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

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

Согласовано:
Председатель УМК института
/Р.А. Гильмутдинова

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Введение в специальность
Б1.В.1.01 (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)
профессор, д-р физ.-мат.
наук, доцент / Исмагилова А.С.

Для приема: 2018 г.

Уфа 2018 г.

Составитель: А.С.Исмагилова

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

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/

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

Заведующий кафедрой ___________________/ _____________Ф.И.О/

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

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

Результаты обучения		Формируемая компетенция (с указанием кода)	Примечание
Знания	1. Знать политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации. 2. Знать общеметодологические принципы теории информационной безопасности. 3. Знать возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации. 4. Знать состояние законодательной базы и стандарты в области информационной безопасности.	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.	
	1. Знать основные нормативные и правовые акты в области информационной безопасности и защиты информации 2. Знать также нормативные методические документы Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю в данной области. 3. Знать методы и средства правовой защиты государственной тайны и информационной безопасности.	ПК-19 Способность соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности; обеспечивать соблюдение режима секретности.	
	1. Знать теоретические и методические основы организационной зашиты информации. 2. Знать правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны. 3. Знать место и роль	ПК-31 Способность принимать участие в создании системы защиты информации на объекте информатизации.	

	информационной безопасности в системе национальной безопасности Российской Федерации.		
Умения	1. Уметь реализовывать на практике принципы политики безопасности. 2. Уметь использовать закономерности преобразования данных в каналах при выполнении комплекса мер по информационной безопасности. 3. Уметь обосновывать организационно-технические мероприятия по защите информации. 4. Уметь использовать возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации.	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.	
	1. Уметь использовать в практической деятельности правовые знания 2. Уметь анализировать и составлять основные правовые акты и осуществлять правовую оценку информации, используемых в профессиональной деятельности. 3. Уметь ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной деятельности и использовать их в своей деятельности. 4. Уметь предвидеть юридические опасности и угрозы и соблюдать основные правовые требования информационной безопасности, в т.ч. для защиты государственной тайны.	ПК-19 Способность соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности; обеспечивать соблюдение режима секретности.	
	1. Уметь осуществлять меры по организованной защите информации. 2. Уметь формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе.	ПК-31 Способность принимать участие в создании системы защиты информации на объекте информатизации.	

	3. Уметь осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты.		
Навыки, опыт деятельности	1. Владеть навыками анализа, обработки и интерпретации результатов решения прикладных задач управления. 2. Владеть навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью. 3. Владеть навыками организации комплекса мероприятий по защите информации в процессах автоматизированной обработки информации. 4. Владеть навыками выявления и устранения угроз информационной безопасности. 5. Владеть навыками эксплуатации современного электронного оборудования и информационно-коммуникационных технологий. 6. Владеть навыками внедрения, адаптации и настройки средств защиты прикладных ИС.	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.	
	1. Владеть основами правового мышления, навыками самостоятельного анализа правовой информации, анализа юридических последствий, связанных с использованием информации. 2. Владеть навыками работы с нормативными правовыми актами, нормативной и технической информацией, необходимой для профессиональной деятельности. 3. Владеть навыками поиска нормативной правовой информации необходимой для профессиональной деятельности. 4. Владеть навыками обеспечения и соблюдения	ПК-19 Способность соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности; обеспечивать соблюдение режима секретности.	

	режима секретности.		
	1. Владеть навыками организации защиты информации. 2. Владеть навыками организации и обеспечения режима секретности.	ПК-31 Способность принимать участие в создании системы защиты информации на объекте информатизации.	

2. Цель и место дисциплины в структуре образовательной программы

Дисциплина «Введение в специальность» относится к группе дисциплин вариативной части образовательной программы.

Дисциплина изучается на 1 курсе в 1 семестре.

Цели изучения дисциплины:

– раскрытие сущности и значения информационной безопасности и защиты информации, их места в системе национальной безопасности;

– определение теоретических, концептуальных, методологических и организационных основ обеспечения безопасности информации;

– классификация и характеристики составляющих информационной безопасности и защиты информации, установление логической взаимосвязи входящих в них компонентов.

