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

Утверждено:
на заседании кафедры
протокол № 11 от «20» июня 2019 г.
Зав. кафедрой _____ / А.С. Исмагилова

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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Информационная безопасность в правоохранительной сфере

Б1.Б.31.01 (базовая)

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)
к.х.н., ст.преподаватель _____ / А.А. Корнилова

Ст.преподаватель _____ / И.В. Салов

Для приема: 2019 г.

Уфа 2019 г.

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

Рабочая программа дисциплины актуализирована на заседании кафедры управления информационной безопасностью № 11 от «20» июня 2019 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	основные понятия информатики; разделы информатики, состав программного обеспечения, файловые системы, технические средства, актуальные характеристики основных периферийных устройств компьютеров, виды операционных систем, историю и тенденции их развития	– Способность работать с различными источниками информации, информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации (ОК-12)	
	общеметодологические принципы теории информационной безопасности	– Способность формировать и реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации, с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз (ПК-1)	
	понятие системы управления, основные виды структур, принципы системного подхода к анализу структур	– способностью осуществлять организационно-правовое обеспечение деятельности по получению, накоплению, обработке, анализу, использованию информации и защите объектов информатизации, информационных технологий и ресурсов (ПК-13)	
	средства контроля контента	– Способность анализировать структуру и содержание информационных массивов и информационных процессов на предмет выявления угроз безопасности (ПК-22)	
	способы применения методов аналитической разведки, осуществления оперативно-аналитического поиска, оперативно-розыскного	– Способность применять методы аналитической разведки, осуществлять оперативно-аналитический поиск, оперативно-розыскной анализ, идентификацию, диагностику, прогнозирование;	

	анализа, идентификации, диагностики, прогнозирования; криминалистической диагностики	криминалистическую диагностику (ПК-23)	
Умения	понимать и применять на практике компьютерные технологии для решения различных задач комплексного и гармонического анализа	– Способность работать с различными источниками информации, информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации (ОК-12)	
	реализовывать на практике принципы политики безопасности	– Способность формировать и реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации, с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз (ПК-1)	
	использовать методы количественного представления информации и основные закономерности ее преобразования в каналах при выполнении комплекса мер по информационной безопасности	– способностью осуществлять организационно-правовое обеспечение деятельности по получению, накоплению, обработке, анализу, использованию информации и защите объектов информатизации, информационных технологий и ресурсов (ПК-13)	
	использовать базовые возможности информационных систем для решения задач фирмы	– Способность анализировать структуру и содержание информационных массивов и информационных процессов на предмет выявления угроз безопасности (ПК-22)	
	применять методы аналитической разведки, осуществлять оперативно-аналитический поиск, оперативно-розыскной анализ, идентификацию, диагностику, прогнозирование; криминалистическую	– Способность применять методы аналитической разведки, осуществлять оперативно-аналитический поиск, оперативно-розыскной анализ, идентификацию, диагностику, прогнозирование; криминалистическую диагностику (ПК-23)	

	диагностику		
Владения (навыки / опыт деятельности)	навыками решения практических задач, графическим интерфейсом пользователя, интерфейсом командной строки, стандартными программами, антивирусными программами, сервисным программным обеспечением операционной системы, навыками настройки компьютерной сети, навыками работы с информацией в корпоративных информационных системах	– Способность работать с различными источниками информации, информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации (ОК-12)	
	навыками анализа, обработки и интерпретации результатов решения прикладных задач управления	– Способность формировать и реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации, с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз (ПК-1)	
	навыками организации комплекса мероприятий по защите информации в процессах автоматизированной обработки информации	– способностью осуществлять организационно-правовое обеспечение деятельности по получению, накоплению, обработке, анализу, использованию информации и защите объектов информатизации, информационных технологий и ресурсов (ПК-13)	
	методикой определения видов и форм информации, подверженной угрозам, анализировать угрозы информационно-вычислительным системам	– Способность анализировать структуру и содержание информационных массивов и информационных процессов на предмет выявления угроз безопасности (ПК-22)	
	навыками систематического	– Способность применять методы аналитической разведки,	

	применения методов аналитической разведки, осуществления оперативно-аналитического поиска, оперативно-розыскного анализа, идентификации, диагностики, прогнозирования; криминалистической диагностики	осуществлять оперативно-аналитический поиск, оперативно-розыскной анализ, идентификацию, диагностику, прогнозирование; криминалистическую диагностику (ПК-23)	

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

Дисциплина «Информационная безопасность в правоохранительной сфере» относится к базовой части образовательной программы.

Дисциплина изучается на 3 курсе в 6-м семестре, 4 курс 7-м-семестре.

Цели изучения дисциплины: формирование у студентов основ знаний об информационной безопасности в правоохранительной деятельности, роли и внедрении информации в современном обществе.

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»: «Информатика и информационные технологии в правоохранительной деятельности».

Освоение дисциплины «Информационная безопасность в правоохранительной сфере» служит основой для изучения таких дисциплин, как «Технологии защиты информации в правоохранительной сфере»

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-12: Способность работать с различными источниками информации, информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи 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: основные понятия информатики; разделы информатики, состав программного обеспечения, файловые системы, технические средства, актуальные характеристики	Не знает	В целом знает основные понятия информатики; разделы информатики, состав программного обеспечения, файловые системы, технические средства, актуальные характеристики основных	Знает основные понятия информатики; разделы информатики, состав программного обеспечения, файловые системы,	Знает основные понятия информатики; разделы информатики, состав программного обеспечения, файловые системы, технические средства, актуальные характеристики

