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

Актуализировано:
на заседании кафедры
протокол № 10 от «7» июня 2018 г.
Зав. кафедрой / А.С. Исмагилова

Согласовано:
Председатель УМК института
/ Р.А. Гильмутдинова

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Основы управления информационной безопасностью

Б1.Б.23 (базовая)

программа бакалавриата

Направление
10.03.01 Информационная безопасность

Профиль подготовки
Организация и технология защиты информации

Квалификация
бакалавр

Разработчик (составитель)
ст. преподаватель
/ И.В. Салов

Разработчик (составитель)
к.х.н.
/ А.А. Султанова

Для приема: 2015 г.

Уфа 2018 г.

Составители: И.В. Салов, А.А. Султанова

Рабочая программа дисциплины актуализирована на заседании кафедры управления информационной безопасностью № 10 от «7» июня 2018 г.

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры государственного управления, протокол № __ от «__» _____ 201_ 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/

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 (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

В результате освоения образовательной программы обучающийся должен овладеть следующими результатами обучения по дисциплине (модулю):

Результаты обучения		Формируемая компетенция (с указанием кода)	Примечание
Знания	понятие и методы саморазвития, самообучения и самовоспитания личности	– способностью к самоорганизации и самообразованию (ОК-8)	
	общеметодологические принципы теории информационной безопасности	– способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации (ПК-13)	
	технологии организации деятельности и рабочего места сотрудников	– способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности (ПК-14)	
	нормативные методические документы Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю в данной области	– способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю (ПК-15)	
	общеметодологические принципы теории информационной безопасности	– способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью (ПСК-2)	
	способы организации мероприятий по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств защиты информации	– способностью организовать мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств защиты информации (ПСК-3)	
Умения	самостоятельно ставить самообразовательные задачи	– способностью к самоорганизации и самообразованию (ОК-8)	
	реализовывать на практике принципы	– способностью принимать участие в формировании, организовывать и	

	политики безопасности	поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации (ПК-13)	
	применять современные методы оценки персонала в планировании, контроле и учете деятельности сотрудников и их трудового поведения	– способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности (ПК-14)	
	анализировать и составлять основные правовые акты и осуществлять правовую оценку информации, используемых в профессиональной деятельности	– способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю (ПК-15)	
	обосновывать организационно-технические мероприятия по защите информации	– способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью (ПСК-2)	
	организовать мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств защиты информации	– способностью организовать мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств защиты информации (ПСК-3)	
Владения (навыки / опыт деятельности)	методами самоанализа	– способностью к самоорганизации и самообразованию (ОК-8)	
	навыками анализа, обработки и интерпретации результатов решения прикладных задач управления	– способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации (ПК-13)	
	навыками аттестации и оценки персонала	– способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности (ПК-14)	
	основами правового мышления, навыками самостоятельного	– способностью организовывать технологический процесс защиты информации ограниченного	

	анализа правовой информации, анализа юридических последствий, связанных с использованием информации	доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю (ПК-15)	
	навыками обоснования, выбора, реализации и контроля результатов управленческого решения	– способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью (ПСК-2)	
	навыками систематической организации мероприятий по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств защиты информации	– способностью организовать мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств защиты информации (ПСК-3)	

2. Цель и место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Основы управления информационной безопасностью» относится к базовой части образовательной программы.

Дисциплина изучается на 4 курсе в 7-8-м семестре.

Цели изучения дисциплины: является изучение методов и средств управления информационной безопасностью на объекте, а также на изучение основных подходов к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью определенного объекта.

Изучение дисциплины базируется на знаниях, умениях и навыках, сформированных в результате освоения студентами предшествующих дисциплин образовательной программы по направлению 10.03.01 Информационная безопасность направлению подготовки «Организация и технология защиты информации»: «Организационное и правовое обеспечение информационной безопасности», «Основы управленческой деятельности».

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 с указанием этапов их формирования в процессе освоения образовательной программы. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Для зачета

ОК-8. Способность к самоорганизации и самообразованию

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения	
		Не зачтено	Зачтено
Первый этап (уровень) Пороговый	Знать: понятие и методы саморазвития, самообучения и самовоспитания личности	Отсутствие знаний или неполные представления о понятии и методах саморазвития, самообучения и самовоспитания личности	Знает понятие и методы саморазвития, самообучения и самовоспитания личности
Второй этап (уровень) Базовый	Уметь: самостоятельно ставить самообразовательные задачи	Отсутствие умений ставить самообразовательные задачи	Умеет ставить самообразовательные задачи
Третий этап (уровень) Повышенный	Владеть: методами самоанализа	Отсутствие или не систематическое владение методами самоанализа	Владеет методами самоанализа

ПК-13. Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения	
		Не зачтено	Зачтено
Первый этап (уровень) Пороговый	Знать: общеметодологические принципы теории информационной безопасности	Отсутствие знаний или неполные представления о общеметодологических принципах теории информационной безопасности	Знает общеметодологические принципы теории информационной безопасности
Второй этап (уровень) Базовый	Уметь: реализовывать на практике принципы политики безопасности	Отсутствие умений реализовывать на практике принципы политики безопасности	Умеет реализовывать на практике принципы политики безопасности
Третий этап (уровень) Повышенный	Владеть: навыками анализа, обработки и интерпретации результатов решения прикладных задач управления	Отсутствие владений навыками анализа, обработки и интерпретации результатов решения прикладных задач управления	Владеет навыками анализа, обработки и интерпретации результатов решения прикладных задач управления

ПК-14. Способность организовывать работу малого коллектива исполнителей в профессиональной деятельности

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения	
		Не зачтено	Зачтено
Первый этап (уровень) Пороговый	Знать: технологии организации деятельности и рабочего места сотрудников	Отсутствие знаний или неполные представления о технологии организации деятельности и рабочего места сотрудников	Знает технологии организации деятельности и рабочего места сотрудников
Второй этап (уровень) Базовый	Уметь: применять современные методы оценки персонала в планировании, контроле и учете деятельности сотрудников и их трудового поведения	Отсутствие умений применять современные методы оценки персонала в планировании, контроле и учете деятельности сотрудников и их трудового поведения	Умеет применять современные методы оценки персонала в планировании, контроле и учете деятельности сотрудников и их трудового поведения
Третий этап (уровень) Повышенный	Владеть: навыками аттестации и оценки персонала	Отсутствие владений навыками аттестации и оценки персонала	Владеет навыками аттестации и оценки персонала

ПК-15. Способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения	
		Не зачтено	Зачтено
Первый этап (уровень) Пороговый	Знать: нормативные методические документы Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю в данной области	Отсутствие знаний или неполные представления о нормативных методических документах Федеральной службы безопасности РФ	Знает нормативные методические документы Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю в данной области

