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

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

Согласовано:
Председатель УМК института
/ Р.А. Гильмутдинова

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Организация и управление службой защиты информации
Б1.В.1.ДВ.02.01 (дисциплина по выбору)

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)
Доцент, канд.филос.наук / Миронова Н.Г.

Для приема: 2014 г.

Уфа 2018 г.

Составитель: Н.Г. Миронова

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

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры управления информационной безопасностью, протокол № __ от «__» _____ 20__ г.

Заведующий кафедрой / Исмагилова А.С.

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

Заведующий кафедрой _____/ _____Ф.И.О/

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

Заведующий кафедрой _____/ _____Ф.И.О/

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

Заведующий кафедрой _____/ _____Ф.И.О/

Список документов и материалов

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с 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 принципы функционирования профессионального коллектива, 2. Знать психологические основы профессионального общения и психологические основы предупреждения и разрешения конфликтов в профессиональной деятельности 3. Знать социальные, этнические, конфессиональные и культурные особенности представителей тех или иных социальных общностей. 4. Знать роль корпоративных норм и стандартов.	ОК-5: Способность работать в коллективе, толерантно воспринимая социальные, культурные, конфессиональные и иные различия, предупреждать и конструктивно разрешать конфликтные ситуации в процессе профессиональной деятельности	
	1. Знать источники вредных и опасных факторов среды обитания 2. Знать анатомо-физиологические свойства человека и его реакции на воздействие негативных факторов	ПК-11. Способность выполнять профессиональные задачи в особых условиях, чрезвычайных обстоятельствах, чрезвычайных ситуациях, в условиях режима чрезвычайного положения и в военное время	
	1. Знать политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации 2. Знать понятие системы управления, основные виды структур, принципы системного подхода к анализу структур;	ПК-13: Способность осуществлять организационно-правовое обеспечение деятельности по получению, накоплению, обработке, анализу, использованию информации и защите объектов информатизации, информационных технологий и ресурсов	
	1. Знать технологии организации деятельности и рабочего места сотрудников 2. Знать основы планирования, контроля и учета результатов деятельности 3. Знать основы формирования модели трудового поведения	ПК-14: Способность планировать и организовывать служебную деятельность подчиненных, осуществлять контроль и учет ее результатов	
	1. Знать понятие документирования и документооборота. 2. Знать виды и формы документов, требования к их оформлению. 3. Знать нормативные правовые и организационные основы делопроизводства и документационного обеспечения управленческой и информационно-аналитической деятельности в правоохранительных органах.	ПК-16: Способность осуществлять документационное обеспечение управленческой деятельности	
	1. Знать способы применения методов аналитической разведки, осуществления оперативно-аналитического поиска,	ПК-23. Способность применять методы аналитической разведки, осуществлять оперативно-	

	оперативно-розыскного анализа, идентификации, диагностики, прогнозирования; криминалистической диагностики	аналитический поиск, оперативно-розыскной анализ, идентификацию, диагностику, прогнозирование; криминалистическую диагностику.	
Умения	1. Уметь правильно строить общение с коллегами в служебном коллективе и гражданами, в т.ч. с представителями различных социальных групп, национальностей и конфессий. 2. Уметь диагностировать причины конфликта, вырабатывать и применять стратегии поведения в ходе конфликта, использовать различные методы и способы предотвращения и позитивного разрешения конфликтов. 3. Уметь анализировать механизмы возникновения и разрешения социальных конфликтов, природу и возможные пути предупреждения девиантного поведения в различных группах социального риска.	ОК-5: Способность работать в коллективе, толерантно воспринимая социальные, культурные, конфессиональные и иные различия, предупреждать и конструктивно разрешать конфликтные ситуации в процессе профессиональной деятельности	
	1. Уметь проводить анализ возможных вредных и опасных факторов и возможных чрезвычайных ситуаций 2. Уметь прогнозировать возможность выполнения профессиональной деятельности в особых условиях 3. Уметь разрабатывать стратегию обеспечения личной безопасности и безопасности граждан с использованием современных средств защиты[информации]	ПК-11. Способность выполнять профессиональные задачи в особых условиях, чрезвычайных обстоятельствах, чрезвычайных ситуациях, в условиях режима чрезвычайного положения и в военное время	
	1. Уметь реализовывать на практике принципы политики безопасности. 2.Уметь использовать методы количественного представления информации и основные закономерности ее преобразования в каналах при выполнении комплекса мер по информационной безопасности.	ПК-13: Способность осуществлять организационно-правовое обеспечение деятельности по получению, накоплению, обработке, анализу, использованию информации и защите объектов информатизации, информационных технологий и ресурсов	
	1. Уметь применять современные методы оценки персонала в планировании, контроле и учете деятельности сотрудников и их трудового поведения.	ПК-14: Способность планировать и организовывать служебную деятельность подчиненных, осуществлять контроль и учет ее результатов	
	1. Уметь применять нормы информационного права в профессиональной деятельности 2. Уметь использовать в профессиональной деятельности нормативные правовые акты и методические документы в области защиты информации и обеспечения информационной безопасности.	ПК-16: Способность осуществлять документационное обеспечение управленческой деятельности	
	1. Уметь применять методы аналитической разведки, осуществлять оперативно-аналитический поиск, оперативно-розыскной анализ, идентификацию, диагностику, прогнозирование; криминалистическую диагностику	ПК-23. Способность применять методы аналитической разведки, осуществлять оперативно-аналитический поиск, оперативно-розыскной анализ, идентификацию, диагностику, прогнозирование;	

		криминалистическую диагностику	
Навыки, опыт деятельности	1. Владеть навыками установления психологического контакта. 2. Владеть правильного поведения в конфликтной ситуации.	ОК-5: Способность работать в коллективе, толерантно воспринимая социальные, культурные, конфессиональные и иные различия, предупреждать и конструктивно разрешать конфликтные ситуации в процессе профессиональной деятельности	
	1. Владеть навыками выполнения профессиональных задач в особых условиях 2.Владеть принимать адекватные меры по обеспечению личной безопасности и безопасности граждан в процессе решения служебных задач	ПК-11. Способность выполнять профессиональные задачи в особых условиях, чрезвычайных обстоятельствах, чрезвычайных ситуациях, в условиях режима чрезвычайного положения и в военное время	
	1. Владеть навыками анализа, обработки и интерпретации результатов решения прикладных задач управления; навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью 2. Владеть навыками организации комплекса мероприятий по защите информации в процессах автоматизированной обработки информации	ПК-13: Способность осуществлять организационно-правовое обеспечение деятельности по получению, накоплению, обработке, анализу, использованию информации и защите объектов информатизации, информационных технологий и ресурсов	
	1. Владеть навыками аттестации и оценки персонала.	ПК-14: Способность планировать и организовывать служебную деятельность подчиненных, осуществлять контроль и учет ее результатов	
	1. Владеть навыками работы с документами ограниченного доступа и обеспечения их защиты.	ПК-16: Способность осуществлять документационное обеспечение управленческой деятельности	
	1. Владеть навыками систематического применения методов аналитической разведки, осуществления оперативно-аналитического поиска, оперативно-розыскного анализа, идентификации, диагностики, прогнозирования; криминалистической диагностики	ПК-23. Способность применять методы аналитической разведки, осуществлять оперативно-аналитический поиск, оперативно-розыскной анализ, идентификацию, диагностику, прогнозирование; криминалистическую диагностику	

2. Цели и место дисциплины в структуре образовательной программы

Дисциплина «Организация и управление службой защиты информации» относится к дисциплинам вариативной части образовательной программы.

Дисциплина «Организация и управление службой защиты информации» изучается на 5 курсе в семестре А.

