МИНОБРНАУКИ РОССИИ

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

Кафедра радиоэлектроники и защиты информации

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

Рабочая программа дисциплины

АУДИТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СИСТЕМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Код УМК 81661

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 вариативную 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

Направления подготовки	10.05.03 Информационная безопасность автоматизированных систем (направленность: Безопасность открытых информационных систем)
форма обучения	очная
№№ триместров, выделенных для изучения дисциплины	13
Объем дисциплины (з.е.)	6
Объем дисциплины (ак.час.)	216
Контактная работа с преподавателем (ак.час.), в том числе:	84
Проведение лекционных занятий	42
Проведение практических занятий, семинаров	0
Проведение лабораторных работ, занятий по иностранному языку	42
Самостоятельная работа (ак.час.)	132
Формы текущего контроля	Входное тестирование (1) Итоговое контрольное мероприятие (1) Письменное контрольное мероприятие (3)
Формы промежуточной аттестации	Экзамен (13 триместр)

5. Аннотированное описание содержания разделов и тем дисциплины

Аудит информационных технологий и систем обеспечения информационной безопасности. Первый семестр

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.

Итоговое контрольное мероприятие

Экзамен проводится в устной форме, по билетам, содержащим два теоретических вопроса. Перечень вопросов к экзамену по дисциплине:

1. Процессы и системы. Структура и свойства процессов и систем.
2. Процессный подход и информационная безопасность.
3. Понятие аудита.
4. Циклическая модель менеджмента качества процессов и систем.
5. Способы контроля и проверки процессов и систем.
6. Внутренний и внешний аудит.
7. Модели безопасности бизнеса.
8. Для каких целей предназначены сетевые сканеры?
9. Приведите примеры сетевых сканеров и опишите сценарии их использовании.
10. Какие практические подходы используются при проведении аудита ИБ?
11. Назовите задачи аудита ИБ на предприятии.
12. Модель построения системы информационной безопасности предприятия. Методы и средства построения системы информационной безопасности предприятия.
13. Система управления информационной безопасностью (СУИБ). Понятие аудита безопасности. Методы анализа данных при аудите ИБ.
14. Инвентаризация активов. Понятие актива. Типы активов. Источники информации об активах организации.
15. 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.
16. Средства проведения аудита информационной безопасности информационных систем.
17. Стандарты в области информационной безопасности ISO/IEC 25999, ГОСТ Р ИСО/МЭК 27001,
18. Стандарты в области информационной безопасности 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.
19. Стандарт управления информационной безопасностью ГОСТ Р ИСО 17799.
20. Основные положения политики обеспечения информационной безопасности.
21. Приведите классификацию ресурсов и опишите уровни их защиты.
22. Перечислите правила безопасности при выборе и работе с персоналом.
23. 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.
24. Система оценки информационной безопасности организаций банковской системы Российской Федерации.
25. Аудит управления непрерывностью бизнеса и восстановления после сбоев.
26. Особенности аудита безопасности в области поиска средств негласного съема информации
27. Аттестация объектов информатизации.
28. Особенности аудита информационной безопасности организаций, использующих аутсорсинг

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. Милославская, Н.Г. Проверка и оценка деятельности по управлению информационной безопасностью. Серия «Вопросы управление информационной безопасностью". Выпуск 5 : учебное пособие / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. — Москва : Горячая линия-Телеком, 2012. — 166 с. — ISBN 978-5-9912-0275-6. — Текст : электронный // Лань : электронно-библиотечная система. https://elis.psu.ru/node/619857

2. Миргородская Т. В. Аудит:учебное пособие/Т. В. Миргородская.-Москва:КНОРУС,2016, ISBN 978-5-406-02669-4.-3071.-Библиогр.: с. 271-274

3. Грекул, В.И. Аудит информационных технологий : учебник / В.И. Грекул. — Москва : Горячая линия-Телеком, 2015. — 154 с. — ISBN 978-5-9912-0528-3. — Текст : электронный // Лань : электронно-библиотечная система. https://elis.psu.ru/node/619685

4. 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

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
https://dialognauka.ru/ Сайт компании "Диалог наука"

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:
- 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:
- MS Windows 7, 8, 10
- 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 практических 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 и критерии их оценивания