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

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 («Не удовлетво-рительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)

Первый этап (уровень)	1. Знать политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации. 2. Знать общеметодологические принципы теории информационной безопасности. 3. Знать возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации. 4. Знать состояние законодательной базы и стандарты в области информационной безопасности.	Не способен формировать и реализовывать комплекс мер по обеспечению безопасности информации.	Знает стандарты в области информационной безопасности. Не реализует на практике принципы политики безопасности.	Знает стандарты в области информационной безопасности, возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации.	Знает стандарты в области информационной безопасности, возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации, политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации.

Второй этап (уровень)	1. Уметь реализовывать на практике принципы политики безопасности. 2. Уметь использовать закономерности преобразования данных в каналах при выполнении комплекса мер по информационной безопасности. 3. Уметь обосновывать организационно-технические мероприятия по защите информации. 4. Уметь использовать возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации.	Не умеет реализовывать на практике принципы политики безопасности, использовать возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации.	Умеет использовать некоторые возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации.	Умеет обосновывать организационно-технические мероприятия по защите информации, использует возможности организационных, аппаратных и программных средств безопасности и защиты информации.	Умеет обосновывать организационно-технические мероприятия по защите информации, использовать закономерности преобразования данных в каналах при выполнении комплекса мер по информационной безопасности, реализовывать на практике принципы политики безопасности.
Третий этап (уровень)	1. Владеть навыками анализа, обработки и интерпретации результатов решения прикладных задач управления. 2. Владеть навыками формирования комплекса мер	Не владеет навыками анализа, обработки и интерпретации результатов решения прикладных задач управления, формирова	Владеет некоторыми навыками выявления и устранения угроз информационной безопасности.	Владеет навыками выявления и устранения угроз информационной безопасности, эксплуатации современного	Владеет навыками формирования комплекса мер для управления информационной безопасностью, навыками выявления и устранения

	(правила, процедуры, практические приемы и пр.) для управления информационной безопасностью. 3. Владеть навыками организации комплекса мероприятий по защите информации в процессах автоматизированной обработки информации. 4. Владеть навыками выявления и устранения угроз информационной безопасности. 5. Владеть навыками эксплуатации современного электронного оборудования и информационно-коммуникационных технологий. 6. Владеть навыками внедрения, адаптации и настройки средств защиты прикладных ИС.	ния комплекса мер для управления информацион-ной безопасностью.		электронного оборудования и информационно-коммуника-ционных технологий.	угроз информационной безопасности, навыками эксплуатации современного электронного оборудования и информационно-коммуникационных технологий, навыками внедрения, адаптации и настройки средств защиты прикладных ИС.

ПК-19 Способность соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности; обеспечивать соблюдение режима секретности.

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения			
		2 («Не удовлетво-рительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
Первый этап (уровень)	1. Знать основные нормативные и правовые акты в области информационной безопасности и защиты информации 2. Знать также нормативные методические документы Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю в данной области. 3. Знать методы и средства правовой защиты государственной тайны и информационной безопасности.	Не знает, как соблюдать все требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности; обеспечивать соблюдение режима секретности	Знает основные нормативные и правовые акты в области информационной безопасности.	Знает нормативные и правовые акты в области информационной безопасности, нормативные методические документы ФСБ, ФСТЭК.	Знает нормативные и правовые акты в области информационной безопасности, нормативные методические документы ФСБ и ФСТЭК, методы и средства правовой защиты государственной тайны и информационной безопасности.
Второй этап (уровень)	1. Уметь использовать в практической	Не умеет использовать в	Умеет составлять основные	Умеет ориентироваться в	Умеет анализировать и

	деятельности правовые знания 2. Уметь анализировать и составлять основные правовые акты и осуществлять правовую оценку информации, используемых в профессиональной деятельности. 3. Уметь ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной деятельности и использовать их в своей деятельности. 4. Уметь предвидеть юридические опасности и угрозы и соблюдать основные правовые требования информационной безопасности, в т.ч. для защиты государственной тайны.	практической деятельности правовые знания.	правовые акты, осуществляет правовую оценку информации, используемой в профессиональной.	нормативно-правовых актах, регламентирующих сферу профессиональной деятельности и использовать их в своей деятельности.	составлять основные правовые акты и осуществлять правовую оценку информации, используемых в профессиональной деятельности, предвидеть юридические опасности и угрозы и соблюдать основные правовые требования информационной безопасности.
Третий этап (уровень)	1. Владеть основами правового мышления,	Не владеет основами правового мышления,	Владеет навыками поиска нормативно	Владеет навыками работы с нормативны	Владеет навыками работы с нормативны

