МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Российский государственный гуманитарный университет»
(ФГБОУ ВО «РГГУ»)

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
Кафедра информационной безопасности

АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

по направлению подготовки (специальности)
10.03.01 Информационная безопасность
по профилю:
Безопасность автоматизированных систем
Уровень квалификация выпускника - бакалавр
Форма обучения очная

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва *2021*

Аудит информационной безопасности
Рабочая программа дисциплины
Составитель:
Кандидат технических наук, доцент,
к.и.н., доцент, заведующая кафедрой
информационной безопасности Г.А. Шевцова

Ответственный редактор
к.и.н., доцент, заведующая кафедрой
информационной безопасности Г.А. Шевцова

УТВЕРЖДЕНО
Протокол заседания кафедры информационной безопасности
№ 10 от 20.05.2021

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цели дисциплины: изучение методов и средств управления информационной безопасностью (ИБ) на объекте, а также изучение основных подходов к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью определенного объекта (СУИБ) на основе организации и проведения аудита информационной безопасности.

Задачи дисциплины:

изучение:

- основных понятий аудита ИБ;
- процессного подхода к построению СУИБ;
- основных требований к содержанию аудита информационной безопасности;
- основ контроля и проверки процессов и систем;
- процесса комплексного обследования ИБ;
- методов оценивания ИБ;

формирование умений:

- оценивания ИБ на основе показателей ИБ;
- исследования полученных оценок информационной безопасности;

овладение навыками использования методологии, стандартов и нормативных требований в области аудита ИБ.

1.2. Формируемые компетенции, соотнесённые с планируемыми результатами обучения по дисциплине:

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
ОПК-4.1	ОПК-4.1.1 Знает нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации	1) Знать: место и роль информационной безопасности в системе национальной безопасности Российской Федерации; принципы построения системы управления информационной безопасностью (СУИБ) в организации; основные понятия аудита информационной безопасности; процессный подход к организации информационной безопасности; нормативно-правовые и методологические основы аудита информационной безопасности 2) Уметь: использовать нормативно-правовые акты по основам аудита ИБ; оценивать эффективность процессов управления ИБ организации; оценивать эффективность СУИБ
	ОПК-4.1.2 Умеет разрабатывать документы в области обеспечения безопасности информации в автоматизированной системе при ее эксплуатации (включая управление инцидентами информационной безопасности)	
	ОПК-4.1.3 Владеет навыками планирования мероприятий по обеспечению защиты информации и	

	организацию работы персонала автоматизированной системы с учетом требований по защите информации	организации. анализировать и оценивать текущее состояние ИБ на предприятии 3) Владеть: терминологией и процессным подходом к построению СУИБ; навыками анализа активов организации, угроз ИБ и уязвимостей в рамках области деятельности СУИБ; методами научного исследования уязвимости и защищенности информационных процессов по результатам аудита информационной безопасности 1
ПК-6	ПК-6.1 Знает оценки работоспособности применяемых средств защиты информации с использованием штатных средств и методик ПК-6.2Умеет оценить эффективности применяемых средств защиты информации с использованием штатных средств и методик ПК-6.3Владеет навыками определения уровня защищенности и доверия средств защиты информации	) Знать: основные понятия аудита информационной безопасности; процессный подход к организации информационной безопасности; нормативно-правовые и методологические основы аудита информационной безопасности; основные требования к содержанию аудита информационной безопасности. 2) Уметь: оценивать эффективность СУИБ организации. анализировать и оценивать текущее состояние ИБ на предприятии исследовать полученные оценки информационной безопасности; оценивать результаты аудита и самооценки информационной безопасности. 3) Владеть: методами научного исследования уязвимости и защищенности информационных процессов по результатам аудита информационной безопасности; навыками использования методологии, правовых и нормативных требований и

		рекомендаций в области аудита информационной безопасности.
ПК-9	ПК-9.1Знает нормативные правовые акты в области защиты информации, национальные, межгосударственные и международные стандарты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации	1) Знать: принципы построения системы управления информационной безопасностью (СУИБ) в организации; основные понятия аудита информационной безопасности; процессный подход к организации информационной безопасности; основные требования к содержанию аудита информационной безопасности. 2) Уметь: использовать нормативно-правовые акты по основам аудита ИБ; оценивать эффективность СУИБ организации. анализировать и оценивать текущее состояние ИБ на предприятии оценивать результаты аудита и самооценки информационной безопасности. 3) Владеть: навыками анализа активов организации, угроз ИБ и уязвимостей в рамках области деятельности СУИБ; методами научного исследования уязвимости и защищенности информационных процессов по результатам аудита информационной безопасности; навыками использования методологии, правовых и нормативных требований и рекомендаций в области аудита информационной безопасности.
	ПК-9.2 Владеет организационными мерами по защите информации	
	ПК-9.3Умеет работать с программным обеспечением с соблюдением действующих требований по защите информации	
ПК-10	ПК-10.1Знает нормативные правовые акты в области защиты информации, национальные, межгосударственные и международные стандарты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации	
	ПК-10.2 Умеет анализировать данные о назначении, функциях, условиях функционирования объектов и систем обработки информации ограниченного доступа, установленных на объектах информатизации,	

