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

Утверждено:
на заседании кафедры
протокол № 9 от 24.04.2020
Зав. кафедрой / А.С. Исмагилова

Согласовано:
Председатель УМК института
/ Р.А. Гильмутдинова

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Управление информационной безопасностью

Б1.В.1.02 (вариативная)

Программа специалитета

Специальность
10.05.05 Безопасность информационных технологий в правоохранительной сфере

Специализация
Технологии защиты информации в правоохранительной сфере

Квалификация
Специалист по защите информации

Разработчик (составитель)
Старший преподаватель И.В. Салов

к.х.н. / А.А. Корнилова

Для приема: 2020 г.

Уфа 2020 г.

Составитель / составители: И.В. Салов, А.А. Корнилова

Рабочая программа дисциплины актуализирована на заседании кафедры управления информационной безопасностью № 9 от 24.04.2020

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	базовые и основные принципы организации профессионального коллектива	– Способность принимать организационно-управленческие решения (ОК-8)	
	природу преступности и её основные характеристики и детерминанты, особенности лиц, совершивших преступления	– Способность участвовать в выявлении, предупреждении, пресечении, раскрытии и расследовании преступлений в качестве специалиста, реализовывать мероприятия по получению информации, анализировать, оценивать ее и эффективно использовать в интересах выявления, предупреждения, пресечения, раскрытия и расследования преступлений (ПК-8)	
	подходы обоснования затрат на информационную безопасность	– Способность принимать управленческие решения преступлений (ПК-15)	
	понятие документирования и документооборота	– Способность осуществлять документационное обеспечение управленческой деятельности (ПК-16)	
	тенденции в области развития информационных систем и динамику проблем информационной безопасности	– Способность разрабатывать предложения по совершенствованию системы управления безопасностью информации (ПК-18)	
	методы воздействия на индивидуальное и массовое сознание	– Способность осуществлять противодействие деструктивным и негативным информационно-психологическим воздействиям (ПК-24)	
	стандарты построения систем информационной безопасности и стандарты оценки степени защиты систем информационной безопасности объектов	– Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности (ПСК-3)	
Умения	находить организационно-	– Способность принимать организационно-управленческие	

	управленческие решения в нестандартных условиях, в том числе и в условиях риска	решения (ОК-8)	
	выявлять обстоятельства, способствующие преступности, планировать и осуществлять деятельность по предупреждению и профилактике преступлений и иных правонарушений	– Способность участвовать в выявлении, предупреждении, пресечении, раскрытии и расследовании преступлений в качестве специалиста, реализовывать мероприятия по получению информации, анализировать, оценивать ее и эффективно использовать в интересах выявления, предупреждения, пресечения, раскрытия и расследования преступлений (ПК-8)	
	оценивать эффективность управленческих решений и анализировать экономические показатели деятельности подразделения	– Способность принимать управленческие решения преступлений (ПК-15)	
	применять нормы информационного права в профессиональной деятельности	– Способность осуществлять документационное обеспечение управленческой деятельности (ПК-16)	
	использовать базовые возможности информационных систем для решения задач фирмы и внедрять компоненты АИС предприятия, обеспечивающие информационную безопасность и достижение стратегических целей и организовать поддержку обеспечения выполнения этой организацией своих функций на основе безопасных АИС	– Способность разрабатывать предложения по совершенствованию системы управления безопасностью информации (ПК-18)	
	использовать различные методы и способы предотвращения и позитивного разрешения конфликтов	– Способность осуществлять противодействие деструктивным и негативным информационно-психологическим воздействиям (ПК-24)	
	интерпретировать и обобщать данные,	– Способность проводить анализ исходных данных для	