Второй этап (уровень) Базовый	Уметь: анализировать и составлять основные правовые акты и осуществлять правовую оценку информации, используемых в профессиональной деятельности	Отсутствие умений анализировать и составлять основные правовые акты	Умеет анализировать и составлять основные правовые акты и осуществлять правовую оценку информации, используемых в профессиональной деятельности
Третий этап (уровень) Повышенный	Владеть: основами правового мышления, навыками самостоятельного анализа правовой информации, анализа юридических последствий, связанных с использованием информации	Отсутствие владений основами правового мышления	Владеет основами правового мышления, навыками самостоятельного анализа правовой информации, анализа юридических последствий, связанных с использованием информации

ПСК-2. Способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения	
		Не зачтено	Зачтено
Первый этап (уровень) Пороговый	Знать: общеметодологические принципы теории информационной безопасности	Отсутствие знаний или неполные представления о общеметодологических принципах теории информационной безопасности	Знает общеметодологические принципы теории информационной безопасности
Второй этап (уровень) Базовый	Уметь: обосновывать организационно-технические мероприятия по защите информации	Отсутствие умений обосновывать организационно-технические мероприятия по защите информации	Умеет обосновывать организационно-технические мероприятия по защите информации
Третий этап (уровень) Повышенный	Владеть: навыками обоснования, выбора, реализации и контроля результатов управленческого решения	Отсутствие владений навыками обоснования, выбора, реализации и контроля результатов управленческого решения	Владеет навыками обоснования, выбора, реализации и контроля результатов управленческого решения

ПСК-3. Способность организовать мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств защиты информации

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения	
		Не зачтено	Зачтено
Первый этап (уровень) Пороговый	Знать: способы организации мероприятий по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств защиты информации	Не знает	Знает способы организации мероприятий по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств
Второй этап (уровень) Базовый	Уметь: организовать мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств защиты информации	Не умеет	Умеет организовать мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств защиты информации
Третий этап (уровень) Повышенный	Владеть: навыками систематической организации мероприятий по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств защиты информации	Не владеет	Владеет навыками систематической организации мероприятий по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств защиты информации

Для экзамена

ОК-8. Способность к самоорганизации и самообразованию

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения			
		2 («неудовлетворительно»)	3 («удовлетворительно»)	4 («хорошо»)	5 («отлично»)
Первый этап (уровень) Пороговый	Знать: понятие и методы саморазвития, самообучения и самовоспитания личности	Не знает	Знает понятие и методы саморазвития, самообучения и самовоспитания личности, но допускает ошибки при их описании	Знает понятие и методы саморазвития, самообучения и самовоспитания личности, но допускает незначительные ошибки при их описании	Знает понятие и методы саморазвития, самообучения и самовоспитания личности
Второй этап (уровень) Базовый	Уметь: самостоятельно ставить самообразовательные задачи	Не умеет	Умеет ставить самообразовательные задачи, но допускает ошибки	Умеет ставить самообразовательные задачи, но допускает незначительные ошибки	Умеет ставить самообразовательные задачи
Третий этап (уровень) Повышенный	Владеть: методами самоанализа	Не владеет	Владеет методами самоанализа, но допускает ошибки	Владеет методами самоанализа, но допускает незначительные ошибки	Владеет методами самоанализа

ПК-13. Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения			
		2 («неудовлетворительно»)	3 («удовлетворительно»)	4 («хорошо»)	5 («отлично»)
Первый этап (уровень) Пороговый	Знать: общеметодологические принципы теории информационной безопасности	Не знает	Знает общеметодологические принципы теории информационной безопасности, но допускает ошибки при их описании	Знает общеметодологические принципы теории информационной безопасности, но допускает незначительные ошибки при их описании	Знает общеметодологические принципы теории информационной безопасности
Второй этап (уровень) Базовый	Уметь: реализовывать на практике принципы политики безопасности	Не умеет	Умеет реализовывать на практике принципы политики безопасности, но допускает ошибки	Умеет реализовывать на практике принципы политики безопасности, но допускает незначительные ошибки	Умеет реализовывать на практике принципы политики безопасности
Третий этап (уровень) Повышенный	Владеть: навыками анализа, обработки и интерпретации результатов решения прикладных задач управления	Не владеет	Владеет навыками анализа, обработки и интерпретации результатов решения прикладных задач управления, но допускает ошибки	Владеет навыками анализа, обработки и интерпретации результатов решения прикладных задач управления, но допускает незначительные ошибки	Владеет навыками анализа, обработки и интерпретации результатов решения прикладных задач управления

ПК-14. Способность организовывать работу малого коллектива исполнителей в профессиональной деятельности

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения			
		2 («неудовлетворительно»)	3 («удовлетворительно»)	4 («хорошо»)	5 («отлично»)
Первый этап (уровень) Пороговый	Знать: технологии организации деятельности и рабочего места сотрудников	Не знает	Знает технологии организации деятельности и рабочего места сотрудников, но допускает ошибки при их описании	Знает технологии организации деятельности и рабочего места сотрудников, но допускает незначительные ошибки при их описании	Знает технологии организации деятельности и рабочего места сотрудников
Второй этап (уровень) Базовый	Уметь: применять современные методы оценки персонала в планировании, контроле и учете деятельности сотрудников и их трудового поведения	Не умеет	Умеет применять современные методы оценки персонала в планировании, контроле и учете деятельности сотрудников и их трудового поведения, но допускает ошибки	Умеет применять современные методы оценки персонала в планировании, контроле и учете деятельности сотрудников и их трудового поведения, но допускает незначительные ошибки	Умеет применять современные методы оценки персонала в планировании, контроле и учете деятельности сотрудников и их трудового поведения
Третий этап (уровень) Повышенный	Владеть: навыками аттестации и оценки персонала	Не владеет	Владеет навыками аттестации и оценки персонала, но допускает ошибки	Владеет навыками аттестации и оценки персонала, но допускает незначительные ошибки	Владеет навыками аттестации и оценки персонала