	и характере обрабатываемой на них информации	
	ПК-10.3 Владеет навыком разработки аналитического обоснования необходимости создания системы защиты информации в организации	
ПК-8	ПК-8.1 Знает основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах, организационные меры по защите информации	
	ПК-8.2 Умеет анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах; вести протоколы и журналы учета при осуществлении аудита систем защиты информации автоматизированных систем	
	ПК-8.3 Владеет навыками выработки рекомендаций для	

	принятия решения о модернизации системы защиты информации автоматизированной системы	

1.3. Место дисциплины в структуре основной образовательной программы

Дисциплина «Аудит информационной безопасности» относится к вариативной части блока дисциплин учебного плана.

Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин и прохождения практик: Основы информационной безопасности, Организационное обеспечение информационной безопасности, Правовое обеспечение информационной безопасности, Специальные нормативные документы и стандарты по информационной безопасности, Основы управления информационной безопасностью, Системы управления информационной безопасностью, Управление информационными рисками.

В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин и прохождения практик: Комплексное обеспечение безопасности объекта информатизации, Информационная безопасность в банковской сфере, преддипломная практика.

2. Структура дисциплины

Структура дисциплины для очной формы обучения

Общая трудоемкость дисциплины составляет 3 з. е., 114 ч., в том числе контактная работа обучающихся с преподавателем 60 ч., самостоятельная работа обучающихся 54 ч.

№ п/п	Раздел дисциплины/темы	Семестр	Виды учебной работы (в часах)						Формы текущего контроля успеваемости, форма промежуточной аттестации *(по семестрам)*
			контактная					Самостоятельная работа	
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточная аттестация		
1	*Базовые вопросы управления ИБ*	**8**	**2**		**2**			***2***	Участие в дискуссии на практическом занятии, опрос
2	*Область деятельности, ролевая структура СУИБ и политика СУИБ*	**8**	**4**		**2**			***2***	Участие в дискуссии на практическом занятии, опрос
3	*Рискология ИБ*	**8**	**2**		**4**			***4***	Участие в дискуссии на практическом занятии, опрос
4	*Основные процессы СУИБ. Обязательная документация СУИБ*	**8**	**2**		**4**			***4***	Участие в дискуссии на практическом занятии, выступление с

									докладом
5	*Внедрение разработанных процессов. Документ «Положение о применимости»*	**8**	**2**		**4**			***4***	Участие в дискуссии на практическом занятии, опрос
6	*Процесс «Управление инцидентами ИБ»*	**8**	**2**		**4**			***4***	Участие в дискуссии на практическом занятии, опрос
7	*Процесс «Обеспечение непрерывности ведения бизнеса»*	**8**	**2**		**4**			***4***	Участие в дискуссии на практическом занятии, опрос
8	*Обеспечение соответствия требованиям законодательства РФ*	**8**	**2**		**4**			***4***	Участие в дискуссии на практическом занятии, опрос
9	*Эксплуатация и независимый аудит СУИБ*	**8**	**4**		**4**			***4***	Участие в дискуссии на практическом занятии, опрос
10	*Программные средства аудита ИБ*	**8**	**4**		**4**			***4***	Опрос, выступление с докладом
	Зачет с оценкой	**8**						***18***	*Зачет по билетам*
	итого:		**24**		**36**			54	

3. Содержание дисциплины

№	Наименование раздела дисциплины	Содержание
1.	Базовые вопросы управления ИБ	Сущность и функции управления. Наука управления. Принципы, подходы и виды управления. Цели и задачи управления ИБ. Понятие системы управления. Понятие СУИБ. Место СУИБ в рамках общей системы управления предприятием. Стандартизация в области построения систем управления. История развития. Процессный подход Понятие процесса. Методы формализации процессов. Цели и задачи формализации процессов. Понятие процессного подхода. 9
2.	Область деятельности, ролевая структура СУИБ и политика СУИБ	Понятие области деятельности СУИБ. Механизм выбора области деятельности. Состав области деятельности (процессы, структурные подразделения организации, кадры). Ролевая структура СУИБ Понятие роли. Использование ролевого принципа в рамках СУИБ. Преимущества

