ФГБОУ ВО «БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ИНСТИТУТ ИСТОРИИ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

Утверждено:
на заседании кафедры
протокол№ 8 от « 24 » февраля 2021 г.
Зав. кафедрой _____ /Исмагилова А.С.

Согласовано:
Председатель УМК института
_____ / Гильмутдинова Р.А.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина
Управление информационной безопасностью

Обязательная часть (Б1.О.05)

программа магистратуры

Направление подготовки
10.04.01 Информационная безопасность

Направленность подготовки (программа магистратуры)
Информационная безопасность цифровых технологий

Квалификация
магистр

Разработчики: К.филос.н., доц. каф. Управления информационной безопасностью; ст. преподаватель каф. УИБ	_____ / Миронова Н.Г. _____ / Салов И.В.

Для приема: 2021 г.

Уфа 2021 г.

Составители: к.филос.н. Миронова Наталия Геннадьевна, Салов Игорь Владимирович

Рабочая программа дисциплины утверждена на заседании кафедры протокол от «_24_» _февраля_____ 2021 г. № _8_

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании
кафедры_____
_____
_____,
протокол № ____ от «____» _____ 20 _ г.

Заведующий кафедрой / Исмагилова А.С. /

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании
кафедры_____
_____
_____,
протокол № ____ от «____» _____ 20 _ г.

Заведующий кафедрой _____/ Исмагилова А.С. /

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры _____
_____
_____,
протокол № ____ от «____» _____ 20 _ г.

Заведующий кафедрой _____/ _____Ф.И.О./

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры _____
_____
_____,
протокол № ____ от «____» _____ 20 _ г.

Заведующий кафедрой _____/ _____Ф.И.О./

Список документов и материалов

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций

По итогам освоения дисциплины обучающийся должен достичь следующих результатов обучения:

Категория (группа) компетенций (при наличии ОПК)	**Формируемая компетенция (с указанием кода)**	**Код и наименование индикатора достижения компетенции**	**Результаты обучения по дисциплине**
Системное и критическое мышление	УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.	ИУК 1.1. Знает: методы критического анализа и оценки современных научных достижений; основные принципы критического анализа и синтеза информации; основы системного подхода при решении поставленных задач.	Знать методы критического анализа и оценки современных научных достижений; основные принципы критического анализа и синтеза информации; основы системного подхода при решении поставленных задач.
		ИУК 1.2. Умеет: получать новые знания на основе анализа и синтеза информации; собирать и обобщать данные по научным проблемам, относящимся к профессиональной области; осуществлять поиск информации и применять системный подход для решения поставленных задач; определять и оценивать практические последствия возможных решений задачи.	Уметь получать новые знания на основе анализа и синтеза информации; собирать и обобщать данные по научным проблемам, относящимся к профессиональной области; осуществлять поиск информации и применять системный подход для решения поставленных задач; определять и оценивать практические последствия возможных решений задачи.
		ИУК 1.3. Владеет: навыками исследования проблем профессиональной деятельности с применением анализа, синтеза и других методов интеллектуальной деятельности; выявления научных проблем и использования адекватных методов для их решения; формулирования оценочных суждений при	Владеть навыками исследования проблем профессиональной деятельности с применением анализа, синтеза и других методов интеллектуальной деятельности; выявления научных проблем и использования адекватных методов для их решения; формулирования

		решении профессиональных задач.	оценочных суждений при решении профессиональных задач.
Командная работа и лидерство	УК-3. Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели.	ИУК 3.1. Знает: способы подбора эффективной команды, основные условия эффективной командной работы; стратегии и принципы командной работы; основы психологии личности, среды, группы, коллектива.	Знать способы подбора эффективной команды, основные условия эффективной командной работы; стратегии и принципы командной работы; основы психологии личности, среды, группы, коллектива.
		ИУК 3.2. Умеет: вырабатывать командную стратегию; применять принципы и методы организации командной деятельности.	Уметь вырабатывать командную стратегию; применять принципы и методы организации командной деятельности.
		ИУК 3.3. Владеет: навыками социального взаимодействия и реализации своей роли в команде; создания команды для выполнения практических задач; участия в разработке стратегии командной работы.	Владеть навыками социального взаимодействия и реализации своей роли в команде; создания команды для выполнения практических задач; участия в разработке стратегии командной работы.
	ОПК-1. Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание.	ОПК-1.1 Знает основные требования к системе обеспечения информационной безопасности; требования стандартов, законов, регуляторов к уровню защищенности автоматизированных систем с учетом классов защищенности; требования стандартов к разработке и эксплуатации ИС/АС в защищенном исполнении; знает угрозы и уязвимости ИС/АС.	Знать основные требования к системе обеспечения информационной безопасности; требования стандартов, законов, регуляторов к уровню защищенности автоматизированных систем с учетом классов защищенности; требования стандартов к разработке и эксплуатации ИС/АС в защищенном исполнении; знает угрозы и уязвимости ИС/АС.
		ОПК-1.2 Умеет разрабатывать технический проект создания СОИБ (описание технических решений и мероприятий по подготовке СОИБ, спецификации на	Уметь разрабатывать технический проект создания СОИБ (описание технических решений и мероприятий по подготовке СОИБ, спецификации на комплекс технических и

		комплекс технических и программных средств СОИБ); способен обосновать требования к СОИБ.	программных средств СОИБ); способен обосновать требования к СОИБ
		ОПК-1.3 Владеет основными методами разработки проекта технического задания на создание системы обеспечения информационной безопасности; владеет навыками обследования информационного объекта, разработки технического задания на разработку СОИБ объекта.	Владеть основными методами разработки проекта технического задания на создание системы обеспечения информационной безопасности; владеет навыками обследования информационного объекта, разработки технического задания на разработку СОИБ объекта.

2. Цель и место дисциплины в структуре образовательной программы

Дисциплина «Управление информационной безопасностью» относится к обязательной части учебной программы.

Дисциплина изучается на 2 курсе магистратуры в 3 семестре.

Целью учебной дисциплины «Управление информационной безопасностью» является формирование навыков обоснования требований к системе обеспечения информационной безопасности, разработки проектов технического задания на ее создание, осуществления критического анализа проблемных ситуаций при обеспечении информационной безопасности и руководства командной работой.

