МИНОБРНАУКИ РОССИИ

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

ИНСТИТУТ ИНФОРМАЦИОННННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
Кафедра информационной безопасности

СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

по направлению подготовки (специальности)
10.03.01 Информационная безопасность
по профилю:
Организация и технология защиты информации
Уровень квалификация выпускника - бакалавр
Форма обучения очная

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва *2021*

Название дисциплины «Системы управления информационной безопасностью»
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: формирование у обучающихся теоретических знаний, необходимых умений и практических навыков в области управления информационной безопасностью, касающихся разработки и реализации управленческих решений по управлению деятельностью современной российской организации по обеспечению информационной безопасности (ИБ).

Задачи дисциплины:

- привитие обучаемым основ культуры обеспечения информационной безопасности;
- формирование у обучаемых понимания роли процессов управления в обеспечении информационной безопасности организаций, объектов и систем;
- ознакомление обучаемых с основными методами управления информационной безопасностью организаций, объектов и систем;
- обучение различным методам реализации процессов управления информационной безопасностью, направленных на эффективное управление ИБ конкретной организации.

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

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
ОПК-2.2- Способен формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы	ОПК-2.2.1 Знает организационные меры по защите информации, основные методы управления защитой информации	Знать: - современные подходы к управлению ИБ и направления развития; - основные стандарты, регламентирующие управление ИБ; - принципы построения систем управления ИБ (СУИБ); - принципы разработки процессов управления ИБ; - взаимосвязи отдельных процессов управления ИБ в рамках общей СУИБ; - подходы к интеграции СУИБ в общую систему управления предприятием. Уметь: - анализировать текущее состояние ИБ на предприятии с целью разработки требований к разрабатываемым процессам управления ИБ; - определять цели и задачи, решаемые разрабатываемыми процессами управления ИБ; - применять процессный подход к управлению ИБ в различных сферах деятельности; - используя современные методы
	ОПК-2.2.2 Умеет разрабатывать предложения по совершенствованию системы управления защиты информации, осуществлять планирование и организацию работы персонала с учетом требований по защите информации	
	ОПК-2.2.3 Владеет навыками выработки рекомендаций для решения о модернизации системы защиты информации	

		и средства разрабатывать процессы управления ИБ, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность; - практически решать задачи формализации разрабатываемых процессов управления ИБ; - разрабатывать и внедрять СУИБ и оценивать ее эффективность Владеть: - навыками управления информационной безопасностью простых объектов; - терминологией и процессным подходом построения систем управления ИБ; - навыками анализа активов организации, их угроз ИБ и уязвимостей в рамках области деятельности СУИБ; - навыками построения как отдельных процессов управления ИБ, так и системы процессов в целом.
ПК-13 - Способен принимать участие в формировании, организации и поддержания выполнения комплекса мер по обеспечению информационной безопасности, управлении процессом их реализации	ПК-13.1 Знает процедуру организации установки и настройки технических, программных (программно-технических) средств защиты информации, входящих в состав системы защиты информации организации, в соответствии с техническим проектом и инструкциями по эксплуатации ПК-13.2 Владеет навыками организации и сопровождения аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации	Знать: - современные подходы к управлению ИБ и направления развития; - основные стандарты, регламентирующие управление ИБ; - принципы построения систем управления ИБ (СУИБ); - принципы разработки процессов управления ИБ; - взаимосвязи отдельных процессов управления ИБ в рамках общей СУИБ; - подходы к интеграции СУИБ в общую систему управления предприятием. Уметь: - анализировать текущее состояние ИБ на предприятии с целью разработки требований к разрабатываемым процессам управления ИБ; - определять цели и задачи, решаемые разрабатываемыми

	ПК-13.3 Умеет разрабатывать и реализовывать организационные меры, обеспечивающие эффективность системы защиты информации	процессами управления ИБ; - применять процессный подход к управлению ИБ в различных сферах деятельности; - используя современные методы и средства разрабатывать процессы управления ИБ, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность; - практически решать задачи формализации разрабатываемых процессов управления ИБ; - разрабатывать и внедрять СУИБ и оценивать ее эффективность Владеть: - навыками управления информационной безопасностью простых объектов; - терминологией и процессным подходом построения систем управления ИБ; - навыками анализа активов организации, их угроз ИБ и уязвимостей в рамках области деятельности СУИБ; - навыками построения как отдельных процессов управления ИБ, так и системы процессов в целом.