		использования ролевого принципа. Ролевая структура СУИБ (основные и дополнительные роли). Понятие Политики СУИБ. Цели Политики СУИБ. Структура и содержание Политики СУИБ.
3.	Рискология 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
4.	Основные процессы СУИБ. Обязательная документация СУИБ	Процессы «Управление документами» и «Управление записями» (цели и задачи процессов, входные/выходные данные, роли участников, обязательные этапы процессов, связи с другими процессами СУИБ). Процессы улучшения СУИБ («Внутренний аудит», «Корректирующие действия», «Предупреждающие действия»). Процесс «Мониторинг эффективности» (включая разработку метрик эффективности). Понятие «Зрелость процесса». Процесс «Анализ со стороны высшего руководства». Процесс «Обучение и обеспечение осведомленности».
5.	Внедрение разработанных процессов. Документ «Положение о применимости»	Этапы внедрения процессов и их последовательность. Обучение сотрудников, как один из этапов внедрения. Сложности, возникающие при внедрении процессов управления ИБ, и способы их решения. Контроль над внедрением процессов.
6.	Процесс «Управление инцидентами ИБ»	Цели и задачи процесса «Управления инцидентами ИБ, важность процесса с точки зрения управления ИБ. Входные/выходные данные процесса. Участники процесса. Обязательные этапы процесса. Связи с другими процессами СУИБ.
7.	Процесс «Обеспечение непрерывности ведения бизнеса»	Цели и задачи процесса «Обеспечение непрерывности ведения бизнеса». Входные/выходные данные процесса. Участники процесса. Обязательные этапы процесса. Связи с другими процессами СУИБ.
8.	Обеспечение соответствия требованиям законодательства РФ	Российское законодательство, затрагивающее аспекты и механизмы обеспечения безопасности в рамках СУИБ (авторское право, защита персональных данных и т.д.).
9.	Эксплуатация и независимый аудит СУИБ	Ввод системы в эксплуатацию. Возможные проблемы и способы их решения. Внешние аудиты ИБ на соответствие требованиям нормативных документов. Этапы проведения аудита ИБ. Результаты аудита ИБ и их интерпретация. Сертификация по ISO/IEC 27001 или ГОСТ Р ИСО/МЭК 27001. Период эксплуатации СУИБ перед сертификацией. Органы по сертификации, работающие 10 в РФ (их различия и требования).

		Этапы сертификационного аудита. Решение о сертификации.
10.	Программные средства аудита ИБ	Проведение анализа рисков информационной безопасности. Моделирование угроз информационной безопасности и уязвимостей. Разработка и управление политикой безопасности ИС.

4. Образовательные технологии

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1	**2**	**3**	**4**
1.	Базовые вопросы управления ИБ	*Лекция 1.* *Практическое занятие 1.* *Самостоятельная работа*	*Лекция с использованием видеоматериалов* *Развернутая беседа с обсуждением лекции. Опрос.* *Консультирование и проверка домашних заданий посредством электронной почты*
2.	Область деятельности, ролевая структура СУИБ и политика СУИБ	*Лекция 2.* *Практическое занятие 2.* *Самостоятельная работа*	*Лекция с использованием видеоматериалов* *Развернутая беседа с обсуждением лекции. Опрос.* *Консультирование и проверка домашних заданий посредством электронной почты*
3.	Рискология ИБ	*Лекция 3.* *Практическое занятие 3.* *Самостоятельная работа*	*Лекция с использованием видеоматериалов* *Развернутая беседа с обсуждением лекции. Опрос.* *Консультирование и проверка домашних заданий посредством электронной почты*
4.	Основные процессы СУИБ. Обязательная документация СУИБ	*Лекция 4.* *Практическое занятие 4.* *Самостоятельная работа*	*Лекция с использованием видеоматериалов* *Развернутая беседа с обсуждением лекции. Выступления с докладами.* *Консультирование и проверка домашних заданий посредством электронной почты*
5.	Внедрение разработанных процессов. Документ «Положение о применимости»	*Лекция 5.* *Практическое занятие 5.* *Самостоятельная работа*	*Лекция с использованием видеоматериалов* *Развернутая беседа с обсуждением лекции. Опрос.* *Консультирование и проверка домашних заданий посредством электронной почты*
6.	Процесс «Управление инцидентами ИБ»	*Лекция 6.* *Практическое занятие 6.*	*Лекция с использованием видеоматериалов* *Развернутая беседа с обсуждением лекции. Опрос.*

		Самостоятельная работа	*Консультирование и проверка домашних заданий посредством электронной почты*
7	Процесс «Обеспечение непрерывности ведения бизнеса»	*Лекция 7.* *Практическое занятие 7.* *Самостоятельная работа*	*Лекция с использованием видеоматериалов* *Развернутая беседа с обсуждением лекции. Опрос.* *Консультирование и проверка домашних заданий посредством электронной почты*
8	Обеспечение соответствия требованиям законодательства РФ	*Лекция 8.* *Практическое занятие 8.* *Самостоятельная работа*	*Лекция с использованием видеоматериалов* *Развернутая беседа с обсуждением лекции. Опрос.* *Консультирование и проверка домашних заданий посредством электронной почты*
9	Эксплуатация и независимый аудит СУИБ	*Лекция 9.* *Практическое занятие 9.* *Самостоятельная работа*	*Лекция с использованием видеоматериалов* *Развернутая беседа с обсуждением лекции. Опрос.* *Консультирование и проверка домашних заданий посредством электронной почты*
10	Программные средства аудита ИБ	*Лекция 10.* *Практическое занятие 10.* *Самостоятельная работа*	*Лекция с использованием видеоматериалов* *Опрос. Выступления с докладами.* *Консультирование и проверка домашних заданий посредством электронной почты*