3. Содержание рабочей программы (объем дисциплины, типы и виды учебных занятий, учебно-методическое обеспечение самостоятельной работы обучающихся)

Содержание рабочей программы представлено в Приложении № 1.

4. Фонд оценочных средств по дисциплине

4.1. Перечень компетенций и индикаторов достижения компетенций с указанием соотнесенных с ними запланированных результатов обучения по дисциплине. Описание критериев и шкал оценивания результатов обучения по дисциплине.

УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	Критерии оценивания результатов обучения	
		Не зачтено	Зачтено
ИУК 1.1. Знает: методы критического анализа и оценки современных научных достижений; основные принципы	Знать методы критического анализа и оценки современных научных достижений; основные принципы	Не знает или показывает очень слабые знания.	Знает методы критического анализа и оценки современных научных достижений;

критического анализа и синтеза информации; основы системного подхода при решении поставленных задач.	критического анализа и синтеза информации; основы системного подхода при решении поставленных задач.		основные принципы критического анализа и синтеза информации; основы системного подхода при решении поставленных задач.
ИУК 1.2. Умеет: получать новые знания на основе анализа и синтеза информации; собирать и обобщать данные по научным проблемам, относящимся к профессиональной области; осуществлять поиск информации и применять системный подход для решения поставленных задач; определять и оценивать практические последствия возможных решений задачи.	Уметь получать новые знания на основе анализа и синтеза информации; собирать и обобщать данные по научным проблемам, относящимся к профессиональной области; осуществлять поиск информации и применять системный подход для решения поставленных задач; определять и оценивать практические последствия возможных решений задачи.	Не умеет.	Умеет получать новые знания на основе анализа и синтеза информации; собирать и обобщать данные по научным проблемам, относящимся к профессиональной области; осуществлять поиск информации и применять системный подход для решения поставленных задач; определять и оценивать практические последствия возможных решений задачи.
ИУК 1.3. Владеет: навыками исследования проблем профессиональной деятельности с применением анализа, синтеза и других методов интеллектуальной деятельности; выявления научных проблем и использования адекватных методов для их решения; формулирования оценочных суждений при решении профессиональных задач.	Владеть навыками исследования проблем профессиональной деятельности с применением анализа, синтеза и других методов интеллектуальной деятельности; выявления научных проблем и использования адекватных методов для их решения; формулирования оценочных суждений при решении профессиональных задач.	Не владеет.	Владеет навыками исследования проблем профессиональной деятельности с применением анализа, синтеза и других методов интеллектуальной деятельности; выявления научных проблем и использования адекватных методов для их решения; формулирования оценочных суждений при решении профессиональных задач.

УК-3. Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели.

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	Критерии оценивания результатов обучения	
		Не зачтено	Зачтено

ИУК 3.1. Знает: способы подбора эффективной команды, основные условия эффективной командной работы; стратегии и принципы командной работы; основы психологии личности, среды, группы, коллектива.	Знать способы подбора эффективной команды, основные условия эффективной командной работы; стратегии и принципы командной работы; основы психологии личности, среды, группы, коллектива.	Не знает или показывает очень слабые знания.	Знает способы подбора эффективной команды, основные условия эффективной командной работы; стратегии и принципы командной работы; основы психологии личности, среды, группы, коллектива.
ИУК 3.2. Умеет: вырабатывать командную стратегию; применять принципы и методы организации командной деятельности.	Уметь вырабатывать командную стратегию; применять принципы и методы организации командной деятельности.	Не умеет.	Умеет вырабатывать командную стратегию; применять принципы и методы организации командной деятельности.
ИУК 3.3. Владеет: навыками социального взаимодействия и реализации своей роли в команде; создания команды для выполнения практических задач; участия в разработке стратегии командной работы.	Владеть навыками социального взаимодействия и реализации своей роли в команде; создания команды для выполнения практических задач; участия в разработке стратегии командной работы.	Не владеет.	Владеет навыками социального взаимодействия и реализации своей роли в команде; создания команды для выполнения практических задач; участия в разработке стратегии командной работы.

ОПК-1. Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание.

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	Критерии оценивания результатов обучения	
		Не зачтено	Зачтено
ОПК-1.1 Знает основные требования к системе обеспечения информационной безопасности; требования стандартов, законов, регуляторов к уровню защищенности автоматизированных систем с учетом классов защищенности; требования стандартов	Знать основные требования к системе обеспечения информационной безопасности; требования стандартов, законов, регуляторов к уровню защищенности автоматизированных систем с учетом классов защищенности; требования стандартов к разработке и эксплуатации ИС/АС в	Не знает или показывает очень слабые знания.	Знает основные требования к системе обеспечения информационной безопасности; требования стандартов, законов, регуляторов к уровню защищенности автоматизированных систем с учетом классов защищенности;

к разработке и эксплуатации ИС/АС в защищенном исполнении; знает угрозы и уязвимости ИС/АС.	защищенном исполнении; знает угрозы и уязвимости ИС/АС.		требования стандартов к разработке и эксплуатации ИС/АС в защищенном исполнении; знает угрозы и уязвимости ИС/АС.
ОПК-1.2 Умеет разрабатывать технический проект создания СОИБ (описание технических решений и мероприятий по подготовке СОИБ, спецификации на комплекс технических и программных средств СОИБ); способен обосновать требования к СОИБ.	Уметь разрабатывать технический проект создания СОИБ (описание технических решений и мероприятий по подготовке СОИБ, спецификации на комплекс технических и программных средств СОИБ); способен обосновать требования к СОИБ	Не умеет.	Умеет разрабатывать технический проект создания СОИБ (описание технических решений и мероприятий по подготовке СОИБ, спецификации на комплекс технических и программных средств СОИБ); способен обосновать требования к СОИБ.
ОПК-1.3 Владеет основными методами разработки проекта технического задания на создание системы обеспечения информационной безопасности; владеет навыками обследования информационного объекта, разработки технического задания на разработку СОИБ объекта.	Владеть основными методами разработки проекта технического задания на создание системы обеспечения информационной безопасности; владеет навыками обследования информационного объекта, разработки технического задания на разработку СОИБ объекта.	Не владеет.	Владеет основными методами разработки проекта технического задания на создание системы обеспечения информационной безопасности; владеет навыками обследования информационного объекта, разработки технического задания на разработку СОИБ объекта.

