МИНОБРНАУКИ РОССИИ

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

Физико-математический институт

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 базовую часть Блока « С.1 » образовательной программы по направлениям подготовки (специальностям):

Специальность: **10.05.04** Информационно-аналитические системы безопасности
направленность Информационная безопасность финансовых и экономических структур

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:

10.05.04 Информационно-аналитические системы безопасности (направленность : Информационная безопасность финансовых и экономических структур)

ОПК.11 Способен осуществлять синтез технологий и основных компонентов функциональной и обеспечивающей частей создаваемых информационно-аналитических систем, в том числе выбор мероприятий по защите информации

Индикаторы

ОПК.11.1 Контролирует эффективность принятых мер по реализации политик безопасности информации автоматизированных систем

ОПК.11.2 Анализирует программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации

ОПК.15 Способен осуществлять автоматизированную информационно-аналитическую поддержку процессов принятия решений на базе ситуационных центров

Индикаторы

ОПК.15.3 Проводит мероприятия по аттестации на предмет соответствия требованиям по защите сооружений и автоматизированных систем от НСД

4. Объем и содержание дисциплины

Специальность	10.05.04 Информационно-аналитические системы безопасности (направленность: Информационная безопасность финансовых и экономических структур)
форма обучения	очная
№№ семестров, выделенных для изучения дисциплины	10
Объем дисциплины (з.е.)	3
Объем дисциплины (ак.час.)	108
Контактная работа с преподавателем (ак.час.), в том числе:	42
Проведение лекционных занятий	14
Проведение лабораторных работ, занятий по иностранному языку	28
Самостоятельная работа (ак.час.)	66
Формы текущего контроля	Входное тестирование (1) Итоговое контрольное мероприятие (1) Письменное контрольное мероприятие (3)
Формы промежуточной аттестации	Зачет (10 семестр)

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 безопасности. 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 тану, 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 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-образовательной 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:
- 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 SIEM Splunk свободно распространяемая версия
- ПО "Wingdocs"свободно распространяемая версия
- ПО оценки рисков "RA 2A" свободно распространяемая 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: специализированной мебелью, презентационной техникой (проектор, экран, компьютер/ноутбук), а также меловой (и) или маркерной доской.

Аудитория для лабораторных занятий - Компьютерный класс со специализированным лабораторным оборудованием и программным обеспечением, оснащенный: специализированной мебелью, экраном/телевизором, проектором, персональными компьютерами, а также меловой (и) или маркерной доской.

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.11

Способен осуществлять синтез технологий и основных компонентов функциональной и обеспечивающей частей создаваемых информационно-аналитических систем, в том числе выбор мероприятий по защите информации

Индикатор	Планируемые результаты обучения	Критерии оценивания результатов обучения
ОПК.11.2 Анализирует программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации	Анализирует программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации	**Неудовлетворител** 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. **Удовлетворительн** 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. **Хорошо** 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-

Индикатор	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Хорошо технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации. **Отлично** Сформированные знания программных, архитектурно-технических и схемотехнических решений компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации. Умение анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации.
ОПК.11.1 Контролирует эффективность принятых мер по реализации политик безопасности информации автоматизированных систем	Контролирует эффективность принятых мер по реализации политик безопасности информации автоматизированных систем	**Неудовлетворител** Отсутствие знаний о мерах по реализации политик безопасности информации автоматизированных систем. Отсутствие умений оценивать эффективность принятых мер по реализации политик безопасности информации автоматизированных систем. **Удовлетворительн** Общие, но не структурированные знания о мерах по реализации политик безопасности информации автоматизированных систем. Частично сформированное умение оценивать эффективность принятых мер по реализации политик безопасности информации автоматизированных систем. **Хорошо** Сформированные, но содержащие отдельные пробелы знания о мерах по реализации политик безопасности информации автоматизированных систем. В целом успешные, но содержащие отдельные пробелы умения оценивать эффективность принятых мер по реализации политик безопасности информации автоматизированных систем. **Отлично**

Индикатор	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично Сформированные систематические знания о мерах по реализации политик безопасности информации автоматизированных систем. Сформированное умение оценивать эффективность принятых мер по реализации политик безопасности информации автоматизированных систем.