	основных периферийных устройств компьютеров, виды операционных систем, историю и тенденции их развития		периферийных устройств компьютеров, виды операционных систем, историю и тенденции их развития, но испытывает трудности при их описании	технические средства, актуальные характеристики основных периферийных устройств компьютеров, виды операционных систем, историю и тенденции их развития, но допускает незначительные ошибки при их описании	основных периферийных устройств компьютеров, виды операционных систем, историю и тенденции их развития
Второй этап (уровень) Базовый	Уметь: понимать и применять на практике компьютерные технологии для решения различных задач комплексного и гармонического анализа	Не умеет	В целом умеет понимать и применять на практике компьютерные технологии для решения различных задач комплексного и гармонического анализа, но допускает значительные ошибки	Умеет понимать и применять на практике компьютерные технологии для решения различных задач комплексного и гармонического анализа, но допускает незначительные ошибки	Умеет понимать и применять на практике компьютерные технологии для решения различных задач комплексного и гармонического анализа
Третий этап (уровень) Повышенный	Владеть: навыками решения практических задач, графическим интерфейсом пользователя, интерфейсом командной строки, стандартными программами, антивирусными программами, сервисным программным обеспечением операционной системы, навыками настройки компьютерной сети, навыками работы с информацией в корпоративных информационных системах	Не владеет	В целом владеет навыками решения практических задач, графическим интерфейсом пользователя, интерфейсом командной строки, стандартными программами, антивирусными программами, сервисным программным обеспечением операционной системы, навыками настройки компьютерной сети, навыками работы с информацией в корпоративных информационных системах, но допускает ошибки	Владеет навыками решения практических задач, графическим интерфейсом пользователя, интерфейсом командной строки, стандартными программами, антивирусными программами, сервисным программным обеспечением операционной системы, навыками настройки компьютерной сети, навыками работы с информацией в корпоративных информационных системах, но допускает незначительные ошибки	Владеет навыками решения практических задач, графическим интерфейсом пользователя, интерфейсом командной строки, стандартными программами, антивирусными программами, сервисным программным обеспечением операционной системы, навыками настройки компьютерной сети, навыками работы с информацией в корпоративных информационных системах

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения	
		«Не зачтено»	«Зачтено»
Первый этап (уровень)	Знать: основные понятия информатики; разделы информатики, состав программного обеспечения, файловые системы, технические	Не знает	Знает основные понятия информатики; разделы информатики, состав программного обеспечения, файловые системы, технические средства, актуальные характеристики основных периферийных устройств компьютеров, виды операционных систем, историю и тенденции их развития

	средства, актуальные характеристики основных периферийных устройств компьютеров, виды операционных систем, историю и тенденции их развития		
Второй этап (уровень)	Уметь: понимать и применять на практике компьютерные технологии для решения различных задач комплексного и гармонического анализа	Не умеет	Умеет понимать и применять на практике компьютерные технологии для решения различных задач комплексного и гармонического анализа
Третий этап (уровень)	Владеть: навыками решения практических задач, графическим интерфейсом пользователя, интерфейсом командной строки, стандартными программами, антивирусными программами, сервисным программным обеспечением операционной системы, навыками настройки компьютерной сети, навыками работы с информацией в корпоративных информационных системах	Не владеет	Владеет навыками решения практических задач, графическим интерфейсом пользователя, интерфейсом командной строки, стандартными программами, антивирусными программами, сервисным программным обеспечением операционной системы, навыками настройки компьютерной сети, навыками работы с информацией в корпоративных информационных системах

ПК-1. Способность формировать и реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений,

составляющих государственную тайну, на объекте информатизации, с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз

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	В целом знает общеметодологические принципы теории информационной безопасности, но допускает значительные ошибки при их описании	Знает общеметодологические принципы теории информационной безопасности, но допускает незначительные ошибки при их описании	Демонстрирует целостные знания об общеметодологических принципах теории информационной безопасности
Второй этап (уровень) Базовый	Уметь: реализовывать на практике принципы политики безопасности	Не умеет	В целом 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	В целом владеет навыками анализа, обработки и интерпретации результатов решения прикладных задач управления, но испытывает затруднения в условиях конкретной задачи	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

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения	
		«Не зачтено»	«Зачтено»
Первый этап (уровень)	Знать: общеметодологические принципы теории информационной безопасности	Не знает	Демонстрирует целостные знания об общеметодологических принципах теории информационной безопасности
Второй этап (уровень)	Уметь: реализовывать на практике принципы политики безопасности	Не умеет	Умеет реализовывать на практике принципы политики безопасности
Третий этап (уровень)	Владеть: навыками анализа, обработки и интерпретации результатов решения прикладных задач управления	Не владеет	Владеет навыками анализа, обработки и интерпретации результатов решения прикладных задач управления

ПК-13. Способность осуществлять организационно-правовое обеспечение деятельности по получению, накоплению, обработке, анализу, использованию информации и защите объектов информатизации, информационных технологий и ресурсов.

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 системы управления, основные виды структур, принципы системного подхода к анализу структур	Не знает	В целом знает понятие системы управления, основные виды структур, принципы системного подхода к анализу структур, но допускает значительные ошибки	Знает понятие системы управления, основные виды структур, принципы системного подхода к анализу структур, но допускает незначительные ошибки	Знает понятие системы управления, основные виды структур, принципы системного подхода к анализу структур
Второй этап (уровень) Базовый	Уметь: использовать методы количественного представления информации и основные закономерности ее преобразования в каналах при выполнении комплекса мер по информационной безопасности	Не умеет	В целом умеет использовать методы количественного представления информации и основные закономерности ее преобразования в каналах при выполнении комплекса мер по информационной безопасности, но допускает значительные ошибки	Умеет использовать методы количественного представления информации и основные закономерности ее преобразования в каналах при выполнении комплекса мер по информационной безопасности, но допускает незначительные ошибки	использовать методы количественного представления информации и основные закономерности ее преобразования в каналах при выполнении комплекса мер по информационной безопасности
Третий этап (уровень) Повышенный	Владеть: навыками организации комплекса мероприятий по защите информации в процессах автоматизированной обработки информации	Не владеет	В целом владеет навыками организации комплекса мероприятий по защите информации в процессах автоматизированной обработки информации, но допускает существенные ошибки	Владеет навыками организации комплекса мероприятий по защите информации в процессах автоматизированной обработки информации, допускает незначительные ошибки	Владеет навыками организации комплекса мероприятий по защите информации в процессах автоматизированной обработки информации

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения	
		«Не зачтено»	«Зачтено»
Первый этап (уровень)	Знать: понятие системы управления, основные виды структур, принципы системного подхода к анализу структур	Не знает	Знает понятие системы управления, основные виды структур, принципы системного подхода к анализу структур
Второй этап (уровень)	Уметь: использовать методы количественного представления	Не умеет	использовать методы количественного представления информации и основные закономерности ее преобразования в каналах при

	информации и основные закономерности ее преобразования в каналах при выполнении комплекса мер по информационной безопасности		выполнении комплекса мер по информационной безопасности
Третий этап (уровень)	Владеть: навыками организации комплекса мероприятий по защите информации в процессах автоматизированной обработки информации	Не владеет	Владеет навыками организации комплекса мероприятий по защите информации в процессах автоматизированной обработки информации