1.3. Место дисциплины в структуре основной образовательной программы

Дисциплина «Системы управления информационной безопасностью» 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, Основы управления информационной безопасностью.

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, Аудит информационной безопасности, преддипломная практика.

2. Структура дисциплины

Структура дисциплины для очной формы обучения

Общая трудоемкость дисциплины составляет 2 з. е., 76 ч., в том числе контактная работа обучающихся с преподавателем 40 ч., самостоятельная работа обучающихся 36 ч.

№	Раздел	Се	Виды учебной работы	Формы

п/п	дисциплины/темы		(в часах)						текущего контроля успеваемости, форма промежуточной аттестации *(по семестрам)*
			контактная					Самостоятельная работа	
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточная аттестация		
1	*Методология построения систем управления информационной безопасностью с учетом особенностей функционирования объекта информационной среды*	**8**	**2**		**4**				Участие в дискуссии на практическом занятии
2	*Нормативная база систем и процессов управления информационной безопасностью. Отраслевые стандарты в области управления ИБ.*	**8**	**2**		**4**			4	Опрос, выступление с докладом
3	*Политика информационной безопасности*	**8**	**2**		**4**			4	Опрос, участие в дискуссии на практическом занятии
4	*Основные принципы построения систем управления информационной безопасностью*	**8**	**4**		**4**			10	Опрос, участие в дискуссии на практическом занятии
5	*Основы управления рисками ИБ*	**8**	**2**		**4**			10	Опрос, участие в дискуссии на практическом занятии, выступление с докладом
6	*Технические и организационные вопросы управления информационной безопасностью*	**8**	**4**		**4**				Опрос, участие в дискуссии на практическом занятии
	зачёт с оценко)	**8**							*Зачет с оценкой по вопросам билетов*

	итого:		**16**		**24**			36	

3. Содержание дисциплины

№	Наименование раздела дисциплины	Содержание
1.	Методология построения систем управления информационной безопасностью с учетом особенностей функционирования объекта информационной среды	Понятие информационной безопасности. Эволюция понятия «информационная безопасность» (ИБ). Нормативное толкование понятия «информационная безопасность». ИБ организации. Системный и процессный подходы к задаче эффективного управления ИБ объекта. Базовые методы системного анализа. Моделирование систем. Понятие процесса. Методы формализации процессов, цели и задачи. Основные вопросы управления информационной безопасностью. Сущность и функции управления. Принципы, подходы и виды управления. Циклическая модель PDCA. Понятие системы управления информационной безопасностью (СУИБ). Цели и задачи управления информационной безопасностью.
2.	Нормативная база систем и процессов управления информационной безопасностью. Отраслевые стандарты в области управления ИБ.	Линейка стандартов ISO/IEC 27000 «Информационные технологии. Методы обеспечения безопасности». Стандарты на отдельные процессы управления ИБ и оценку безопасности информационных технологий. Стандарты банковской системы Российской Федерации как пример отраслевых стандартов в области управления информационной безопасностью
3.	Политика информационной безопасности	Понятие Политики информационной безопасности. Цели политики ИБ. Структура и содержание Политики ИБ. Источники информации для разработки Политики ИБ. Анализ и обновление. Характеристики Политик ИБ. Особенности корпоративных и частных Политик ИБ. Жизненный цикл Политики ИБ. Ответственность за выполнение Политики ИБ.
4.	Основные принципы построения систем управления информационной безопасностью	Стратегии построения и внедрения СУИБ в организации. Обоснование необходимости применения СУИБ. Выполнение комплекса мероприятий по внедрению СУИБ: определение области действия СУИБ, подготовка документов СУИБ, разработка Политики безопасности, ролевой структуры СУИБ. Определение роли высшего руководства организации в СУИБ. Использование процессного подхода при управлении ИБ организации. Планирование, внедрение, анализ функционирования СУИБ, дальнейшее развитие и модернизация компонентов СУИБ.
5.	Основы управления рисками	Системный подход к управлению рисками.