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.30 способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы	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.	**Неудовлетворител** Не знает комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной системы. Не умеет проверять наличее и эффективность мер и средств защиты информации в автоматизированных системах предприятия. **Удовлетворительн** 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 наличее и эффективность мер и средств защиты информации в автоматизированных системах предприятия. **Хорошо** Сформированные, но содержащие отдельные пробелы знания комплекса мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной системы. Умение проверять наличее и эффективность мер и средств защиты информации в автоматизированных системах предприятия. **Отлично** Сформированные знания комплекса мер (правила, процедуры, практические приемы,

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной системы. Умение проверять наличее и эффективность мер и средств защиты информации в автоматизированных системах предприятия.
ПК.24 способность проводить анализ особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите	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	**Неудовлетворител** Отсутствие знаний основных понятий аудита информационной безопасности; методов оценивания информационной безопасности ; основ контроля и проверки процессов и систем. Отсутствие умений оценивать информационную безопасность на основе показателей информационной безопасности. Отсутствие навыков разработки и исследования процессов защиты информации и ее компонентов по результатам аудита информационной безопасности **Удовлетворительн** Общие, но не структурированные знания основных понятий аудита информационной безопасности; методов оценивания информационной безопасности ; Частично сформированное умение оценивать информационную безопасность на основе показателей информационной безопасности. Фрагментарное применение навыков разработки и исследования процессов защиты информации и ее компонентов по результатам аудита информационной безопасности **Хорошо** Сформированные, но содержащие отдельные пробелы знания основных понятий аудита информационной безопасности; методов оценивания информационной безопасности ;

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Хорошо 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 **Отлично** 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
ПК.21 способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы	Знать и уметь находить сновные подходы к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью автоматизированной системы.	**Неудовлетворител** Отсутствие знаний и умения находить сновные подходы к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью автоматизированной системы **Удовлетворительн** 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 **Хорошо**

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Хорошо 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 **Отлично** Хорошо сформированные знания и умения находить сновные подходы к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью автоматизированной системы
ПК.31 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 обследования информационной безопасности; основы контроля и проверки процессов и систем; направления обеспечения и оценки информационной безопасности. Уметь исследовать полученные оценки информационной безопасности АС; Уметь владеть навыками разработки и исследования процессов защиты информации и ее компонентов по результатам аудита информационной безопасности	**Неудовлетворител** 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 и проверки процессов и систем. Отсутствие умения исследовать полученные оценки информационной безопасности АС ; Отсутствие владения навыков разработки и исследования процессов защиты информации и ее компонентов по результатам аудита информационной безопасности **Удовлетворительн** 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

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Удовлетворительн 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 **Хорошо** 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 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 **Отлично** 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;

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично 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
ПК.26 способность формировать комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной системы	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. Формирование навыков использования методологии, стандартов и нормативных требования в области аудита информационной безопасности АС.	**Неудовлетворител** Не знает 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 Отсутствие умений исследовать полученные оценки информационной безопасности; оценивать результаты аудита и самооценки информационной безопасности АС. Отсутствие навыков использования методологии, стандартов и нормативных требования в области аудита информационной безопасности АС. **Удовлетворительн** 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. Частично сформированное умение исследовать полученные оценки информационной безопасности; оценивать результаты аудита и самооценки информационной безопасности АС.

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Удовлетворительн Фрагментарное применение навыков использования методологии, стандартов и нормативных требования в области аудита информационной безопасности АС. **Хорошо** 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. В целом успешные, но содержащие отдельные пробелы умения исследовать полученные оценки информационной безопасности; оценивать результаты аудита и самооценки информационной безопасности АС. В целом успешное, но содержащее отдельные пробелы применение навыков использования методологии, стандартов и нормативных требования в области аудита информационной безопасности АС. **Отлично** 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. Успешное и систематическое применение навыков использования методологии, стандартов и нормативных требования в области аудита информационной безопасности АС