ПК-22. Способность анализировать структуру и содержание информационных массивов и информационных процессов на предмет выявления угроз 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: средства контроля контента	Не знает	В целом знает средства контроля контента, но допускает значительные ошибки	Знает средства контроля контента, но допускает незначительные ошибки	Знает средства контроля контента
Второй этап (уровень) Базовый	Уметь: использовать базовые возможности информационных систем для решения задач фирмы	Не умеет	В целом умеет использовать базовые возможности информационных систем для решения задач фирмы, но допускает значительные ошибки	Умеет использовать базовые возможности информационных систем для решения задач фирмы, но допускает незначительные ошибки	Умеет использовать базовые возможности информационных систем для решения задач фирмы
Третий этап (уровень) Повышенный	Владеть: методикой определения видов и форм информации, подверженной угрозам, анализировать угрозы информационно-вычислительным системам	Не владеет	В целом владеет базовыми методиками определения видов и форм информации, подверженной угрозам	Владеет навыками публичной речи, методикой определения видов и форм информации, подверженной угрозам, анализировать угрозы информационно-вычислительным системам, допускает незначительные ошибки	Владеет методикой определения видов и форм информации, подверженной угрозам, анализировать угрозы информационно-вычислительным системам

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения	
		«Не зачтено»	«Зачтено»

Первый этап (уровень)	Знать: средства контроля контента	Не знает	Знает средства контроля контента
Второй этап (уровень)	Уметь: использовать базовые возможности информационных систем для решения задач фирмы	Не умеет	Умеет использовать базовые возможности информационных систем для решения задач фирмы
Третий этап (уровень)	Владеть: методикой определения видов и форм информации, подверженной угрозам, анализировать угрозы информационно-вычислительным системам	Не владеет	Владеет методикой определения видов и форм информации, подверженной угрозам, анализировать угрозы информационно-вычислительным системам

ПК-23. Способность применять методы аналитической разведки, осуществлять оперативно-аналитический поиск, оперативно-розыскной анализ, идентификацию, диагностику, прогнозирование; криминалистическую диагностику

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: способы применения методов аналитической разведки, осуществления оперативно-аналитического поиска, оперативно-розыскного анализа, идентификации, диагностики, прогнозирования; криминалистической диагностики	Не знает	В целом знает способы применения методов аналитической разведки, осуществления оперативно-аналитического поиска, оперативно-розыскного анализа, идентификации, диагностики, прогнозирования; криминалистической диагностики, но допускает значительные ошибки	Знает способы применения методов аналитической разведки, осуществления оперативно-аналитического поиска, оперативно-розыскного анализа, идентификации, диагностики, прогнозирования; криминалистической диагностики, но допускает незначительные ошибки	Знает способы применения методов аналитической разведки, осуществления оперативно-аналитического поиска, оперативно-розыскного анализа, идентификации, диагностики, прогнозирования; криминалистической диагностики
Второй этап (уровень) Базовый	Уметь: применять методы аналитической разведки, осуществлять оперативно-аналитический поиск, оперативно-розыскной анализ, идентификацию, диагностику, прогнозирование; криминалистическую диагностику	Не умеет	В целом умеет применять методы аналитической разведки, осуществлять оперативно-аналитический поиск, оперативно-розыскной анализ, идентификацию, диагностику, прогнозирование; криминалистическую диагностику, но допускает значительные ошибки	Умеет применять методы аналитической разведки, осуществлять оперативно-аналитический поиск, оперативно-розыскной анализ, идентификацию, диагностику, прогнозирование; криминалистическую диагностику, но допускает незначительные ошибки	Умеет применять методы аналитической разведки, осуществлять оперативно-аналитический поиск, оперативно-розыскной анализ, идентификацию, диагностику, прогнозирование; криминалистическую диагностику
Третий этап (уровень) Повышенный	Владеть: навыками систематического применения методов аналитической разведки,	Не владеет	В целом владеет навыками систематического применения методов аналитической разведки,	Владеет навыками систематического применения методов аналитической	Владеет навыками систематического применения методов аналитической разведки,

	осуществления оперативно-аналитического поиска, оперативно-розыскного анализа, идентификации, диагностики, прогнозирования; криминалистической диагностики		осуществления оперативно-аналитического поиска, оперативно-розыскного анализа, идентификации, диагностики, прогнозирования; криминалистической диагностики	разведки, осуществления оперативно-аналитического поиска, оперативно-розыскного анализа, идентификации, диагностики, прогнозирования; криминалистической диагностики, допускает незначительные ошибки	осуществления оперативно-аналитического поиска, оперативно-розыскного анализа, идентификации, диагностики, прогнозирования; криминалистической диагностики

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения	
		«Не зачтено»	«Зачтено»
Первый этап (уровень)	Знать: способы применения методов аналитической разведки, осуществления оперативно-аналитического поиска, оперативно-розыскного анализа, идентификации, диагностики, прогнозирования; криминалистической диагностики	Не знает	Знает способы применения методов аналитической разведки, осуществления оперативно-аналитического поиска, оперативно-розыскного анализа, идентификации, диагностики, прогнозирования; криминалистической диагностики
Второй этап (уровень)	Уметь: применять методы аналитической разведки, осуществлять оперативно-аналитический поиск, оперативно-розыскной анализ, идентификацию, диагностику, прогнозирование; криминалистическую	Не умеет	Умеет применять методы аналитической разведки, осуществлять оперативно-аналитический поиск, оперативно-розыскной анализ, идентификацию, диагностику, прогнозирование; криминалистическую диагностику

	диагностику		
Третий этап (уровень)	Владеть: навыками систематического применения методов аналитической разведки, осуществления оперативно-аналитического поиска, оперативно-розыскного анализа, идентификации, диагностики, прогнозирования; криминалистической диагностики	Не владеет	Владеет навыками систематического применения методов аналитической разведки, осуществления оперативно-аналитического поиска, оперативно-розыскного анализа, идентификации, диагностики, прогнозирования; криминалистической диагностики

Критериями оценивания являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения модулей дисциплины, перечисленных в рейтинг-плане дисциплины:

Зачет: текущий контроль – максимум 50 баллов; рубежный контроль – максимум 50 баллов, поощрительные баллы – максимум 10.

Шкалы оценивания для зачета:

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

Экзамен:

- 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.