Цели изучения дисциплины - получение знаний, компетенций в следующих областях: организация и задачи службы информационной безопасности, организационно-технические мероприятия по защите информации, порядок организации работ по защите информации в ведомствах и на предприятиях (порядок проведения охраны предприятия, организация пропускного режима, проведение разработки системы защиты информации, порядок проведения аттестации и лицензирование объекта информатизации др. организационные меры информационной защиты).

Для освоения дисциплины «Организация и управление службой защиты информации» необходимы знания и компетенции ОК-5; ПК-11, ПК-13; ПК-14; ПК-16, ПК-23, сформированные в процессе изучения дисциплин: «Информационная безопасность в правоохранительной сфере», «Кадровая безопасность в правоохранительной сфере», «Менеджмент», «Безопасность жизнедеятельности», «Международные и российские акты и стандарты по информационной безопасности», «Организационная зашита информации», «Правовая защита информации», «Правовая охрана результатов интеллектуальной деятельности», «Системы организационного управления», «Управление информационной безопасностью», «Управление персоналом», «Управление трудовыми конфликтами», «Электронный документооборот». Полученные знания, навыки и умения используются при прохождении преддипломной практики и в ходе выполнения выпускной квалификационной работы.

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-5: Способность работать в коллективе, толерантно воспринимая социальные, культурные, конфессиональные и иные различия, предупреждать и конструктивно разрешать конфликтные ситуации в процессе профессиональной деятельности.

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения	
		«Не зачтено»	«Зачтено»
Первый этап (уровень)	Знание принципов функционирования профессионального коллектива, роли корпоративных норм и стандартов.	Не знает	Демонстрирует целостные, системные знания в указанной сфере.
Второй этап	Умение правильно строить общение с коллегами в служебном коллективе, применять стратегии поведения в ходе конфликта, способы предотвращения и позитивного разрешения конфликтов.	Не умеет	Демонстрирует уверенное, свободное владение указанными социальными навыками при решении задач организации службы защиты информации

Третий этап	Владение навыками установления психологического контакта, правильного поведения в конфликтной ситуации. Знать, понимать психологически основы поведения и мотивацию потенциальных нарушителей (злоумышленников) при планировании и реализации стратегии и тактики ИБ.	Не владеет	Демонстрирует уверенное, свободное владение указанными социальными навыками при решении задач организации службы защиты информации

ПК-11. Способность выполнять профессиональные задачи в особых условиях, чрезвычайных обстоятельствах, чрезвычайных ситуациях, в условиях режима чрезвычайного положения и в военное время

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения	
		«Не зачтено»	«Зачтено»
Первый этап (уровень)	1. Знать источники вредных и опасных факторов среды обитания 2.Знать анатомо-физиологические свойства человека и его реакции на воздействие негативных факторов 3.Знать основы оказания первой помощи	Не знает	Демонстрирует целостные, системные знания в указанной сфере.
Второй этап	1. Уметь проводить анализ возможных вредных и опасных факторов и возможных чрезвычайных ситуаций 2. Уметь оказывать первую помощь 3. Уметь прогнозировать возможность выполнения профессиональной деятельности в особых условиях 4. Уметь разрабатывать стратегию обеспечения личной безопасности и безопасности граждан с использованием современных средств защиты	Не умеет	Демонстрирует уверенное, свободное владение указанными социальными навыками при решении задач организации службы защиты информации

Третий этап	1. Владеть навыками выполнения профессиональных задач в особых условиях 2.Владеть принимать адекватные меры по обеспечению личной безопасности и безопасности граждан в процессе решения служебных задач	Не владеет	Демонстрирует уверенное, свободное владение указанными социальными навыками при решении задач организации службы защиты информации

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	
		«Не зачтено»	«Зачтено
Первый этап	Знание политики и стратегии информационной безопасности, технологий и способов организации защиты информации и их оптимизации. Знание понятийи принципов управления.	Не знает	Демонстрирует целостные, системные знания в указанной сфере.
Второй этап	Умение применять на практике принципы политики безопасности, использовать методы количественного представления информации при выполнении комплекса мер по информационной безопасности.	Не умеет	Демонстрирует уверенное, свободное владение указанными навыками при решении задач организации службы защиты информации
Третий этап	Владение навыками анализа, обработки и интерпретации результатов	Не владеет	Демонстрирует уверенное, свободное владение указанными навыками при решении задач организации службы защиты информации.

	решения задач управления, формирования комплекса мер (правил, процедур, приемов и пр.) для управления информационной безопасностью, навыками организации мероприятий по защите информации в процессах автоматизированнй обработки информации		

ПК-14: Способность планировать и организовывать служебную деятельность подчиненных, осуществлять контроль и учет ее результатов

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения	
		«Не зачтено»	«Зачтено»
Первый этап	Знание технологии организации деятельности и рабочего места сотрудников, основы планирования, контроля и учета результатов деятельности.	Не знает	Демонстрирует целостные, системные знания в указанной сфере.
Второй этап	Умение применять современные методы оценки персонала в планировании, контроле и учете деятельности сотрудников и их трудового поведения.	Не умеет	Демонстрирует уверенное, свободное владение указанными навыками при решении задач организации службы защиты информации

Третий этап	Владение навыками аттестации и оценки персонала	Не владеет	Демонстрирует уверенное, свободное владение актуальными указанными знаниями и навыками при решении задач организации службы защиты информации.

ПК-16: Способность осуществлять документационное обеспечение управленческой деятельности.

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения	
		«Не зачтено»	«Зачтено»
Первый этап	Представление о документировании и документообороте, видах документов, требованиях к их оформлению. Знание правовых и организационных основ документационного обеспечения управленческой и информационно-аналитической деятельности (при решении задач организации службы защиты информации)	Не демонстрирует указанных знаний	Демонстрирует целостные, системные знания в указанной сфере, свободно ориентируется в них при решении практических задач.
Второй этап	Умение применять нормы информационного права, нормативные правовые и методические документы в области защиты информации и обеспечения информационной безопасности.	Не умеет	Демонстрирует уверенное, свободное владение указанными навыками при решении задач организации службы защиты информации
Третий этап	Владение навыками работы с документами ограниченного	Не владеет и не имеет теоретических знаний об этой сфере	Демонстрирует уверенное, свободное владение навыками при решении задач организации службы ЗИ.

	доступа и обеспечения их защиты.		

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	
		«Не зачтено»	«Зачтено»
Первый этап	Знание способов применения методов аналитической разведки, осуществления оперативно-аналитического поиска, оперативно-розыскного анализа, идентификации, диагностики, прогнозирования; криминалистической диагностики	Не демонстрирует указанных знаний	Демонстрирует целостные, системные знания в указанной сфере, свободно ориентируется в них при решении практических задач.
Второй этап	Умение применять методы аналитической разведки, осуществлять оперативно-аналитический поиск, оперативно-розыскной анализ, идентификацию, диагностику, прогнозирование; криминалистическую диагностику	Не умеет	Демонстрирует уверенное, свободное владение указанными навыками при решении задач организации службы защиты информации
Третий этап	Владение навыками систематического применения методов аналитической разведки, осуществления оперативно-	Не владеет и не имеет теоретических знаний об этой сфере	Демонстрирует уверенное, свободное владение указанными навыками при решении задач организации службы защиты информации.

	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, перечисленных в рейтинг-плане дисциплины (для зачета: текущий контроль – максимум 50 баллов; рубежный контроль – максимум 50 баллов, поощрительные баллы – максимум 10).