	навыками самостоятельного анализа правовой информации, анализа юридических последствий, связанных с использованием информации. 2. Владеть навыками работы с нормативными правовыми актами, нормативной и технической информацией, необходимой для профессиональной деятельности. 3. Владеть навыками поиска нормативной правовой информации необходимой для профессиональной деятельности. 4. Владеть навыками обеспечения и соблюдения режима секретности.	навыками самостоятельного анализа правовой информации, анализа юридических последствий, связанных с использованием информации.	й правовой информации необходимой для профессиональной деятельности.	ми правовыми актами, нормативной и технической информацией, необходимой для профессиональной деятельности; навыками поиска нормативной правовой информации необходимой для профессиональной деятельности.	ми правовыми актами, нормативной и технической информацией, необходимой для профессиональной деятельности, навыками поиска нормативной правовой информации необходимой для профессиональной деятельности, навыками обеспечения и соблюдения режима секретности.

ПК-31 Способность принимать участие в создании системы защиты информации на объекте информатизации

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения	Критерии оценивания результатов обучения			
		2 («Не удовлетво-рительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)

	заданного уровня освоения компетенций)				
Первый этап (уровень)	1.Знать теоретические и методические основы организационной зашиты информации; 2. Знать правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны; 3. Знать место и роль информационной безопасности в системе национальной безопасности РФ.	Не знает, как создавать системы защиты информации на объекте информатизации	Знает теоретические основы организационной защиты информации.	Знает теоретические и методические основы организационной защиты информации.	Знает теоретические и методические основы организационной защиты информации, правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны.
Второй этап (уровень)	1. Уметь осуществлять меры по организованной защите информации; 2. Уметь формулировать и настраивать политику безопасности распространенных операционных систем, а также	Не умеет осуществлять меры по организованной защите информации.	Умеет осуществлять меры по организованной защите информации.	Умеет формулировать и настраивать политику безопасности распространенных операционных систем.	Умеет формулировать и настраивать политику безопасности распространенных операционных систем, осуществлять меры противодействия нарушениям сетевой

	локальных вычислительных сетей, построенных на их основе; 3. Уметь осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты.				безопасности с использованием различных программных и аппаратных средств защиты.
Третий этап (уровень)	1. Владеть навыками организации защиты информации; 2. Владеть навыками организации и обеспечения режима секретности.	Не владеет навыками организации защиты информации	Владеет основными навыками организации защиты информации	Владеет навыками организации защиты информации.	Владеет навыками организации защиты информации, организации и обеспечения режима секретности.

Критериями оценивания являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения модулей (разделов дисциплины), перечисленных в рейтинг-плане дисциплины (для экзамена: текущий контроль – максимум 40 баллов; рубежный контроль – максимум 30 баллов, поощрительные баллы – максимум 10).

Шкалы оценивания:

от 45 до 59 баллов – «удовлетворительно»;

от 60 до 79 баллов – «хорошо»;

от 80 баллов – «отлично».

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 освоени	Результаты обучения	Компетенция	Оценочные средства

я			
1-й этап Знания	Знание методологических и правовых основ и принципов формирования политики, стратегии информационной безопасности и защиты информации, их организации и оптимизации, возможности и особенности организационных и других средств безопасности и защиты информации. Знание законодательной базы и стандартов в области информационной безопасности.	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.	Практические задания, устный опрос, тестирование, экзамен
	Знание нормативных и правовых актов, нормативные методические документы Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю в области информационной безопасности и защиты информации. Знание методов и средств правовой защиты гос.тайны и информационной безопасности.	ПК-19 - Способность соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности; обеспечивать соблюдение режима секретности.	Практические задания, устный опрос, тестирование, экзамен
	Знание теоретических и методических основ организационной зашиты информации, правовых основ организации защиты государственной тайны и конфиденциальной информации, задач органов защиты государственной тайны Знание места и роли информационной безопасности в системе национальной безопасности Российской Федерации.	ПК-31 - Способность принимать участие в создании системы защиты информации на объекте информатизации.	Практические задания, устный опрос, тестирование, экзамен
2-й этап Умения	Умение реализовывать на практике принципы политики безопасности, обосновывать организационно-технические мероприятия по защите информации, использовать возможности и особенности организационных, аппаратных и программных средств	ПК-1. Способность формировать и реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на	Практические задания, устный опрос, тестирование, экзамен