ПК-15. Способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения			
		2 («неудовлетворительно»)	3 («удовлетворительно»)	4 («хорошо»)	5 («отлично»)
Первый этап (уровень) Пороговый	Знать: нормативные методические документы Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю в данной области	Не знает	Знает нормативные методические документы Федеральной службы безопасности РФ	Знает нормативные методические документы Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю в данной области, допускает незначительные ошибки	Знает нормативные методические документы Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю в данной области
Второй этап (уровень) Базовый	Уметь: анализировать и составлять основные правовые акты и осуществлять правовую оценку информации, используемых в профессиональной деятельности	Не умеет	Умеет анализировать и составлять основные правовые акты	Умеет анализировать и составлять основные правовые акты и осуществлять правовую оценку информации, используемых в профессиональной деятельности, допускает незначительные ошибки	Умеет анализировать и составлять основные правовые акты и осуществлять правовую оценку информации, используемых в профессиональной деятельности
Третий этап (уровень) Повышенный	Владеть: основами правового мышления, навыками самостоятельного анализа правовой информации, анализа юридических последствий, связанных с использованием информации	Не владеет	Владеет основами правового мышления	Владеет основами правового мышления, навыками самостоятельного анализа правовой информации, анализа юридических последствий, связанных с использованием информации, допускает незначительные ошибки	Владеет основами правового мышления, навыками самостоятельного анализа правовой информации, анализа юридических последствий, связанных с использованием информации

ПСК-2. Способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения			
		2 («неудовлетворительно»)	3 («удовлетворительно»)	4 («хорошо»)	5 («отлично»)
Первый этап (уровень) Пороговый	Знать: общеметодологические принципы теории информационной безопасности	Не знает	Знает общеметодологические принципы теории информационной безопасности, но допускает ошибки при их описании	Знает общеметодологические принципы теории информационной безопасности, но допускает незначительные ошибки при их описании	Знает общеметодологические принципы теории информационной безопасности
Второй этап (уровень) Базовый	Уметь: обосновывать организационно-технические мероприятия по защите информации	Не умеет	Умеет обосновывать организационно-технические мероприятия по защите информации, но допускает ошибки	Умеет обосновывать организационно-технические мероприятия по защите информации, но допускает незначительные ошибки	Умеет обосновывать организационно-технические мероприятия по защите информации
Третий этап (уровень) Повышенный	Владеть: навыками обоснования, выбора, реализации и контроля результатов управленческого решения	Не владеет	Владеет навыками обоснования, выбора, реализации и контроля результатов управленческого решения, но допускает ошибки	Владеет навыками обоснования, выбора, реализации и контроля результатов управленческого решения, но допускает незначительные ошибки	Владеет навыками обоснования, выбора, реализации и контроля результатов управленческого решения

ПСК-3. Способность организовать мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств защиты информации

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения			
		2 («неудовлетворительно»)	3 («удовлетворительно»)	4 («хорошо»)	5 («отлично»)
Первый этап (уровень)	Знать: способы организации мероприятий	Не знает	Знает способы организации	Знает способы организации мероприятий по охране	Знает способы организации

Пороговый	по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств защиты информации		мероприятий по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств, допускает ошибки	труда и технике безопасности в процессе эксплуатации и технического обслуживания средств, но допускает незначительные ошибки	мероприятий по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств
Второй этап (уровень) Базовый	Уметь: организовать мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств защиты информации	Не умеет	Умеет организовать мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств защиты информации, допускает ошибки	Умеет организовать мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств защиты информации, но допускает незначительные ошибки	Умеет организовать мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств защиты информации
Третий этап (уровень) Повышенный	Владеть: навыками систематической организации мероприятий по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств защиты информации	Не владеет	Владеет навыками систематической организации мероприятий по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств защиты информации, допускает ошибки	Владеет навыками систематической организации мероприятий по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств защиты информации, но допускает незначительные ошибки	Владеет навыками систематической организации мероприятий по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств защиты информации

4.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и опыта деятельности, характеризующих этапы формирования компетенций

Этапы освоения	Результаты обучения	Компетенция	Оценочные средства
1-й этап Знать	понятие и методы саморазвития, самообучения и самовоспитания личности	ОК-8	тестирование, практическое задание, контрольная работа, лабораторная работа
	общеметодологические принципы теории информационной безопасности	ПК-13	тестирование, практическое задание, контрольная работа, лабораторная работа
	технологии организации деятельности и рабочего места сотрудников	ПК-14	тестирование, практическое задание, контрольная работа, лабораторная работа
	нормативные методические документы Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю в данной области	ПК-15	тестирование, практическое задание, контрольная работа, лабораторная работа
	общеметодологические принципы теории информационной безопасности	ПСК-2	тестирование, практическое задание, контрольная работа, лабораторная работа

	способы организации мероприятий по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств защиты информации	ПСК-3	тестирование, практическое задание, контрольная работа, лабораторная работа
2-й этап Уметь	самостоятельно ставить самообразовательные задачи	ОК-8	тестирование, практическое задание, контрольная работа, лабораторная работа
	реализовывать на практике принципы политики безопасности	ПК-13	тестирование, практическое задание, контрольная работа, лабораторная работа
	применять современные методы оценки персонала в планировании, контроле и учете деятельности сотрудников и их трудового поведения	ПК-14	тестирование, практическое задание, контрольная работа, лабораторная работа
	анализировать и составлять основные правовые акты и осуществлять правовую оценку информации, используемых в профессиональной деятельности	ПК-15	тестирование, практическое задание, контрольная работа, лабораторная работа
	обосновывать организационно-технические мероприятия по защите информации	ПСК-2	тестирование, практическое задание, контрольная работа, лабораторная работа
	организовать мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств защиты информации	ПСК-3	тестирование, практическое задание, контрольная работа, лабораторная работа
3-й этап Владеть	методами самоанализа	ОК-8	тестирование, практическое задание, контрольная работа, лабораторная работа
	навыками анализа, обработки и интерпретации результатов решения прикладных задач управления	ПК-13	тестирование, практическое задание, контрольная работа, лабораторная работа
	навыками аттестации и	ПК-14	тестирование,

	оценки персонала		практическое задание, контрольная работа, лабораторная работа
	основами правового мышления, навыками самостоятельного анализа правовой информации, анализа юридических последствий, связанных с использованием информации	ПК-15	тестирование, практическое задание, контрольная работа, лабораторная работа
	навыками обоснования, выбора, реализации и контроля результатов управленческого решения	ПСК-2	тестирование, практическое задание, контрольная работа, лабораторная работа
	навыками систематической организации мероприятий по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств защиты информации	ПСК-3	тестирование, практическое задание, контрольная работа, лабораторная работа

4.3. Рейтинг-план дисциплины

Рейтинг–план дисциплины представлен в приложении 1.

Типовые вопросы для зачета

1. Основные понятия информационной безопасности.
2. Угрозы информационной безопасности в информационных системах.
3. Оценочные стандарты в информационной безопасности.
4. Стандарты управления информационной безопасностью.
5. Создание СУИБ на предприятии.
6. Методика оценки рисков информационной безопасности компании Digital Security.
7. Методики и технологии управления рисками.
8. Разработка корпоративной методики анализа рисков.
9. Современные методы и средства анализа и управление рисками информационных систем
10. компаний.
11. 10.Правовые меры обеспечения информационной безопасности.
12. 11.Организационные меры обеспечения безопасности компьютерных информационных
13. систем.
14. 12.Программно-технические меры обеспечения информационной безопасности.
15. Идентификация, аутентификация, управление доступом.
16. 13.Протоколирование и аудит, шифрование, контроль целостности.
17. Понятие информационной безопасности.