Шкала оценивания для зачета:

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

не зачтено – от 0 до 59 рейтинговых 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 Знания	Знание принципов функционирования профессионального коллектива, роли корпоративных норм и стандартов.	ОК-5: Способность работать в коллективе, толерантно воспринимая социальные, культурные, конфессиональные и иные различия, предупреждать и конструктивно разрешать конфликтные ситуации в процессе профессиональной деятельности	Тесты, практические и лабораторные задания, контрольная работа, доклад, собеседование (коллоквиум).
	Знание опасных факторов среды.	ПК-11. Способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	Тесты, практические и лабораторные задания, контрольная работа, доклад, собеседование (коллоквиум).
	Знание политики и стратегии информационной безопасности, технологий и способов организации защиты информации и их оптимизации. Знание понятий и принципов управления.	ПК-13: Способность осуществлять организационно-правовое обеспечение деятельности по получению, накоплению, обработке, анализу, использованию информации и защите объектов информатизации, информационных технологий и ресурсов	Тесты, практические и лабораторные задания, контрольная работа, доклад, собеседование (коллоквиум).
	Знание технологии	ПК-14: Способность	Тесты, практические и

	организации деятельности и рабочего места сотрудников, основы планирования, контроля и учета результатов деятельности.	планировать и организовывать служебную деятельность подчиненных, осуществлять контроль и учет ее результатов	лабораторные задания, контрольная работа, доклад, собеседование (коллоквиум).
	Представление о документировании и документообороте, видах документов, требованиях к их оформлению. Знание правовых и организационных основ документационного обеспечения управленческой и информационно-аналитической деятельности (при решении задач организации службы защиты информации)	ПК-16: Способность осуществлять документационное обеспечение управленческой деятельности	Тесты, практические и лабораторные задания, контрольная работа, доклад, собеседование (коллоквиум).
	Знание способов применения методов аналитической разведки, осуществления оперативно-аналитического поиска, оперативно-розыскного анализа, идентификации, диагностики, прогнозирования; криминалистической диагностики	ПК-23. Способность применять методы аналитической разведки, осуществлять оперативно-аналитический поиск, оперативно-розыскной анализ, идентификацию, диагностику, прогнозирование; криминалистическую диагностику.	Тесты, практические задания, контрольная работа, доклад, собеседование (коллоквиум).
2-й этап Умения	Умение правильно строить общение с коллегами в служебном коллективе, применять стратегии поведения в ходе конфликта, способы предотвращения и позитивного разрешения конфликтов.	ОК-5: Способность работать в коллективе, толерантно воспринимая социальные, культурные, конфессиональные и иные различия, предупреждать и конструктивно разрешать конфликтные ситуации в процессе профессиональной деятельности	Тесты, практические задания, контрольная работа, доклад, собеседование (коллоквиум).
	Навык проведения анализа возможных опасных факторов, прогнозирования возможности выполнения профессиональной деятельности в особых условиях, способность разрабатывать стратегию обеспечения личной безопасности и безопасности граждан с использованием	ПК-11. Способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	Тесты, практические задания, контрольная работа, доклад, собеседование (коллоквиум).

	современных средств защиты[информации].		
	Умение применять на практике принципы политики безопасности, использовать методы количественного представления информации при выполнении комплекса мер по информационной безопасности.	ПК-13: Способность осуществлять организационно-правовое обеспечение деятельности по получению, накоплению, обработке, анализу, использованию информации и защите объектов информатизации, информационных технологий и ресурсов	Тесты, практические задания, контрольная работа, доклад, собеседование (коллоквиум).
	Умение применять современные методы оценки персонала в планировании, контроле и учете деятельности сотрудников и их трудового поведения.	ПК-14: Способность планировать и организовывать служебную деятельность подчиненных, осуществлять контроль и учет ее результатов	Тесты, практические задания, контрольная работа, доклад, собеседование (коллоквиум).
	Умение применять нормы информационного права, нормативные правовые и методические документы в области защиты информации и обеспечения информационной безопасности.	ПК-16: Способность осуществлять документационное обеспечение управленческой деятельности	Тесты, практические задания, контрольная работа, доклад, собеседование (коллоквиум).
	Умение применять методы аналитической разведки, осуществлять оперативно-аналитический поиск, оперативно-розыскной анализ, идентификацию, диагностику, прогнозирование; криминалистическую диагностику	ПК-23. Способность применять методы аналитической разведки, осуществлять оперативно-аналитический поиск, оперативно-розыскной анализ, идентификацию, диагностику, прогнозирование; криминалистическую диагностику.	Тесты, практические задания, контрольная работа, доклад, собеседование (коллоквиум).
3-й этап владение навыками	Владение навыками установления психологического контакта, правильного поведения в конфликтной ситуации. Знать, понимать психологически основы поведения и мотивацию потенциальных нарушителей (злоумышленников) при планировании и реализации стратегии и тактики ИБ.	ОК-5: Способность работать в коллективе, толерантно воспринимая социальные, культурные, конфессиональные и иные различия, предупреждать и конструктивно разрешать конфликтные ситуации в процессе профессиональной деятельности	Тесты, практические задания, контрольная работа, доклад, собеседование (коллоквиум).
	Владение навыками выполнения профессиональных задач в	ПК-11. Способность проводить эксперименты по заданной методике,	Тесты, практические задания, контрольная работа, доклад,

	особых условиях	обработку, оценку погрешности и достоверности их результатов	собеседование (коллоквиум).
	Владение навыками анализа, обработки и интерпретации результатов решения задач управления, формирования комплекса мер (правил, процедур, приемов и пр.) для управления информационной безопасностью, навыками организации мероприятий по защите информации в процессах автоматизированной обработки информации	ПК-13: Способность осуществлять организационно-правовое обеспечение деятельности по получению, накоплению, обработке, анализу, использованию информации и защите объектов информатизации, информационных технологий и ресурсов	Тесты, практические задания, контрольная работа, доклад, собеседование (коллоквиум).
	Владение навыками аттестации и оценки персонала	ПК-14: Способность планировать и организовывать служебную деятельность подчиненных, осуществлять контроль и учет ее результатов	Тесты, практические задания, контрольная работа, доклад, собеседование (коллоквиум).
	Владение навыками работы с документами ограниченного доступа и обеспечения их защиты.	ПК-16: Способность осуществлять документационное обеспечение управленческой деятельности	Тесты, практические задания, контрольная работа, доклад, собеседование (коллоквиум).
	Владение навыками систематического применения методов аналитической разведки, осуществления оперативно-аналитического поиска, оперативно-розыскного анализа, идентификации, диагностики, прогнозирования; криминалистической диагностики	ПК-23. Способность применять методы аналитической разведки, осуществлять оперативно-аналитический поиск, оперативно-розыскной анализ, идентификацию, диагностику, прогнозирование; криминалистическую диагностику.	Тесты, практические задания, контрольная работа, доклад, собеседование (коллоквиум).

Формы и виды контроля:

Типовые задания для тестирования

Цель проведения тестирований – проверка качества и полноты усвоения материалов дисциплины. При изучении дисциплины используются 2 теста в Модуле 1; тестовые задания - открытого типа.

Методические указания:

Каждое тестовое задание включает вопрос и несколько вариантов ответов к нему либо предполагает вписывание правильного словосочетания, термина, даты и т.п. в текст тестового вопроса. Тестирование выполняется в письменной форме или в виде on-line-

тестирования (в системе Moodle, http://moodle.bashedu.ru/) во время практических занятий по результату изучения теоретического материала. Критерии оценки каждого теста различны (баллы за тесты приводятся в конце теста).

Тест 1. Нормативная международная и отечественная база по защите информации

Внесите информацию в пустые поля в названиях нормативных документов:.