	безопасности и защиты информации.	объекте информатизации, с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз.	
	Навык использования правовых знаний, навык правовой оценки информации, используемых в профессиональной практической деятельности. Способность ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной деятельности и использовать их в своей деятельности; предвидеть юридические опасности и угрозы и соблюдать основные правовые требования информационной безопасности, в т.ч. для защиты государственной тайны.	ПК-19 - Способность соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности; обеспечивать соблюдение режима секретности.	Практические задания, устный опрос, тестирование, экзамен
	Умение осуществлять меры по организованной защите информации, формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе, осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты.	ПК-31 - Способность принимать участие в создании системы защиты информации на объекте информатизации.	Практические задания, устный опрос, тестирование, экзамен
3-й этап владение навыками	Владение навыками формирования комплекса мер по управлению информационной безопасностью, по защите информации в процессах автоматизированной обработки информации. Владение навыками использования информационно-коммуникационных технологий, внедрения средств защиты прикладных ИС.	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	Практические задания, устный опрос, тестирование, экзамен

		угроз.	
	Владение навыками правового мышления, анализа правовой информации, способность предвидеть юридические последствия использования информации. Владение навыками работы с нормативными документами, нормативной и технической информацией, навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности. Владение навыками соблюдения режима секретности.	ПК-19 - Способность соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности; обеспечивать соблюдение режима секретности.	Практические задания, устный опрос, тестирование, экзамен
	Владения навыками организации защиты информации, организации и обеспечения режима секретности.	ПК-31 - Способность принимать участие в создании системы защиты информации на объекте информатизации.	Практические задания, устный опрос, тестирование, экзамен

Практические задания

Для самостоятельного освоения и/или расширения знаний, умений, владений предусмотрены несколько практических заданий − представление докладов с последующим обсуждением.

Типовые темы докладов

Модуль 1. Сущность безопасности информационных технологий в правоохранительной сфере и ее место в системе национальной безопасности

1. Становление и развитие, сущность и структура понятия «информационная безопасность в правоохранительной сфере».
2. Объекты информационной безопасности
3. Связь информационной безопасности с информатизацией общества.
4. Национальные интересы в информационной сфере как объект информационной безопасности.
5. Понятие и современная концепция национальной безопасности.
6. Место информационной безопасности в системе национальной безопасности.

Модуль 2. Современная доктрина информационной безопасности Российской Федерации

1. Понятие и назначение доктрины информационной безопасности.
2. Составляющие национальных интересов в информационной сфере, пути их достижения.
3. Виды и состав угроз информационной безопасности.
4. Принципы обеспечения информационной безопасности.
5. Особенности обеспечения информационной безопасности в различных сферах общественной жизни.

Критерии и методика оценивания докладов:

10-8 баллов студент получает, если работа выполнена в полном объеме и изложена грамотным языком в правильной логической последовательности с точным использованием специализированной терминологии; если при этом показано уверенное

владение материалом; подготовлен реферативный отчет и презентация.

7-5 баллов студент получает за работу, если она выполнена в полном объеме, но имеет некоторые недостатки. К примеру, в работе допущены один-два недочета при освещении основного содержания ответа и/или нет определенной логической последовательности, неточно используется специализированная терминология.

4-1 балл студент получает, если 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 (пропорционально количеству недочетов, ошибок, пробелов в знаниях).

Устный опрос

Устный индивидуальный опрос проводится после изучения модуля с целью выяснения наиболее сложных вопросов, степени усвоения информации. Студент излагает содержание вопроса изученной темы.