18. Основные составляющие информационной безопасности.
19. Управление информационной безопасностью.
20. Важность и сложность проблемы информационной безопасности
21. Основные определения и критерии классификации угроз.
22. Основные угрозы доступности.
23. Основные угрозы целостности.
24. Основные угрозы конфиденциальности.
25. Вредительские программы
26. Роль стандартов ИБ.
27. "Оранжевая книга" как оценочный стандарт.
28. Международный стандарт ISO/IEC 15408. Критерии оценки безопасности информационных систем.
29. Стандарты управления информационной безопасностью BS 7799 и ISO/IEC 17799. Их основные положения.
30. Серия стандартов ISO/IEC 27000 «Информационные технологии. Методы обеспечения безопасности».
31. Стандарт ISO/IEC 27000:2009 -СУИБ: определения и основные принципы.
32. Стандарт ISO/IEC 27001:2005 и ГОСТ Р ИСО/МЭК 27001-2006 -Требования к СУИБ.
33. Стандарт ISO/IEC 27002:2005 и ГОСТ Р ИСО/МЭК 17799-2005 - практические правила управления ИБ.
34. Стандарт ISO/IEC 27003:2010 – руководство по внедрению СУИБ.
35. Стандарт ISO/IEC 27004:2009 и ГОСТ Р ИСО/МЭК 27004-2011 - оценка функционирования СУИБ.
36. Стандарт ISO/IEC 27005:2011 и ГОСТ Р ИСО/МЭК 27005-2010 - управление рисками ИБ. ISO/IEC 27006:2011 и I ОСТ Р ИСО/МЭК 27006-2008 - требования к органам, осуществляющим аудит и сертификацию СУИБ.
37. Стандарт ISO/IEC 27007:2011 и ISO/IEC 27008:2011 - руководства по аудиту СУИБ и средств управления ИБ, реализованных в СУИБ.
38. Стандарт ISO/IEC 27011:2008 - руководство по управлению ИБ для телекоммуникационных компаний на основе ISO/IEC 27002. ISO/IEC 27013 - руководство по интегрированному внедрению стандартов ISO/IEC 20000 и 27001.
39. Стандарт ISO/IEC 27014 - инфраструктура руководства ИБ. ISO/IEC 27015 - руководство но управлению ИБ для финансовых сервисов.
40. Стандарт ISO/IEC 27031:2011 - руководство по готовности информационных и телекоммуникационных технологий для обеспечения непрерывности бизнеса.
41. Стандарт ISO/IEC 27033 - управление безопасностью сетей.
42. Стандарт ISO/IEC 27035:2011 - управление инцидентами ИБ.
43. Стандарт ISO/IEC 27037 - руководство по идентификации, сбору и/или получению и обеспечению сохранности свидетельств, представленных в электронной форме.
44. Стандарт ISO/IEC 13335 - методы и средства обеспечения безопасности информационных технологий. ISO/IEC 15408 и ISO/IEC 18045:2008 - общие критерии и методология оценки безопасности информационных технологий.
45. Стандарт ISO 19011:2011 и ГОСТ Р ИСО 19011-2003 - рекомендации по аудиту систем менеджмента. BS 25999 и ГОСТ Р 53647 – управление непрерывностью бизнеса.
46. Стандарт СТО БР ИББС-1.0 - общие положения в области обеспечения ИБ организаций банковской системы Российской Федерации.
47. Стандарт СТО БР ИББС-1.1- аудит ИБ.
48. Стандарт СТО БР ИББС-1.2 - методика оценки соответствия ИБ организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0.

49. Сертификация СУИБ на соответствие ISO 27001.
50. Метод оценки рисков на основе модели угроз и уязвимостей
51. Расчет рисков по угрозе информационной безопасности
52. Задание контрмер
53. Качественные методики управления рисками.
54. Количественные методики управления рисками. Метод CRAMM.
55. Обоснование необходимости инвестиций в информационную безопасность компании.
56. Методика FRAP.
57. Методика OCTAVE.
58. Методика Risk Watch.
59. Основные направления обеспечения информационной безопасности.
60. Законодательно-правовая база обеспечения информационной безопасности на предприятии.
61. Нормативные акты предприятия по информационной безопасности.
62. Формы правовой защиты информации на предприятии.
63. Другие документы предприятия, в которых отражаются вопросы обеспечения информационной безопасности.
64. Общие положения организационной защиты.
65. Особенности организационной защиты компьютерных информационных систем и сетей.
66. Служба безопасности предприятия.
67. Основные программно-технические меры.
68. Идентификация и аутентификация.
69. Управление доступом
70. Протоколирование
71. Контроль целостности.

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).

Экзамен

Структура экзаменационного билета

Экзаменационный билет состоит из двух вопросов, отражающих соответственно материал первого и второго модуля.

Типовые экзаменационные материалы

1. Понятие информационной безопасности. Термины и определения.
2. Система информационной безопасности.
3. Проверка безопасности информационных систем. Аудит систем.
4. Общие сведения об информационной безопасности.
5. Проверка безопасности информационных систем. Мониторинг систем.
6. Основные составляющие информационной безопасности.
7. Внешний аудит.
8. Обоснование необходимости рассмотрения вопросов информационной безопасности.
9. Внутренний аудит.