1. «_____ требования и рекомендации по технической защите конфиденциальной информации» (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.
2. «Сборник временных методик оценки защищенности конфиденциальной информации от утечки по _____каналам». Гостехкомиссия России. - М., 2002.
3. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические _____Госстандарт России. - М., 1995.
4. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие _____. Госстандарт России. - М., 2006.
5. ГОСТ Р 50922-2006. Защита информации. Основные термины и _____. - М., 2006.
6. Приказ _____ России от 08 августа 2009 г. № 149/7/2/6-1173 «Об утверждении типового регламента проведения в пределах полномочий мероприятий по контролю (надзору) за выполнением требований, установленных Правительством РФ, к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

И т.д**…**

Критерий оценивания Теста № 1: 40 вопросов – до 16 баллов (1 правильно сделанный вопрос теста = 0,4 балла)

Тест 2. Отечественные нормативные документы в области криптографической защиты

1. Постановление Правительства Российской Федерации от 16 апреля 2012 г. № _____ «Об утверждении положения о лицензировании деятельности по разработке, производству, распространению _____средств, информационных систем и телекоммуникационных систем, защищенных с использованием _____средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию _____ средств, информационных систем и телекоммуникационных систем, защищенных с использованием _____ средств (за исключением случая, если техническое обслуживание _____средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)».
2. Приказ ФСБ России от _____июля _____г. № _____ «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».
3. ГОСТ 28147-89. Государственный стандарт Российской Федерации. Системы обработки _____Защита криптографическая. Алгоритм криптографического преобразования.
4. ГОСТ Р 34.10-2001. Государственный стандарт Российской Федерации. Информационная технология. _____защита информации. Процессы формирования и проверки электронной цифровой подписи.
5. ГОСТ Р 34.10- _____ Государственный стандарт Российской Федерации. Информационная технология. _____защита информации. Процессы формирования и проверки электронной цифровой подписи.

И т.д.

Критерий оценивания Теста № 2: 10 вопросов – до 4 баллов (1 правильно сделанный вопрос теста = 0,4 балла)

Примерные темы практических занятий

Модуль 1.Основные организационные меры по защите информации

Тема 1.1. Взаимосвязь организационных, технологических, координационных задач и функций службы защиты информации (2 часа)

Цель занятия: ознакомление с задачами и функциями службы защиты информации.

Содержание занятия: усвоение материала студентами и подготовка отчетов в форме докладов на нижеприведенные темы. Тестирование.

Список тем для изучения:

1. Государственная политика РФ в области защиты информации.
2. Состав, структура и основные направления деятельности служб безопасности
3. Организация защиты информации – основные направления.
4. Классификация защищаемой информации.
5. Правовое обеспечение информационной безопасности. Российские документы по защите информации.
6. Организационное обеспечение информационной безопасности
7. Нормативные документы ФСТЭК и ГОСТы, регулирующие работу службы защиты информации предприятий и ведомственных организаций.
8. Тестирование (тест 1).

Тема 1.2. Структурная схема службы защиты информации. Факторы, влияющие на задачи и функции службы защиты информации. Должностной состав сотрудников службы защиты информации (2 часа)

Цель занятия: дальнейшее ознакомление с функциональными обязанностями специалистов службы защиты информации.

Содержание занятия: усвоение материала студентами и подготовка отчетов в форме докладов на нижеприведенные темы. Тестирование.

Список тем для изучения:

1. Основные направления деятельности служб безопасности фирм, организаций, ведомственных учреждений.
2. Функции службы защиты информации в организации/на предприятии.
3. Организационно-функциональные документы системы безопасности предприятия.
4. Концептуальные модели компонентов системы безопасности предприятия
5. Организационно-функциональные документы системы безопасности предприятия. - Виды нормативных документов
6. Структура и содержание положения о службе защиты информации.
7. Составление организационно-функциональных документов СЗИ предприятия/организации.
8. **Практическое задание 1:** Соотнесите функции службы управления персоналом с функциями службы безопасности организации и заполните таблицу:

Функции службы управления персоналом	Функции службы безопасности организации
Отбор персонала	…
Оформление на работу	…
Адаптация работника	…
Управление конфликтами	…
Управление трудовой дисциплиной	…

9. Тестирование (тест 2).

Тема 1.3. Структура и содержание положения о службе защиты информации. Задачи, функции, права и ответственность сотрудников службы защиты информации. Распределение обязанностей между сотрудниками службы защиты информации (2 часа)

Цель занятия: нормативное регулирование деятельности службы защиты информации. Задачи и права специалистов СЗИ. Практическое решение проблем.

Содержание занятия: усвоение материала студентами и подготовка отчетов в форме докладов на нижеприведенные темы, а также решение конкретных практических проблем.

Список тем для изучения:

1. Законодательные и нормативные акты РФ в области защиты информации. Основные законы в области информационной безопасности.
2. Указы президента РФ и постановления правительства РФ в области информации и информационной безопасности.
3. **Практическое задание 2:** Методические документы ФСТЭК по организации и функционированию службы информационной безопасности (ознакомиться самостоятельно, сделать краткий обзор изученных документов с характеристикой содержания каждого)
4. Трудовой кодекс – об ответственности за нарушение требований к защите конфиденциальной и секретной информации.
5. Задачи, функции, права и ответственность сотрудников службы защиты информации.
6. Распределение обязанностей между сотрудниками службы защиты информации.

Практическое задание 3: Вы - руководитель службы безопасности - включены в состав комиссии по разработке программы экономической безопасности предприятия.
Задание:
- определите возможные кадровые риски;
- оцените вероятность этих рисков;
- разработайте мероприятия, снижающие вероятность кадровых рисков.

Тема 1.4. Методы получения информации о кандидатурах на должности службы защиты информации. Влияние социально-психологических факторов на расстановку сотрудников службы защиты информации (2 часа)

Цель занятия: оценка и расстановка сотрудников службы защиты информации.

Содержание занятия: усвоение материала студентами, решение конкретных практических проблем.

Список тем для изучения:

1. Единый квалификационный справочник должностей руководителей, специалистов и других служащих (ЕКС, 2018) – об требованиях к уровню квалификации специалистов в области управления и ЗИ.
2. Требования к уровню квалификации специалиста по информационной безопасности. Уровни допуска к секретной и конфиденциальной информации.
3. Методы и источники получения сведений о кандидатах на должность специалистов службы защиты информации.
4. Автоматизированная информационная система «Кадры».
5. Понятие информационных технологий следственной, оперативно-розыскной и экспертной деятельности.
6. Влияние социально-психологических факторов на расстановку сотрудников службы защиты информации
7. Должностные инструкции специалистов (инженеров, руководителей) СЗИ.
8. **Практическое задание 4:** Проанализируйте, какие кадровые позиции являются наиболее рискованными в различных видах бизнеса (торговые фирмы, финансовые организации, промышленные компании, туристические фирмы, государственные учреждения и т.д.).

Тема 1.5. Организационные задачи службы защиты информации (2 часа)

Цель занятия: организационная деятельность СЗИ.

Содержание занятия: усвоение материала студентами, решение конкретных практических проблем.

Список тем для изучения:

1. Рациональная структура службы информационной безопасности на предприятии /в фирме.
2. Задачи службы безопасности предприятия.
3. Состав и размер группы безопасности (варианты штатного расписания с распределением функциональных обязанностей).
4. Организационно-правовой статус службы информационной безопасности предприятия/организации.
5. Функциональные обязанностей конкретных специалистов (руководителя СИБ, администратора безопасности, инженеров и специалистов СИБ и т.д.)
6. Мероприятия по обеспечению контроля и функционирования системы защиты информации, меры реагирования на нарушение режима безопасности, планирование и организация восстановительных работ и др. (общая характеристика организационных мер, реализуемых СИБ).
7. **Практическое задание 5:** Вам как руководителю службы кадровой безопасности – директор предлагает разработать мероприятия, повышающие уровень производственной дисциплины на предприятии. **Задание**:
   - сформулируйте алгоритм Ваших действий;
   - определите оценочные показатели;
   - оцените условный социальный и экономический эффект Ваших мероприятий.