Типовые вопросы для устного опроса

1. Прогресс информационных технологий и необходимость обеспечения информационной безопасности.
2. Основные понятия информационной безопасности.
3. Структура понятия информационная безопасность.
4. Система защиты информации и ее структура.
5. Профессиональные тайны, их виды.
6. Персональные данные и их защита.
7. Информационные угрозы, их виды и причины возникновения.
8. Информационные угрозы для государства.
9. Информационные угрозы для организации.
10. Информационные угрозы для личности (физического лица).

Критерии и методика оценивания ответов:

Студенту предлагается 5 вопросов из приведенного перечня в процессе изучения материала курса (т.о. студент может набрать до 5 баллов за устные ответы), в т.ч. за каждый вопрос устного опроса начисляется:

- 1 балл, если ответ на вопрос дан верно и достаточно полно;
- 0,5 балла за неполный ответ;
- 0 баллов если ответ на устный вопрос не дан или дан неверно.

Тестирование

1. Какие законы существуют в России в области компьютерного права?
1) О государственной тайне
2) об авторском праве и смежных правах
3) о гражданском долге
4) о правовой охране программ для ЭВМ и БД
5) о правовой ответственности
6) об информации, информатизации, защищенности информации

2. Какие существуют основные уровни обеспечения защиты информации?
1) законодательный
2) административный
3) программно-технический
4) физический
5) вероятностный

6) процедурный
7) распределительный

3. Утечка информации
1) несанкционированное изменение информации, корректное по форме, содержанию, но отличное по смыслу
2) ознакомление постороннего лица с содержанием секретной информации
3) потеря, хищение, разрушение или неполучение переданных данных
Установите соответствие.

4. Укажите соответствие для всех 4 вариантов ответа:
1) это комплекс мероприятий, исключающих или ослабляющих возможность неконтролируемого выхода конфиденциальной информации за пределы контролируемой зоны за счет электромагнитных полей побочного характера и наводок
2) это комплекс мероприятий, исключающих или уменьшающих возможность неконтролируемого выхода конфиденциальной информации за пределы контролируемой зоны в виде производственных или промышленных отходов
3) это комплекс мероприятий, исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет акустических полей
4) это комплекс мероприятий, исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет распространения световой энергии
- защита информации от утечки по акустическому каналу
- Защита информации от утечки по визуально-оптическому каналу
- Защита информации от утечки по электромагнитным каналам
- Защита информации от утечки по материально-вещественному каналу

5. Установите соответствие
1) наука о скрытой передаче информации путем сохранения в тайне самого факта передачи
2) наука скрывающая содержимое секретного сообщения
- стеганография
- криптография

6. Экранирование на сетевом уровне может обеспечить:
1) разграничение доступа по сетевым адресам
2) выборочное выполнение команд прикладного протокола
3) контроль объема данных, переданных по TCP-соединению

7. В рамках программы безопасности нижнего уровня определяются:
1) совокупность целей безопасности
2) набор используемых механизмов безопасности
3) наиболее вероятные угрозы безопасности

8. Что из перечисленного относится к числу основных аспектов информационной безопасности:
1) подотчетность - полнота регистрационной информации о действиях субъектов
2) приватность - сокрытие информации о личности пользователя
3) конфиденциальность - защита от несанкционированного ознакомления

9. На современном этапе развития законодательного уровня информационной

безопасности в России важнейшее значение имеют:
1) меры ограничительной направленности
2) направляющие и координирующие меры
3) меры по обеспечению информационной независимости

10. Меры информационной безопасности направлены на защиту от:
1) нанесения неприемлемого ущерба
2) нанесения любого ущерба
3) подглядывания в замочную скважину

Критерии и методика оценивания ответов:
Всего студенту предлагается 25 вопросов из материала изученного модуля.