10. Процессный подход в рамках управления ИБ.
11. Проблемы построения современных систем безопасности.
12. Слежение за доступом к системам и их использованием.
13. Стандарты информационной безопасности ISO/IEC серии 27000.
14. Отраслевые стандарты информационной безопасности
15. Стандарты и нормативные акты РФ в области информационной безопасности.
16. Оценка рисков нарушения безопасности.
17. Средства управления информационной безопасностью.
18. Защита от вредоносного программного обеспечения.
19. Ключевые средства контроля информационной безопасности.
20. Ответственность за информационные ресурсы.
21. Требование бизнеса по обеспечению контроля доступа.
22. Факторы, необходимые для успешной реализации системы информационной безопасности в организации.
23. Управление доступом пользователей. Обязанности пользователей.
24. Группы требований к информационной безопасности организации.
25. Система планирования бесперебойной работы организации.
26. Политика информационной безопасности.
27. Классификация информации.
28. Инфраструктура информационной безопасности.
29. Безопасность информации в должностных инструкциях.
30. Обучение пользователей правилам информационной безопасности.
31. Реагирование на события, таящие угрозу безопасности.
32. Оперирование с носителями информации и их защита.
33. Термины и определения информационной безопасности.
34. Понятие информационной безопасности.
35. Циклическая модель улучшения процессов.
36. Системный подход к управлению организацией.
37. Процессный подход к управлению организацией.
38. Планирование СУИБ.
39. Совершенствование СУИБ.
40. Стратегии построения и внедрения СУИБ.
41. Построение и внедрение процессов СУИБ по отдельности.
42. Идентификация процессов СУИБ организации.
43. Документирование и описание процесса СУИБ.
44. Работа с процессами СУИБ организации.
45. Задание процесса СУИБ.
46. Метод оценки рисков на основе модели информационных потоков.
47. Расчет рисков по угрозе целостности.
48. Управление безопасностью как элемент системы управления рисками.
49. Качественные методики управления рисками.
50. Программное обеспечение управление рисками COBRA.
51. Программное обеспечение управление рисками RA Software Tool.
52. Количественные методики управления рисками.
53. Метод управления рисками CRAMM.
54. Метод оценки рисков на основе модели угроз и уязвимостей.
55. Расчет рисков по угрозе информационной безопасности.
56. Методика оценки рисков информационной безопасности компании Digital Security.
57. Деятельность по обеспечению ИБ организации как процесс.
58. Управление ИБ информационно-телекоммуникационных технологий организации.

59. Система управления ИБ организации.
60. Область действия СУИБ.
61. Документальное обеспечение СУИБ.
62. Поддержка СУИБ со стороны руководства организации.
63. Контроль сетевого доступа.

Пример экзаменационного билета:

Форма 1.4.-33

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ИНСТИТУТ ИСТОРИИ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

Направление 10.03.01 Информационная безопасность

Дисциплина Основы управления информационной безопасностью

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Понятие информационной безопасности. Термины и определения.
2. Проверка безопасности информационных систем. Аудит систем.

Зав. Кафедрой УИБ А.С. Исмагилова

Кафедра управления информационной безопасностью

Устанавливается следующая градация перевода оценки из многобалльной в четырехбалльную:

Экзамены:

- отлично – от 80 до 110 баллов (включая 10 поощрительных баллов),
- хорошо – от 60 до 79 баллов,
- удовлетворительно – от 45 до 59 баллов,
- неудовлетворительно – менее 45 баллов.

Критерии оценивания результатов экзамена для ОФО:

Критерии оценки (в баллах):

- 25-30 баллов выставляется студенту, если студент дал полные, развернутые ответы на все теоретические вопросы билета, продемонстрировал знание терминологии, основных понятий, умение применять теоретические знания при выполнении практических заданий. Студент без затруднений ответил на все дополнительные вопросы.

- 17-24 баллов выставляется студенту, если студент раскрыл в основном теоретические вопросы, однако допущены неточности в определении основных понятий. При ответе на дополнительные вопросы допущены небольшие неточности.

- 10-16 баллов выставляется студенту, если при ответе на теоретические вопросы студентом допущено несколько существенных ошибок в толковании основных понятий. Логика и полнота ответа страдают заметными изъянами. Заметны пробелы в знании основных методов. Теоретические вопросы в целом изложены достаточно, но с пропусками материала. Имеются принципиальные ошибки в логике построения ответа на вопрос.

- 1-10 баллов выставляется студенту, если ответ на теоретические вопросы свидетельствует о непонимании и крайне неполном знании основных понятий и методов. Обнаруживается отсутствие навыков применения теоретических знаний при выполнении практических заданий. Студент не смог ответить ни на один дополнительный вопрос.

Темы лабораторных работ

Цель проведения лабораторных работы – практическое освоение материала дисциплины.

1) Классификация ресурсов и контроль за ними.
2) Разработка модели угроз безопасности персональных данных для ИСПДн.
3) Выбор СКЗИ для ИСПДн.
4) Разработка должностных инструкций пользователей АС с учетом требований информационной безопасности.

Типовая лабораторная работа

Модуль 1 (8 семестр). Основы управления рисками ИБ.

Тема: Модель угроз безопасности информации.

Цель: Практическая разработка модели угроз безопасности персональных данных для ИСПДн.

Задание: Разработать модель угроз безопасности персональных данных для ИСПДн выбранной организации (торговое предприятие, ЗАГС, поликлиника).

Порядок выполнения:

1. Дополнительно изучить федеральное законодательство: Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»; Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»; Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденное постановлением Правительства Российской Федерации от 17 ноября 2007 года № 781; Порядок проведения классификации информационных систем персональных данных, утвержденный приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 года № 55/86/20 (зарегистрирован Минюстом России 3 апреля 2008 года, регистрационный № 11462); Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Утверждена Заместителем директора ФСТЭК России 15 февраля 2008г.); Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Утверждена Заместителем директора ФСТЭК России 14 февраля 2008г.).
2. Описать структуру ИСПДн организации.
3. Определить состав и режим обработки ПДн.
4. Провести классификацию потенциальных нарушителей ИСПДн.
5. Оценить исходный уровень защищенности.
6. Произвести анализ угроз безопасности персональных данных (описание угроз, оценку вероятности возникновения угроз, реализуемости угроз, опасности угроз, определение актуальности угроз).
7. Оформить модель угроз.
8. Ответить на контрольные вопросы:
   a) Понятие угрозы нарушения информационной безопасности.
   b) Перечислите виды угроз ИБ.
   c) В чем сущность модели угроз?

d) Укажите источники угроз нарушения целостности, доступности и конфиденциальности информации.

9. Защита лабораторной работы. Проводится в форме устного опроса после выполнения работы.

Критерии оценки лабораторной работы

Структура работы	Критерии оценки	Распределение баллов
Одно лабораторное задание	работа выполнена с ошибками и не получены ответы на все контрольные вопросы/ работа выполнена, но не получены ответы на все контрольные вопросы/ работа выполнена и получены ответы на все контрольные вопросы	0/3/7

Типовые задания для контрольной работы

Цель проведения контрольной работы – оценка уровня владения базовой профессиональной терминологией в сфере управления информационной безопасностью. Контрольная работа проводится в письменной форме.

Примеры заданий

Модуль 1. Основы управления рисками ИБ

Письменная контрольная работа

1. Методы и средства построения систем информационной безопасности
2. Структура системы информационной безопасности
3. Морально-этические средства
4. Криптология
5. Организационные средства

Критерии оценки контрольных работ:

Структура работы	Критерии оценки	Распределение баллов
Один вопрос	Нет ответа / Неполный ответ / Полный ответ	0/5/10

Типовые тестовые задания

При изучении дисциплины используются тестовые задания закрытого типа. Каждое тестовое задание включает вопрос и 4 варианта ответов к нему. Тестирование выполняется в письменной форме.

Необходимо выбрать один ответ из предложенных вариантов.