	формулировать выводы и рекомендации	проектирования подсистем и средств обеспечения информационной безопасности (ПСК-3)	
Владения (навыки / опыт деятельности)	способностью проявлять инициативу	– Способность принимать организационно-управленческие решения (ОК-8)	
	навыками применения средств предупреждения и профилактики правонарушений	– Способность участвовать в выявлении, предупреждении, пресечении, раскрытии и расследовании преступлений в качестве специалиста, реализовывать мероприятия по получению информации, анализировать, оценивать ее и эффективно использовать в интересах выявления, предупреждения, пресечения, раскрытия и расследования преступлений (ПК-8)	
	навыками обоснования, выбора, реализации и контроля результатов управленческого решения	– Способность принимать управленческие решения преступлений (ПК-15)	
	навыками работы с документами ограниченного доступа и обеспечения их защиты	– Способность осуществлять документационное обеспечение управленческой деятельности (ПК-16)	
	навыками выявления и устранения угроз информационной безопасности	– Способность разрабатывать предложения по совершенствованию системы управления безопасностью информации (ПК-18)	
	навыками установления психологического контакта, визуальной психодиагностики и психологического воздействия	– Способность осуществлять противодействие деструктивным и негативным информационно-психологическим воздействиям (ПК-24)	
	интерпретации и обобщения результатов, формулирования рекомендаций и принятия решений	– Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности (ПСК-3)	

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

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

Дисциплина изучается на 5 курсе в 9-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 специальности 10.05.05 Безопасность информационных технологий в правоохранительной сфере специализации «Технологии защиты информации в правоохранительной сфере»: «Информационная безопасность автоматизированных систем».

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

ОК-8: Способность принимать организационно-управленческие решения

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения для экзамена и курсового проекта			
		2 («неудовлетворительно»)	3 («удовлетворительно»)	4 («хорошо»)	5 («отлично»)
Первый этап (уровень) Пороговый	Знать: базовые и основные принципы организации профессионального коллектива	Не знает	В целом знает базовые и основные принципы организации профессионального коллектива, но испытывает трудности при их описании	Знает базовые и основные принципы организации профессионального коллектива, но допускает незначительные ошибки при их описании	Знает базовые и основные принципы организации профессионального коллектива
Второй этап (уровень) Базовый	Уметь: находить организационно-управленческие решения в нестандартных условиях, в том числе и в условиях риска	Не умеет	В целом умеет находить организационно-управленческие решения в нестандартных условиях, в том числе и в условиях риска, но допускает значительные ошибки	Умеет находить организационно-управленческие решения в нестандартных условиях, в том числе и в условиях риска, но допускает незначительные ошибки	Умеет находить организационно-управленческие решения в нестандартных условиях, в том числе и в условиях риска
Третий этап (уровень) Повышенный	Владеть: способностью проявлять инициативу	Не владеет	В целом владеет способностью проявлять инициативу, но испытывает трудности в условиях конкретной задачи	Владеет способностью проявлять инициативу, но допускает незначительные ошибки	Владеет способностью проявлять инициативу

ПК-8: Способность участвовать в выявлении, предупреждении, пресечении, раскрытии и расследовании преступлений в качестве специалиста, реализовывать мероприятия по получению информации, анализировать, оценивать ее и эффективно использовать в интересах выявления, предупреждения, пресечения, раскрытия и расследования преступлений

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: природу преступности и её основные	Не знает	В целом знает природу преступности и её основные характеристики	Знает природу преступности и её основные	Знает природу преступности и её основные

	характеристики и детерминанты, особенности лиц, совершивших преступления		и детерминанты, особенности лиц, совершивших преступления, но испытывает трудности при их описании	характеристики и детерминанты, особенности лиц, совершивших преступления, но допускает незначительные ошибки при их описании	характеристики и детерминанты, особенности лиц, совершивших преступления
Второй этап (уровень) Базовый	Уметь: выявлять обстоятельства, способствующие преступности, планировать и осуществлять деятельность по предупреждению и профилактике преступлений и иных правонарушений	Не умеет	В целом умеет выявлять обстоятельства, способствующие преступности, планировать и осуществлять деятельность по предупреждению и профилактике преступлений и иных правонарушений, но допускает значительные ошибки	Умеет выявлять обстоятельства, способствующие преступности, планировать и осуществлять деятельность по предупреждению и профилактике преступлений и иных правонарушений, но допускает незначительные ошибки	Умеет выявлять обстоятельства, способствующие преступности, планировать и осуществлять деятельность по предупреждению и профилактике преступлений и иных правонарушений
Третий этап (уровень) Повышенный	Владеть: навыками применения средств предупреждения и профилактики правонарушений	Не владеет	В целом владеет навыками применения средств предупреждения и профилактики правонарушений, но испытывает трудности в условиях конкретной задачи	Владеет навыками применения средств предупреждения и профилактики правонарушений, но допускает незначительные ошибки	Владеет навыками применения средств предупреждения и профилактики правонарушений