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	основные понятия информатики; разделы информатики, состав программного обеспечения, файловые системы, технические средства, актуальные	ОК-12	Тест, практическая работа, экзамен

	характеристики основных периферийных устройств компьютеров, виды операционных систем, историю и тенденции их развития		
	общеметодологические принципы теории информационной безопасности	ПК-1	Тест, практическая работа, экзамен
	понятие системы управления, основные виды структур, принципы системного подхода к анализу структур	ПК-13	Тест, практическая работа, экзамен
	средства контроля контента	ПК-22	Тест, практическая работа, экзамен
	способы применения методов аналитической разведки, осуществления оперативно-аналитического поиска, оперативно-розыскного анализа, идентификации, диагностики, прогнозирования; криминалистической диагностики	ПК-23	Тест, практическая работа, экзамен
2-й этап Уметь	понимать и применять на практике компьютерные технологии для решения различных задач комплексного и гармонического анализа	ОК-12	Тест, практическая работа, экзамен
	реализовывать на практике принципы политики безопасности	ПК-1	Тест, практическая работа, экзамен
	использовать методы количественного представления информации и основные закономерности ее преобразования в каналах при выполнении комплекса мер по информационной безопасности	ПК-13	Тест, практическая работа, экзамен
	использовать базовые возможности информационных систем для решения задач фирмы	ПК-22	Тест, практическая работа, экзамен
	применять методы	ПК-23	Тест, практическая

	аналитической разведки, осуществлять оперативно-аналитический поиск, оперативно-розыскной анализ, идентификацию, диагностику, прогнозирование; криминалистическую диагностику		работа, экзамен
3-й этап Владеть	навыками решения практических задач, графическим интерфейсом пользователя, интерфейсом командной строки, стандартными программами, антивирусными программами, сервисным программным обеспечением операционной системы, навыками настройки компьютерной сети, навыками работы с информацией в корпоративных информационных системах	ОК-12	Тест, практическая работа, экзамен
	навыками анализа, обработки и интерпретации результатов решения прикладных задач управления	ПК-1	Тест, практическая работа, экзамен
	навыками организации комплекса мероприятий по защите информации в процессах автоматизированной обработки информации	ПК-13	Тест, практическая работа, экзамен
	методикой определения видов и форм информации, подверженной угрозам, анализировать угрозы информационно-вычислительным системам	ПК-22	Тест, практическая работа, экзамен
	навыками систематического применения методов аналитической разведки,	ПК-23	Тест, практическая работа, экзамен

	осуществления оперативно-аналитического поиска, оперативно-розыскного анализа, идентификации, диагностики, прогнозирования; криминалистической диагностики		

Типовые вопросы для зачета:

1. Понятие и защита государственной и коммерческой тайны в системе защиты информации. Принципы защиты защита государственной и коммерческой тайны.
2. Отнесение сведений к коммерческой, служебной и профессиональной тайнам.
3. Правовой режим информационных ресурсов.
4. Признаки охраноспособности информации.
5. Цели защиты информации.
6. Режим защиты информации.
7. Виды защищаемой информации.
8. Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации».
9. Общедоступная информация.
10. Ограничение доступа к информации.
11. Конфиденциальная информация.
12. Виды тайн в российском законодательстве.
13. Персональные данные.
14. Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных».
15. Защита коммерческой тайны.
16. Федеральный закон от 29.07.2004 N 98-ФЗ «О коммерческой тайне».
17. Юридические меры защиты коммерческой тайны.
18. Административно-организационные меры защиты коммерческой тайны.
19. Социально-психологические меры защиты коммерческой тайны.
20. Технические средства защиты коммерческой тайны.
21. Служебная тайна.
22. Признаки профессиональной тайны.
23. Тайна в юридической практике.
24. Тайна в сфере экономической деятельности.
25. Тайна, связанная с этическими соображениями.
26. Государственная тайна и порядок отнесения к ней информации.
27. Закон РФ от 21.7.93 г. № 5485-1 «О государственной тайне»
28. Засекречивание сведений, составляющих государственную тайну.
29. Рассекречивание сведений, составляющих государственную тайну
30. Допуск к государственной тайне.
31. Защита государственной тайны.
32. Организация режима секретности, его особенности и содержание.
33. Организационные и технические способы защиты государственной тайны.
34. Основные нормативные правовые акты в области информационной безопасности и защиты информации.
35. Отечественные и зарубежные стандарты в области информационной безопасности.
36. ГОСТ Р 50922-2006 — Защита информации. Основные термины и определения.

37. Р 50.1.053-2005 — Информационные технологии. Основные термины и определения в области технической защиты информации.
38. ГОСТ Р 51188—98 — Защита информации. Испытание программных средств на наличие компьютерных вирусов. Типовое руководство.
39. ГОСТ Р 51275-2006 — Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.
40. ГОСТ Р ИСО/МЭК 15408-1-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.
41. ГОСТ Р ИСО/МЭК 15408-2-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности.
42. ГОСТ Р ИСО/МЭК 15408-3-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности.
43. ГОСТ Р ИСО/МЭК 15408 — «Общие критерии оценки безопасности информационных технологий» — стандарт, определяющий инструменты и методику оценки безопасности информационных продуктов и систем; он содержит перечень требований, по которым можно сравнивать результаты независимых оценок безопасности — благодаря чему потребитель принимает решение о безопасности продуктов. Сфера приложения «Общих критериев» — защита информации от несанкционированного доступа, модификации или утечки, и другие способы защиты, реализуемые аппаратными и программными средствами.
44. ГОСТ Р ИСО/МЭК 17799 — «Информационные технологии. Практические правила управления информационной безопасностью». Прямое применение международного стандарта с дополнением — ISO/IEC 17799:2005.
45. ГОСТ Р ИСО/МЭК 27001 — «Информационные технологии. Методы безопасности. Система управления безопасностью информации. Требования». Прямое применение международного стандарта — ISO/IEC 27001:2005.
46. ГОСТ Р 51898-2002 — Аспекты безопасности. Правила включения в стандарты.
47. РД СВТ. Защита от НСД. Показатели защищенности от НСД к информации — содержит описание показателей защищенности информационных систем и требования к классам защищенности (Проверено 26 июля 2017).
48. Нормативные документы ИБ
49. Стандарт Банка России СТО БР ИББС-1.0-2014 — Стандарт Банка России: «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения».
50. PCI DSS (Payment Card Industry Data Security Standard) — Стандарт безопасности данных индустрии платёжных карт.