Тестирование

Модуль 1. Основы управления рисками ИБ

1Кто является основным ответственным за определение уровня классификации информации?

А) Руководитель среднего звена

Б) Высшее руководство

В) Владелец

Г) Пользователь

2. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?

А) Сотрудники

Б) Хакеры

В) Атакующие

Г) Контрагенты (лица, работающие по договору)

3. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?

А) Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования

Б) Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации

В) Улучшить контроль за безопасностью этой информации

Г) Снизить уровень классификации этой информации

Критерии оценки тестовых заданий

Структура работы	Критерии оценки	Распределение баллов
7 семестр, Модуль 1. Системы управления ИБ Один тестовый вопрос (всего в тесте 25 вопросов) Тест (все 25 вопросов)	Не правильный ответ/ Правильный ответ	 0/1,2 0/30
7 семестр, Модуль 2 Основы управления ИБ, Один тестовый вопрос (всего в тесте 25 вопросов) Тест (все 25 вопросов)	Не правильный ответ/ Правильный ответ	 0/0,4 0/10
8 семестр Модуль 1. Основы управления рисками ИБ, 8 семестр, Модуль 2. Процессы управления ИБ Один тестовый вопрос (всего в тесте 25 вопросов) Тест (все 25 вопросов)		 0/0,6 0/15

Темы практических работ

1) Принципы классификации ресурсов.
2) Методы контроля ресурсов.
3) Разработать положение о порядке выявления и реагирования на инциденты информационной безопасности.
4) Журналы регистрации событий на примере ОС Windows.
5) Возможности системы управления событиями информационной безопасности (SIEM -системы).
6) Система контроля и управления доступом (СКУД) на примере гуманитарного корпуса БашГУ.
7) Системы сигнализации на примере гуманитарного корпуса БашГУ.
8) Виды проверок СУИБ.

Типовая практическая работа

Модуль 1 (8 семестр). Основы управления рисками ИБ.

Тема: Журналы регистрации событий на примере ОС Windows.

Цель: Практическое ознакомление с системой журналирования, применяемой в ОС Windows.

Задание: Ознакомиться с системой журналирования ОС Windows.

Порядок выполнения:

1) Ознакомиться с системой журналирования ОС Windows.
2) Показать ключевые журналы ОС Windows.
3) Указать типичные проблемы, возникающие при обработке указанных журналов.
4) Перечислить типовые пути решения возникающих проблем.

Критерии оценки практической работы

Структура работы	Критерии оценки	Распределение баллов
7 семестр	работа выполнена неполно, не показано общее понимание вопроса, имелись затруднения или допущены ошибки в	0/5/10
8 семестр	определении понятий, использовании терминологии /работа выполнена в полном объеме, но допущены один-два недочета при освещении основного содержания ответа, нет определенной логической последовательности, неточно используется специализированная терминология/ работа выполнена в полном объеме и изложена грамотным языком в определенной логической последовательности с точным использованием специализированной терминологии; показано уверенное владение прикладными программами	0/3/6

5. Учебно-методическое и информационное обеспечение дисциплины

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

Основная литература

1. 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). - Библиогр. в кн. - ISBN 978-5-9912-0272-5 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=253576 (07.04.2019).

2. Курило А.П. Основы управления информационной безопасностью : учебное пособие для вузов / А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. - Москва : Горячая линия - Телеком, 2013. - 244 с. : ил. - (Вопросы управления информационной безопасностью. Вып. 1). - Библиогр. в кн. - ISBN 978-5-9912-0271-8 ; То

же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=253575 (07.04.2019).

Дополнительная литература

3. Милославская, Н.Г. Проверка и оценка деятельности по управлению информационной безопасностью : учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. - Москва : Горячая линия - Телеком, 2013. - 166 с. : ил. - (Вопросы управления информационной безопасностью. Вып. 5). - Библиогр. в кн. - ISBN 978-5-9912-0275-6 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=253579 (07.04.2019).

4. Милославская, Н.Г. Технические, организационные и кадровые аспекты управления информационной безопасностью : учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. - Москва : Горячая линия - Телеком, 2013. - 216 с. : ил. - (Вопросы управления информационной безопасностью. Вып. 4). - Библиогр. в кн. - ISBN 978-5-9912-0274-9 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=253578 (07.04.2019).

5. Веселов, Г.Е. Менеджмент риска информационной безопасности : учебное пособие / Г.Е. Веселов, Е.С. Абрамов, А.К. Шилов ; Министерство образования и науки РФ, Южный федеральный университет, Инженерно-технологическая академия. - Таганрог : Издательство Южного федерального университета, 2016. - 109 с. : схем., табл. - Библиогр.: с.85-86 - ISBN 978-5-9275-2327-5; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=493331 (07.04.2019).

6. Уколов, А.И. Управление корпоративными рисками: инструменты хеджирования : учебник / А.И. Уколов, Т.Н. Гупалова. - 2-е изд., стер. - Москва : Директ-Медиа, 2017. - 554 с. : ил., схем., табл. - Библиогр.: с. 547 - ISBN 978-5-4475-9318-6 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=273678 (07.04.2019).