5. Оценка планируемых результатов обучения

5.1. Система оценивания

Форма контроля	**Макс. количество баллов**	
	За одну работу	**Всего**
Текущий контроль:		
- опрос пр. занятии	*4 баллов*	*32 балла*
- участие в дискуссии на пр. занятии	*2 балла*	*18 баллов*
- выступление с докладом	*5 баллов*	*10 баллов*
Промежуточная аттестация *(зачет с оценкой)*		*40 баллов*
Итого за семестр *(дисциплину)*		*100 баллов*

Перечень компетенций с указанием этапов их формирования в процессе освоения дисциплины представляется в виде таблицы:

№ п/п	*Контролируемые разделы дисциплины*	*Код контролируемой компетенции*	*Наименование оценочного средства*
1.	1-5	ОПК-4.1; ПК-6; ПК-9; ПК-10; ПК-8	- оценка по итогам опроса на пр. занятии - оценка по итогам участия в дискуссии на пр. занятии - оценка выступления с докладом
2.	6-10	ОПК-4.1; ПК-6; ПК-9; ПК-10; ПК-8	

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

100-балльная шкала	Традиционная шкала		Шкала ECTS
95 – 100	отлично	зачтено	A
83 – 94			B
68 – 82	хорошо		C
56 – 67	удовлетворительно		D
50 – 55			E
20 – 49	неудовлетворительно	не зачтено	FX
0 – 19			F

5.2.Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
100-83/ A,B	«отлично»/ «зачтено (отлично)»/ «зачтено»	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации. Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения. Свободно ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».
82-68/ C	«хорошо»/ «зачтено (хорошо)»/	Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
	«зачтено»	промежуточной аттестации, не допуская существенных неточностей. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».
67-50/ D,E	«удовлетвори-тельно»/ «зачтено (удовлетвори-тельно)»/ «зачтено»	Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F,FX	«неудовлетворите льно»/ не зачтено	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный»,

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		закреплённые за дисциплиной, не сформированы.

5.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

Примерные темы докладов - ***проверка сформированности компетенций*** ОПК-4.1; ПК-6; ПК-9; ПК-10; ПК-8

1. Аудит ИБ
2. Стандарты СУИБ
3. Сертификация в сфере ИБ
4. Направления ИБ
5. Анализ рисков ИБ
6. Оценка рисков ИБ Психология восприятия рисков ИБ
7. Моделирование угроз ИБ
8. Программные средства аудита ИБ
9. Инциденты ИБ

Перечень вопросов для проведения опроса на практическом занятии - ***проверка сформированности компетенций*** ОПК-4.1; ПК-6; ПК-9; ПК-10; ПК-8

1. Приведите убедительные доводы того, что информационная безопасность - одна из важнейших проблем современной жизни.
2. Что понимается под системой безопасности?
3. Какие вопросы, касающиеся информационной безопасности, содержатся в Конституции РФ?
4. Какие вопросы, касающиеся информационной безопасности, содержатся в Гражданском кодексе РФ?
5. Какие статьи Уголовного кодекса напрямую касаются информационной безопасности?
6. Дайте определение информационной безопасности, прокомментируйте его составляющие. Перечислите основные категории информационной безопасности.
7. Какие Вам известны американские законы, напрямую связанные с ИБ? Что можно сказать о законодательстве ФРГ по вопросам ИБ?
8. Охарактеризуйте понятия доступности, целостности и конфиденциальности информации
9. Дайте определение угроз конфиденциальной информации. Какие действия определяют угрозы конфиденциальной информации?
10. Приведите основные направления деятельности по вопросам ИБ на законодательном уровне.

Промежуточная аттестация (примерные контрольные вопросы по курсу) - проверка сформированности компетенций - ОПК-4.1; ПК-6; ПК-9; ПК-10; ПК-8

1. Процессный подход к построению СУИБ и циклическая модель PDCA.
2. Цели и задачи, решаемые СУИБ.
3. Стандартизация в области построения СУИБ: сходства и различия стандартов.
4. Стратегии выбора области деятельности СУИБ.