ПК-15: Способность принимать управленческие решения преступлений

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: подходы обоснования затрат на информационную безопасность	Не знает	В целом знает подходы обоснования затрат на информационную безопасность, но испытывает трудности при их описании	Знает подходы обоснования затрат на информационную безопасность, но допускает незначительные ошибки при их описании	Знает подходы обоснования затрат на информационную безопасность
Второй этап (уровень) Базовый	Уметь: оценивать эффективность управленческих решений и анализировать экономические показатели деятельности подразделения	Не умеет	В целом умеет оценивать эффективность управленческих решений и анализировать экономические показатели деятельности подразделения, но допускает значительные ошибки	Умеет оценивать эффективность управленческих решений и анализировать экономические показатели деятельности подразделения, но допускает незначительные ошибки	Умеет оценивать эффективность управленческих решений и анализировать экономические показатели деятельности подразделения
Третий этап (уровень) Повышенный	Владеть: навыками обоснования, выбора, реализации и контроля результатов управленческого решения	Не владеет	В целом владеет навыками обоснования, выбора, реализации и контроля результатов управленческого решения, но испытывает трудности в условиях конкретной задачи	Владеет навыками обоснования, выбора, реализации и контроля результатов управленческого решения, но допускает незначительные ошибки	Владеет навыками обоснования, выбора, реализации и контроля результатов управленческого решения

ПК-16: Способность осуществлять документационное обеспечение управленческой 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: понятие документирования и документооборота	Не знает	В целом знает понятие документирования и документооборота, но испытывает трудности при их описании	Знает понятие документирования и документооборота, но допускает незначительные	Знает понятие документирования и документооборота

				ошибки при их описании	
Второй этап (уровень) Базовый	Уметь: применять нормы информационного права в профессиональной деятельности	Не умеет	В целом умеет применять нормы информационного права в профессиональной деятельности, но допускает значительные ошибки	Умеет применять нормы информационного права в профессиональной деятельности, но допускает незначительные ошибки	Умеет применять нормы информационного права в профессиональной деятельности
Третий этап (уровень) Повышенный	Владеть: навыками работы с документами ограниченного доступа и обеспечения их защиты	Не владеет	В целом владеет навыками работы с документами ограниченного доступа и обеспечения их защиты, но испытывает трудности в условиях конкретной задачи	Владеет навыками работы с документами ограниченного доступа и обеспечения их защиты, но допускает незначительные ошибки	Владеет навыками работы с документами ограниченного доступа и обеспечения их защиты

ПК-18: Способность разрабатывать предложения по совершенствованию системы управления безопасностью 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) Пороговый	Знать: тенденции в области развития информационных систем и динамику проблем информационной безопасности	Не знает	В целом знает тенденции в области развития информационных систем и динамику проблем информационной безопасности, но испытывает трудности при их описании	Знает тенденции в области развития информационных систем и динамику проблем информационной безопасности, но допускает незначительные ошибки при их описании	Знает тенденции в области развития информационных систем и динамику проблем информационной безопасности
Второй этап (уровень) Базовый	Уметь: использовать базовые возможности информационных систем для решения задач фирмы и внедрять компоненты АИС предприятия, обеспечивающие информационную безопасность и достижение стратегических целей и организовать поддержку обеспечения выполнения этой организацией своих функций на основе безопасных АИС	Не умеет	В целом умеет использовать базовые возможности информационных систем для решения задач фирмы и внедрять компоненты АИС предприятия, обеспечивающие информационную безопасность и достижение стратегических целей и организовать поддержку обеспечения выполнения этой организацией своих функций на основе безопасных АИС, но допускает значительные ошибки	Умеет использовать базовые возможности информационных систем для решения задач фирмы и внедрять компоненты АИС предприятия, обеспечивающие информационную безопасность и достижение стратегических целей и организовать поддержку обеспечения выполнения этой организацией своих функций на основе безопасных АИС, но допускает незначительные ошибки	Умеет использовать базовые возможности информационных систем для решения задач фирмы и внедрять компоненты АИС предприятия, обеспечивающие информационную безопасность и достижение стратегических целей и организовать поддержку обеспечения выполнения этой организацией своих функций на основе безопасных АИС
Третий этап (уровень) Повышенный	Владеть: навыками выявления и устранения угроз информационной безопасности	Не владеет	В целом владеет навыками выявления и устранения угроз информационной безопасности, но испытывает трудности в условиях конкретной задачи	Владеет навыками выявления и устранения угроз информационной безопасности, но допускает незначительные ошибки	Владеет навыками выявления и устранения угроз информационной безопасности