Критерии оценки

Даны верные ответы на количество вопросов	Распределение баллов
25-21	10-9
20-16	8-7
15-11	6-5
10-6	4-3
5-0	2-0

Экзамен

Типовые экзаменационные вопросы

1. Становление и развитие понятия «информационная безопасность».
2. Современные подходы к определению понятия «безопасности информационных технологий в правоохранительной сфере».
3. Программно-аппаратные средства обеспечения безопасности информационных технологий в правоохранительной сфере.
4. Сущность и структура понятия «информационная безопасность».
5. Объекты информационной безопасности в правоохранительной системе.
6. Связь информационной безопасности с информатизацией общества.
7. Определение понятия «информационная безопасность».
8. Значение информационной безопасности и ее место в правоохранительной сфере.
9. Значение информационной безопасности для субъектов информационных отношений.
10. Национальные интересы в информационной сфере как объект информационной безопасности.
11. Национальные интересы и их содержание. Социальные интересы личности в информационной сфере.
12. Интересы общества в информационной сфере.
13. Интересы государства в информационной сфере.
14. Интересы сохранения национальной идентичности.
15. Безопасность национальных интересов в информационной сфере.
16. Соотношение национальных интересов и национальной безопасности.
17. Национальные интересы и безопасность России.
18. История развития представлений о национальной безопасности.
19. Современная концепция национальной безопасности.
20. Место информационной безопасности в системе национальной безопасности.
21. Понятие и назначение доктрины информационной безопасности.
22. Интересы личности, общества и государства в информационной сфере.

23. Составляющие национальных интересов в информационной сфере, пути их достижения.
24. Виды и состав угроз информационной безопасности.
25. Состояние информационной безопасности Российской Федерации и основные задачи по ее обеспечению.
26. Принципы обеспечения информационной безопасности.
27. Общие методы обеспечения информационной безопасности.
28. Особенности обеспечения информационной безопасности в различных сферах общественной жизни.
29. Основные положения государственной политики обеспечения информационной безопасности, мероприятия по их реализации.
30. Организационная основа системы обеспечения информационной безопасности.
31. Существующие подходы к содержательной части понятия «защита информации».
32. Понятие уязвимости информации.
33. Виды уязвимости информации.
34. Формы и причины проявления уязвимости информации.
35. Несовершенство или нарушения организации работы с информацией или с носителем информации как причина проявления ее уязвимости.
36. Несовершенство системы защиты информации или нарушения в обеспечении информационной безопасности как причина проявления ее уязвимости.
37. Негативные социальные и психологические явления, происходящие в организации или ее структурном подразделении как причина проявления уязвимости информации.
38. Высокая ценность информации как причина проявления ее уязвимости.
39. Уязвимость и информационный риск.
40. Понятие, причины и условия утечки защищаемой информации.

Образец экзаменационного билета

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
«Введение в специальность»

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Сущность и структура понятия «информационная безопасность».
2. Несовершенство системы защиты информации или нарушения в обеспечении информационной безопасности как причина проявления ее уязвимости.

Зав. кафедрой управления информационной безопасностью /А.С. Исмагилова /

Перевод оценки из 100-балльной в пятибалльную производится следующим образом:
- отлично – от 80 до 110 баллов (включая 10 поощрительных баллов);

- хорошо – от 60 до 79 баллов;
- удовлетворительно – от 45 до 59 баллов;
- неудовлетворительно – менее 45 баллов.

Критерии оценивания результатов экзамена: При выставлении баллов именно за экзамен (до 30 баллов в дополнение к баллам, полученным за другие виды отчетности) действует такой критерий оценки:

25-30 баллов

Студент дал полные, развернутые ответы на теоретический вопрос билета и правильно выполнил практическое задание, продемонстрировал знание функциональных возможностей, терминологии, умение применять теоретические знания при выполнении практических заданий. Студент без затруднений ответил на дополнительные вопросы. Практическая часть работы выполнена полностью без неточностей и ошибок.

17-24 баллов

Студент раскрыл в основном теоретический вопрос, однако допущены неточности в определении основных понятий. При ответе на дополнительные вопросы допущены небольшие неточности. При выполнении практической части работы допущены несущественные ошибки, но все задание выполнено до конца.

10-16 баллов

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. Теоретические вопросы в целом изложены достаточно, но с пропусками материала. Имеются принципиальные ошибки в логике построения ответа на вопрос. Студент сделал практическое задание лишь частично.