4.2. Типовые контрольные задания или иные материалы, необходимые для оценивания результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине

УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Оценочные средства
ИУК 1.1. Знает: методы критического анализа и оценки современных научных достижений;	Знать методы критического анализа и оценки современных научных достижений; основные	тестирование, практическое задание

основные принципы критического анализа и синтеза информации; основы системного подхода при решении поставленных задач.	принципы критического анализа и синтеза информации; основы системного подхода при решении поставленных задач.	
ИУК 1.2. Умеет: получать новые знания на основе анализа и синтеза информации; собирать и обобщать данные по научным проблемам, относящимся к профессиональной области; осуществлять поиск информации и применять системный подход для решения поставленных задач; определять и оценивать практические последствия возможных решений задачи.	Уметь получать новые знания на основе анализа и синтеза информации; собирать и обобщать данные по научным проблемам, относящимся к профессиональной области; осуществлять поиск информации и применять системный подход для решения поставленных задач; определять и оценивать практические последствия возможных решений задачи.	тестирование, практическое задание
ИУК 1.3. Владеет: навыками исследования проблем профессиональной деятельности с применением анализа, синтеза и других методов интеллектуальной деятельности; выявления научных проблем и использования адекватных методов для их решения; формулирования оценочных суждений при решении профессиональных задач.	Владеть навыками исследования проблем профессиональной деятельности с применением анализа, синтеза и других методов интеллектуальной деятельности; выявления научных проблем и использования адекватных методов для их решения; формулирования оценочных суждений при решении профессиональных задач.	тестирование, практическое задание

УК-3. Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели.

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	**Оценочные средства**
ИУК 3.1. Знает: способы подбора эффективной команды, основные условия эффективной командной работы; стратегии и принципы командной работы; основы психологии личности, среды, группы, коллектива.	Знать способы подбора эффективной команды, основные условия эффективной командной работы; стратегии и принципы командной работы; основы психологии личности, среды, группы, коллектива.	тестирование, практическое задание
ИУК 3.2. Умеет: вырабатывать командную стратегию; применять принципы и методы	Уметь вырабатывать командную стратегию; применять принципы и методы организации командной деятельности.	тестирование, практическое задание

организации командной деятельности.		
ИУК 3.3. Владеет: навыками социального взаимодействия и реализации своей роли в команде; создания команды для выполнения практических задач; участия в разработке стратегии командной работы.	Владеть навыками социального взаимодействия и реализации своей роли в команде; создания команды для выполнения практических задач; участия в разработке стратегии командной работы.	тестирование, практическое задание

ОПК-1. Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание.

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	**Оценочные средства**
ОПК-1.1 Знает основные требования к системе обеспечения информационной безопасности; требования стандартов, законов, регуляторов к уровню защищенности автоматизированных систем с учетом классов защищенности; требования стандартов к разработке и эксплуатации ИС/АС в защищенном исполнении; знает угрозы и уязвимости ИС/АС.	Знать основные требования к системе обеспечения информационной безопасности; требования стандартов, законов, регуляторов к уровню защищенности автоматизированных систем с учетом классов защищенности; требования стандартов к разработке и эксплуатации ИС/АС в защищенном исполнении; знает угрозы и уязвимости ИС/АС.	тестирование, практическое задание
ОПК-1.2 Умеет разрабатывать технический проект создания СОИБ (описание технических решений и мероприятий по подготовке СОИБ, спецификации на комплекс технических и программных средств СОИБ); способен обосновать требования к СОИБ.	Уметь разрабатывать технический проект создания СОИБ (описание технических решений и мероприятий по подготовке СОИБ, спецификации на комплекс технических и программных средств СОИБ); способен обосновать требования к СОИБ	тестирование, практическое задание
ОПК-1.3 Владеет основными методами разработки проекта технического задания на создание системы обеспечения информационной безопасности; владеет навыками обследования информационного объекта, разработки технического задания на разработку СОИБ объекта.	Владеть основными методами разработки проекта технического задания на создание системы обеспечения информационной безопасности; владеет навыками обследования информационного объекта, разработки технического задания на разработку СОИБ объекта.	тестирование, практическое задание

Критериями оценивания при модульно-рейтинговой системе являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения разделов № 1-2 дисциплины, перечисленных в рейтинг-плане дисциплины.

Для зачета текущий контроль – максимум 50 баллов; рубежный контроль – максимум 50 баллов, поощрительные баллы – максимум 10).

Шкалы оценивания для зачета:

зачтено – от 60 до 110 рейтинговых баллов (включая 10 поощрительных баллов),

не зачтено – от 0 до 59 рейтинговых баллов).

Рейтинг – план дисциплины
«Управление информационной безопасностью»

Специальность: 10.04.01 Информационная безопасность

курс 2, семестр 3

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1. Создание СУИБ на предприятии.				
Текущий контроль				
Практическая работа	8	3	14	24
Рубежный контроль				
Тест 1	14	1	6	14
Модуль 2. Особенности реализация СМИБ.				
Текущий контроль				
Практическая работа	8	6	30	48
Рубежный контроль				
Тест 2 (или зачетное собеседование)	14	1	10	14
Поощрительные баллы				
1. Участие в студенческой олимпиаде по дисциплине	3	1	0	3
2.Публикация научной статьи	4	1	0	4
3.Участие в научно-практической конференции по профилю	3	1	0	3
Всего		3	0	10
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
1. Посещение лекционных занятий			0	-6
2. Посещение практических (семинарских, лабораторных занятий)			0	-10
Итоговый контроль				
1. Зачет	60	1	60	100

Зачетное собеседование

Вопросы для собеседования:

1. Понятия «информационная безопасность (ИБ)», риск ИБ, угрозы ИБ.