	ИБ	Составляющие процесса управления рисками ИБ. Этапы оценки рисков ИБ. Нормативные документы по управлению рисками. Анализ рисков ИБ. Понятие актива. Типы активов. Инвентаризация активов. Источники информации об активах организации. Определение угроз ИБ, уязвимостей и последствий на этапе инвентаризации активов. Оценивание рисков ИБ. Подходы к оценке рисков ИБ. Планирование мер по обработке выявленных рисков ИБ. Утверждение результатов анализа рисков ответственными руководителями организации. Использование полученных результатов анализа рисков. Обеспечение управления рисками ИБ. Документальная составляющая обеспечения. Внутренняя нормативная база организации в области управления рисками ИБ. Инструментальные средства управления рисками ИБ. Основные продукты и разработчики. Управление инцидентами ИБ. Определение инцидента информационной безопасности. Описание процедуры управления инцидентами безопасности на основе модели PDCA. Обнаружение и регистрация инцидента. Устранение причин, последствий инцидента и его расследование. Корректирующие и превентивные действия. Нормативная база процедуры управления ИТ-инцидентами. Стандарт ISO/IEC 20000:2005. Управление непрерывностью услуг Задачи процесса управления непрерывностью услуг (ITSCM). Понятие процесса управления непрерывностью бизнеса (BCM). Планы обеспечения непрерывности бизнеса, обеспечения непрерывности и восстановления услуг. Жизненный цикл ITSCM. Анализ влияния на бизнес (BIA) процессов управления непрерывностью бизнеса. Анализ BIA как индикатор последствий потерь услуг для бизнеса. Построение диаграммы оценки влияния потери услуги или бизнес-процесса на бизнес в целом.
6.	Технические и организационные вопросы управления информационной безопасностью	Технические аспекты управления ИБ. Управление доступом к активам организации. Управление защищенной передачей данных в организации. Обеспечение ИБ информационных систем. Физическая защита информационных объектов организации. Использование программных средств для поддержки управления безопасностью. Организационные вопросы управления ИБ. Эксплуатация и независимый аудит системы управления ИБ. 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.

4. Образовательные технологии

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1	**2**	**3**	**4**
1.	Методология построения систем управления информационной безопасностью с учетом особенностей функционирования объекта информационной среды	*Лекция 1.* *Практическое занятие 1.* *Самостоятельная работа*	*Лекция с использованием видеоматериалов* *Развернутая беседа с обсуждением лекции.* *Консультирование и проверка домашних заданий посредством электронной почты*
2.	Нормативная база систем и процессов управления информационной безопасностью. Отраслевые стандарты в области управления ИБ.	*Лекция 2.* *Практическое занятие 2.* *Самостоятельная работа*	*Лекция с использованием видеоматериалов* *Опрос. Выступление с докладом.* *Консультирование и проверка домашних заданий посредством электронной почты*
3.	Политика информационной безопасности	*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 принципы построения систем управления информационной безопасностью	*Лекция 4.* *Практическое занятие 4.* *Самостоятельная работа*	*Лекция с использованием видеоматериалов* *Развернутая беседа с обсуждением лекции. Опрос.* *Консультирование и проверка домашних заданий посредством электронной почты*
5.	Основы управления рисками ИБ	*Лекция 5.* *Практическое занятие 5.* *Самостоятельная работа*	*Лекция с использованием видеоматериалов* *Развернутая беседа с обсуждением лекции. Опрос. Выступление с докладом.* *Консультирование и проверка домашних заданий посредством электронной почты*

6.	Технические и организационные вопросы управления информационной безопасностью	*Лекция 6.* *Практическое занятие 6.* *Самостоятельная работа*	*Лекция с использованием видеоматериалов* *Развернутая беседа с обсуждением лекции. Опрос.* *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	*5 баллов*	*25 баллов*
- участие в дискуссии на пр. занятии	*5 баллов*	*25 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.	1-6	ОПК-2.2; ПК-13	- оценка по итогам опроса на пр. занятии - оценка по итогам участия в дискуссии на пр. занятии - оценка выступления с докладом

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)»/ «зачтено»	Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе 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

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
		с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F,FX	«неудовлетворительно»/ 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», закреплённые за дисциплиной, не сформированы.