1-10 баллов

Ответ на теоретический вопрос свидетельствует о непонимании и крайне неполном знании основных понятий и методов. Студент не смог ответить ни на один дополнительный вопрос. При этом студент не решил задачу или лишь частично (на ½ от задания).

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. Технологии защиты информации в компьютерных сетях / Н.А.Руденков, А.В.Пролетарский, Е.В.Смирнова, А.М.Суровов. - 2-е изд., испр. - М.: Национальный Открытый Университет «ИНТУИТ», 2016. - 369 с.: ил.; То же [Электронный ресурс]. - http://biblioclub.ru/index.php?page=book&id=428820
2. Прохорова О.В. Информационная безопасность и защита информации : учебник / О.В.Прохорова. - Самара: Самарский государственный архитектурно-строительный университет, 2014. - 113 с.: - ISBN 978-5-9585-0603-3. То же [Электронный ресурс]. - http://biblioclub.ru/index.php?page=book&id=438331

Дополнительная литература:

3. Бирюков, А.А. Информационная безопасность: защита и нападение [Электронный

ресурс] / А.А. Бирюков. - Электрон. дан. – М.: ДМК Пресс, 2017. - 434 с. - Режим доступа: https://e.lanbook.com/book/93278
4. Бирюков, А.А. Информационная безопасность: защита и нападение [Электронный ресурс]: учебник / А.А. Бирюков. - Электрон. дан. – М.: ДМК Пресс, 2012. - 474 с. - Режим доступа: https://e.lanbook.com/book/39990
5. Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации: учебное пособие / Ю.Н.Загинайлов. - М., Берлин: Директ-Медиа, 2015. - 253 с. ISBN 978-5-4475-3946-7. То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=276557

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

- Словари и энциклопедии On-Line – http://www.dic.academic.ru
- Наиболее обширная электронная база учебников и методических материалов на сайте информационной системы «Единое окно доступа к образовательным ресурсам»; http://window.edu.ru/
- Электронная библиотечная система БашГУ – http://www.bashlib.ru
- Электронная библиотечная система «ЭБ БашГУ» – https://elib.bashedu.ru/
- Электронная библиотечная система «Университетская библиотека онлайн» – https://biblioclub.ru/
- Научная электронная библиотека – http://www.elibrary.ru
- Электронная библиотечная система издательства «Лань» – https://e.lanbook.com/
- Электронный каталог Библиотеки БашГУ – http://www.bashlib.ru/catalogi/
- Справочная правовая система «Консультант Плюс» – http://www.consultant-plus.ru
- Сайт ФСТЭК России – www.fstec.ru
- Сайт ФСБ России – www.fsb.ru
- Справочная правовая система «КонсультантПлюс» – http://www.consultant-plus.ru
- Система централизованного тестирования БашГУ (Moodle).GNU General Public License

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

Наименование специализированных аудиторий, кабинетов, лабораторий	Вид занятий	Наименование оборудования, программного обеспечения
1	2	3
1. учебная аудитория для проведения занятий лекционного типа: аудитория № 403 (гуманитарный корпус), аудитория № 405 (гуманитарный корпус), аудитория № 413 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный	Лекционные занятия	Аудитория № 403 Учебная мебель, доска, Мультимедийный-проектор Panasonic PT-LB78VE – 1 шт., Экран настенный Classic Norma 244*183 – 1 шт., учебно-наглядные пособия. Аудитория № 405 Учебная мебель, доска, вокальные радиомикрофоны AKGWMS 40 – 2шт., Интер-ая система со встроенным короткофокусным проекто-ром PrometheanActivBoard 387 RPOMOUNTEST -1 шт., Ком-ер встраиваемый в кафедру INTELCorei3-4150/DDr3 4 Gb/HDD, Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт., Настольный интерактивный дисплей , ActivPanel 21S – 1 шт. , Матричный коммутатор