2. Основные классы рисков и угроз ИБ.
3. Основные наиболее распространенные способы нарушения информационной безопасности.
4. Структура деятельности в сфере информационной безопасности. Основные задачи организационно-управленческой деятельности в сфере ИБ.
5. Иерархия и взаимосвязь уровней организационной работы в сфере информационной безопасности.
6. Задачи, роли и методы, используемые на различных уровнях организационной работы в сфере информационной безопасности.
7. Деятельность международных организаций в сфере информационной безопасности. Работа международных профессиональных объединений.
8. Деятельность международных организаций (в т.ч. и специализированных международных объединений (альянсов)) в сфере информационной безопасности.
9. Деятельность международных организаций в сфере информационной безопасности. Международная организация по стандартизации.
1. Управление информационной безопасностью на государственном уровне. Предпосылки развития.
2. Общая методология и структура организационного обеспечения информационной безопасности на уровне государств.
3. Управление информационной безопасностью на уровне предприятия: основные направления.
4. Общая структура управленческой работы по обеспечению информационной безопасности на уровне предприятия.
5. Структура политики информационной безопасности и процесс ее разработки.
6. Назначение и сфера применения стандартов ISO/IEC 27XXX.
7. История возникновения и развития в мире и России стандартов ISO/IEC 27XXX.
8. Структура стандарта ISO/IEC 27001. Основные принципы СУИБ.
9. Реализация модели PDCA в стандарте ISO/IEC 2700. Определение СУИБ.
10. Ориентировочная последовательность действий при разработке СУИБ. Краткая характеристика этапов.
11. Управление рисками. Методика управления рисками GASSP. Модель качественной оценки рисков.
12. Управление рисками. Количественная модель оценки рисков.
13. Управление рисками. Краткая структура отчета об оценке рисков.
14. Характеристика этапа внедрения и функционирования СУИБ. Требования.
15. Мониторинг СУИБ и анализ СУИБ со стороны руководства. Требования.
16. Характеристика этапа поддержания и улучшения СУИБ. Требования.
17. Требования стандарта ISO/IEC 27001 к составу и управлению документацией.
18. Краткая характеристика раздела стандарта ISO/IEC 27001 «Ответственность руководства». Требования.
19. Краткая характеристика раздела стандарта ISO/IEC 27001 «Совершенствование СУИБ». Требования.
20. Основные международные стандарты в сфере управления рисками информационной безопасности. Краткая характеристика.
21. Система управления информационными рисками. Процессная модель управления рисками. Краткая характеристика этапов.
22. Процесс управления рисками информационной безопасности в соответствии с ISO 27005. Краткая характеристика.
23. Процесс управления рисками информационной безопасности в соответствии с ISO 27005 (идентификация угроз, уязвимостей, последствий).
24. Оценка рисков информационной безопасности. Основные методики (из ISO 27005). Оценка вероятности. Оценка последствий. Обработка рисков информационной безопасности.

25. Коммуникации риска информационной безопасности в соответствии с ISO 27005.
26. Мониторинг и пересмотр риска информационной безопасности в соответствии с ISO 27005.

Зачетное собеседование проводится в том случае, если студент не смог набрать 60 баллов по результатам выполнения практических заданий (до 14 баллов).

Критериями оценивания являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения модулей (разделов дисциплины), перечисленных в рейтинг-плане дисциплины (для зачета: текущий контроль – максимум 50 баллов; рубежный контроль – максимум 50 баллов, поощрительные баллы – максимум 10).

Шкалы оценивания:

- зачтено – от 60 до 110 рейтинговых баллов (включая 10 поощрительных баллов),
- не зачтено – от 0 до 59 рейтинговых баллов).

Практические занятия

Раздел (модуль) 1. Теоретические аспекты управления информационной безопасности

Практические занятия 1-2. Нормативно-законодательная регламентация управления информационной безопасностью (государственный, объектовый уровень) (4 часа)

Содержание (темы для исследования и обсуждения):

1. Законодательные новации в сфере информационной безопасности (анализ состояния и и последних изменений в руководящих и методических документах регуляторов и законодателей по вопросам управления ИБ).
2. Деятельность международных организаций в сфере информационной безопасности. Работа международных профессиональных объединений.
3. Деятельность международных организаций в сфере информационной безопасности. Международный союз электросвязи.
4. Деятельность международных организаций в сфере информационной безопасности. Институт инженеров по электронике и электротехнике.
5. Деятельность международных организаций в сфере информационной безопасности. Ассоциация вычислительной техники (ACM). World Wide Web Consortium.
6. Деятельность международных организаций в сфере информационной безопасности. Международная организация по стандартизации.
7. Деятельность специализированных международных организаций в сфере информационной безопасности.
8. Деятельность специализированных международных объединений (альянсов) в сфере информационной безопасности.
9. Управление информационной безопасностью на уровне крупных поставщиков информационных систем. Внутренняя организационная работа.
10. Управление информационной безопасностью на государственном уровне: методология, структура организационного обеспечения информационной безопасности на уровне государств.
11. Управление информационной безопасностью объектового уровня (субъекты, основные направления защиты, полномочия и обязательства, и т.п.).

Практические занятия 3-4. Цели, задачи, компетенции управления информационной безопасностью (4 часа)

Содержание (темы для исследования и обсуждения):

1. Структура деятельности в сфере информационной безопасности. Основные задачи организационно-управленческой деятельности в сфере ИБ и содержание деятельности по решению этих задач, в т.ч.:
   - создание мер по обработке киберрисков;
   - сбор, аналитика информации о текущем состоянии кибербезопасности;
   - выявление необходимого уровня обеспечения кибербезопасности,
   - формирование задач для профильных специалистов;
   - оценивание информационных рисков;
   - интеграция и формирование необходимых механизмов по контролю, распределению ролей и ответственности;
   - обучение, повышение цифровой грамотности сотрудников компании в сфере информационной безопасности;
   - отслеживание механизмов контроля, оценка их эффективности, внедрение необходимых изменений в их работу, если требуется.
2. Иерархия и взаимосвязь уровней организационной работы в сфере информационной безопасности.
3. Задачи, роли и методы, используемые на различных уровнях организационной работы в сфере информационной безопасности.
4. Способы нарушения информационной безопасности.
5. Общая структура управленческой работы по обеспечению информационной безопасности на уровне предприятия.
6. Формализация задач автоматизированной информационно-аналитической поддержки процессов принятия решений в сфере безопасности.

Дополнительные вопросы:

7. Актуальные проблемы управления информационной безопасностью гос.учреждений
8. Актуальные проблемы управления информационной безопасностью финансовых и экономически структур.
9. Актуальные проблемы управления информационной безопасностью предприятий.