ПК-24: Способность осуществлять противодействие деструктивным и негативным информационно-психологическим воздействиям

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: методы воздействия на индивидуальное и	Не знает	В целом знает методы воздействия на индивидуальное и	Знает методы воздействия на индивидуальное и	Знает методы воздействия на индивидуальное и

	массовое сознание		массовое сознание, но допускает значительные ошибки при их описании	массовое сознание, но допускает незначительные ошибки при их описании	массовое сознание
Второй этап (уровень) Базовый	Уметь: использовать различные методы и способы предотвращения и позитивного разрешения конфликтов	Не умеет	В целом умеет использовать различные методы и способы предотвращения и позитивного разрешения конфликтов, но допускает ошибки	Умеет использовать различные методы и способы предотвращения и позитивного разрешения конфликтов, но допускает незначительные ошибки	Умеет использовать различные методы и способы предотвращения и позитивного разрешения конфликтов
Третий этап (уровень) Повышенный	Владеть: навыками установления психологического контакта, визуальной психодиагностики и психологического воздействия	Не владеет	В целом владеет психологического контакта, визуальной психодиагностики и психологического воздействия, но испытывает затруднения в условиях конкретной задачи	Владеет психологического контакта, визуальной психодиагностики и психологического воздействия, но допускает незначительные ошибки	Владеет психологического контакта, визуальной психодиагностики и психологического воздействия

ПСК-3: Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности

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: стандарты построения систем информационной безопасности и стандарты оценки степени защиты систем информационной безопасности объектов	Не знает	В целом знает стандарты построения систем информационной безопасности и стандарты оценки степени защиты систем информационной безопасности объектов, но допускает значительные ошибки	Знает стандарты построения систем информационной безопасности и стандарты оценки степени защиты систем информационной безопасности объектов, но допускает незначительные ошибки	Знает стандарты построения систем информационной безопасности и стандарты оценки степени защиты систем информационной безопасности объектов
Второй этап (уровень) Базовый	Уметь: интерпретировать и обобщать данные, формулировать выводы и рекомендации	Не умеет	В целом умеет интерпретировать и обобщать данные, формулировать выводы и рекомендации, но допускает значительные ошибки	Умеет интерпретировать и обобщать данные, формулировать выводы и рекомендации, но допускает незначительные ошибки	Умеет интерпретировать и обобщать данные, формулировать выводы и рекомендации
Третий этап (уровень) Повышенный	Владеть: интерпретации и обобщения результатов, формулирования рекомендаций и принятия решений	Не владеет	В целом владеет интерпретации и обобщения результатов, формулирования рекомендаций и принятия решений, но допускает ошибки	Владеет интерпретации и обобщения результатов, формулирования рекомендаций и принятия решений, допускает незначительные ошибки	Владеет интерпретации и обобщения результатов, формулирования рекомендаций и принятия решений

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	базовые и основные принципы организации	ОК-8	практическая работа, тест

Знать	профессионального коллектива		
	природу преступности и её основные характеристики и детерминанты, особенности лиц, совершивших преступления	ПК-8	практическая работа, тест
	подходы обоснования затрат на информационную безопасность	ПК-15	практическая работа, тест
	понятие документирования и документооборота	ПК-16	практическая работа, тест
	тенденции в области развития информационных систем и динамику проблем информационной безопасности	ПК-18	практическая работа, тест
	методы воздействия на индивидуальное и массовое сознание	ПК-24	практическая работа, тест
	стандарты построения систем информационной безопасности и стандарты оценки степени защиты систем информационной безопасности объектов	ПСК-3	практическая работа, тест
2-й этап Уметь	находить организационно-управленческие решения в нестандартных условиях, в том числе и в условиях риска	ОК-8	практическая работа, тест
	выявлять обстоятельства, способствующие преступности, планировать и осуществлять деятельность по предупреждению и профилактике преступлений и иных правонарушений	ПК-8	практическая работа, тест
	оценивать эффективность управленческих решений и анализировать экономические показатели деятельности подразделения	ПК-15	практическая работа, тест
	применять нормы	ПК-16	практическая работа,