Экзамен

Экзамен является оценочным средством для всех этапов освоения компетенции.

Структура экзаменационного билета

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

Типовые экзаменационные материалы

Типовые экзаменационные вопросы:

1. Понятие и защита государственной и коммерческой тайны в системе защиты информации. Принципы защиты защита государственной и коммерческой тайны.
2. Отнесение сведений к коммерческой, служебной и профессиональной тайнам.
3. Правовой режим информационных ресурсов.
4. Признаки охраноспособности информации.
5. Цели защиты информации.
6. Режим защиты информации.
7. Виды защищаемой информации.
8. Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации».
9. Общедоступная информация.
10. Ограничение доступа к информации.
11. Конфиденциальная информация.
12. Виды тайн в российском законодательстве.
13. Персональные данные.
14. Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных».
15. Защита коммерческой тайны.
16. Федеральный закон от 29.07.2004 N 98-ФЗ «О коммерческой тайне».
17. Юридические меры защиты коммерческой тайны.
18. Административно-организационные меры защиты коммерческой тайны.
19. Социально-психологические меры защиты коммерческой тайны.
20. Технические средства защиты коммерческой тайны.
21. Служебная тайна.
22. Признаки профессиональной тайны.
23. Тайна в юридической практике.
24. Тайна в сфере экономической деятельности.
25. Тайна, связанная с этическими соображениями.
26. Государственная тайна и порядок отнесения к ней информации.
27. Закон РФ от 21.7.93 г. № 5485-1 «О государственной тайне»
28. Засекречивание сведений, составляющих государственную тайну.
29. Рассекречивание сведений, составляющих государственную тайну
30. Допуск к государственной тайне.
31. Защита государственной тайны.
32. Организация режима секретности, его особенности и содержание.
33. Организационные и технические способы защиты государственной тайны.

34. Основные нормативные правовые акты в области информационной безопасности и защиты информации.
35. Отечественные и зарубежные стандарты в области информационной безопасности.
36. ГОСТ Р 50922-2006 — Защита информации. Основные термины и определения.
37. Р 50.1.053-2005 — Информационные технологии. Основные термины и определения в области технической защиты информации.
38. ГОСТ Р 51188—98 — Защита информации. Испытание программных средств на наличие компьютерных вирусов. Типовое руководство.
39. ГОСТ Р 51275-2006 — Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.
40. ГОСТ Р ИСО/МЭК 15408-1-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.
41. ГОСТ Р ИСО/МЭК 15408-2-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности.
42. ГОСТ Р ИСО/МЭК 15408-3-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности.
43. ГОСТ Р ИСО/МЭК 15408 — «Общие критерии оценки безопасности информационных технологий» — стандарт, определяющий инструменты и методику оценки безопасности информационных продуктов и систем; он содержит перечень требований, по которым можно сравнивать результаты независимых оценок безопасности — благодаря чему потребитель принимает решение о безопасности продуктов. Сфера приложения «Общих критериев» — защита информации от несанкционированного доступа, модификации или утечки, и другие способы защиты, реализуемые аппаратными и программными средствами.
44. ГОСТ Р ИСО/МЭК 17799 — «Информационные технологии. Практические правила управления информационной безопасностью». Прямое применение международного стандарта с дополнением — ISO/IEC 17799:2005.
45. ГОСТ Р ИСО/МЭК 27001 — «Информационные технологии. Методы безопасности. Система управления безопасностью информации. Требования».

Прямое применение международного стандарта — ISO/IEC 27001:2005.
46. ГОСТ Р 51898-2002 — Аспекты безопасности. Правила включения в стандарты.
47. РД СВТ. Защита от НСД. Показатели защищенности от НСД к информации — содержит описание показателей защищенности информационных систем и требования к классам защищенности (Проверено 26 июля 2017).
48. Нормативные документы ИБ
49. Стандарт Банка России СТО БР ИББС-1.0-2014 — Стандарт Банка России: «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения».
50. PCI DSS (Payment Card Industry Data Security Standard) — Стандарт безопасности данных индустрии платёжных карт.
51. Доктрина информационной безопасности Российской Федерации.
52. Единая система информационно-аналитического обеспечения деятельности МВД России.
53. Основные задачи обеспечения информационной безопасности в правоохранительных органах.
54. Угрозы по добыванию, обработке и использованию оперативно-розыскной информации.
55. Виды категорируемых объектов информации в правоохранительных органах.
56. Специальная проверка.
57. Специальное исследование объекта защиты информации.
58. Специальное обследование.
59. Вопросы безопасности, связанные с персоналом.
60. Соглашения о конфиденциальности.
61. Особенности работы с персоналом, владеющим конфиденциальной информацией.
62. Подбор и подготовка кадров.
63. Проверка персонала на благонадежность.
64. Принципы построения разрешительной системы доступа.
65. Доступ к отчуждаемым носителям конфиденциальной информации.
66. Доступ к средствам вычислительной техники, обрабатывающей конфиденциальную информацию.
67. Текущая работа с персоналом, владеющим конфиденциальной информацией.
68. Служебное расследование.
69. Особенности увольнения сотрудников, владеющих конфиденциальной информацией.

70. Одностороннее соглашение о неразглашении.
71. Взаимное соглашение о неразглашении.
72. Распространенные недостатки соглашений о неразглашении.
73. Организация противодействия компьютерной преступности.
74. Виды компьютерной преступности в сфере вычислительных сетей.
75. Способы совершения компьютерных преступлений.
76. Ответственность за компьютерные преступления.
77. Методика раскрытия и расследования компьютерных преступлений.
78. Типичные следственные ситуации первоначального этапа и следственные действия в расследовании компьютерных преступлений.
79. Поиск и изъятие информации и следов воздействия на нее в ЭВМ и ее устройствах.
80. Использование специальных познаний и назначение экспертиз.
81. Понятие информационной безопасности. Термины и определения.
82. Система информационной безопасности.
83. Проверка безопасности информационных систем. Аудит систем.
84. Общие сведения об информационной безопасности.
85. Проверка безопасности информационных систем. Мониторинг систем.
86. Основные составляющие информационной безопасности.
87. Внешний аудит.
88. Обоснование необходимости рассмотрения вопросов информационной безопасности.
89. Внутренний аудит.
90. Процессный подход в рамках управления ИБ.
91. Проблемы построения современных систем безопасности.
92. Слежение за доступом к системам и их использованием.
93. Стандарты информационной безопасности ISO/IEC серии 27000.
94. Отраслевые стандарты информационной безопасности
95. Стандарты и нормативные акты РФ в области информационной безопасности.
96. Оценка рисков нарушения безопасности.
97. Средства управления информационной безопасностью.
98. Защита от вредоносного программного обеспечения.
99. Ключевые средства контроля информационной безопасности.
100. Ответственность за информационные ресурсы.
101. Требование бизнеса по обеспечению контроля доступа.