Практические занятия 5-6. Стандартизация управления информационной безопасностью. Модели и методы УИБ (4 часа)

Содержание (темы для исследования и обсуждения):

1. Анализ и особенности применения отечественных и зарубежных стандартов в области защиты информации для проектирования, разработки и оценки защищенности компьютерных систем.
2. Модель кибербезопасности в РФ в новых условиях: проблемы, пути их решения, содержание трансформации модели управления ИБ.
3. Методы и подходы к управлению ИБ, их сравнительный анализ и оценка.
4. Процессный подход к разработке, реализации, эксплуатации и анализу системы управления.
5. Особенности реализации непрерывной модели управления информационной безопасностью.
6. Назначение и сфера применения стандартов ISO/IEC 27XXX.Структура стандарта ISO/IEC 27001.
7. Основные принципы СУИБ. Основные этапы МИБ:
   - Формулировке плана обработки рисков.
   - Реализации плана обработки рисков.
   - Формировании и применении средств управления.
   - Оценке эффективности принятых средств управления.
   - Подготовке и осуществлении плана повышения осведомленности персонала.

- Управлении деятельностью системы менеджмента информационной безопасности.
- Управлении ресурсами системы менеджмента информационной безопасности.
- Внедрении в действие систем обнаружения инцидентов информационной безопасности.

8. Характеристика раздела стандарта ISO/IEC 27001 «Ответственность руководства». Требования.
9. Реализация модели PDCA в стандарте ISO/IEC 2700x.
10. Основные международные стандарты в сфере управления рисками информационной безопасности. Краткая характеристика.
11. Новые практические решения в области моделей и методов управления информационной безопасностью как инструментарий при разработке систем защиты информации.

Практическая часть:

Анализ содержания стандартов по управлению ИБ (в т.ч. 27000, 29001, 27002, 26003, 27004, 27005, 27007, 270011, 27006 и т.д.)

Раздел (модуль) 2. Особенности практической реализация УИБ. СУИБ

Практические занятия 7, 8. Система управления информационной безопасности (СУИБ) – управленческие аспекты (4 часа)

Содержание (темы для исследования и обсуждения):

1. Управление ИБ: задача, ответственность отдела ИБ, полномочия, управленческий ресурс отдела ИБ.
2. Определение СУИБ. Место СУИБ в рамках общей системы управления объектом
3. Этапы создания и внедрения СУИБ (планирование, реализация, контроль, совершенствование); комплекс решаемых управленческих задач и работ; документальное обеспечение СУИБ.
4. Требования к процессам СУИБ, работа с процессами СУИБ (документирование, описание процесса СУИБ; построение и внедрение процессов СУИБ; мониторинг и измерение параметров процесса СУИБ).
5. Требования стандарта ISO/IEC 27001 к составу и управлению документацией.
6. Подготовка проектов нормативно-распорядительных документов (приказов, указаний, инструкций) по вопросам ИБ
7. Определение перечня нормативно–правовых актов, требования которых учитываются при обеспечении ИБ ОИ.
8. Мониторинг СУИБ и анализ СУИБ со стороны руководства.
9. Функции руководителя и специалистов отдела/службы ИБ.
10. Характеристика раздела стандарта ISO/IEC 27001 «Совершенствование СУИБ». Требования. Характеристика этапа поддержания и улучшения СУИБ. Требования.

1. Практическая работа 9-10. Внедрение/модернизация СУИБ объекта информатизации. Управление инцидентами ИБ (4 часа)

Цель: Практическое ознакомление с положением о порядке выявления и реагирования на инциденты информационной безопасности.

Содержание:

Задание. Разработать типовое положение о порядке выявления и реагирования на инциденты информационной безопасности.

Методические указания по порядку выполнения задания:

1. Ознакомиться с ГОСТ Р ИСО/МЭК ТО 18044-2007 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности, ISO/IEC 27035:2011 - управление инцидентами ИБ и ISO/IEC 27037 - Руководство по идентификации, сбору и/или получению и обеспечению сохранности свидетельств, представленных в электронной форме.
2. Ознакомиться типовым Положением о реагирования на инциденты информационной безопасности.
3. Назовите основные разделы Положения о реагирования на инциденты информационной безопасности.
4. Ответить на контрольные вопросы:
    a) Назовите этапы менеджмента инцидентов ИБ.
    b) Какие мероприятия включает в себя этап «Планирование и подготовка»?
    c) Какие процессы необходимо осуществить при использовании системы менеджмента инцидентов ИБ?
    d) Какие действия по анализу состояния ИБ необходимо предпринять после разрешения/закрытия инцидентов ИБ?
    e) В чем заключаются преимущества структурного подхода менеджмента инцидентов информационной безопасности?
5. Отчет о результатах выполнения в письменной или устной форме.

Практические занятия 11-12. Управление политикой информационной безопасности (2 часов)

Содержание (темы для исследования и обсуждения):

1. Политика ИБ. Структура политики информационной безопасности и процесс ее разработки.
2. Идентификация активов, моделирование угроз (общие положения методики ФСТЭК 2021 года и проч.), оценка уровня защищенности (идентификация уязвимостей).
3. Категорирование защищаемой информации. Определение границ защищаемого объекта. Периметр объекта информатизации. Инвентаризация информационных и проч. активов.
4. Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации (обзорно).
5. Организационные аспекты УИБ.: Методы управления доступом, правила разграничения доступа.
6. Программные и технические средства ИБ.
7. Контроль и мониторинг (в т.ч. инструментальные средства). Мониторинг и ситуационный анализ обстановки в сфере безопасности.
8. Организация аудита ИБ.

Практические занятия 13-14. Практические аспекты управления информационной безопасностью (2 часа)

Содержание:

1. Установление режима обработки информации.
2. Методики определения угроз безопасности информации в информационных системах.
3. Средства и методы мониторинга событий безопасности; журналы регистрации событий операционной системы и проч.
4. Виды инструментальных проверок.
5. Средства анализа уровня защищенности информационной системы.
6. Системы управления событиями информационной безопасности (SIEM).