	информационного права в профессиональной деятельности		тест
	использовать базовые возможности информационных систем для решения задач фирмы и внедрять компоненты АИС предприятия, обеспечивающие информационную безопасность и достижение стратегических целей и организовать поддержку обеспечения выполнения этой организацией своих функций на основе безопасных АИС	ПК-18	практическая работа, тест
	использовать различные методы и способы предотвращения и позитивного разрешения конфликтов	ПК-24	практическая работа, тест
	интерпретировать и обобщать данные, формулировать выводы и рекомендации	ПСК-3	практическая работа, тест
3-й этап Владеть	способностью проявлять инициативу	ОК-8	практическая работа, тест
	навыками применения средств предупреждения и профилактики правонарушений	ПК-8	практическая работа, тест
	навыками обоснования, выбора, реализации и контроля результатов управленческого решения	ПК-15	практическая работа, тест
	навыками работы с документами ограниченного доступа и обеспечения их защиты	ПК-16	практическая работа, тест
	навыками выявления и устранения угроз информационной безопасности	ПК-18	практическая работа, тест
	навыками установления психологического контакта, визуальной психодиагностики и психологического воздействия	ПК-24	практическая работа, тест

	интерпретации и обобщения результатов, формулирования рекомендаций и принятия решений	ПСК-3	практическая работа, тест

Экзамен

Экзамен является оценочным средством для всех этапов освоения компетенции.

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

Специальность 10.05.05 Безопасность информационных технологий в правоохранительной сфере

Дисциплина Управление информационной безопасностью

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Политика информационной безопасности.
2. Методика оценки рисков информационной безопасности компании Digital Security.

Зав. Кафедрой УИБ А.С. Исмагилова

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.

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.

Темы практических работ

1) Разработка нормативных документов организации на основе стандартов 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) Метод оценки рисков на основе модели угроз и уязвимостей.
3) Расчет рисков по угрозе информационной безопасности. Методика оценки рисков информационной безопасности компании Digital Security.
4) Использование средства полного анализа рисков экспертной системы «Авангард».
5) Журналы регистрации событий на примере ОС Windows.
6) Инструментальные средства проверки ИБ.
7) Виды проверок СУИБ.
8) Возможности системы управления событиями информационной безопасности (SIEM -системы).

Типовая практическая работа

Модуль 2. Особенности реализация СМИБ.

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
Модуль 1, Модуль 2	работа выполнена неполно, не показано общее понимание вопроса, имелись затруднения или допущены ошибки в 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	0/3/5

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.

Модуль 1, 2

Тестирование

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
Один вопрос теста Тест (все 25 вопросов)	Неправильный ответ / Правильный ответ	0/0,6 0/15

Примерная тематика курсовых проектов

1. Средства полного анализа рисков.
2. Анализ рисков в области защиты информации. Национальные особенности защиты информации.
3. Анализ рисков в области защиты информации и технология управления информационными рисками.
4. Ведомственные и корпоративные стандарты управления ИБ.
5. Организация аудита безопасности.
6. Стандарт США NIST SP 800-30.
7. Инструментальные средства анализа рисков. COBRA.
8. Международная практика защиты информации.
9. Актуальность аудита безопасности.
10. Международный стандарт ISO 17799.
11. Основные понятия и определения аудита безопасности.
12. Инструментальные средства анализа рисков. RA Software Tool.
13. Идентификация угроз и уязвимостей.
14. Средства полного анализа рисков. Метод CRAMM.
15. Варианты аудита безопасности.
16. Средства полного анализа рисков. Экспертная система «Авангард».
17. Вопросы анализа рисков и управления ими. Выбор допустимого уровня риска.
18. Информационная безопасность бизнеса.
19. Развитие службы информационной безопасности.
20. Постановка задачи анализа рисков.
21. Обзор стандарта BS 7799.
22. Развитие стандарта ISO 17799.
23. Германский стандарт BSI.
24. Сравнение стандартов ISO 17799 и BSI.
25. Вопросы анализа рисков и управления ими. Идентификация рисков
26. Вопросы анализа рисков и управления ими. Оценивание рисков.
27. Вопросы анализа рисков и управления ими. Измерение рисков.