102. Факторы, необходимые для успешной реализации системы информационной безопасности в организации.
103. Управление доступом пользователей. Обязанности пользователей.
104. Группы требований к информационной безопасности организации.
105. Система планирования бесперебойной работы организации.
106. Политика информационной безопасности.
107. Классификация информации.
108. Инфраструктура информационной безопасности.
109. Безопасность информации в должностных инструкциях.
110. Обучение пользователей правилам информационной безопасности.
111. Реагирование на события, таящие угрозу безопасности.
112. Оперирование с носителями информации и их защита.
113. Термины и определения информационной безопасности.
114. Понятие информационной безопасности.
115. Циклическая модель улучшения процессов.

Пример экзаменационного билета:

Форма 1.4.-33

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

Специальность 10.05.05 Безопасность информационных технологий в правоохранительной сфере

Дисциплина Информационная безопасность в правоохранительной сфере

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Основные задачи информационной безопасности.
2. Классификация угроз информационной безопасности.
3. Укажите один из основных нормативных актов, осуществляющих правовое регулирование защиты информации. Какое определение термину «информация» дается в этом нормативном акте?

Зав. Кафедрой УИБ А.С. Исмагилова

2018-2019 учебный год
Кафедра управления информационной безопасностью

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 функциональных возможностей, терминологии, основных элементов, умение применять теоретические знания при выполнении практических заданий. Студент без затруднений ответил на все дополнительные вопросы. Практическая часть работы выполнена полностью без неточностей и ошибок;

- 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. При выполнении практической части работы допущены несущественные ошибки;

- 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. Студент не решил задачу или при решении допущены грубые ошибки;

- 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 лабораторных работ

Цель проведения лабораторных работы – практическое освоение материала дисциплины.

1) Отнесение сведений к коммерческой, служебной и профессиональной тайнам..
2) Ограничение доступа к информации.
3) Технические средства защиты коммерческой тайны.
4) Признаки служебной тайны.
5) Порядок отнесения сведений к государственной тайне.
6) Засекречивание сведений, составляющих государственную тайну.
7) Допуск к государственной тайне.
8) Организация режима секретности.

Типовая лабораторная работа

Модуль 2. Государственная тайна.
Тема: Засекречивание сведений, составляющих государственную тайну.
Цель: Практическая проверка усвоения пройденного материала..
Задание: Ответить на поставленные вопросы.
Порядок выполнения:

1. Ответить на контрольные вопросы:
   а) Дайте определение термину «Государственная тайна».

b) Дайте определение термину «носители сведений, составляющих государственную тайну».
c) Какие виды тайн включает в себя государственная тайна? Дайте их определения.
d) Что такое «Система защиты государственной тайны»?
e) Что такое «допуск к государственной тайне»?
f) Что такое «доступ к сведениям, составляющим государственную тайну»?
g) Что такое «гриф секретности»?
h) Что такое «степень секретности»?
i) Что такое «режим секретности»?
j) Что такое ПДТК, и какие первоочередные задачи она решает?
k) Из каких составляющих состоит правовой институт государственной тайны?
l) На каком нормативно-правовом акте основывается система защиты государственных секретов в Российской Федерации?
m) Кто является субъектами правоотношений в соответствии со статьей 1 закона РФ “О государственной тайне”?
n) Относится ли гриф «Для служебного пользования» к грифам секретности?
o) Что такое засекречивание сведений и их носителей?
p) Каким нормативно-правовым актом утвержден перечень сведений, отнесенных к государственной тайне?
q) Какая информация не может быть отнесена к государственной тайне информация?
r) С какого момента информация считается государственной тайной?
s) На каком основании осуществляются снижение степени секретности информации или отмена решения об отнесении ее к государственной тайне?
t) В чем заключается обоснованность засекречивания сведений?
u) В чем заключается своевременность засекречивания сведений?
v) Какие реквизиты в обязательном порядке должны наноситься на носители сведений, составляющих государственную тайну?
w) В каких случаях производится рассекречивание сведений, составляющих государственную тайну?
x) В каких случаях носители сведений, составляющих государственную тайну, рассекречиваются ранее сроков, установленных при их засекречивании?
y) Что предусматривает допуск должностных лиц и граждан к государственной тайне?
z) Назовите формы допуска к секретным сведениям.
aa) Какие ограничения могут вводиться в отношении граждан, допущенные к государственной тайне?
bb) В компетенцию каких органов входит защита государственной тайны?
cc) Какие лица не допускаются к секретным работам и документам?
dd) Какие группы мер включает в себя режим секретности?
ee) Какие особенности имеет режим секретности?

2. 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 контрольные вопросы/ работа выполнена, но получены ответы не на все контрольные вопросы/	0/2/4

	работа выполнена и получены ответы на все контрольные вопросы	

Типовые задания для практической работы

Цель проведения практической работы – оценка уровня владения базовой профессиональной терминологией в сфере государственного и муниципального управления. Практическая работа проводится в письменной форме.

Темы практических работ Модуль 1, 2, семестр 6

1. Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных».
3. Служебная тайна.
4. Закон РФ от 21.7.93 г. № 5485-1 «О государственной тайне».
5. Допуск к государственной тайне.
6. Организация режима секретности, его особенности и содержание.

Темы практических работ Модуль 3, 4, семестр 7

1. ГОСТ Р 50922-2006 — Защита информации. Основные термины и определения.
2. ГОСТ Р 51275-2006 — Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.
3. ГОСТ Р ИСО/МЭК 15408-3-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.
4. ГОСТ Р ИСО/МЭК 27001 — «Информационные технологии. Методы безопасности. Система управления безопасностью информации. Требования.
5. Стандарт Банка России СТО БР ИББС-1.0-2014 — Стандарт Банка России: «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения.
6. Доктрина информационной безопасности Российской Федерации.
7. Виды компьютерной преступности в сфере вычислительных сетей.
8. Аудит информационных систем.
9. Реагирование на события, таящие угрозу безопасности.