Практические занятия 15-16. Управление рисками и инцидентами информационной безопасности. (4 часов)

Содержание:

1. Управление информационными рисками. Методика управления рисками GASSP.
2. Система управления информационными рисками.
3. Процессная модель управления рисками. Процесс управления рисками информационной безопасности в соответствии с ISO 27005. Краткая их характеристика, в т.ч.:
   - этап «Установление контекста». Основные критерии.
   - этап «Установление контекста». Область применения и границы и т.д.
1. Модель качественной оценки рисков. Количественная модель оценки рисков.
2. Оценка рисков информационной безопасности. - Основные методики.
3. Анализ рисков информационной безопасности в соответствии с ISO 27005. Этап идентификации рисков.
4. Коммуникации риска информационной безопасности в соответствии с ISO 27005.
5. Мониторинг и пересмотр риска информационной безопасности в соответствии с ISO 27005.
6. Расчет и оценка эффективности управления риском. Особые аспекты управления риском.

Практические занятия 17-18. Место планирования, прогнозирования в УИБ (4 часа)

1. Современные модели и методы измерения, прогнозирования, планирования, принятия решений при решении задач поддержки процессов принятия решений;
2. Место планирования в управлении ИБ. Цели, методы, инструменты планирования при реализации задач управления информационной безопасностью
3. Место прогнозирования в управлении ИБ.
4. Методы прогнозирования, принятия решений по УИБ в условиях неопределенности; оценка эффективности и качества в задачах прогнозирования, планирования, принятия этих решений.
5. Прогнозирование на основе вероятностного и статистического анализа.
6. Реализация обратной связи в управлении информационной безопасностью.

Практическая часть. Выполнение расчетов по оценке риска ИБ.

Тестирование

По результатам изучения 2 модуле курса предполагается проверка знаний с помощью тестов (№1 и №2). При изучении дисциплины используются тестовые задания закрытого типа. Каждое тестовое задание включает вопрос и варианты ответов к нему. Тестирование выполняется в письменной форме. Необходимо выбрать один ответ из предложенных вариантов (если не оговорено иное).

Тест № 1. Модуль 1. Создание СУИБ на предприятии

Примерные тестовые задания

1. Метрикой какого процесса может стать количество достигнутых целевых показателей услуг?

a) управление Портфелем услуг
b) управление уровнем услуг
c) управление изменениями
d) управление Каталогом услуг

2. Целью какого процесса является определение и контроль компонентов услуг и конфигурационных единиц, а также предоставление достоверной информации о состоянии услуг и инфраструктур?

a) планирование и поддержка внедрения
b) управление изменениями
c) управление активами и конфигурациями
d) управление релизами и развертыванием

3. Какой метод может использовать организация для сравнения своей деятельности с деятельностью конкурента?

a) VOI
b) подход «большой взрыв»
c) сравнение состояний
d) ROI

… и т.д. – см. в ФОС дисциплины.

Тест №2. Модуль 2. Особенности реализация СМИБ

1. Как называется сегмент бизнеса, который имеет свои собственные метрики, планы, доходы и расходы?

a) процесс
b) бизнес-единица
c) функция

2. Как называется среда, которая используется для проверки функциональности, производительности, восстанавливаемости и полезности отдельных компонентов услуги?

a) единичная среда тестирования
b) среда внедрения
c) среда сборки
d) среда интеграции

3. Поставщики какого типа больше других сталкиваются со сложностями свободного рынка?

a) второго типа
b) третьего типа
c) первого типа

… и т.д. – см. в ФОС дисциплины.

Критерии оценки тестирования: каждый тест из 25 тестовых заданий оценивается, суммарно и максимально, в 14 баллов (за 0,56 балла за 1 правильно выполненное тестовое задание).

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература

1. Чекулаева, Е. Н. Управление информационной безопасностью : учебное пособие : [16+] / Е. Н. Чекулаева, Е. С. Кубашева ; Поволжский государственный технологический университет. – Йошкар-Ола : Поволжский государственный технологический университет, 2020. – 156 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=612591. – Библиогр.: с. 127-129. – ISBN 978-5-8158-2165-1. – Текст : электронный.

2. Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Основы управления информационной безопасностью. Учебное пособие для вузов. 2-е изд., испр. Серия «Вопросы управления информационной безопасностью. Выпуск 1» - 2022. - 244 стр.

3. Шилов, А. К. Управление информационной безопасностью : учебное пособие : [16+] / А. К. Шилов ; Южный федеральный университет, Институт компьютерных технологий и информационной безопасности. – Ростов-на-Дону; Таганрог: Южный федеральный университет, 2018. – 121 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=500065. – Библиогр.: с. 81-82. – ISBN 978-5-9275-2742-7. – Текст : электронный.

Дополнительная литература

4. Дронова, Г. А. Управление информационной безопасностью: учебно-методическое пособие : [16+] / Г. А. Дронова. – Новосибирск: Новосибирский государственный технический университет, 2016. – 28 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=575356. – Библиогр. в кн. – ISBN 978-5-7782-3113-9. – Текст : электронный.

5. Милославская, Н. Г. Управление рисками информационной безопасности: учебное пособие для вузов / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. – Москва : Горячая линия – Телеком, 2013. – 130 с. : ил. – (Вопросы управления информационной безопасностью. Вып. 2). – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=253576. – Библиогр. в кн. – ISBN 978-5-9912-0272-5. – Текст : электронный.

6. Абденов, А. Современные системы управления информационной безопасностью : учебное пособие : [16+] / А. Абденов, Г. Дронова, В. Трушин ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2017. – 48 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=574594. – Библиогр.: с.43-44. – ISBN 978-5-7782-3236-5. – Текст : электронный.