Тема 1.6. Обеспечение информационной безопасности предприятия службой защиты информации (4 часа)

Цель занятия: обеспечение информационной безопасности предприятия в составе деятельности СЗИ.

Содержание занятия: усвоение материала студентами, решение конкретных практических проблем.

Список тем для изучения:

1. Законодательное регулирование в области ответственности за нарушение требований к работе с информацией ограниченного доступа и секретной информации.
2. Организация доступа к грифованной информации.
3. Требования к персоналу, допущенного к защищаемой информации.
4. Порядок доступа и работы с информацией, содержащий сведения, отнесенные к государственной тайне. Уголовная и административная ответственность за нарушение этих требований.
5. Организация защиты коммерческой тайны.
6. Порядок изменения степени секретности.
7. Организация защиты информации в процессе проведения открытых мероприятий (международных конференций, симпозиумов, обмена специалистами и др.)
8. **Практическое задание 6:** Официант ресторана был уволен с работы по п. 5. ст. 81 ТК РФ за грубое обращение с клиентом и не оказание последнему услуг в полном объеме и с надлежащим качеством (до этого случая у официанта уже были взыскания в виде выговоров). О случае грубого обращения с клиентом администрации кафе стало известно, поскольку в зале ресторана были установлены устройства видеозаписи (персонал ресторана о наличии этих устройств уведомлен не был). Бывший работник обратился в суд, обжалуя увольнение. Представитель работодателя, возражая в суде против иска, заявил, что устройства видеозаписи были установлены в зале ресторана, то есть в месте общего пользования, где не предполагается частной жизни работника и, соответственно, охраны его частной жизни. Какое решение примет суд в этой ситуации?

Модуль 2. Организация и управление службой безопасности

Тема 2.1. Состав и содержание управленческих функций. Принципы управления службой защиты информации. Системы методов управления (2 часа)

Цель занятия: изучение организации управления службой защиты информации.

Содержание занятия: усвоение материала студентами, решение конкретных практических проблем.

Список тем для изучения:

1. Управленческие функции. Место службы безопасности в структуре управления организацией/предприятием.
2. Принципы управления службой защиты информации.
3. Документационное обеспечение СлЗИ.
4. Информационное обеспечение СлЗИ.
5. **Практическое задание 7.** Охранник учинил обыск работницы на предмет

возможного хищения ею материальных ценностей фирмы, чем вызвал ее бурную реакцию. **Задание:**

- оцените ситуацию, дав правовую оценку действий сторон,
- сформулируйте мероприятия, исключающие повторение подобных ситуаций.

Тема 2.2. Структура и содержание должностных инструкций сотрудников службы защиты информации (2 часа)

Цель занятия: должностные обязанности сотрудников службой защиты информации, составление должностной инструкции.

Содержание занятия: усвоение материала студентами, решение конкретных практических проблем.

Список тем для изучения:

1. Деловые процессы и место информации в них. Понятие технологических схем менеджмента.
2. Специфика проектной работы и технологии менеджмента.
3. Моделирование организационной структуры предприятия. Разработка орг.структуры СлЗИ.
4. Разработка должностных инструкций специалистов по ЗИ.
5. **Практическое задание 8.** Председатель Арбитражного суда Костромской области Г. установила в рабочих кабинетах некоторых судей этого суда скрытую видео- и звукозаписывающую аппаратуру, которая фиксировала все происходящее в данных помещениях в течение года. В связи с этим решением Высшей квалификационной коллегии судей РФ на Г. наложено дисциплинарное взыскание в виде досрочного прекращения ее полномочий в качестве председателя и судьи. Считая названное решение неправомерным, Г. обжаловала его в Верховный суд РФ. В жалобе Г. приводила доводы о том, что как руководитель суда она имела право установить скрытую видео- и звукозаписывающую аппаратуру в рабочих кабинетах судей на основании Закона Российской Федерации «О безопасности». Какое решение, по вашему мнению, должен принять Верховный суд РФ? Ответ обоснуйте ссылками на НПА.

Тема 2.3. Организация и технология планирования работы СЗИ (4 часа)

Цель занятия: планирование деятельности службы защиты информации.

Содержание занятия: усвоение материала студентами, решение конкретных практических проблем.

Список тем для изучения:

1. Планирование как управленческая функция.
2. Рациональные методы планирование.
3. Методики и технология планирования.
4. Методические документы ФСТЭК по работе СлЗИ, в т.ч. в области планирования СЗИ.
5. Содержание и структура планов.
6. Средства разработки и контроля планов.
7. Планирование орг.мероприятий ЗИ.
8. Контроль выполнения планов, корректировка планов. Ответственность

специалистов СЗИ.

9. **Практическое задание 9**: разработка плана работы СЗИ/СИБ.

Тема 2.4. Методы оценки эффективности и качества службы защиты информации (2 часа)

Цель занятия: оценка эффективности и качества работы службы защиты информации

Содержание занятия: усвоение материала студентами, решение конкретных практических проблем.

Список тем для изучения:

1. Порядок проведения проверок и оценка эффективности работы СЗИ. Составление отчетной документации по результатам проверок.
2. Обеспечение персональной ответственности за сохранность носителей информации. Оформление актов по результатам проверки и по выявленным нарушениям.
3. Подходы к оценке эффективности, методы и критерии оценки работы СЗИ.
4. Оценка эффективности работы службы защиты информации.
5. Аттестация объектов информатизации.
6. **Практическое задание 10.** Руководство предприятия заинтересовано в получении объективной информации в режиме реального времени о морально-психологическом климате в коллективе. **Задание:**

- дать общую характеристику мониторинга внутренней среды;
- раскрыть технику и основные показатели мониторинга.

Тема 2.5. Обеспечение персональной ответственности за сохранность носителей информации (2 часа)

Цель занятия: ответственность специалистов службы защиты информации.

Содержание занятия: усвоение материала студентами, решение конкретных практических проблем.

Список тем для изучения:

1. Административно-правовые меры и методы управления в работе СЗИ.
2. Социально-психологические методы управления в работе СЗИ.
3. Экономические методы оценки эффективности работы СЗИ.
4. Уровни и порядок допуска к информации ограниченного доступа.
5. Порядок обращения с носителями конфиденциальной информации.
6. Режим допуска с информации ограниченного доступа.
7. Санкции за нарушение требований информационной безопасности и т.п. в Административном и Уголовном Кодексе РФ.

Тема 2.6. Пути и способы повышения эффективности управления службой защиты информации (2 часа)

Цель занятия: способы повышения эффективности управления службой защиты информации.

Содержание занятия: усвоение материала студентами, решение конкретных практических проблем.

Список тем для изучения:

1. Методы контроля и оценки работы СЗИ.
2. Пути и способы повышения эффективности управления службой защиты информации.
3. Новые угрозы информационной безопасности в современных условиях.
4. Проблемы функционирования СЗИ, СИБ. Зарубежная и отечественная практика решения подобных проблем.

Тема 2.7. Административно-правовые, экономические и социально-психологические методы управления (4 часа)

Цель занятия: изучение методов управления персоналом.

Содержание занятия: усвоение материала студентами, защита самостоятельной работы.