5. Стратегии построения СУИБ (построение системы в целом, построение отдельных процессов управления ИБ с последующим объединением в систему).
6. Основные этапы разработки СУИБ и роль руководства организации на каждом из этапов.
7. Политика ИБ и политика СУИБ: сходства и различия.
8. Распределение ролей и ответственности в рамках СУИБ: базовая ролевая структура, дополнительные роли в рамках процессов управления ИБ.
9. Анализ рисков ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
10. Анализ рисков ИБ: основные подходы, основные этапы процесса.
11. Управление инцидентами ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
12. Расследование инцидентов ИБ: виды расследования инцидентов, критерии выбора необходимого вида расследования, основные этапы расследования (для различных видов расследования).
13. Внутренние аудиты ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
14. Анализ со стороны руководства: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
15. Обучение и обеспечение осведомленности пользователей: цели и задачи процесса, роль процесса в рамках СУИБ.
16. Внедрение процессов управления ИБ: этапы и последовательность.
17. Ввод СУИБ в эксплуатацию: возможные проблемы и способы их решения.
18. Дайте определение информационной системы. Перечислите структурные компоненты информационных систем. Что понимают под информационными ресурсами и процессами?
19. Перечислите основные компоненты концептуальной модели ИБ. Изобразите графически схему концептуальной модели системы ИБ.
20. Что такое объекты угроз ИБ? В чем выражаются угрозы информации? Каковы основные источники угроз защищаемой информации? Каковы цели угроз информации со стороны злоумышленников?
21. Дайте определение информационной безопасности, прокомментируйте ее составляющие. Перечислите основные категории информационной безопасности.
22. Что такое атака? Что такое окно опасности? Какие события происходят во время существования окна опасности?
23. Назовите главную цель мер административного уровня ИБ. Что понимается под политикой безопасности? Приведите примерный список решений верхнего уровня политики безопасности.
24. Что такое угрозы утечки информации? Какие угрозы называются преднамеренными и случайными?
25. Что такое управление рисками? Почему управление рисками рассматривается на административном уровне ИБ? В чем заключается суть мероприятий по управлению рисками?
26. Охарактеризуйте государственную структуру органов, обеспечивающих информационную безопасность.
27. В чем заключается основная специфика процедурного уровня ИБ? Перечислите основные классы мер процедурного уровня ИБ. Почему вопросы поддержания работоспособности ИС являются принципиальными на процедурном уровне ИБ?
28. Что такое источник угроз безопасности информации? Назовите основные источники преднамеренных угроз.
29. Перечислите основные причины важности программно-технического уровня ИБ. Назовите основные сервисы ИБ программно-технического уровня.

30. В чем заключается основная задача аудита, как сервиса безопасности?

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

Основная литература

а) основная:

1. Аверченков, В. И. Аудит информационной безопасности: учеб. пособие для вузов / В. И. Аверченков. – 2-е изд., стереотип. – М.: Флинта, 2011. – 269 с. [Электронный ресурс] — Режим доступа: http://znanium.com/catalog/product/453734, свободный. — Загл. с экрана. — Яз. рус.

2. Проверка и оценка деятельности по управлению информационной безопасностью: Уч.пос./ Н.Г. Милославская и др. - М.: Гор. линия-Телеком, 2012. - 166 с.: [Электронный ресурс] — Режим доступа: http://znanium.com/catalog/product/560784, свободный. — Загл. с экрана. — Яз. рус.

3. Вопросы управления информационной безопасностью: Учебное пособие для вузов. Основы управления информационной безопасностью / Курило А.П., Милославская Н.Г., Сенаторов М.Ю. - М.: Гор. линия-Телеком, 2013. - 244 с. [Электронный ресурс] — Режим доступа: http://znanium.com/catalog/author/74047029-373f-11e4-b05e-00237dd2fde2, свободный. — Загл. с экрана. — Яз. рус.

б) Дополнительная литература

4. Технические, организационные и кадровые аспекты управления информационной безопасностью: Учебное пособие для вузов / Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. - М.:Гор. линия-Телеком, 2013. - 214 с. [Электронный ресурс] — Режим доступа: http://znanium.com/catalog/product/560783, свободный. — Загл. с экрана. — Яз. рус.

в) Информационно-справочная литература

6. Вопросы управления информационной безопасностью: Учебное пособие для вузов. Управление рисками информационной безопасности / Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. - М.: Гор. линия-Телеком, 2013. - 130 с. [Электронный ресурс] — Режим доступа: http://znanium.com/catalog/product/560781, свободный. — Загл. с экрана. — Яз. рус.

7. Управление инцидентами информационной безопасности и непрерывностью бизнеса: Учебное пособие для вузов / Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. - М.:Гор. линия-Телеком, 2013. - 170 с. [Электронный ресурс] — Режим доступа: http://znanium.com/catalog/product/560782, свободный. — Загл. с экрана. — Яз. рус.

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Федеральный портал по научной и инновационной деятельности [Электронный ресурс] — Режим доступа: http://www.sci-innov.ru, свободный. — Загл. с экрана. — Яз. рус., англ.
2. Научная электронная библиотека eLibrary [Электронный ресурс] — Режим доступа: http://www.elibrary.ru, свободный. — Загл. с экрана. — Яз. рус., англ.
3. Росстандарт. Федеральное агентство по техническому регулированию и метрологии [Электронный ресурс] — Режим доступа: http://www.gost.ru, свободный. — Загл. с экрана. — Яз. рус., англ.
4. Консультант плюс [Электронный ресурс] — Режим доступа: http://www.consultant.ru, свободный. — Загл. с экрана. — Яз. рус., англ.