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

Примерные темы докладов - ***проверка сформированности компетенции*** ОПК-2.2; ПК-13

1. Эволюция определений информационной безопасности. Содержание терминов «безопасность информации», «защита информации» и «информационная безопасность» -
2. Этапы обеспечения информационной безопасности организации
3. Сущность системного подхода к исследованию объектов и управлению организацией
4. Определение и содержание процессного подхода к анализу деятельности организации
5. Основные свойства информации как предмета защиты. Характеристики секретной и конфиденциальной информации
6. Понятие объекта угроз ИБ, целей и источников угроз защищаемой информации
7. Основные составляющие процесса управления инцидентами ИБ в организации
8. Основные преимущества использования циклической модели PDCA управления деятельностью организации
9. Основные направления деятельности законодательных органов РФ относящиеся к вопросам ИБ
10. Характеристика статей Уголовного кодекса непосредственно связанных с ИБ

Примерный перечень вопросов для проведения опроса на практическом занятии- ***проверка сформированности компетенции*** ОПК-2.2; ПК-13

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 компетенции - ОПК-2.2; ПК-13

1. Дайте определение информационной системы. Перечислите структурные компоненты информационных систем. Что понимают под информационными ресурсами и процесами?
2. Перечислите основные компоненты концептуальной модели ИБ. Изобразите графически схему концептуальной модели системы ИБ.
3. Какая информация является предметом защиты? Перечислите основные свойства информации как предмета защиты. Охарактеризуйте секретную и конфиденциальную информацию.
4. Что такое объекты угроз ИБ? В чем выражаются угрозы информации? Каковы основные источники угроз защищаемой информации? Каковы цели угроз информации со стороны злоумышленников?
5. Охарактеризуйте свойства информации. Что такое признаковая информация? Почему семантическая информация по отношению к признаковой является вторичной? Какие признаки объектов являются демаскирующими?
6. Назовите основные способы неправомерного овладения конфиденциальной информацией.
7. Какие основные понятия рассматриваются в Законе РФ "Об информации, информационных технологиях и о защите информации"?
8. Что такое «источник конфиденциальной информации»? Перечислите основные источники конфиденциальной информации.
9. Дайте определение и перечислите основные способы НСД к конфиденциальной информации. Охарактеризуйте обобщенную модель взаимодействия способов НСД источников конфиденциальной информации.
10. Дайте определение лицензирования. Кто такие лицензиат и лицензирующие органы? Почему лицензирование и сертификация выступают в качестве средства защиты информации? Перечислите перечень видов деятельности, касающихся ИБ, на осуществление которых требуются лицензии.
11. Что такое утечка конфиденциальной информации? Как осуществляется утечка конфиденциальной информации?

12. Что такое защита информации?
13. Определите понятие «несанкционированный доступ» к конфиденциальной информации, как он реализуется?
14. Какие недостатки информационного законодательства РФ, на ваш взгляд, необходимо устранять в первую очередь?
15. Назовите главную цель мер административного уровня ИБ. Что понимается под политикой безопасности? Приведите примерный список решений верхнего уровня политики безопасности.
16. Перечислите важнейшие задачи обеспечения информационной безопасности РФ.
17. Что такое угрозы утечки информации? Какие угрозы называются преднамеренными и случайными?
18. Что такое программа безопасности, ее уровни.
19. Классифицируйте угрозы ИБ РФ для личности, для общества, для Государства по общей направленности.
20. Что такое канал НСД? Назовите типовые причины их возникновения.
21. Что такое управление рисками? Почему управление рисками рассматривается на административном уровне ИБ? В чем заключается суть мероприятий по управлению рисками?
22. Охарактеризуйте государственную структуру органов, обеспечивающих информационную безопасность.
23. Назовите основные способы добывания конфиденциальной информации злоумышленником.
24. 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?
25. В чем специфика деятельности Межведомственной комиссии по защите государственной тайны?
26. Что такое канал утечки информации? Что такое технический канал утечки информации? Охарактеризуйте случайный и организованный канал утечки информации.
27. Перечислите направления повседневной деятельности системного администратора, обеспечивающие поддержание работоспособности ИС.
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. Почему уровень ИБ в России в настоящее время не соответствует жизненно важным потребностям личности, общества и государства и какие ключевые проблемы необходимо решить безотлагательно, чтобы обеспечить достаточный уровень ИБ в России?
31. Прокомментируйте наиболее распространенные угрозы доступности. Охарактеризуйте программные атаки на доступность.
32. Какие аспекты современных ИС с точки зрения безопасности наиболее существенны?
33. Раскройте содержание политических, экономических и организационно-технических факторов, влияющих на состояние информационной безопасности РФ.
34. Что такое вредоносное программное обеспечение? Дайте определение «бомбы», «червя», «вируса». Какие негативные последствия в функционировании ИС вызывает вредоносное ПО?
35. Что такое идентификация? Дайте толкование понятия «аутентификация». Из-за каких причин затруднена надежная идентификация?