корпус), аудитория № 419 (гуманитарный корпус), аудитория № 515 (гуманитарный корпус), аудитория № 516 (гуманитарный корпус).		сигналов интерфейса HDMICMPRO 4H4H – 1 шт. , Мультимедиа-проектор PanasonicPT-EW640E - 1 шт., Двух-полосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W)(белый) -6 шт., Петличный радиомикрофон AKGWMS45 – 1 шт. , Терминал видео конференц-связи LifeSizeIcon 600 Camera 10xPhone 2ndGeneration – 1 шт., Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт. Аудитория № 413 Учебная мебель, доска, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 6 шт., Микшер-усилитель 120Вт 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. Аудитория № 509 Учебная мебель, доска, мобильное мультимедийное оборудование. Аудитория № 608 Учебная мебель, доска, мобильное мультимедийное оборудование. Аудитория № 609
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).	Практические (семинарские) занятия	
3. 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),	Консультации	

компьютерный класс аудитория № 420 (гуманитарный корпус).		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 1. Windows 8 Russian Russian OLP NL AcademicEdition и Windows Professional 8 Russian Upgrade OLP NL Academic Edition. Договор №104 от 17.06.2013 г. Лицензии бессрочные. 2. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные. 3. Система централизованного тестирования БашГУ (Moodle). GNU General Public License. 4. Правовая система «КонсультантПлюс». Договор №28826 от 09.01.2019 г. Лицензии бессрочные.
4. учебная аудитория для текущего контроля и промежуточной аттестации: аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус), компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус).	Текущий контроль и промежуточная аттестация	
5. помещения для самостоятельной работы: аудитория № 613 (гуманитарный корпус), читальный зал библиотеки аудитория 402 (гуманитарный корпус).	Самостоятельная работа студентов	

Приложение 1

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

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ

дисциплины **Введение в специальность**
на 1 семестр ОФО

Вид работы	**Объем дисциплины**
Общая трудоемкость дисциплины (ЗЕТ / часов)	4 ЗЕТ / 144 часов
Учебных часов на контактную работу с преподавателем:	55,2
лекций	18
практических/ семинарских	36
лабораторных	
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	
Учебных часов на самостоятельную работу обучающихся (СР)	27
Учебных часов на подготовку к экзамену/зачету/дифференцированному зачету (Контроль)	61,8

Форма контроля:
экзамен 1 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	ЛР	СРС			
1	2	4	5	6	7	8	9	10
1	Модуль 1. Сущность безопасности информационных технологий в правоохранительной сфере и ее место в системе национальной безопасности: Становление и развитие, сущность и структура понятия «информационные технологии и безопасность». Объекты информационной безопасности. Связь информационной безопасности с информатизацией общества. Национальные интересы в информационной сфере как объект информационной безопасности. Понятие и современная концепция безопасности информационных технологий в правоохранительной сфере.	9	18	-	13	1-5	Самостоятельное изучение рекомендуемых источников и материалов, подготовка к практическому занятию и тестированию.	ПЗ, СР

	Обеспечение информационной безопасности в правоохранительной сфере.							
2	Модуль 2. Современная доктрина информационной безопасности Российской Федерации: Составляющие национальных интересов в информационной сфере, пути их достижения. Виды и состав угроз информационной безопасности. Принципы обеспечения информационной безопасности. Особенности обеспечения информационной безопасности в различных сферах общественной жизни. Сущность уязвимости и утечки информации.	9	18	-	14	1-5	Самостоятельное изучение рекомендуемых источников и материалов, подготовка к практическому занятию и тестированию.	ПЗ, СР
	Итого	18	36	-	27			

ПЗ – практическое задание, СР – самостоятельная работа

Приложение 2

Рейтинг-план дисциплины

Введение в специальность

Специальность 10.05.05 Безопасность информационных технологий в правоохранительной сфере

Курс – 1, семестр – 1

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1				
Текущий контроль			0	20
Аудиторная работа (практические работы)	10	2	0	20
Рубежный контроль				15
1. Устный опрос	1	5	0	5
2. Тест 1	10	1		10
Всего				**35**
Модуль 2				
Текущий контроль				20
Аудиторная работа (практические работы)	10	2	0	20
Рубежный контроль				15
1. Устный опрос	5	1	0	5
2. Тест 2	10	1	0	10
Всего				**35**
Поощрительные баллы				
1. Студенческая олимпиада			0	4
2. Публикация статей, участие в конференции			0	6
Всего				**10**
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
1. Посещение лекционных занятий				-6
2. Посещение практических занятий				-10
Итоговый контроль				
Экзамен			0	30