5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины

1. Электронная библиотечная система «Университетская библиотека онлайн» – https://biblioclub.ru.
2. Электронная библиотечная система издательства «Лань» – https://e.lanbook.com/
3. Электронный каталог Библиотеки БашГУ – http://www.bashlib.ru/catalogi/
4. Сайт ФСТЭК России – www.fstec.ru
5. Сайт ФСБ России – www.fsb.ru
6. Портал по вопросам информационной безопасности – www.itsec.ru
7. Наиболее обширная электронная база учебников и методических материалов на сайте информационной системы «Единое окно доступа к образовательным ресурсам» – http://window.edu.ru/;
8. Новая электронная библиотека – www.newlibrary.ru;
9. Федеральный портал российского образования – www. edu.ru;
10. Научная электронная библиотека – www.elibrary.ru
11. 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.
12. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные.
13. 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 занятий лекционного типа:* аудитория № 403 (гуманитарный корпус), аудитория № 405 (гуманитарный корпус), аудитория № 413 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 515 (гуманитарный корпус), аудитория № 516 (гуманитарный корпус). **2. *учебная аудитория для проведения лабораторных работ:*** компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус), Лаборатория систем и сетей передачи данных, сетей и систем передачи информации, программно-аппаратных средств обеспечения информационной безопасности аудитория №507 (гуманитарный корпус). **3. *учебная аудитория для проведения занятий семинарского типа:*** аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус),	**Аудитория № 403** Учебная мебель, доска, Мультимедийный-проектор Panasonic PT-LB78VE – 1 шт., Экран настенный Classic Norma 244*183 – 1 шт., учебно-наглядные пособия. **Аудитория № 405** Учебная мебель, доска, вокальные радиомикрофоны AKGWMS 40 – 2шт., Интер-ая система со встроенным короткофокусным проекто-ром PrometheanActivBoard 387 RPOMOUNTEST -1 шт., Ком-ер встраиваемый в кафедру INTELCorei3-4150/DDr3 4 Gb/HDD, Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт., Настольный интерактивный дисплей , ActivPanel 21S – 1 шт. , Матричный коммутатор сигналов интерфейса HDMICMPRO 4H4H – 1 шт. , Мультимедиа-проектор PanasonicPT-EW640E - 1 шт., Двух-полосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W)(белый) -6 шт., Петличный радиомикрофон AKGWMS45 – 1 шт. , Терминал видео конференц-связи LifeSizeIcon 600 Camera 10xPhone 2ndGeneration – 1 шт., Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт. **Аудитория № 413** Учебная мебель, доска, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 6 шт., Микшер-усилитель 120Вт АРАРТ МА1225 – 1 шт. **Аудитория № 415** Учебная мебель, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 2 шт., Интерактивная доска SMART с проектором V25, Микшер-усилитель 120Вт АРАРТ МА1225 – 1 шт. **Аудитория № 416** Учебная мебель, доска, проектор Optoma Ex542 i-1 шт., Экран настенный Dinon – 1 шт. **Аудитория № 418** Учебная мебель, доска, Экран настенный Lumien Master Pikture 153*203 Matte White Fiber Clas(белый корпус) – 1 шт., Проектор Optoma Ex542 i - 1 шт. **Аудитория № 419** Учебная мебель, Проектор Optoma Ex542 i – 1 шт., Экран настенный Dinon – 1 шт. **Аудитория № 515** Учебная мебель, доска, терминал видео конференц-связи LifeSize Icon 600-камера, интер-ая система со встроенным короткофокусным проектором Promethean ActivBoard 387 RPO MOUNT EST, профес-сиональный LCD дисплей Flame 42ST, настольный интерактивный дисплей SMART Podium SP518 с ПО SMART Notebook, матричный коммутатор сигналов интерфейса HDMI CMPRO 4H4H, интер-ая напольная кафедра докладчика, ком-ер встраиваемый в кафедру IN-TEL Core i3-4150/DDr3 4 Gb/HDD 1TB/DVD-RW/Therm altake VL520B1N2E 220W/Win8Pro64, стол, трибуна, кресла секционные последующих рядов с	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.

аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус). **4. *учебная аудитория для проведения групповых и индивидуальных консультаций:*** аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус), компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус). **5. *учебная аудитория для текущего контроля и промежуточной аттестации:*** аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус), компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420	пюпитром. **Аудитория № 516** Учебная мебель, доска, кресла секционные последующих рядов с пюпитром, мобильное мультимедийное оборудование: проектор ASK Proxima, ноутбук HP, экран. **Аудитория № 509** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 608** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 609** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 610** Учебная мебель, доска, учебно-наглядные пособия, LED Телевизор TCLL55P6 USBLACK – 1 шт., кронштейн для телевизора NBP 5 – 1 шт., Кабель HDMI (m)-HDH(m)ver14,10м. **Аудитория № 613** Учебная мебель, доска, моноблок стационарный – 15 шт. **Компьютерный класс аудитория № 420** Учебная мебель, моноблоки стационарные 15 шт. **Компьютерный класс аудитория № 404** Учебная мебель, компьютеры -15 штук. **Аудитория 402 читальный зал библиотеки** Учебная мебель, доска, компьютеры в комплекте (5 шт.): монитор Samsung, системный блок Asus, клавиатура, мышь, стеллажи, шкафы картотечные, комбинированные. **Лаборатория систем и сетей передачи данных, сетей и систем передачи информации, программно-аппаратных средств обеспечения информационной безопасности № 507** Учебная мебель, учебно-наглядные пособия, аудиторная доска трехсекционная, плакаты с тематикой технические средства обработки информации, стенд "Устройство ПК". **Аудитория № 523** Шкаф-стеллаж – 4 шт., стол-1 шт., стул – 2 шт.	

(гуманитарный корпус). **6.** ***помещения для самостоятельной работы:*** читальный зал библиотеки аудитория 402 (гуманитарный корпус), аудитория № 613 (гуманитарный корпус). **7.*помещение для хранения и профилактического обслуживания учебного оборудования:***аудитория № 523 (гуманитарный корпус).		

Приложение 1

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ИНСТИТУТ ИСТОРИИ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ
дисциплины **Основы управления информационной безопасностью**
на 7 семестре
ОФО

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (ЗЕТ / часов)	3 ЗЕТ / 108 часов
Учебных часов на контактную работу с преподавателем:	36,2
лекций	18
практических/ семинарских	18
лабораторных	0
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	0,2
Учебных часов на самостоятельную работу обучающихся (СР)	72
Учебных часов на подготовку к зачету	0

Форма контроля:
Зачет 7 семестр

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ИНСТИТУТ ИСТОРИИ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ
дисциплины Основы управления информационной безопасностью на 8 семестре
ОФО

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (ЗЕТ / часов)	5 ЗЕТ / 180 часов
Учебных часов на контактную работу с преподавателем:	55,2
лекций	18
практических/ семинарских	18
лабораторных	18
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	1,2
Учебных часов на самостоятельную работу обучающихся (СР)	90
Учебных часов на подготовку к экзамену	34,8

Форма контроля:
Экзамен 8 семестр

Семестр 7

№	Тема и содержание	Форма изучения материалов: лекции, практические занятия, семинарские занятия, лабораторные работы, самостоятельная работа и трудоемкость (в часах)				Основная и дополнительная литература, рекомендуемая студентам (номера из списка)	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	9
1	Модуль «Системы управления ИБ»					1- 6	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	тестирование, практическое задание, контрольная работа
	Тема: Введение. Базовая терминология. Системный подход. Процессный подход. Циклическая модель улучшения процессов. Системный подход к управлению организацией. Процессный подход к управлению организацией. Информационная безопасность.	2	2	0	4			
	Тема: Стандартизация систем и процессов управления информационной безопасностью. Серия стандартов ISO/IEC 27000 «Информационные технологии. Методы обеспечения безопасности». ISO/IEC 27000:2009 -СУИБ: определения и основные принципы. ISO/IEC 27001:2005 и ГОСТ Р ИСО/МЭК 27001-2006 -Требования к СУИБ. ISO/IEC 27002:2005 и ГОСТ Р ИСО/МЭК 17799-2005 - практические правила управления ИБ. ISO/IEC 27003:2010 – руководство по внедрению СУИБ. ISO/IEC 27004:2009 и ГОСТ Р ИСО/МЭК 27004-2011 - оценка функционирования СУИБ. ISO/IEC 27005:2011 и ГОСТ Р ИСО/МЭК 27005-2010 - управление рисками ИБ. ISO/IEC 27006:2011 и ГОСТ Р ИСО/МЭК 27006-2008 - требования к органам, осуществляющим аудит и сертификацию СУИБ. ISO/IEC 27007:2011 и ISO/IEC 27008:2011 - руководства по аудиту СУИБ и средств управления ИБ, реализованных в СУИБ.	2	2	0	8			