36. Дайте определение защищаемой информации и охарактеризуйте ее основные признаки.
37. Охарактеризуйте основные угрозы целостности конфиденциальной информации.
38. Прокомментируйте парольную идентификацию. Какие меры позволяют повысить надежность парольной защиты?
39. Что такое государственная тайна? Перечислите сведения, которые могут быть отнесены к государственной тайне. Приведите классификацию сведений, составляющих государственную тайну, по степеням секретности
40. Перечислите основные угрозы конфиденциальности информации.
41. Прокомментируйте возможности биометрической идентификации (аутентификации).
42. Перечислите основные виды конфиденциальной информации, нуждающейся в защите.
43. Дайте определение способа защиты информации. Охарактеризуйте основные способы защиты. Перечислите основные защитные действия при реализации способов ЗИ.
44. В чем заключается основная задача логического управления доступом? Что такое матрица доступа? Какая информация анализируется при принятии решения о предоставлении доступа?
45. Каким требованиям должна отвечать коммерческая тайна? Охарактеризуйте о сновные субъекты права на коммерческую тайну. Какая информация не может быть отнесена к коммерческой тайне?
46. Что такое защита от разглашения?
47. Что такое протоколирование? Прокомментируйте особенности применения данного сервиса безопасности.
48. Перечислите и охарактеризуйте основные объекты профессиональной тайны. Каким требованиям должна удовлетворять информация, чтобы ее можно было бы отнести к профессиональной тайне?
49. Перечислите и прокомментируйте защитные действия от утечки конфиденциальной информации.
50. В чем заключается основная задача аудита, как сервиса безопасности?
51. Каким требованиям должна удовлетворять информация, чтобы ее можно было бы отнести к служебной тайне? Приведите перечень сведений, которые не могут быть отнесены к служебной информации ограниченного распространения.
52. Перечислите и охарактеризуйте защитные действия от НСД к конфиденциальной информации.
53. Охарактеризуйте экранирование в качестве основного сервиса безопасности ИС. Что такое firewall и как он функционирует?
54. Охарактеризуйте шифрование (криптографию) в качестве основного сервиса безопасности ИС.
55. Для каких целей служит сервис анализа защищенности? В чем заключается специфика управления, как сервиса безопасности?

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

Основная литература

а) основная:

1. 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.

2. 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.

3. 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.

б) Дополнительная литература

4. 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.

5. 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

7. Золотарев, В. В. Управление информационной безопасностью. Ч. 1. Анализ информационных рисков [Электронный ресурс] : учеб. пособие/ В. В. Золотарев, Е. А. Данилова. - Красноярск :Сиб. гос. аэрокосмич. ун-т, 2010. - 144 с. [Электронный ресурс] — Режим доступа: http://znanium.com/catalog/product/463037, свободный. — Загл. с экрана. — Яз. рус.

8. Жукова, М. Н. Управление информационной безопасностью. Ч. 2. Управление инцидентами информационной безопасности: учеб. пособие / М. Н. Жукова, В. Г. Жуков, В. В. Золотарев. - Красноярск : Сиб. гос. аэрокосмич. ун-т, 2012. - 100 с. [Электронный ресурс] — Режим доступа: http://znanium.com/catalog/product/463061, 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.