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.25 способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	знать требования для формирования политик информационной безопасности организации и уметь контролировать эффективность ее реализации	**Неудовлетворител** не знает требований формирования политики информационной безопасности организации и не умеет контролировать эффективность ее реализации **Удовлетворительн** Частично сформированные знания требований формирования политики информационной безопасности организации. Частично сформированные умения контролировать эффективность реализации политики информационной безопасности организации **Хорошо** 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 **Отлично** Полностью сформированные знания требований формирования политики информационной безопасности организации. Полностью сформированные умения контролировать эффективность реализации политики информационной безопасности организации

Оценочные средства текущего контроля и промежуточной аттестации

Схема доставки : Базовая

Вид мероприятия промежуточной аттестации : Экзамен
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	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
Входной контроль	1. Введение. Основы аудита. **Входное тестирование**	проверки остаточных знаний по дисциплинам:- основы информационной безопасности;- программно-аппаратные средства обеспечения информационной безопасности;- технические средства защиты информации;- безопасность операционных систем.
ПК.30 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. **Письменное контрольное мероприятие**	Понимание комплексного подхода к обследованию информационной безопасности АС
ПК.26 способность формировать комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной системы	8. Оценка безопасности информационных технологий на основе международных стандартов. Методика проведения аудита информационной б **Письменное контрольное мероприятие**	Понимание основ аудита информационной безопасности и методы его проведения

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПК.24 способность проводить анализ особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите	12. Аттестация объектов информатизации как аудит информационной безопасности объектов информатизации. **Письменное контрольное мероприятие**	Особенности аудита информационной безопасности организаций

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
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.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	Итоговое контрольное мероприятие **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
Полностью ответил на вводный тест	100
Одна ошибка в водном тесте	80
Две ошибки вводном тесте	60
3 ошибки в водном тесте	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
Реализация Технического задания на СЗИСПДн в полном объеме с учетом НМД и данных разработанной модели угроз ПДн.	20
Реализация Технического задания на СЗИСПДн в не в полном объеме с учетом учета применяемых СЗИ и показателей защищенности. С 1 ошибкой в оформлении .	16
Реализация Технического задания на СЗИСПДн в не в полном объеме без учета применяемых СЗИ и без ошибок в показателях защищенности. С 2 ошибками в оформлении .	14
Реализация Технического задания на СЗИСПДн в не в полном объеме без учета применяемых СЗИ, с ошибками в показателях защищенности. С 3 ошибками в оформлении .	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
Представление полного отчета по расчетам системы защиты в банковской сфере без ошибок в показателе, с оформленными итоговыми показателями и диаграммой защищенности по методике аудита ЦБ РФ.	20
Представление полного отчета по расчетам системы защиты в банковской сфере с ошибкой в одном показателе, с оформленными итоговыми показателями и диаграммой защищенности по методике аудита ЦБ РФ.	18
Представление полного отчета по расчетам системы защиты в банковской сфере с ошибкой в 2 показателях, с оформленными итоговыми показателями и диаграммой защищенности по методике аудита ЦБ РФ.	16
Представление неполного отчета по расчетам системы защиты в банковской сфере с ошибкой в 3 показателях, с оформленными итоговыми показателями и без диаграммы	10

защищенности по методике аудита ЦБ РФ.	

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

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
Выступление с оформленной презентацией и защита итоговой лабораторной работы с полным освещением темы , представлением результатов по практической части , освещением классов средств тестирования, с представлением разработанного отчета.	20
Выступление с оформленной презентацией и защита итоговой лабораторной работы с полным освещением темы , представлением результатов по практической части , с неполным освещением классов средств тестирования, представлением неполного разработанного отчета.	18
Выступление с оформленной презентацией и защита итоговой лабораторной работы с не полным освещением темы , представлением не всех результатов по практической части , с неполным освещением классов средств тестирования, представлением неполного разработанного отчета.	16
Выступление с не полностью оформленной презентацией и защита итоговой лабораторной работы с не полным освещением темы , представлением не всех результатов по практической части , без освещения классов средств тестирования, без представления разработанного отчета.	10

Итоговое контрольное мероприятие

Продолжительность проведения мероприятия промежуточной аттестации: **1 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 первый вопрос билета	12
Полный, исчерпывающий ответ на второй вопрос билета	12
Полный ответ на дополнительный вопрос	8
Полный ответ на дополнительный вопрос	8