	Тема: Серия стандартов ISO/IEC 27011:2008 - руководство по управлению ИБ для телекоммуникационных компаний на основе ISO/IEC 27002. ISO/IEC 27013 -руководство по интегрированному внедрению стандартов ISO/IEC 20000 и 27001. ISO/IEC 27014 - инфраструктура руководства ИБ. ISO/IEC 27015 - руководство но управлению ИБ для финансовых сервисов. ISO/IEC 27031:2011 - руководство по готовности информационных и телекоммуникационных технологий для обеспечения непрерывности бизнеса. ISO/IEC 27033 - управление безопасностью сетей.	2	2	0	8			
	Тема: Серия стандартов ISO/IEC 27035:2011 - управление инцидентами ИБ. ISO/IEC 27037 - руководство по идентификации, сбору и/или получению и обеспечению сохранности свидетельств, представленных в электронной форме. Стандарты на отдельные процессы управления ИБ и оценку безопасности ИТ. ISO/IEC 13335 - методы и средства обеспечения безопасности информационных технологий. ISO/IEC 15408 и ISO/IEC 18045:2008 - общие критерии и методология оценки безопасности информационных технологий. ISO 19011:2011 и ГОСТ Р ИСО 19011-2003 - рекомендации по аудиту систем менеджмента. BS 25999 и ГОСТ Р 53647 – управление непрерывностью бизнеса.	2	2	0	8			
	Тема: Отраслевые стандарты в области управления ИБ - стандарты банковской системы Российской Федерации. СТО БР ИББС-1.0 - общие положения в области обеспечения ИБ организаций банковской системы Российской Федерации. СТО БР ИББС-1.1- аудит ИБ. СТО БР ИББС-1.2 - методика оценки соответствия ИБ организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0.	2	2	0	8			
2	Модуль «Основы управления ИБ» Тема: Политика информационной безопасности. Понятия политики обеспечения ИБ и политики ИБ организации. Причины выработки политики ИБ. Основные требования и принципы, учитываемые при	4	4	0	10	1- 6	Самостоятельное изучение рекомендуемой основной и	тестирование, практическое задание, контрольная

	разработке и внедрении политики ИБ. Содержание политики ИБ.						дополнительной литературы.	работа
	Тема: Содержание корпоративной политики ИБ. Содержание частных политик ИБ. Жизненный цикл политики ИБ. Разработка политики ИБ. Внедрение политики ИБ. Применение политики ИБ. Аннулирование политики ИБ. Ответственность за исполнение политики ИБ.	2	2	0	8			
	Тема: Управление и система управления информационной безопасностью. Необходимость управления обеспечением ИБ организации. Деятельность по обеспечению ИБ организации как процесс.	2	2	0	10			
	Тема: Определение управления ИБ организации. Управление ИБ информационно-телекоммуникационных технологий организации. Система управления ИБ организации Область действия СУИБ. Документальное обеспечение СУИБ. Политика СУИБ. Поддержка СУИБ со стороны руководства организации.	2	2	0	8			
Всего:		18	18	0	72			

Семестр 8

№	Тема и содержание	Форма изучения материалов: лекции, практические занятия, семинарские занятия, лабораторные работы, самостоятельная работа и трудоемкость (в часах)				Основная и дополнительная литература, рекомендуемая студентам (номера из списка)	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	9
1	Модуль «Основы управления рисками ИБ»					1- 6	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	тестирование, практическое задание, контрольная работа, лабораторная работа
	Тема: Создание СУИБ на предприятии. Управление рисками. Основные понятия. Метод оценки рисков на основе модели угроз и уязвимостей.	2	2	0	10			
	Тема: Расчет рисков по угрозе информационной безопасности. Методика оценки рисков информационной безопасности компании Digital Security.	2	2	4	12			
	Тема: Метод оценки рисков на основе модели информационных потоков. Расчет рисков по угрозе целостности. Управление безопасностью как элемент системы управления рисками.	2	2		10			
	Качественные методики управления рисками. COBRA. RA Software Tool. Количественные методики управления рисками. Метод CRAMM.	2	2	4	12			
2	Модуль «Процессы управления ИБ»					1- 6	Самостоятельное изучение рекомендуемой основной и дополнительной литературы.	тестирование, практическое задание, контрольная работа, лабораторная работа
	Тема: Процессный подход в рамках управления ИБ.	2	0	0	24			
	Тема: Планирование СУИБ. Реализация СУИБ. Проверка СУИБ. Совершенствование СУИБ.	2	2		12			
	Тема: Работа с процессами СУИБ организации. Задание процесса СУИБ. Идентификация процессов СУИБ организации. Документирование и описание процесса СУИБ.	2	2	4	12			
	Тема: Стратегии построения и внедрения СУИБ. Построение и внедрение СУИБ в целом. Построение и внедрение процессов СУИБ по отдельности..	2	2	0	10			
	Тема: Мониторинг и измерение параметров процесса СУИБ. Внешний аудит. Внутренний аудит	2	4	6	12			

Всего:	18	18	18	90	

Приложение 2

Рейтинг-план дисциплины

Основы управления информационной безопасностью

Направление 10.03.01 Информационная безопасность курс 4, семестр 7

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1. Системы управления ИБ				
Текущий контроль				20
1. Практическая работа	10	2	0	20
Рубежный контроль				
1. Тест	30	1	0	30
Всего		3	0	50
Модуль 2 Основы управления ИБ				
Текущий контроль				30
1. Практическая работа	10	3	0	30
Рубежный контроль				
1. Контрольная работа	10	1	0	10
2. Тест	10	1	0	10
Всего		4	0	50
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				

Рейтинг-план дисциплины

Основы управления информационной безопасностью

Направление 10.03.01 Информационная безопасность курс 4, семестр 8

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1. Основы управления рисками ИБ				
Текущий контроль				20
1. Лабораторная работа	7	2	0	14
2. Практическая работа	6	1	0	5
Рубежный контроль				
Тест	15	1	0	15
Всего		3	0	35
Модуль 2. Процессы управления ИБ				
Текущий контроль				20
1. Лабораторная работа	7	2	0	14
2. Практическая работа	6	1	0	5
Рубежный контроль				
Тест	15	1	0	15
Всего		3	0	35
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.Экзамен	30	1	0	30