Список тем для изучения:

1. Административно-правовые методы управления персоналом при решении задач информационной безопасности.
2. Экономические методы управления при решении задач информационной безопасности.
3. Социально-психологические методы управления при решении задач информационной безопасности.
4. **Защита отчетов студентов по самостоятельным контрольным работам.**

Критерии и методика оценки работы студентов во время практических занятий:

А) Оценка результата выполнения практической части занятий:
- 3 балла выставляется студенту за правильное и полное выполнение практического задания (всего предполагается 10 практических заданий),
- 2 балла также выставляется за решение практического задания, но отчет о решении содержит мелкие ошибки или неактуальные/устаревшие сведения.
- 1 балл – если отчет по выполнении задания сдан с опозданием либо содержит неоптимальное или неверное решение.

Б) Критерии и методика оценки результата доклада на семинарском занятии:

- 4 балла за 1 доклад – если тема изложена исчерпывающе, доклад содержит актуальные сведения, не грешит избыточностью, лаконичен и точен по содержанию, и при этом студент демонстрирует свободное владение материалом (не пользуется записями, излагает наизусть).
- 3 балла за доклад выставляется студенту - если студент точно использует специализированную терминологию, сравнительно уверенно владеет темой, методами, нормативной базой, но читает материал доклада по конспекту, а не рассказывает своими словами.
- 2 балла за доклад выставляется студенту - если студент точно использует специализированную терминологию, но ответ неполон или содержит устаревшие сведения, либо содержит значительные погрешности.

- 1 балл выставляется студенту за 1 доклад по теме занятия, но тема не раскрыта и не показано свободное владение материалом темы, студент некорректно пользуется терминологией, не отрывается при изложении от конспекта.

Типовые задания для самостоятельной контрольной работ

Цель практической контрольной работы – оценка полученных знаний и навыков, уровень освоения профессиональной терминологией.

Содержание и примерные формулировки практических контрольных заданий:

1. Анализ законодательной базы в области информационной безопасности деятельности.
2. Понятие технологических схем менеджмента.
3. Специфика проектной работы и технологии менеджмента.
4. Указы президента РФ и постановления правительства РФ в области информации и информационной безопасности.
5. Основные законы в области информационной безопасности.
6. Значимые IT-достижения и перспективы информатизации юридической деятельности.
7. Дать определение нижестоящим понятиям: «информатизация»; «информационные технологии»; «информационные технологии в юридической деятельности»
8. Правовое обеспечение информационной безопасности. Российские документы по защите информации. Организационное обеспечение информационной безопасности
9. Законодательные и нормативные акты РФ в области защиты информации.
10. Как организуется научно-техническое сотрудничество с зарубежными партнерами в США, Германии, Великобритании, Франции, Японии?
11. Как организуется защита информации в процессе проведения международных конференций, симпозиумов, обмена специалистами и др.
12. Автоматизированная информационная система «Кадры».
13. Понятие информационных технологий следственной, оперативно-розыскной и экспертной деятельности.
14. Организация защиты информации в США по национальной безопасности.
15. Классификация защищаемой информации в США.
16. Порядок изменения степени секретности в США.
17. Организация доступа в США к грифованной информации.
18. Организация защиты коммерческой тайны в США.
19. Основные направления деятельности служб безопасности фирм.
20. Требования к персоналу, допущенного к защищаемой информации в Германии.
21. Государственная политика Великобритании в области защиты информации.
22. Организация системы специальных служб в Франции.
23. Состав, структура и основные направления деятельности служб безопасности в Израиле.
24. Государственная политика Японии в области защиты информации.
25. Научно-техническое сотрудничество с зарубежными странами в области защиты информации.
26. Организация защиты информации в процессе сотрудничества с зарубежными странами в области защиты информации.
27. Порядок предоставления защищаемой информации другим странам.
28. Международный опыт защиты информации в банковской сфере.
29. Международная защита интеллектуальной собственности.
30. Международные договоры в области информационной безопасности и защиты

информации.
31. Особенности международно-правовых документов в области информационной безопасности и защиты информации.
32. Привести пример компании и разобрать элементы ее КИС.
33. Принципы и общая схема проведения экономической оценки проекта.
34. Коммерциализация интеллектуальной собственности.

Методические указания: Контрольная работа (до 6 контрольных задач в течение семестра – до 3 баллов за каждый вопрос) проводится в письменной форме, оценка ставится по результатам устной защиты контрольной работы студентом на последнем практическом занятии.

Критерии и методика оценивания контрольной работы:
- 0 баллов выставляется студенту, если в контрольной работе не показано понимание терминов, темы ;
- 1 балл выставляется студенту, если он частично владеет содержанием практической работы;
- 2 балла выставляется студенту, если он владеет содержанием практической работы, но не может объяснить полученные результаты;
– 3 балла выставляется студенту, если он владеет содержанием практической работы, может объяснить полученные результаты.

Типовые материалы к зачетному собеседованию (коллоквиуму)

1. Требования, предъявляемые к специалисту по защите информации.
2. Нормативные акты правового регулирования вопросов информатизации и защиты информации в Российской Федерации.
3. Основные принципы организации службы защиты информации на предприятии.
4. Структура и основные функции государственной системы защиты информации.
5. Организация и координация работ по защите информации в оборонной сфере.
6. Организация и координация работ по защите информации в экономической деятельности.
7. Перечень видов деятельности, на осуществление которых требуется лицензия.
8. Органы, уполномоченные на ведение лицензионной деятельности.
9. Основные нормативно-техническим документам по вопросам обеспечения безопасности информации.
10. Что устанавливает государственная система аттестации объектов информатизации.
11. Основные принципы, организационная структура и порядок проведения аттестации.
12. Какие объекты информатизации подлежат обязательной аттестации.
13. Что такое безопасность информационных технологий.
14. Основные свойства информации и система ее обработки.
15. Что понимается под защитой информации.
16. Назовите основные элементы типовой системы защиты информации.
17. Назначение службы защиты информации.
18. Типовая организационно-штатная структура службы защиты информации.
19. Организационные и технологические задачи службы защиты информации.
20. Координационные задачи и функции службы защиты информации.
21. Основы технологического процесса по управлению службой защиты информации.
22. Значение управленческих функций службы защиты информации.
23. Виды планирования и их назначение.
24. Основные методы контроля выполнения планов.
25. Основные формы контроля выполнения планов.

26. Цели и основные принципы планирования деятельности службой защиты информации.
27. Принципы управления службой защиты информации.
28. Применяемая система методов управления службой защиты информации.
29. Установление персональной ответственности за сохранность носителей информации.
30. Структура должностных инструкций сотрудников службы защиты информации.
31. Краткое содержание должностных инструкций сотрудников службы защиты информации.
32. Административно-правовые методы управления.
33. Экономические методы управления.
34. Социально-психологические методы управления.
35. Критерии оценки эффективности службы защиты информации.

Критерии оценки результатов собеседования (коллоквиума)

Собеседование предполагает устные ответы студента на 2 вопроса из вышеприведенного списка (до 6 баллов за устный ответ на 1 вопрос, максимально).

- 0 баллов выставляется студенту, если он не смог ответить ни на один вопрос из 2-х в процессе собеседования (коллоквиума),
- 1 -2 балла за 1 вопрос выставляется если студент не дал внятного ответа, использует терминологию неправильно, или не может дать удовлетворительного ответа без подготовки;
- 3-4 балла выставляется студенту, если он владеет терминологией, не испытывает затруднений понимания и диалога в собеседовании, либо ответ неполон, неточен, или содержит устаревшие и неактуальные сведения по теме вопроса;
– 5 баллов выставляется студенту, если он владеет материалом, правильно использует терминологию, сведения актуальные, но содержат мелкие неточности;
- 6 баллов выставляется за ответ на 1 вопрос, если студент дал полный, точный, адекватный современным обстоятельствам в области ЗИ ответ.