6.3. Перечень БД и ИСС

№п/п	Наименование
	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2017 г. Web of Science Scopus
	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2017 г. Журналы Oxford University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis
	Компьютерные справочные правовые системы Консультант Плюс, Гарант

7. Материально-техническое обеспечение дисциплины/модуля

Материально-техническая база включает учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Современный компьютерный класс оснащен

Перечень ПО

№п/п	Наименование ПО	Производитель	Способ распространения (*лицензионное или свободно распространяемое*)
1	Microsoft Office 2010	Microsoft	лицензионное
2	Windows XP	Microsoft	лицензионное
3	Kaspersky Endpoint Security	Kaspersky	лицензионное

включающий наряду с компьютерами, подключёнными к сети Интернет, экран и проектор.

Для проведения занятий лекционного типа предлагаются тематические иллюстрации в формате презентаций PowerPoint.

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
- письменные задания выполняются на компьютере со специализированным программным обеспечением, или могут быть заменены устным ответом;

- обеспечивается индивидуальное равномерное освещение не менее 300 люкс;
- для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;
- письменные задания оформляются увеличенным шрифтом;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

- для глухих и слабослышащих:

- лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования;
- письменные задания выполняются на компьютере в письменной форме;
- экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.

- для лиц с нарушениями опорно-двигательного аппарата:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
- письменные задания выполняются на компьютере со специализированным программным обеспечением;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих:

- в печатной форме увеличенным шрифтом;
- в форме электронного документа;
- в форме аудиофайла.

- для глухих и слабослышащих:

- в печатной форме;
- в форме электронного документа.

- для обучающихся с нарушениями опорно-двигательного аппарата:

- в печатной форме;
- в форме электронного документа;
- в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих:

- устройством для сканирования и чтения с камерой SARA CE;
- дисплеем Брайля PAC Mate 20;
- принтером Брайля EmBraille ViewPlus;

- для глухих и слабослышащих:

- автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих;
- акустический усилитель и колонки;

- для обучающихся с нарушениями опорно-двигательного аппарата:
- передвижными, регулируемыми эргономическими партами СИ-1;
- компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1. Планы практических занятий ***- проверка сформированности компетенций -*** ОПК-4.1; ПК-6; ПК-9; ПК-10; ПК-8

Практическое занятие:
Тема 1 (2 ч.) (Базовые вопросы управления ИБ)
Задания:
1. Дискуссия по обсуждению вопросов лекции.
2. Опрос по теме занятия.
Указания по выполнению заданий:
1. В ходе обсуждения вопросов лекции обучаемые должны продемонстрировать степень усвоения материала соответствующей лекции, при необходимости задать вопросы и получить разъяснения преподавателя
2. Ответить на вопросы по теме занятия и ранее изученному материалу.
Список литературы:
[3, 4] (см. Подраздел 6.1)
Материально-техническое обеспечение занятия: ноутбук для проведения презентации, с предустановленным ПО, подключенный к проектору; экран; оборудованная аудитория; учебные пособия и учебно-методическая литература для преподавателя, доска магнито-маркерная, магнитный стиратель и маркеры цветные для доски.

Практическое занятие:
Тема 2 (2 ч.) (Область деятельности, ролевая структура СУИБ и политика СУИБ)
Задания:
1. Дискуссия по обсуждению вопросов лекции.
2. Опрос по теме занятия.
Указания по выполнению заданий:
1. В ходе обсуждения вопросов лекции обучаемые должны продемонстрировать степень усвоения материала соответствующей лекции, при необходимости задать вопросы и получить разъяснения преподавателя
2. Ответить на вопросы по теме занятия и ранее изученному материалу.
Список литературы:
[3, 4] (см. Подраздел 6.1)
Материально-техническое обеспечение занятия: ноутбук для проведения презентации, с предустановленным ПО, подключенный к проектору; экран; оборудованная аудитория; учебные пособия и учебно-методическая литература для преподавателя, доска магнито-маркерная, магнитный стиратель и маркеры цветные для доски.

Практическое занятие:
Тема 3 (2 ч.) (Рискология ИБ)
Задания:
1. Дискуссия по обсуждению вопросов лекции.
2. Опрос по теме занятия.

Указания по выполнению заданий:
1. В ходе обсуждения вопросов лекции обучаемые должны продемонстрировать степень усвоения материала соответствующей лекции, при необходимости задать вопросы и получить разъяснения преподавателя
2. Ответить на вопросы по теме занятия и ранее изученному материалу.
Список литературы:
[3, 5, 6] (см. Подраздел 6.1)
Материально-техническое обеспечение занятия: ноутбук для проведения презентации, с предустановленным ПО, подключенный к проектору; экран; оборудованная аудитория; учебные пособия и учебно-методическая литература для преподавателя, доска магнито-маркерная, магнитный стиратель и маркеры цветные для доски.

