по реализации политик безопасности информации автоматизированных систем.</p> <p>Отсутствие умений оценивать эффективность принятых мер по реализации политик безопасности информации автоматизированных систем.</p> <p style="text-align: center;"><b>Удовлетворительн</b></p> <p>Общие, но не структурированные знания о мерах по реализации политик безопасности информации автоматизированных систем.</p> <p>Частично сформированное умение оценивать эффективность принятых мер по реализации политик безопасности информации автоматизированных систем.</p> <p style="text-align: center;"><b>Хорошо</b></p> <p>Сформированные, но содержащие отдельные пробелы знания о мерах по реализации политик безопасности информации автоматизированных систем.</p> <p>В целом успешные, но содержащие отдельные пробелы умения оценивать эффективность принятых мер по реализации политик безопасности информации автоматизированных систем.</p> <p style="text-align: center;"><b>Отлично</b></p> |

| Компетенция<br>(индикатор) | Планируемые результаты<br>обучения | Критерии оценивания результатов<br>обучения   |
|----------------------------|------------------------------------|---|
|                            |                                    | <p style="text-align: center;"><b>Отлично</b></p> <p>Сформированные систематические знания о мерах по реализации политик безопасности информации автоматизированных систем.<br/>Сформированное умение оценивать эффективность принятых мер по реализации политик безопасности информации автоматизированных систем.</p> |

### ОПК.13

**Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений**

| Компетенция<br>(индикатор)   | Планируемые результаты<br>обучения   | Критерии оценивания результатов<br>обучения  |
|--|--|--|
| <p><b>ОПК.13.1</b><br/>Определяет структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов</p> | <p>Определяет структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов</p> | <p style="text-align: center;"><b>Неудовлетворител</b></p> <p>Отсутствие знаний и умения определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов.</p> <p style="text-align: center;"><b>Удовлетворительн</b></p> <p>Общие, но не структурированные знания и частично сформированное умение определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов.</p> <p style="text-align: center;"><b>Хорошо</b></p> <p>Сформированные, но содержащие отдельные пробелы знания и умения определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов.</p> <p style="text-align: center;"><b>Отлично</b></p> <p>Хорошо сформированные знания и умения определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов.</p> |
| <p><b>ОПК.13.2</b></p>   | <p>Оценивает эффективность и</p>   | <p style="text-align: center;"><b>Неудовлетворител</b></p>   |

| Компетенция<br>(индикатор)  | Планируемые результаты<br>обучения  | Критерии оценивания результатов<br>обучения  |
|---|---|--|
| Оценивает эффективность и надежность средств защиты информации программного обеспечения автоматизированных систем | надежность средств защиты информации программного обеспечения автоматизированных систем | <p><b>Неудовлетворител</b><br/>Отсутствие владения навыками оценивать эффективность и надежность средств защиты информации программного обеспечения автоматизированных систем.</p> <p><b>Удовлетворительн</b><br/>Частично сформированное владение навыками оценивать эффективность и надежность средств защиты информации программного обеспечения автоматизированных систем.</p> <p><b>Хорошо</b><br/>В целом успешные, но содержащие отдельные пробелы применение навыков оценивать эффективность и надежность средств защиты информации программного обеспечения автоматизированных систем.</p> <p><b>Отлично</b><br/>Успешное и систематическое применение навыков оценивать эффективность и надежность средств защиты информации программного обеспечения автоматизированных систем.</p> |

### ОПСК.1

#### Способен разрабатывать и реализовывать политику информационной безопасности открытых информационных систем

| Компетенция<br>(индикатор)   | Планируемые результаты<br>обучения  | Критерии оценивания результатов<br>обучения  |
|--|---|--|
| <b>ОПСК.1.2</b><br>Проводит сбор, систематизацию и оценку сведений об угрозах безопасности информации, оценивает необходимость защиты информации, формулирует требования к защите информации | Проводит сбор, систематизацию и оценку сведений об угрозах безопасности информации, оценивает необходимость защиты информации, формулирует требования к защите информации | <p><b>Неудовлетворител</b><br/>Не умеет проводить сбор, систематизацию и оценку сведений об угрозах безопасности информации.<br/>Отсутствуют знания оценки необходимости защиты информации.<br/>Не может формулировать требования к защите информации.</p> <p><b>Удовлетворительн</b><br/>Частично сформированные умения проводить сбор, систематизацию и оценку сведений об угрозах безопасности информации. знания требований формирования политики информационной безопасности организации.</p> |