28. Вопросы анализа рисков и управления ими. Выбор контрмер и оценка их эффективности.
29. Разработка корпоративной методики анализа рисков. Постановка задачи.
30. Разработка корпоративной методики анализа рисков. Методы оценивания информационных рисков.
31. Разработка корпоративной методики анализа рисков. Табличные методы оценки рисков.
32. Инструментальные средства анализа рисков. Инструментарий базового уровня.
33. Инструментальные средства анализа рисков. Справочные и методические материалы.
34. Средства полного анализа рисков. Средства компании MethodWare.
35. Средства полного анализа рисков. RiskWatch.
36. Аудит безопасности в соответствии с BS 7799, часть 2.
37. Сертификация и аудит: организационные аспекты.
38. Аудит безопасности. Методика проведения аудита.
39. Аудит безопасности. Этапы проведения аудита.

Критерии оценивания курсового проекта

Оценка «отлично»:
работа выполнена в полном объеме и изложена грамотным языком в определенной логической последовательности с точным использованием специализированной терминологии; показано уверенное владение прикладными программами.
Оценка «хорошо»:
работа выполнена в полном объеме, но имеет один из недостатков: в работе допущены один-два недочета при освещении основного содержания ответа; нет определенной логической последовательности, неточно используется специализированная терминология;
Оценка «удовлетворительно»:
работа выполнена неполно, не показано общее понимание вопроса, имелись затруднения или допущены ошибки в определении понятий, использовании терминологии, при знании теоретического материала выявлена недостаточная сформированность основных умений и навыков.

4.3. Рейтинг-план дисциплины

Рейтинг–план дисциплины представлен в приложении 1.

5. Учебно-методическое и информационное обеспечение дисциплины

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

Основная литература

1. Шаньгин, В.Ф. Информационная безопасность [Электронный ресурс] : учебное пособие / В.Ф. Шаньгин. — Электрон. дан. — Москва : ДМК Пресс, 2014. — 702 с. — Режим доступа: https://e.lanbook.com/book/50578. — Загл. с экрана.

Дополнительная литература

2. Шаньгин, В.Ф. Защита компьютерной информации [Электронный ресурс] : учебное пособие / В.Ф. Шаньгин. — Электрон. дан. — Москва : ДМК Пресс, 2010. — 544 с. — Режим доступа: https://e.lanbook.com/book/1122. — Загл. с экрана.

3. Малюк, А.А. Защита информации в информационном обществе : учебное пособие / А.А. Малюк. - Москва : Горячая линия-Телеком, 2015. - 229 с. : ил., схем., табл. - Библиогр. в кн. - ISBN 978-5-9912-0481-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=457170

4. Милославская, Н.Г. Управление инцидентами информационной безопасности и непрерывностью бизнеса : учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. - Москва : Горячая линия - Телеком, 2013. - 170 с. : ил. - (Вопросы управления информационной безопасностью. Вып. 3). - Библиогр. в кн. - ISBN 978-5-9912-0273-2 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=253577