Примеры заданий

Модуль 1, 2, семестр 6, 7

Письменная практическая работа

1. Укажите виды гражданско-правовых режимов информации.
2. Укажите содержание правового режима информационных ресурсов.
3. Укажите обязанности обладателя информации.
4. Укажите права обладателя информации.
5. Укажите цели защиты информации.

Критерии оценки практических работ:

Структура работы	Критерии оценки	Распределение баллов
6 семестр Модуль 1. Защита государственной и	Нет ответа / Неполный ответ / Полный ответ	0/2/3

коммерческой тайны в системе защиты информации. Модуль 2. Государственная тайна 7 семестр Модуль 3. Нормативные правовые акты в области информационной безопасности Модуль 4. Информационная безопасность в правоохранительных органах		 0/2/3 0/2/5 0/2/4

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, 3, 4 семестр 6, 7
Тестирование

1. Защита информации не направлена на:

а) соблюдение конфиденциальности информации ограниченного доступа;

б) нет правильного ответа;

в) реализацию права на доступ к информации;

г) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также иных неправомерных действий в отношении такой информации.

2. Защита информации не осуществляется от:

а) законного требования органа государственной власти об ограничения доступа к информационному ресурсу;

б) утечки (неконтролируемого распространения защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации разведками);

в) разглашения (несанкционированного доведения защищаемой информации до потребителей, не имеющих права доступа к этой информации);

г) разведки (получения защищаемой информации технической, агентурной разведкой).

3. Не может относиться к категории «служебная тайна»:

а) врачебная тайна;

б) тайна усыновления;

в) коммерческая тайна;

г) нет правильного ответа.

Критерии оценки тестовых заданий

Структура работы	Критерии оценки	Распределение баллов
6 семестр Один вопрос теста Все (25 вопросов теста) 7 семестр Один вопрос теста	Неправильный ответ / Правильный ответ	0/1 0/25 0/0,6

Все (25 вопросов теста)		0/15

4.3. Рейтинг-план дисциплины

Рейтинг–план дисциплины представлен в приложении 2.

5. Учебно-методическое и информационное обеспечение дисциплины

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

Основная литература

1. Ковалев, Д.В. Информационная безопасность : учебное пособие / Д.В. Ковалев, Е.А. Богданова ; Министерство образования и науки РФ, Южный федеральный университет. - Ростов-на-Дону : Издательство Южного федерального университета, 2016. - 74 с. : схем., табл., ил. - Библиогр. в кн. - ISBN 978-5-9275-2364-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=493175 (14.04.2019).

2. 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

Дополнительная литература

3. 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

4. Шилов, А.К. Управление информационной безопасностью : учебное пособие / А.К. Шилов ; Министерство науки и высшего образования РФ, Федеральное государственное автономное образовательное учреждение высшего образования «Южный федеральный университет», Институт компьютерных технологий и информационной безопасности. - Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2018. - 121 с. : ил. - Библиогр.: с. 81 - 82 - ISBN 978-5-9275-2742-7 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=500065 (14.04.2019).

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 (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	Лекции, практические занятия, текущий контроль, промежуточная аттестация, экзамен	**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 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 APART 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 APART 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.,

(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		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. **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.

(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). **6. *помещения для самостоятельной работы:*** аудитория № 613 (гуманитарный корпус), читальный зал библиотеки аудитория 402 (гуманитарный корпус).		

Приложение 1

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

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ
дисциплины Информационная безопасность в правоохранительной сфере на 6 семестре ОФО

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (ЗЕТ / часов)	3 ЗЕТ / 108 часов
Учебных часов на контактную работу с преподавателем:	64,2
лекций	16
практических/ семинарских	16
лабораторных	32
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	0,2
Учебных часов на самостоятельную работу обучающихся (СР)	44
Учебных часов на подготовку к экзамену/зачету/дифференцированному зачету (Контроль)	0

Форма контроля:
Зачет 6 семестр

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

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ
дисциплины Информационная безопасность в правоохранительной сфере на 7 семестре
ОФО

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (ЗЕТ / часов)	3 ЗЕТ / 108 часов
Учебных часов на контактную работу с преподавателем:	39,2
лекций	18
практических/ семинарских	18
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)	43
Учебных часов на подготовку к экзамену/зачету/дифференцированному зачету (Контроль)	25,8

Форма контроля:
Экзамен 7 семестр

Семестр 6

№	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. Защита государственной и коммерческой тайны в системе защиты информации					1- 4	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Тест, лабораторная работа
	Тема: Понятие и защита государственной и коммерческой тайны в системе защиты информации. Принципы защиты защита государственной и коммерческой тайны. Отнесение сведений к коммерческой, служебной и профессиональной тайнам. Правовой режим информационных ресурсов. Признаки охраноспособности информации. Цели защиты информации. Режим защиты информации.	2		4	5			
	Тема: Виды защищаемой информации. Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации». Общедоступная информация. Ограничение доступа к информации. Конфиденциальная информация.	2	2	4	5			
	Тема: Виды тайн в российском законодательстве. Персональные данные. Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных». Защита коммерческой тайны. Федеральный закон от 29.07.2004 N 98-ФЗ «О коммерческой тайне». Юридические меры защиты коммерческой тайны. Административно-организационные меры защиты коммерческой тайны. Социально-психологические меры защиты коммерческой тайны. Технические средства защиты коммерческой тайны.	2	2	4	6			

	Тема: Служебная тайна. Признаки профессиональной тайны. Тайна в юридической практике. Тайна в сфере экономической деятельности. Тайна, связанная с этическими соображениями.	2	4	4	6			
2	Модуль 2. Государственная тайна Тема: Государственная тайна и порядок отнесения к ней информации. Закон РФ от 21.7.93 г. № 5485-1 «О государственной тайне» Засекречивание сведений, составляющих государственную тайну. Рассекречивание сведений, составляющих государственную тайну. Допуск к государственной тайне. Защита государственной тайны. Организация режима секретности, его особенности и содержание. Организационные и технические способы защиты государственной тайны.	 2 2 2 2	 2 2 4	 4 4 4 4	 5 5 6 6	1- 4	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Тест, лабораторная работа
	Всего часов	16	16	32	44			