| Компетенция<br>(индикатор) | Планируемые результаты<br>обучения | Критерии оценивания результатов<br>обучения  |
|----------------------------|------------------------------------|--|
|                            |                                    | <p style="text-align: center;"><b>Удовлетворительн</b></p> <p>Частично сформированные знания оценки необходимости защиты информации.<br/>Частично сформированы умения формулировать требования к защите информации.</p> <p style="text-align: center;"><b>Хорошо</b></p> <p>Сформированные, но содержащие определенные пробелы умения проводит сбор, систематизацию и оценку сведений об угрозах безопасности информации. знания требований.</p> <p>Сформированные, но содержащие определенные пробелы знания оценки необходимости защиты информации.<br/>Сформированные умения формулировать требования к защите информации.</p> <p style="text-align: center;"><b>Отлично</b></p> <p>Умеет проводит сбор, систематизацию и оценку сведений об угрозах безопасности информации.<br/>Полностью сформированные знания оценки необходимости защиты информации.<br/>Полностью сформированные умения формулировать требования к защите информации.</p> |

## ПК.6

### Способен проводить контроль защищенности информации от утечки по техническим каналам

| Компетенция<br>(индикатор)   | Планируемые результаты<br>обучения   | Критерии оценивания результатов<br>обучения   |
|--|--|---|
| <p><b>ПК.6.2</b><br/>Подготавливает отчетные материалы по результатам специальных исследований</p> | <p>Подготавливает отчетные материалы по результатам специальных исследований</p> | <p style="text-align: center;"><b>Неудовлетворител</b></p> <p>Не знает отчетные материалы по результатам специальных исследований. Отсутствуют навыки подготавливать отчетные материалы по результатам специальных исследований.</p> <p style="text-align: center;"><b>Удовлетворительн</b></p> <p>Общие, но не структурированные знания отчетных материалов по результатам специальных исследований.<br/>Фрагментарное применение навыков подготавливать отчетные материалы по результатам специальных исследований.</p> |



| Компетенция<br>(индикатор)   | Планируемые результаты<br>обучения   | Критерии оценивания результатов<br>обучения   |
|--|--|---|
|  |  | <p style="text-align: center;"><b>Хорошо</b></p> <p>Сформированные, но содержащие отдельные пробелы знания отчетных материалов по результатам специальных исследований. В целом успешное, но содержащее отдельные пробелы применение навыков подготавливать отчетные материалы по результатам специальных исследований.</p> <p style="text-align: center;"><b>Отлично</b></p> <p>Сформированные систематические знания отчетных материалов по результатам специальных исследований. Успешное и систематическое применение навыков подготавливать отчетные материалы по результатам специальных исследований.</p>  |
| <p><b>ПК.6.3</b><br/>Проводит контроль защищенности информации от несанкционированного доступа и специальных воздействий</p> | <p>Проводит контроль защищенности информации от несанкционированного доступа и специальных воздействий</p> | <p style="text-align: center;"><b>Неудовлетворител</b></p> <p>Нет знаний критериев и методов оценки защищенности информации от несанкционированного доступа и специальных воздействий. Не сформированные умения проводить оценку защищенности информации от несанкционированного доступа и специальных воздействий.</p> <p style="text-align: center;"><b>Удовлетворительн</b></p> <p>Частично сформированные знания критериев и методов оценки защищенности информации от несанкционированного доступа и специальных воздействий. Частично сформированные умения проводить оценку защищенности информации от несанкционированного доступа и специальных воздействий.</p> <p style="text-align: center;"><b>Хорошо</b></p> <p>Сформированные, но содержащие определенные пробелы знания критериев и методов оценки защищенности информации от несанкционированного доступа и специальных воздействий. Сформированные, но содержащие определенные пробелы умения проводить оценку защищенности информации от несанкционированного доступа и специальных воздействий.</p> |

| Компетенция<br>(индикатор) | Планируемые результаты<br>обучения | Критерии оценивания результатов<br>обучения  |
|----------------------------|------------------------------------|--|
|                            |                                    | <p style="text-align: center;"><b>Отлично</b></p> <p>Полностью сформированные знания критериев и методов оценки защищенности информации от несанкционированного доступа и специальных воздействий. Полностью сформированные умения проводить оценку защищенности информации от несанкционированного доступа и специальных воздействий.</p> |