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 компетенции - ПК-13***

Практическое занятие:
Тема 1 (4 ч.) (Методология построения систем управления информационной безопасностью с учетом особенностей функционирования объекта информационной среды) - ***проверка сформированности компетенции*** ОПК-2.2; ПК-13

Задания:
Дискуссия по обсуждению вопросов лекции.
Указания по выполнению заданий:
В ходе обсуждения вопросов лекции обучаемые должны продемонстрировать степень усвоения материала соответствующей лекции, при необходимости задать вопросы и получить разъяснения преподавателя.
Список литературы:
[1, 5] (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.) (Нормативная база систем и процессов управления информационной безопасностью. Отраслевые стандарты в области управления ИБ) - ***проверка сформированности компетенции*** ОПК-2.2; ПК-13

Задания:
1. Опрос по теме занятия.
2. Выступления с докладами.
Указания по выполнению заданий:
1. Ответить на вопросы по теме занятия и ранее изученнному материалу.
2. Выступить с докладом с использованием презентации. Ответить на заданные вопросы.
Список литературы:
[1, 5] (см. Подраздел 6.1), [3] (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.

Практическое занятие:
Тема 3 (2 ч.) (Политика информационной безопасности) - ***проверка сформированности компетенции*** ОПК-2.2; ПК-13

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 изученнному материалу.
Список литературы:
[1, 4, 5] (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 (4 ч.) (Основные принципы построения систем управления информационной безопасностью) - ***проверка сформированности компетенции*** ОПК-2.2; ПК-13

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 изученнному материалу.
Список литературы:
[1, 4, 5] (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 (4 ч.) (Основы управления рисками ИБ) - ***проверка сформированности компетенции*** ОПК-2.2; ПК-13

Задания:
1. Дискуссия по обсуждению вопросов лекции.
2. Опрос по теме занятия.
3. 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. Ответить на вопросы по теме занятия и ранее изученнному материалу.
3. Выступить с докладом с использованием презентации. Ответить на заданные вопросы.
Список литературы:
[1, 2, 6, 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.

Практическое занятие:
Тема 6 (4 ч.) (Технические и организационные вопросы управления информационной безопасностью) - ***проверка сформированности компетенции*** ОПК-2.2; ПК-13

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 изученнному материалу.

Список литературы:

[1, 3, 5, 8] (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 «Системы управления информационной безопасностью» реализуется на *факультете информационных систем и безопасности Института информационных наук и технологий безопасности кафедрой информационной безопасности*.

Цели дисциплины: формирование у обучающихся теоретических знаний, необходимых умений и практических навыков в области управления информационной безопасностью, касающихся разработки и реализации управленческих решений по управлению деятельностью современной российской организации по обеспечению информационной безопасности.

Задачи:

- привитие обучаемым основ культуры обеспечения информационной безопасности;
- формирование у обучаемых понимания роли процессов управления в обеспечении информационной безопасности организаций, объектов и систем;
- ознакомление обучаемых с основными методами управления информационной безопасностью организаций, объектов и систем;
- обучение различным методам реализации процессов управления информационной безопасностью, направленных на эффективное управление ИБ конкретной организации.

Дисциплина (модуль) направлена на формирование следующих компетенций:

- ОПК-2.2- Способен формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы

В результате освоения дисциплины (модуля) обучающийся должен:

- Знает организационные меры по защите информации, основные методы управления защитой информации
- Умеет разрабатывать предложения по совершенствованию системы управления защиты информации, осуществлять планирование и организацию работы персонала с учетом требований по защите информации
- Владеет навыками выработки рекомендаций для решения о модернизации системы защиты информации

- ПК-13 - Способен принимать участие в формировании, организации и поддержания выполнения комплекса мер по обеспечению информационной безопасности, управлении процессом их реализации

В результате освоения дисциплины (модуля) обучающийся должен:

- Знает процедуру организации установки и настройки технических, программных (программно-технических) средств защиты информации, входящих в состав системы защиты информации организации, в соответствии с техническим проектом и инструкциями по эксплуатации
- Владеет навыками организации и сопровождения аттестации объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации
- Умеет разрабатывать и реализовывать организационные меры, обеспечивающие эффективность системы защиты информации

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

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