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 3. Нормативные правовые акты в области информационной безопасности					1- 7	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Тест, практическая работа
1	Основные нормативные правовые акты в области информационной безопасности и защиты информации. Отечественные и зарубежные стандарты в области информационной безопасности. ГОСТ Р 50922-2006 — Защита информации. Основные термины и определения.	2	2		4			
2	ГОСТ Р 50.1.053-2005 — Информационные технологии. Основные термины и определения в области технической защиты информации. ГОСТ Р 51188—98 — Защита информации. Испытание программных средств на наличие компьютерных вирусов. Типовое руководство. ГОСТ Р 51275-2006 — Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. ГОСТ Р ИСО/МЭК 15408-1-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. ГОСТ Р ИСО/МЭК 15408-2-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности	2	2		4			
3	ГОСТ Р ИСО/МЭК 15408-3-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. ГОСТ Р ИСО/МЭК 15408 — «Общие	2	2		4			

	критерии оценки безопасности информационных технологий» — стандарт, определяющий инструменты и методику оценки безопасности информационных продуктов и систем; он содержит перечень требований, по которым можно сравнивать результаты независимых оценок безопасности — благодаря чему потребитель принимает решение о безопасности продуктов. Сфера приложения «Общих критериев» — защита информации от несанкционированного доступа, модификации или утечки, и другие способы защиты, реализуемые аппаратными и программными средствами.							
4	ГОСТ Р ИСО/МЭК 17799 — «Информационные технологии. Практические правила управления информационной безопасностью». ISO/IEC 17799:2005. ГОСТ Р ИСО/МЭК 27001 — «Информационные технологии. Методы безопасности. Система управления безопасностью информации. Требования».Прямое применение международного стандарта с дополнением —Прямое применение международного стандарта — ISO/IEC 27001:2005. ГОСТ Р 51898-2002 — Аспекты безопасности. Правила включения в стандарты. РД СВТ. Защита от НСД. Показатели защищенности от НСД к информации — содержит описание показателей защищенности информационных систем и требования к классам защищенности.	2	2		4			
5	Стандарт Банка России СТО БР ИББС-1.0-2014 — Стандарт Банка России: «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения». PCI DSS (Payment Card Industry Data Security Standard) — Стандарт безопасности данных индустрии платёжных карт.	2	2		4			
2	Модуль 4. Информационная безопасность в правоохранительных органах. Доктрина информационной безопасности Российской Федерации. Единая система информационно-аналитического обеспечения деятельности МВД России. Основные задачи обеспечения информационной безопасности в правоохранительных органах. Угрозы по добыванию, обработке и использованию оперативно-розыскной информации. Виды категорируемых объектов информации в правоохранительных органах. Специальная проверка. Специальное исследование объекта защиты информации. Специальное обследование. Вопросы безопасности, связанные с персоналом. Соглашения о конфиденциальности. Особенности работы с персоналом, владеющим конфиденциальной информацией. Подбор и подготовка кадров. Проверка персонала на благонадежность. Принципы построения разрешительной системы доступа. Доступ к отчуждаемым носителям конфиденциальной	2	2		4	1- 7	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Тест, практическая работа

	информации. Доступ к средствам вычислительной техники, обрабатывающей конфиденциальную информацию. Текущая работа с персоналом, владеющим конфиденциальной информацией. Служебное расследование. Особенности увольнения сотрудников, владеющих конфиденциальной информацией. Одностороннее соглашение о неразглашении. Взаимное соглашение о неразглашении. Распространенные недостатки соглашений о неразглашении.							
	Виды компьютерной преступности в сфере вычислительных сетей. Способы совершения компьютерных преступлений. Ответственность за компьютерные преступления. Методика раскрытия и расследования компьютерных преступлений. Типичные следственные ситуации первоначального этапа и следственные действия в расследовании компьютерных преступлений. Поиск и изъятие информации и следов воздействия на нее в ЭВМ и ее устройствах. Использование специальных познаний и назначение экспертиз. Организация противодействия компьютерной преступности.	2	2		4			
	Понятие информационной безопасности. Термины и определения. Система информационной безопасности. Проверка безопасности информационных систем. Аудит систем. Общие сведения об информационной безопасности. Проверка безопасности информационных систем. Мониторинг систем. Основные составляющие информационной безопасности. Внешний аудит. Обоснование необходимости рассмотрения вопросов информационной безопасности. Внутренний аудит. Процессный подход в рамках управления ИБ. Проблемы построения современных систем безопасности. Слежение за доступом к системам и их использованием. Оценка рисков нарушения безопасности. Средства управления информационной безопасностью. Защита от вредоносного программного обеспечения. Ключевые средства контроля информационной безопасности. Ответственность за информационные ресурсы. Требование бизнеса по обеспечению контроля доступа. Факторы, необходимые для успешной реализации системы информационной безопасности в организации. Управление доступом пользователей. Обязанности пользователей. Группы требований к информационной безопасности организации. Система планирования бесперебойной работы организации. Политика информационной безопасности.	2	2		4			

	Классификация информации. Инфраструктура информационной безопасности. Безопасность информации в должностных инструкциях. Обучение пользователей правилам информационной безопасности. Реагирование на события, таящие угрозу безопасности. Оперирование с носителями информации и их защита. Термины и определения управления информационной безопасностью. Понятие управления информационной безопасностью Циклическая модель улучшения процессов.	2	2		4			
	Всего часов	18	18	0	36			

Приложение 2

Рейтинг-план дисциплины

Информационная безопасность в правоохранительной сфере

Специальность 10.05.05 Безопасность информационных технологий в правоохранительной сфере курс 3, семестр 6

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1. Защита государственной и коммерческой тайны в системе защиты информации				
Текущий контроль				
1. Лабораторная работа	4	4	0	16
2. Практическая работа	3	3	0	9
Рубежный контроль				
1. Тест	25	1	0	25
Всего		5	0	50
Модуль 2. Государственная тайна				
Текущий контроль				
1. Лабораторная работа	4	4	0	16
2. Практическая работа	3	3	0	9
Рубежный контроль				
1. Тест	25	1	0	25
Всего		5	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
Информационная безопасность в правоохранительной сфере

Специальность 10.05.05 Безопасность информационных технологий в правоохранительной сфере курс 4, семестр 7

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 3. Нормативные правовые акты в области информационной безопасности				
Текущий контроль				
1. Практическая работа	5	4	0	20
Рубежный контроль				
1. Тест	15	1	0	15
Всего		5	0	35
Модуль 4. Информационная безопасность в правоохранительных органах.				
Текущий контроль				
1. Практическая работа	4	5	0	20
Рубежный контроль				15
1. 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