### ПК.3

#### Способен управлять функционированием и защищенностью автоматизированных систем

| Компетенция<br>(индикатор)  | Планируемые результаты<br>обучения  | Критерии оценивания результатов<br>обучения   |
|---|---|---|
| <p><b>ПК.3.3</b><br/>Проводит мероприятия по аттестации на предмет соответствия требованиям по защите сооружений и автоматизированных систем от НСД</p> | <p>Проводит мероприятия по аттестации на предмет соответствия требованиям по защите сооружений и автоматизированных систем от НСД</p> | <p style="text-align: center;"><b>Неудовлетворител</b></p> <p>Отсутствие знаний основных методов и средств по аттестации на предмет соответствия требованиям по защите сооружений и автоматизированных систем от НСД.<br/>Отсутствие умения исследовать полученные результаты аттестации на предмет соответствия требованиям по защите сооружений и автоматизированных систем от НСД .</p> <p style="text-align: center;"><b>Удовлетворительн</b></p> <p>Общие, но не структурированные знания основных методов и средств по аттестации на предмет соответствия требованиям по защите сооружений и автоматизированных систем от НСД.<br/>Частично сформированное умение исследовать полученные результаты аттестации на предмет соответствия требованиям по защите сооружений и автоматизированных систем от НСД .</p> <p style="text-align: center;"><b>Хорошо</b></p> <p>Сформированные, но содержащие отдельные пробелы знания основных методов и средств по аттестации на предмет соответствия требованиям по защите сооружений и автоматизированных систем от НСД.</p> |

| Компетенция<br>(индикатор) | Планируемые результаты<br>обучения | Критерии оценивания результатов<br>обучения  |
|----------------------------|------------------------------------|--|
|                            |                                    | <p style="text-align: center;"><b>Хорошо</b></p> <p>В целом успешные, но содержащие отдельные пробелы умения исследовать полученные результаты аттестации на предмет соответствия требованиям по защите сооружений и автоматизированных систем от НСД .</p> <p style="text-align: center;"><b>Отлично</b></p> <p>Хорошо сформированные систематические знания основных методов и средств по аттестации на предмет соответствия требованиям по защите сооружений и автоматизированных систем от НСД.<br/>Сформированное умение исследовать полученные результаты аттестации на предмет соответствия требованиям по защите сооружений и автоматизированных систем от НСД .</p> |

### ПК.5

#### Способен анализировать уязвимости внедряемой системы защиты информации

| Компетенция<br>(индикатор)  | Планируемые результаты<br>обучения   | Критерии оценивания результатов<br>обучения  |
|---|--|--|
| <p><b>ПК.5.3</b><br/>Строит модели угроз безопасности информации автоматизированной системы</p> | <p>Знать основные виды угроз информации автоматизированной системы;<br/>уметь строить модели угроз безопасности информации автоматизированной системы;<br/>владеть навыками определения потенциального нарушителя автоматизированной системы</p> | <p style="text-align: center;"><b>Неудовлетворител</b></p> <p>не знает основные виды угроз информации автоматизированной системы; не умеет строить модели угроз безопасности информации автоматизированной системы; не владеет навыками определения потенциального нарушителя автоматизированной системы</p> <p style="text-align: center;"><b>Удовлетворительн</b></p> <p>Частично сформированные знания основных видов угроз информации автоматизированной системы; частично сформированное умение строить модели угроз безопасности информации автоматизированной системы; посредственное владение навыками определения потенциального нарушителя автоматизированной системы</p> <p style="text-align: center;"><b>Хорошо</b></p> |

| Компетенция<br>(индикатор) | Планируемые результаты<br>обучения | Критерии оценивания результатов<br>обучения  |
|----------------------------|------------------------------------|--|
|                            |                                    | <p style="text-align: center;"><b>Хорошо</b></p> <p>Сформированные, но содержащие пробелы знания основных видов угроз информации автоматизированной системы;<br/>сформированное, но содержащее пробелы умение строить модели угроз безопасности информации автоматизированной системы;<br/>неуверенное владение навыками определения потенциального нарушителя автоматизированной системы</p> <p style="text-align: center;"><b>Отлично</b></p> <p>Сформированные знания основных видов угроз информации автоматизированной системы; сформированное умение строить модели угроз безопасности информации автоматизированной системы; уверенное владение навыками определения потенциального нарушителя автоматизированной системы</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<br>(индикатор)  | Мероприятие<br>текущего контроля                          | Контролируемые элементы<br>результатов обучения   |
|---|---|---|
| <b>Входной контроль</b><br><b>ОПК.13.2</b><br>Оценивает эффективность и надежность средств защиты информации программного обеспечения автоматизированных систем<br><b>ОПК.13.1</b><br>Определяет структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов | 1. Введение. Основы аудита<br><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. |