Практическое занятие:
Тема 4 (2 ч.) (Основные процессы СУИБ. Обязательная документация СУИБ)
Задания:
1. Дискуссия по обсуждению вопросов лекции.
2. Выступления с докладами.
Указания по выполнению заданий:
1. В ходе обсуждения вопросов лекции обучаемые должны продемонстрировать степень усвоения материала соответствующей лекции, при необходимости задать вопросы и получить разъяснения преподавателя.
2. Выступить с докладом с использованием презентации. Ответить на заданные вопросы.
Список литературы:
[2, 3, 4] (см. Подраздел 6.1)
Материально-техническое обеспечение занятия: ноутбук для проведения презентации, с предустановленным ПО, подключенный к проектору; экран; оборудованная аудитория; учебные пособия и учебно-методическая литература для преподавателя, доска магнито-маркерная, магнитный стиратель и маркеры цветные для доски.

Практическое занятие:
Тема 5 (2 ч.) (Внедрение разработанных процессов. Документ «Положение о применимости»)
Задания:
1. Дискуссия по обсуждению вопросов лекции.
2. Опрос по теме занятия.
Указания по выполнению заданий:
1. В ходе обсуждения вопросов лекции обучаемые должны продемонстрировать степень усвоения материала соответствующей лекции, при необходимости задать вопросы и получить разъяснения преподавателя
2. Ответить на вопросы по теме занятия и ранее изученному материалу.
Список литературы:
[1, 2, 3, 4] (см. Подраздел 6.1)
Материально-техническое обеспечение занятия: ноутбук для проведения презентации, с предустановленным ПО, подключенный к проектору; экран; оборудованная аудитория; учебные пособия и учебно-методическая литература для преподавателя, доска магнито-маркерная, магнитный стиратель и маркеры цветные для доски.

Практическое занятие:
Тема 6 (2 ч.) (Процесс «Управление инцидентами ИБ»)
Задания:
1. Дискуссия по обсуждению вопросов лекции.

2. Опрос по теме занятия.
Указания по выполнению заданий:
1. В ходе обсуждения вопросов лекции обучаемые должны продемонстрировать степень усвоения материала соответствующей лекции, при необходимости задать вопросы и получить разъяснения преподавателя
2. Ответить на вопросы по теме занятия и ранее изученному материалу.
Список литературы:
[1, 3, 7] (см. Подраздел 6.1)
Материально-техническое обеспечение занятия: ноутбук для проведения презентации, с предустановленным ПО, подключенный к проектору; экран; оборудованная аудитория; учебные пособия и учебно-методическая литература для преподавателя, доска магнито-маркерная, магнитный стиратель и маркеры цветные для доски, раздаточный материал для тестирования.

Практическое занятие:
Тема 7 (2 ч.) (Процесс «Обеспечение непрерывности ведения бизнеса»)
Задания:
1. Дискуссия по обсуждению вопросов лекции.
2. Опрос по теме занятия.
Указания по выполнению заданий:
1. В ходе обсуждения вопросов лекции обучаемые должны продемонстрировать степень усвоения материала соответствующей лекции, при необходимости задать вопросы и получить разъяснения преподавателя
2. Ответить на вопросы по теме занятия и ранее изученному материалу.
Список литературы:
[1, 3, 7] (см. Подраздел 6.1)
Материально-техническое обеспечение занятия: ноутбук для проведения презентации, с предустановленным ПО, подключенный к проектору; экран; оборудованная аудитория; учебные пособия и учебно-методическая литература для преподавателя, доска магнито-маркерная, магнитный стиратель и маркеры цветные для доски, раздаточный материал для тестирования.

Практическое занятие:
Тема 8 (2 ч.) (Обеспечение соответствия требованиям законодательства РФ)
Задания:
1. Дискуссия по обсуждению вопросов лекции.
2. Опрос по теме занятия.
Указания по выполнению заданий:
1. В ходе обсуждения вопросов лекции обучаемые должны продемонстрировать степень усвоения материала соответствующей лекции, при необходимости задать вопросы и получить разъяснения преподавателя
2. Ответить на вопросы по теме занятия и ранее изученному материалу.
Список литературы:
[1, 2] (см. Подраздел 6.1), [3, 4] (см. Подраздел 6.2)
Материально-техническое обеспечение занятия: ноутбук для проведения презентации, с предустановленным ПО, подключенный к проектору; экран; оборудованная аудитория; учебные пособия и учебно-методическая литература для преподавателя, доска магнито-маркерная, магнитный стиратель и маркеры цветные для доски, раздаточный материал для тестирования.