Общая сумма баллов за собеседование/коллоквиум по 2 вопросам не может превышать 12 баллов.

Критерии оценки деятельности студента в течение семестра (в баллах):

- «Зачтено» выставляется студенту, если он набрал по результатам изучения дисциплины 60 баллов и более;

- «Не зачтено» выставляется студенту, если он набрал менее 59 баллов.

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

А) Основная учебная литература:

1. Аверченков, В.И. Служба защиты информации: организация и управление: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - М.: Флинта, 2011. – 186 с. -

[Электронный ресурс]. Режим доступа: URL: http://biblioclub.ru/index.php?page=book&id=93356
2. Аверченков, В.И. Служба защиты информации: организация и управление [Электронный ресурс] : учебное пособие / В.И. Аверченков, М.Ю. Рытов. — Электрон. дан. — Москва : ФЛИНТА, 2011. — 186 с. — Режим доступа: https://e.lanbook.com/book/44740
3. Аверченков, В.И. Организационная защита информации: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - 3-е изд., стер. - М.: Флинта, 2011. - 184 с. - [Электронный ресурс]. - URL:http://biblioclub.ru/index.php?page=book&id=93343

Б) Дополнительная учебная литература:

4. Галатенко, В.А. Основы информационной безопасности: Курс лекций : учебное пособие / В.А. Галатенко ; под ред. В.Б. Бетелина. - Изд. 3-е. - Москва : Интернет-Университет Информационных Технологий, 2006. - 208 с. - (Основы информационных технологий). - ISBN 5-9556-0052-3; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=233063
5. Бирюков, А.А. Информационная безопасность: защита и нападение [Электронный ресурс] : учебник / А.А. Бирюков. — Электрон. дан. — Москва : ДМК Пресс, 2012. — 474 с. — Режим доступа: https://e.lanbook.com/book/39990.

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

1. Электронная библиотечная система БашГУ – www.bashlib.ru
2. Электронная библиотечная система «ЭБ БашГУ» - https://elib.bashedu.ru
3. Электронная библиотечная система «Университетская библиотека онлайн» - https://biblioclub.ru
4. Электронная библиотечная система издательства «Лань» - https://e.lanbook.com
5. Электронный каталог Библиотеки БашГУ - http://www.bashlib.ru/catalogi - http://www.garant.ru
6. Словари и энциклопедии On-Line- http://www.dic.academic.ru
7. Справочная правовая система «КонсультантПлюс» - http://www.consultant-plus.ru
8. Антиплагиат.ВУЗ. Договор № 81 от 27.04.2018 г. Срок действия лицензии до 04.05.2019 г., договор № 1104 от 18.04.2019 г. Срок действия лицензии до 04.05.2020 г
9. Справочная правовая система Консультант Плюс. Договор №31705775411 от 07.12.2017 г.
10. База данных «Вестники Московского университета» (на платформе East View) (вход без регистрации). - Ссылка http://www.ebiblioteka.ru/browse/udb/12.
11. База данных «Издания по общественным и гуманитарным наукам» (на платформе East View) - Ссылка http://www.ebiblioteka.ru (вход из сети вуза без регистрации).
12. Электронная база данных диссертаций РГБ (авторизованный доступ по паролю в сети вуза) – Ссылка: http://dvs.rsl.ru
13. Web of Science - наукометрическая, библиографическая и реферативная база данных издательской корпорации Thomson Reuters. Язык английский, вход после регистрации или из сети вуза. – Ссылка: http://apps.webofknowledge.com/
14. SCOPUS - наукометрическая, библиографическая и реферативная база данных издательской корпорации Elsevier. Язык английский, вход после регистрации или из сети вуза. – Ссылка: http://www.scopus.com/
15. Computers & Applied Sciences Complete (EBSCO) - доступ в сети вуза, язык английский. - Ссылка: http://search.ebscohost.com/

16. Annual Reviews – обзор журналов по общественно-научной тематике и др. – доступ из сети вуза. – Ссылка: http://www.annualreviews.org/
17. Taylor and Francis – База полнотекстовых научных журналов, книг. Язык английский. – доступ из сети вуза. – Ссылка: http://www.tandf
18. Wiley - Полнотекстовая база данных статей из 1400 журналов издательства Wiley по всем отраслям знаний. Язык английский. Доступ из сети вуза без регистрации. – Ссылка: http://onlinelibrary.wiley.com/
19. Нормативные документы и материалы сайта ФСТЭК России (Федеральной службы по техническому и экспортному контролю России): https://fstec.ru/ Раздел Национальные старты информационной безопасности: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/113-gosudarstvennye-standarty/377-gosudarstvennye-standarty
20. Банк данных "Копии правовых актов: Российская Федерация» - http://giod.consultant.ru/
21. Национальные стандарты РФ в области информационной безопасности: http://www.iso27000.ru/standarty/gost-r-nacionalnye-standarty-rossiiskoi-federacii-v-oblasti-zaschity-informacii

Программное обеспечение:

1. Windows 8 Russian Russian OLP NL AcademicEdition и Windows Professional 8 Russian Upgrade OLP NL Academic Edition. Договор №104 от 17.06.2013 г. Лицензии бессрочные.
2. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные.
3. Система централизованного тестирования БашГУ (Moodle). GNU General Public License.
4. 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 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус). **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), компьютерный класс аудитория № 420 (гуманитарный корпус). **4.** ***учебная аудитория для***	Лекции, практические занятия, групповые и индивидуальные консультации, текущий контроль, промежуточная аттестация	**Аудитория № 403** Учебная мебель, доска, Мультимедийный-проектор Panasonic PT-LB78VE – 1 шт., Экран настенный Classic Norma 244*183 – 1 шт., учебно-наглядные пособия. **Аудитория № 405** Учебная мебель, доска, вокальные радиомикрофоны AKGWMS 40 – 2шт., Интер-ая система со встроенным короткофокусным проекто-ром PrometheanActivBoard 387 RPOMOUNTEST -1 шт., Ком-ер встраиваемый в кафедру INTELCorei3-4150/DDr3 4 Gb/HDD, Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт., Настольный интерактивный дисплей , ActivPanel 21S – 1 шт. , Матричный коммутатор сигналов интерфейса HDMICMPRO 4H4H – 1 шт. , Мультимедиа-проектор Pana-sonicPT-EW640E - 1 шт., Двух-полосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W)(белый) -6 шт., Петличный радиомикрофон AKGWMS45 – 1 шт. , Терминал видео конференц-связи LifeSizeIcon 600 Camera 10xPhone 2ndGeneration – 1 шт., Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт. **Аудитория № 413** Учебная мебель, доска, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 6 шт., Микшер-усилитель 120Вт АРАРТ МА1225 – 1 шт. **Аудитория № 415** Учебная мебель, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 2 шт., Интерактивная доска SMART с проектором V25, Микшер-усилитель 120Вт АРАРТ МА1225 – 1 шт. **Аудитория № 416** Учебная мебель, доска, проектор Optoma Ex542 i- 1 шт., Экран настенный Dinon – 1 шт. **Аудитория № 418** Учебная мебель, доска, Экран настенный Lumien Master Pikture 153*203 Matte White Fiber Clas(белый корпус) – 1 шт., Проектор Optoma Ex542 i - 1 шт. **Аудитория № 419** Учебная мебель, Проектор Optoma Ex542 i – 1 шт., Экран настенный Dinon – 1 шт. **Аудитория № 515** Учебная мебель, доска, терминал видео конференц-связи LifeSize Icon 600-камера, интер-ая система со встроенным короткофокусным проектором Promethean ActivBoard 387 RPO MOUNT EST, профессиональный 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

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). **5. *помещения для самостоятельной работы:*** аудитория № 613 (гуманитарный корпус), читальный зал библиотеки аудитория 402 (гуманитарный корпус).		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 **Программное обеспечение:** 1. Windows 8 Russian Russian OLP NL AcademicEdition и Windows Professional 8 Russian Upgrade OLP NL Academic Edition. Договор №104 от 17.06.2013 г. Лицензии бессрочные. 2. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные. 3. Система централизованного тестирования БашГУ (Moodle). GNU General Public License. 4. Правовая система «КонсультантПлюс». Договор №28826 от 09.01.2019 г. Лицензии бессрочные.