| Компетенция<br>(индикатор)   | Мероприятие<br>текущего контроля   | Контролируемые элементы<br>результатов обучения                                     |
|--|--|---|
| <p><b>ОПСК.1.2</b><br/>Проводит сбор, систематизацию и оценку сведений об угрозах безопасности информации, оценивает необходимость защиты информации, формулирует требования к защите информации</p> <p><b>ПК.6.2</b><br/>Подготавливает отчетные материалы по результатам специальных исследований</p> <p><b>ОПК.13.1</b><br/>Определяет структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов</p> <p><b>ОПК.13.2</b><br/>Оценивает эффективность и надежность средств защиты информации программного обеспечения автоматизированных систем</p> <p><b>ОПК.14.1</b><br/>Контролирует эффективность принятых мер по реализации политик безопасности информации автоматизированных систем</p> <p><b>ОПК.14.2</b><br/>Анализирует программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации</p> | <p>3. Базовые вопросы управления информационной безопасности. Риски информационной безопасности</p> <p><b>Письменное контрольное мероприятие</b></p> | <p>Понимание комплексного подхода к обследованию информационной безопасности АС</p> |

| Компетенция<br>(индикатор)   | Мероприятие<br>текущего контроля   | Контролируемые элементы<br>результатов обучения                                   |
|--|--|---|
| <p><b>ПК.6.2</b><br/>Подготавливает отчетные материалы по результатам специальных исследований</p> <p><b>ОПК.14.1</b><br/>Контролирует эффективность принятых мер по реализации политик безопасности информации автоматизированных систем</p>  | <p>8. Оценка безопасности информационных технологий на основе международных стандартов. Методика проведения аудита информационной безопасности на предприятии</p> <p><b>Письменное контрольное мероприятие</b></p> | <p>Понимание основ аудита информационной безопасности и методы его проведения</p> |
| <p><b>ПК.5.3</b><br/>Строит модели угроз безопасности информации автоматизированной системы</p> <p><b>ОПК.13.2</b><br/>Оценивает эффективность и надежность средств защиты информации программного обеспечения автоматизированных систем</p> <p><b>ОПК.14.2</b><br/>Анализирует программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации</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<br>(индикатор)   | Мероприятие<br>текущего контроля   | Контролируемые элементы<br>результатов обучения   |
|--|--|---|
| <p><b>ОПСК.1.2</b><br/>Проводит сбор, систематизацию и оценку сведений об угрозах безопасности информации, оценивает необходимость защиты информации, формулирует требования к защите информации</p> <p><b>ПК.3.3</b><br/>Проводит мероприятия по аттестации на предмет соответствия требованиям по защите сооружений и автоматизированных систем от НСД</p> <p><b>ПК.5.3</b><br/>Строит модели угроз безопасности информации автоматизированной системы</p> <p><b>ПК.6.2</b><br/>Подготавливает отчетные материалы по результатам специальных исследований</p> <p><b>ПК.6.3</b><br/>Проводит контроль защищенности информации от несанкционированного доступа и специальных воздействий</p> <p><b>ОПК.13.1</b><br/>Определяет структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов</p> <p><b>ОПК.13.2</b><br/>Оценивает эффективность и надежность средств защиты информации программного обеспечения автоматизированных систем</p> <p><b>ОПК.14.2</b><br/>Анализирует программные, архитектурно-технические и схемотехнические решения</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> |



| Компетенция<br>(индикатор)  | Мероприятие<br>текущего контроля | Контролируемые элементы<br>результатов обучения |
|---|----------------------------------|---|
| компонентов<br>автоматизированных систем с<br>целью выявления<br>потенциальных уязвимостей<br>безопасности информации<br><b>ОПК.14.1</b><br>Контролирует эффективность<br>принятых мер по реализации<br>политик безопасности<br>информации<br>автоматизированных систем |                                  |   |

### 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 безопасностью. 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 безопасностью. 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 безопасности на предприятии

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 Российской Федерации. Пример аудита банка на соответствие требованиям ЦБ РФ | 10    |
| 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**

| Показатели оценивания                               | Баллы |
|---|-------|
| 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     |