Практическое занятие:
Тема 9 (2 ч.) (Эксплуатация и независимый аудит СУИБ)

Задания:
1. Дискуссия по обсуждению вопросов лекции.
2. Опрос по теме занятия.
Указания по выполнению заданий:
1. В ходе обсуждения вопросов лекции обучаемые должны продемонстрировать степень усвоения материала соответствующей лекции, при необходимости задать вопросы и получить разъяснения преподавателя
2. Ответить на вопросы по теме занятия и ранее изученному материалу.
Список литературы:
[1, 2, 4] (см. Подраздел 6.1)
Материально-техническое обеспечение занятия: ноутбук для проведения презентации, с предустановленным ПО, подключенный к проектору; экран; оборудованная аудитория; учебные пособия и учебно-методическая литература для преподавателя, доска магнито-маркерная, магнитный стиратель и маркеры цветные для доски, раздаточный материал для тестирования.

Практическое занятие:
Тема 10 (2 ч.) (Программные средства аудита ИБ)
Задания:
1. Опрос по теме занятия.
2. Выступления с докладами.
Указания по выполнению заданий:
1. Ответить на вопросы по теме занятия и ранее изученному материалу.
2. Выступить с докладом с использованием презентации. Ответить на заданные вопросы.
Список литературы:
[1, 2, 4] (см. Подраздел 6.1)
Материально-техническое обеспечение занятия: ноутбук для проведения презентации, с предустановленным ПО, подключенный к проектору; экран; оборудованная аудитория; учебные пособия и учебно-методическая литература для преподавателя, доска магнито-маркерная, магнитный стиратель и маркеры цветные для доски, раздаточный материал для тестирования.

Приложение 1

АННОТАЦИЯ ДИСЦИПЛИНЫ

Дисциплина «Аудит информационной безопасности» реализуется на *факультете информационных систем и безопасности Института информационных наук и технологий безопасности кафедрой информационной безопасности*.

Цели дисциплины: изучение методов и средств управления информационной безопасностью (ИБ) на объекте, а также изучение основных подходов к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью определенного объекта (СУИБ) на основе организации и проведения аудита информационной безопасности.

Задачи:

изучение:

- основных понятий аудита ИБ;
- процессного подхода к построению СУИБ;
- основных требований к содержанию аудита информационной безопасности;
- основ контроля и проверки процессов и систем;
- процесса комплексного обследования ИБ;
- методов оценивания ИБ;

формирование умений:

- оценивания ИБ на основе показателей ИБ;
- исследования полученных оценок информационной безопасности;

овладение навыками использования методологии, стандартов и нормативных требований в области аудита ИБ.

Дисциплина (модуль) направлена на формирование следующих компетенций:

- ОПК-4.1 - Способен проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах;

В результате освоения дисциплины (модуля) обучающийся должен:

- Знает нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации
- Умеет разрабатывать документы в области обеспечения безопасности информации в автоматизированной системе при ее эксплуатации (включая управление инцидентами информационной безопасности)
- Владеет навыками планирования мероприятий по обеспечению защиты информации и организацию работы персонала автоматизированной системы с учетом требований по защите информации

- ПК-6 - Способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации

В результате освоения дисциплины (модуля) обучающийся должен:

- Знает оценки работоспособности применяемых средств защиты информации с использованием штатных средств и методик
- Умеет оценить эффективности применяемых средств защиты информации с использованием штатных средств и методик
- Владеет навыками определения уровня защищенности и доверия средств защиты информации

- ПК-9 - Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности

В результате освоения дисциплины (модуля) обучающийся должен:

- Знает нормативные правовые акты в области защиты информации, национальные, межгосударственные и международные стандарты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации
- Владеет организационными мерами по защите информации
- Умеет работать с программным обеспечением с соблюдением действующих требований по защите информации

- ПК-10 - Способен проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности

В результате освоения дисциплины (модуля) обучающийся должен:

- Знает нормативные правовые акты в области защиты информации, национальные, межгосударственные и международные стандарты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации
- Умеет анализировать данные о назначении, функциях, условиях функционирования объектов и систем обработки информации ограниченного доступа, установленных на объектах информатизации, и характере обрабатываемой на них информации
- Владеет навыком разработки аналитического обоснования необходимости создания системы защиты информации в организации

- ПК-8 - Способен осуществлять мониторинг и аудит защищенности информации в автоматизированных системах

  В результате освоения дисциплины (модуля) обучающийся должен:

  - Знает основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах, организационные меры по защите информации
  - Умеет анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах; вести протоколы и журналы учета при

осуществлении аудита систем защиты информации автоматизированных систем
- Владеет навыками выработки рекомендаций для принятия решения о модернизации системы защиты информации автоматизированной системы

По дисциплине предусмотрена промежуточная аттестация в форме *зачета с оценкой*.

Общая трудоемкость освоения дисциплины (модуля) составляет 3 зачетные единицы.