Приложение 1

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

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ
дисциплины «Организация и управление службой защиты информации»
на семестр А ОФО

Вид работы	Объем дисциплины
	ОФО
Общая трудоемкость дисциплины (ЗЕТ / часов)	4 ЗЕТ / 144 часов
Учебных часов на контактную работу с преподавателем:	64,2
лекций	32
практических/ семинарских	32
лабораторных	-
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	0,2
Учебных часов на самостоятельную работу обучающихся (СР)	79,8
Учебных часов на подготовку к зачету (Контроль)	-

Форма контроля:
Зачет А(10) семестр

№	Тема и содержание	Форма изучения материалов: лекции, практические занятия, семинарские занятия, лабораторные работы, самостоятельная работа и трудоемкость (в часах)				Основная и дополнительная литература, рекомендуемая студентам (номера из списка)	Задания по самостоятельной работе студентов	Форма текущего контроля успеваемости (коллоквиумы, контрольные работы, компьютерные тесты и т.п.)
		ЛК	ПР / Сем	ЛР	СРС			
1	2	3	4	5	6	7	8	9
	Модуль 1. Основные организационные меры по защите информации							
1	**Тема 1.1.** Понятие концепции информационной безопасности. **Содержание.** Цели и задачи организационной защиты информации, ее связь с правовой и инженерно-технической защитой информации. Виды угроз информационной безопасности на объекте защиты и их характеристика. Модели нарушителей информационной безопасности на объекте. Формы преступного посягательства. Оценка ущерба вследствие организационных нарушений информационной безопасности на объекте. Основные направления организационной защиты на объекте. Структура сил и средств организационной защиты информации.	4	4		10,8	1-5	Самостоятельное изучение рекомендуемой литературы, выполнение заданий домашней и самостоятельной работы, подготовка к зачету	ПР, КР
2	**Тема 1.2.** Основные организационно-технические мероприятия по защите информации. Организация работ по защите информации на предприятии. **Содержание.** Типовой перечень задач службы безопасности. Организационно-правовой статус службы безопасности. Организационно технические и режимные меры. Разработка положения об отделе защиты информации и должностной инструкции специалиста по защите информации. Состав документов, необходимых при подборе и приеме сотрудников на работу. Методы проверки кандидатов на должности. Организация обучения персонала, ее методы и формы.	4	4		10	1-5	Самостоятельное изучение рекомендуемой литературы, выполнение заданий домашней и самостоятельной работы, подготовка к зачету	ПР, тест, КР

3	**Тема1.3.** Организация ЗИ в системах и средствах информатизации и связи. Контроль состояния ЗИ. **Содержание.** Эффективность участия государства в формировании информационной политики государственных телерадиовещательных организаций, других государственных средствах массовой информации; обеспечение технологической независимости Российской Федерации в важнейших областях информатизации, телекоммуникации и связи, определяющих ее безопасность.	4	4		10	1-5	Самостоятельное изучение рекомендуемой литературы, выполнение заданий домашней и самостоятельной работы, подготовка к зачету	ПР, КР
	Модуль 2. Организация и управление службой безопасности							
4	**Тема 2.1.** Организация службы безопасности. **Содержание:** Функции, задачи и особенности службы безопасности объекта. Принципы организации службы безопасности объекта. Типовая структура службы безопасности.	4	4		10	1-5	Самостоятельное изучение рекомендуемой литературы, выполнение заданий домашней и самостоятельной работы, подготовка к зачету	ПР, тест, КР
5	**Тема 2.2.** Организационно-технические и режимные меры. Организация доступа и допуска (предоставление, основание отказа, формы допуска). **Содержание:** Организационно-технические мероприятия (перечень)**.** Понятия допуска к секретной (конфиденциальной) информации и доступа к секретным (конфиденциальным) работам, документам и изделиям. Номенклатура должностей работников, подлежащих оформлению на допуск. Формы допусков. Оформление, учет и уничтожение справок о допуске. Организация работы по обеспечению контроля за допуском сотрудников организации и ее посетителей.	4	4		10	1-5	Самостоятельное изучение рекомендуемой литературы, выполнение заданий домашней и самостоятельной работы, подготовка к зачету	ПР, КР

6	**Тема 2.3.** Аттестация объектов информатизации. Система лицензирования. **Содержание:** Порядок проведения аттестации. Исходные данный по аттестуемому объекту. Методика проведения испытаний. Организационная структура системы лицензирования. Функции, цели, задачи. Порядок лицензирования.	4	4		10	1-5	Самостоятельное изучение рекомендуемой литературы, выполнение заданий домашней и самостоятельной работы, подготовка к зачету	ПР, КР
7	**Тема 2.4.** Порядок организации и проведения разработок системы ЗИ в ведомствах и на отдельных предприятиях. **Содержание:** Обеспечение режима секретности при проведении НИОКР по секретной (конфиденциальной) тематике, при разработке и изготовлении изделий, их опытной эксплуатации и серийном производстве, хранении и транспортировке. Стадии создания системы защиты секретной информации.	4	4		14	1-5	Самостоятельное изучение рекомендуемой литературы, выполнение заданий домашней и самостоятельной работы, подготовка к зачету	ПР, КР
8	**Тема 2.5.** Организация охраны предприятия. Организация внутриобъектового и пропускного режимов на предприятиях. **Содержание:** Назначение и требования внутриобъектового режима. Порядок определения перечня предметов, запрещенных к проносу/провозу на территорию организации. Категорирование помещений. Обеспечение режима в выделенных помещениях. Определение границ контролируемых зон. Порядок передвижения сотрудников и перевозки охраняемых изделий по территории организации. Порядок пребывания и организация контроля выполнения посетителями требований режима и секретности на территории организации и в помещениях.	4	4		15	1-5	Самостоятельное изучение рекомендуемой литературы, выполнение заданий домашней и самостоятельной работы, подготовка к зачету	ПР, КР, собеседование
	Всего:	32	32		79,8			

Обозначения: ПР – практические задания, КР- контрольная работа.

Приложение 2

Рейтинг – план дисциплины

Организация и управление службой защиты информации

Направление подготовки: 10.05.05 Безопасность информационных технологий в правоохранительной сфере

Курс 5, семестр 10(А)

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1				
Текущий контроль				**30**
Аудиторная работа:				
- практические работы	3	6	0	18
- доклады на семинарах	4	3		12
Рубежный контроль				**20**
Тест 1	0,4	40	0	16
Тест 2	0,4	10	0	4
Всего			**0**	**50**
Модуль 2				
Текущий контроль			**0**	**20**
Аудиторная работа:				
- практические работы	3	4	0	12
- доклады на семинарах	4	2	0	8
Рубежный контроль				**30**
Контрольная самостоятельная работа	3	6	0	18
Собеседование (коллоквиум)	6	2		12
Всего			**0**	**50**
Поощрительные баллы				
1. Студенческая олимпиада			0	3
2. Публикация статей			0	3
3. Участие в конференции			0	4
Всего				**10**
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
1. Посещение лекционных занятий			0	-6
2. Посещение практических занятий			0	-10
Итоговый контроль				
зачет				