5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины, включая профессиональные базы данных и информационные справочные системы

1. Антиплагиат.ВУЗ. Договор № 81 от 27.04.2018 г. Срок действия лицензии до 04.05.2019 г., договор № 1104 от 18.04.2019 г. Срок действия лицензии до 04.05.2020 г
2. Банк нормативно-правовых актов РФ Министерства юстиции РФ - http://zakon.scli.ru/ru/legal_texts/index.php
3. Национальные стандарты РФ в области информационной безопасности: http://www.iso27000.ru/standarty/gost-r-nacionalnye-standarty-rossiiskoi-federacii-v-oblasti-zaschity-informacii
4. Нормативные документы и материалы сайта ФСТЭК России (Федеральной службы по техническому и экспортному контролю России): https://fstec.ru/ Раздел «Национальные старты информационной безопасности» (https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/113-gosudarstvennye-standarty/377-gosudarstvennye-standarty)
5. Справочная правовая система Консультант Плюс. Договор №31705775411 от 07.12.2017 г. http://www.consultant-plus.ru
6. Электронная библиотечная система «Университетская библиотека онлайн» - https://biblioclub.ru
7. Электронная библиотечная система «ЭБ БашГУ» - https://elib.bashedu.ru
8. Электронная библиотечная система БашГУ – www.bashlib.ru
9. Электронная библиотечная система издательства «Лань» - https://e.lanbook.com

Государственные информационно-правовые системы:

1. Научный центр правовой информации при министерстве Юстиций РФ - http://www.scli.ru
2. Официальный интернет-портал правовой информации - http://pravo.gov.ru
3. Информационно-правовая система «Законодательство России» - http://pravo.fso.gov.ru
4. Модуль «Документы - Президент России» - http://www.kremlin.ru/acts
5. Банк документов, подписанных Президентом России - http://kremlin.ru/acts/bank
6. База данных «Федеральные законы» - http://graph.garant.ru:8080/SESSION/PILOT/main.htm
7. Автоматизированная система обеспечения законодательной деятельности государственной думы (законопроекты и законодательные инициативы) - http://asozd.duma.gov.ru/
8. База данных «Издания по общественным и гуманитарным наукам» (на платформе East View) - Ссылка http://www.ebiblioteka.ru (вход из сети вуза без регистрации).
9. Банк данных "Библиотека копий официальных публикаций правовых актов» при ассоциации юристов России - http://alrf.consultant.ru/
10. Банк данных "Копии правовых актов: Российская Федерация» - http://giod.consultant.ru/
11. Банк данных "Нормативно-правовые акты Федерального Собрания Российской Федерации - http://duma.consultant.ru/

Другие профессиональные базы данных и информационно-справочные системы:

1. Электронная база данных диссертаций РГБ (авторизованный доступ по паролю в сети вуза) – Ссылка: http://dvs.rsl.ru
2. База данных «Вестники Московского университета» (на платформе East View) (вход без регистрации). - Ссылка http://www.ebiblioteka.ru/browse/udb/12.
3. Annual Reviews – обзор журналов по общественно-научной тематике и др. – доступ из сети вуза. – Ссылка: http://www.annualreviews.org/
4. Computers & Applied Sciences Complete (EBSCO) - доступ в сети вуза, язык английский. - Ссылка: http://search.ebscohost.com/
5. SCOPUS - наукометрическая, библиографическая и реферативная база данных

издательской корпорации Elsevier. Язык английский, вход после регистрации или из сети вуза. – Ссылка: http://www.scopus.com/

6. Taylor and Francis – База полнотекстовых научных журналов, книг. Язык английский. – доступ из сети вуза. – Ссылка: http://www.tandf
7. Web of Science - наукометрическая, библиографическая и реферативная база данных издательской корпорации Thomson Reuters. Язык английский, вход после регистрации или из сети вуза. – Ссылка: http://apps.webofknowledge.com/
8. Wiley - Полнотекстовая база данных статей из 1400 журналов издательства Wiley по всем отраслям знаний. Язык английский. Доступ из сети вуза без регистрации. – Ссылка: http://onlinelibrary.wiley.com/
9. Сайт по информационной безопасности: http://securitypolicy.ru/; его раздел: «Документы, стандарты и методики по информационной безопасности»: http://securitypolicy.ru/
10. Докипедия: http://dokipedia.ru
11. Словари и энциклопедии On-Line- http://www.dic.academic.ru

Программное обеспечение

1. Windows 8 Russian Russian OLP NL AcademicEdition и Windows Professional 8 Russian Upgrade OLP NL Academic Edition. Договор №104 от 17.06.2013 г. Лицензии бессрочные.
2. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные.
3. Система централизованного тестирования БашГУ (Moodle).GNU General Public License.

6. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Наименование специализированных аудиторий, кабинетов, лабораторий	Вид занятий	Наименование оборудования, программного обеспечения
1	2	3
1. Учебная аудитория для проведения занятийлекционного типа: Аудитория № 515. Адрес: 450076, Республика Башкортостан, Городской Округ Город Уфа, город Уфа, улица Карла Маркса, дом 3/4, помещение 2	Лекции, практические занятия, текущий контроль, промежуточная аттестация, экзамен	Аудитория № 515. Оборудование: учебная мебель, доска, терминал видео конференц-связи LifeSizeIcon 600-камера, интерактивная система со встроенным короткофокусным проектором PrometheanActivBoard 387 RPOMOUNTEST, профессиональный LCD дисплей Flame 42ST, настольный интерактивный дисплей SMARTPodiumSP518 с ПО SMARTNotebook, матричный коммутатор сигналов интерфейса HDMICMPRO 4H4H, интерактивная напольная кафедра докладчика, ком-ер встраиваемый в кафедру INTELCorei3-4150/DDr3 4 Gb/HDD 1TB/DVD-RW/ThermaltakeVL520B1N2E 220W/Win8Pro64, стол, трибуна, кресла секционные последующих рядов с пюпитром.
2. Учебная аудитория для проведения занятий семинарского типа: Аудитория № 404. Специализированный кабинет с лабораторным оборудованием. Аудитория № 507. Лаборатория управления информационной безопасностью. Адрес: 450076, Республика Башкортостан, Городской Округ Город Уфа, город Уфа, улица Карла Маркса, дом 3/4, помещение 2		Аудитория № 404. Специализированный кабинет с лабораторным оборудованием. Оборудование: учебная мебель, системные блоки\i5-10400 (2.9GHz)\H510M\8Gb\HDD 1Tb\корпус Micro ATX\Win10 Pro, мониторы ЖК 23.8" LG 24MK430H-B (1920x1080, IPS,75 Гц, 5 мс, 1000:1, 250 кд/м2, D-Sub, HDMI, кабель HDMI в комплекте), виртуальный тренажер «Аттестация объекта по требованиям защиты от утечек информации по техническим каналам». Аудитория № 507. Лаборатория управления информационной безопасностью. Оборудование: учебная мебель, доска, мультимедиа, комплекс мониторинга WiFi сетей "Зодиак II", универсальный комплект инструментов для проведения работ по специальным проверкам и специальным обследованиям Калейдоскоп-П2, многофункциональный поисковый прибор ST-031M "Пиранья", нелинейный локатор «Лорнет», анализатор электромагнитного поля "Кордон"
3. Учебная аудитория для проведения групповых и индивидуальных консультаций: Аудитория № 608 Адрес: 450076, Республика Башкортостан, Городской Округ Город Уфа, город Уфа, улица Карла Маркса, дом 3/4, помещение 2		Аудитория № 608 Оборудование: учебная мебель, доска, мобильное мультимедийное оборудование, телевизор TCL-L55P6US. Аудитория № 420. Компьютерный кабинет Оборудование: учебная мебель, моноблоки Lenovo Thinkcentre A70Z.
4. Учебная аудитория для текущего контроля и промежуточной аттестации: Аудитория № 420. Компьютерный кабинет		Аудитория № 420. Компьютерный кабинет Оборудование: учебная мебель, моноблоки Lenovo Thinkcentre A70Z.