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

1. Справочная правовая система «КонсультантПлюс» – http://www.consultant-plus.ru.
2. Электронная библиотечная система «Университетская библиотека онлайн» – https://biblioclub.ru.
3. Электронная библиотечная система издательства «Лань» – https://e.lanbook.com/
4. Электронный каталог Библиотеки БашГУ – http://www.bashlib.ru/catalogi/
5. www.fstec.ru –сайт ФСТЭК России
6. www.fsb.ru – сайт ФСБ России
7. http://window.edu.ru/ – Наиболее обширная электронная база учебников и методических материалов на сайте информационной системы «Единое окно доступа к образовательным ресурсам»;
8. http://univertv.ru/video/matematika/ – Открытый образовательный видеопортал UniverTV.ru. Образовательные фильмы на различные темы. Лекции в ведущих российских и зарубежных вузах. Научная конференция или научно-популярная лекция по интересующему вопросу);
9. www.newlibrary.ru – Новая электронная библиотека;
10. www. edu.ru – Федеральный портал российского образования;
11. www.elibrary.ru – Научная электронная библиотека;
12. www.nehudlit.ru – Электронная библиотека учебных материалов.
13. 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.
14. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные.
15. Система централизованного тестирования БашГУ (Moodle). GNU General Public License.
16. Правовая система «КонсультантПлюс». Договор №28826 от 09.01.2019 г. Лицензии бессрочные.

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	Лекции, практические занятия, текущий контроль, промежуточная аттестация,	**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

(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 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 № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус). **3.** ***учебная аудитория для курсового проектирования (выполнения курсовых работ):*** аудитория № 613 (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),	экзамен	радиомикрофоны AKG WMS 40 – 2шт., Интер-ая система со встроенным короткофокусным проекто-ром Promethean ActivBoard 387 RPO MOUNT EST -1 шт., Ком-ер встраиваемый в кафедру INTEL Core i3-4150/DDr3 4 Gb/HDD, Экран настенный Draper Luma AV(1:1) 96/96”244*244MV (XT1000E) -1 шт., Настольный интерактивный дисплей , ActivPanel 21S – 1 шт. , Матричный коммутатор сигналов интерфейса HDMI CMPRO 4H4H – 1 шт. , Мультимедиа-проектор Panasonic PT-EW640E - 1 шт., Двух-полосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W)(белый) -6 шт., Петличный радиомикрофон AKG WMS45 – 1 шт. , Терминал видео конференц-связи LifeSize Icon 600 Camera 10x Phone 2nd Generation – 1 шт., Экран настенный Draper Luma AV(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 APAPT MA1225 – 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 APAPT MA1225 – 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 пюпитром. **Аудитория № 516** Учебная мебель, доска, кресла секционные последующих рядов с пюпитром, мобильное мультимедийное оборудование: проектор ASK Proxima, ноутбук HP, экран.

компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус). **6. *помещения для самостоятельной работы:*** аудитория № 613 (гуманитарный корпус), читальный зал библиотеки аудитория 402 (гуманитарный корпус).		**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. **Аудитория № 523** Шкаф-стеллаж – 4 шт., стол-1 шт., стул – 2 шт.

Приложение 1

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

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ
дисциплины Управление информационной безопасностью на 9 семестре
ОФО

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (ЗЕТ / часов)	7 ЗЕТ / 252 часов
Учебных часов на контактную работу с преподавателем:	75,2
лекций	36
практических/ семинарских	36
лабораторных	0
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	3,2
Учебных часов на самостоятельную работу обучающихся (СР)	142
Учебных часов на подготовку к экзамену/зачету/дифференцированному зачету (Контроль)	34,8

Форма контроля:
экзамен 9 семестр

№	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 1. Создание СУИБ на предприятии. 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. 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	2 2	0 0	0 0	7 7	1- 5	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	практическая работа, тест

	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. 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. 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. Тема: Создание СУИБ на предприятии. Управление рисками. Основные понятия. Метод оценки рисков на основе модели угроз и уязвимостей. Тема: Расчет рисков по угрозе информационной безопасности. Методика оценки рисков информационной безопасности компании Digital Security. Тема: Метод оценки рисков на основе модели информационных потоков. Расчет рисков по угрозе целостности. Управление безопасностью как элемент системы управления рисками. Тема: Качественные методики управления рисками. COBRA. RA Software Tool. Количественные методики управления рисками. Метод CRAMM. Тема: Средства полного анализа рисков. Экспертная система «Авангард».	2 2 2 2 2 2 2	4 0 4 4 0 0 4	0 0 0 0 0 0 0	8 8 8 8 8 8 8			
2	Модуль 2. Особенности реализация СМИБ. Тема: Методика определения угроз безопасности	2	0	0	8	1- 5	Самостоятельное изучение рекомендуемой	практическая работа, тест