ОПК.15

Способен осуществлять автоматизированную информационно-аналитическую поддержку процессов принятия решений на базе ситуационных центров

Индикатор	Планируемые результаты обучения	Критерии оценивания результатов обучения
ОПК.15.3 Проводит мероприятия по аттестации на предмет соответствия требованиям по защите сооружений и автоматизированных систем от НСД	Знание основных нормативных документов и стандартов, регулирующих защиту информации и аттестацию систем на предмет соответствия требованиям по защите от несанкционированного доступа (НСД);умение проводить оценку состояния информационных технологий и систем, выявляя уязвимости и риски, связанные с НСД, а также определять уровень защищенности объектов;организация и проведение аудита систем обеспечения информационной безопасности, включая анализ архитектуры систем, процессов и процедур, а также оценку эффективности применяемых мер защиты;умение формулировать обоснованные рекомендации по улучшению защиты информационных систем и сооружений на основе проведенного аудита и анализа угроз.	**Неудовлетворител** Показывает:Ограниченное знание нормативных документов, значительные пробелы в понимании стандартов.Ограниченные навыки в оценке состояния систем, выявление только очевидных уязвимостей. Ограниченные навыки в проведении аудита, значительные упущения в анализе систем.Ограниченные навыки в разработке рекомендаций по улучшению безопасности, с недостаточным обоснованием и практической применимостью. **Удовлетворительн** Показывает: Удовлетворительное знание основных документов, но недостаток в понимании некоторых стандартов.Удовлетворительное умение проводить оценку, но с недостаточной глубиной анализа и выявлением некоторых рисков.Удовлетворительное выполнение аудита, но с недостатками в анализе и выявлении важных аспектов.Удовлетворительная способность формулировать рекомендации по улучшению безопасности, но они могут быть недостаточно обоснованными или практичными. **Хорошо** Показывает: Хорошее знание большинства нормативных документов и стандартов, с

Индикатор	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Хорошо небольшими пробелами в деталях.Хорошее умение оценивать системы, выявляя большинство уязвимостей и рисков, с несколькими упущениями.Хорошее выполнение аудита, с небольшими упущениями в анализе архитектуры или процессов.Хорошая способность разрабатывать рекомендации по улучшению безопасности, но с некоторыми недостатками в обосновании. **Отлично** Показывает: Отличное знание всех ключевых нормативных документов и стандартов, уверенное применение в практических ситуациях.Исключительное умение проводить глубокую оценку систем, выявляя все уязвимости и риски с точными рекомендациями.Отличное выполнение аудита с полным анализом архитектуры и процессов, выявление всех критических аспектов.Исключительная способность формулировать обоснованные и практически применимые рекомендации по улучшению безопасности.

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
Входной контроль	1. Введение. Основы аудита **Входное тестирование**	Проверяются остаточные знания студентов по дисциплинам:- основы информационной безопасности;- программно-аппаратные средства обеспечения информационной безопасности;- технические средства защиты информации;- безопасность операционных систем.

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ОПК.11.1 Контролирует эффективность принятых мер по реализации политик безопасности информации автоматизированных систем **ОПК.11.2** Анализирует программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации **ОПК.15.3** Проводит мероприятия по аттестации на предмет соответствия требованиям по защите сооружений и автоматизированных систем от НСД	3. Базовые вопросы управления информационной безопасности. Риски информационной безопасности **Письменное контрольное мероприятие**	Понимание комплексного подхода к обследованию информационной безопасности АС
ОПК.11.1 Контролирует эффективность принятых мер по реализации политик безопасности информации автоматизированных систем **ОПК.15.3** Проводит мероприятия по аттестации на предмет соответствия требованиям по защите сооружений и автоматизированных систем от НСД	8. Оценка безопасности информационных технологий на основе международных стандартов. Методика проведения аудита информационной безопасности на предприятии **Письменное контрольное мероприятие**	Понимание основ аудита информационной безопасности и методы его проведения

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ОПК.11.2 Анализирует программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации **ОПК.15.3** Проводит мероприятия по аттестации на предмет соответствия требованиям по защите сооружений и автоматизированных систем от НСД	10. Аудит управления непрерывностью бизнеса и восстановления после сбоев **Письменное контрольное мероприятие**	Особенности аудита информационной безопасности организаций
ОПК.11.1 Контролирует эффективность принятых мер по реализации политик безопасности информации автоматизированных систем **ОПК.11.2** Анализирует программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации **ОПК.15.3** Проводит мероприятия по аттестации на предмет соответствия требованиям по защите сооружений и автоматизированных систем от НСД	12. Аттестация объектов информатизации как аудит информационной безопасности объектов информатизации **Итоговое контрольное мероприятие**	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

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 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 требования 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