Адрес: 450076, Республика Башкортостан, Городской Округ Город Уфа, город Уфа, улица Карла Маркса, дом 3/4, помещение 2		

Приложение № 1

ФГБОУ ВО «БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ИНСТИТУТ ИСТОРИИ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ

дисциплины **Управление информационной безопасностью** на 3 семестр
___очная_ф/о___

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (ЗЕТ / часов)	2 ЗЕТ / 72 часа
Учебных часов на контактную работу с преподавателем:	60,2
лекций	24
практических/ семинарских	36
лабораторных	–
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	0,2
из них, предусмотренные на выполнение курсовой работы / курсового проекта	–
Учебных часов на самостоятельную работу обучающихся (СР)	11,8
из них, предусмотренные на выполнение курсовой работы / курсового проекта	–
Учебных часов на подготовку к зачету (Контроль)	–

Форма контроля
Зачет 3 семестр

Семестр 3

№	Тема и содержание	Форма изучения материалов: лекции, практические занятия, семинарские занятия, лабораторные работы, самостоятельная работа и трудоемкость (в часах)				Задания по самостоятельной работе студентов	Форма текущего контроля успеваемости (коллоквиумы, контрольные работы, компьютерные тесты и т.п.)
		ЛК	ПР / СЕМ	ЛР	СР		
1	2	3	4	5	6	7	8
Раздел (модуль) 1. Теоретические аспекты управления информационной безопасности							
1	**Тема 1.** Нормативно-законодательная регламентация управления информационной безопасностью (государственный, объектовый уровень): **Содержание:** Законодательные новации в сфере информационной безопасности (руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации). Трансформация модели кибербезопасности в РФ в новых условиях. Актуальные проблемы управления информационной безопасностью гос.учреждений, финансовых и экономически структур, предприятий, т.д.	4	4		2	Самостоятельное изучение нормативно-законодательной базы по УИБ и ЗИ, теоретического материала; рекомендуемой литературы; подготовка к практическим работам	Практические задания, тест
2	**Тема 2.** Цели, задачи, компетенции управления информационной безопасностью; **Содержание:** Формализация задач автоматизированной информационно-аналитической поддержки процессов принятия решений в сфере безопасности; Подготовка проектов нормативно-распорядительных документов (приказов, указаний, инструкций) по вопросам ИБ.	2	4		2	Самостоятельное изучение теоретического материала; подготовка к практическим работам	Практические задания, тест
3	**Тема 3.** Стандартизация управления информационной безопасностью. Модели и методы УИБ. **Содержани**е: Анализ и особенности применения отечественных и зарубежных стандартов в области	4	4		2	Самостоятельное изучение теоретического материала;	Практические задания, тест

	защиты информации для проектирования, разработки и оценки защищенности компьютерных систем. Методы и подходы к управлению ИБ, их сравнительный анализ и оценка. Процессный подход к разработке, реализации, эксплуатации и анализу системы управления. Особенности реализации непрерывной модели управления информационной безопасностью. Новые практические решения в области моделей и методов управления информационной безопасностью как инструментарий при разработке систем защиты информации.					подготовка к практическим работам	
Раздел (модуль) 2. Особенности практической реализация УИБ. СУИБ							
4	**Тема** 4. Система управления информационной безопасности (СУИБ) – управленческие аспекты. **Содержание**: Управление ИБ: задача, ответственность отдела ИБ, полномочия, управленческий ресурс отдела ИБ. Место СУИБ в рамках общей системы управления объектом. Этапы создания и внедрения СУИБ (планирование, реализация, контроль, совершенствование); комплекс решаемых управленческих задач и работ; документальное обеспечение СУИБ; Требования к процессам СУИБ, работа с процессами СУИБ (документирование, описание процесса СУИБ; построение и внедрение процессов СУИБ; мониторинг и измерение параметров процесса СУИБ)	6	10		1,8	Самостоятельное изучение теоретического материала; подготовка к практическим работам	Практические задания, тест
5	**Тема 5.** Практические аспекты управления информационной безопасностью **Содержание:** Угрозы ИБ. Политика ИБ. Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации. Организационные аспекты УИБ. Методы управления доступом, правила разграничения доступа. Программные и технические средства ИБ. Контроль и мониторинг (в т.ч. инструментальные средства). Мониторинг и ситуационный анализ обстановки в сфере безопасности. Организация аудита ИБ.	4	8		2	Самостоятельное изучение теоретического материала; подготовка к практическим работам	Практические задания
6	**Тема 6.** Место планирования, прогнозирования в УИБ.	4	6		2	Самостоятельно	Практические задания

	Управление рисками и инцидентами информационной безопасности. **Содержание:** Методы прогнозирования, планирования, принятия решений по УИБ в условиях неопределенности; оценка эффективности и качества в задачах прогнозирования, планирования, принятия этих решений. Современные модели и методы измерения, прогнозирования, планирования, принятия решений при решении задач поддержки процессов принятия решений; прогнозирование на основе вероятностного и статистического анализа. Управление инцидентами ИБ. Реализация обратной связи в управлении информационной безопасностью. Управление информационными рисками. Расчет и оценка эффективности управления риском. Особые аспекты управления риском.					е изучение теоретического материала; подготовка к практическим работам	
Всего часов:		24	36		11,8		