	информации в информационных системах. Оценка возможностей нарушителей по реализации угроз безопасности информации. Типы нарушителя. Мотивация нарушителя. Виды и потенциал нарушителя. Возможные способы реализации угроз безопасности информации.						основной и дополнительной литературы	
	Тема: Определение актуальных угроз безопасности информации в информационной системе. Оценка вероятности (возможности) реализации угрозы безопасности информации. Показатели, характеризующие проектную защищенность информационной системы. Оценка степени возможного ущерба от реализации угрозы безопасности информации. Возможные негативные последствия от нарушения конфиденциальности, целостности, доступности информации. Характеристика степени ущерба.	2	0	0	8			
	Тема: Определение актуальности угрозы безопасности информации. Рекомендации по формированию экспертной группы и проведению экспертной оценки при определении угроз безопасности информации. Структура модели угроз безопасности информации. Определение потенциала нарушителя, необходимого для реализации угрозы безопасности информации в информационной системе.	2	0	0	8			
	Тема: Журналы регистрации событий. Руководство по управлению журналами регистрации событий компьютерной безопасности (NIST SP 800-92). Журналы регистрации событий в системах защиты информации (СЗИ). Журналы регистрации событий операционных систем. Журналы регистрации событий приложений. Проблемы в управления журналами событий. Нормализация журналов. Генерация и хранение журналов. Обеспечение безопасности журналов. Анализ журналов. Инфраструктура управления журналами. Архитектура системы управления журналами. Функции системы управления журналами. Системы централизованного сбора и хранения журналов, основанные на протоколе syslog. Дополнительные типы ПО управления журналами событий. Планирование управления журналами. Определение и внедрение политик журналирования. Разработка инфраструктуры управления журналами. Операционные аспекты управления журналами.	2	4	0	8			
	Тема: Инструментальные средства проверки ИБ. Национальный стандарт Российской Федерации «Информационная технология. Методы и средства обеспечения безопасности. Рекомендации для аудиторов в отношении мер и средств контроля и управления информационной безопасностью.» Тестирование «вслепую».	2	4	0	8			

	«Дважды слепое» тестирование. Тестирование методом «серого ящика». Тестирование методом «двойного серого ящика». Тестирование методом «тандема». Реверсивное тестирование. Системы анализа защищенности. Системы обнаружения вторжения. Системы предотвращения вторжения.							
	Тема: Мониторинг ИБ. Аудит ИБ. Основные направления деятельности в области аудита безопасности информации. Виды аудита ИБ. Внутренний аудит ИБ. Внешний аудит ИБ. Оценка состояния СМИБ со стороны руководства.	2	4	0	8			
	Тема: Порядок выявления и реагирования на инциденты информационной безопасности. Планирование и подготовка менеджмента инцидентов ИБ. Использование менеджмента инцидентов ИБ. Улучшение менеджмента инцидентов ИБ. Примеры инцидентов информационной безопасности и их причин. Создание группы реагирования на инциденты информационной безопасности	2	4	0	8			
	Тема: . Системы управления событиями информационной безопасности (SIEM -системы). Виды систем управления событиями информационной безопасности.	2	4	0	8			
	Тема: Способы оценки информационной безопасности. Основные элементы процесса оценки ИБ. Мероприятия и выходные данные процесса оценки ИБ. Способы измерения атрибутов объекта оценки ИБ. Модель оценки информационной безопасности на основе оценки процессов. Оценка информационной безопасности на основе модели зрелости процессов. Риск-ориентированная оценка информационной безопасности.	2	0	0	8			
Всего:		36	36	0	142			

Приложение 2

Рейтинг-план дисциплины

Управление информационной безопасностью

Специальность 10.05.05 Безопасность информационных технологий в правоохранительной сфере курс 5, семестр 9

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1. Создание СУИБ на предприятии.				
Текущий контроль				20
1. Практическая работа	5	4	0	20
Рубежный контроль				
Тест	15	1	0	15
Всего		5	0	35
Модуль 2. Особенности реализация СМИБ.				
Текущий контроль				20
1. Практическая работа	5	4	0	20
Рубежный контроль				
Тест	15	1	0	15
Всего		5	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