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

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

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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Техническая защита информации
Б1.Б.23 (базовая)

Программа специалитета

Специальность
10.05.05 Безопасность информационных технологий в правоохранительной сфере

Специализация
Технологии защиты информации в правоохранительной сфере

Квалификация
Специалист по защите информации

Разработчики (составители)
Старший преподаватель _____ Салов И.В.

Доцент, канд.биол.наук _____ Байрушин Ф.Т.

Для приема: 2019 г.

Уфа 2019 г.

Составитель / составители: И.В.Салов, Ф.Т.Байрушин

Рабочая программа дисциплины актуализирована на заседании кафедры управления информационной безопасностью протокол №11 от «20» июня2019 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/

Список документов и материалов

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных спланируемыми 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	Знать способы проведения мероприятий по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств обработки и защиты информации	ОПК-2: Способность проводить мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств обработки и защиты информации	Контроль-тестирование, экзамен
	Знать политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации, общеметодологические принципы теории информационной безопасности, возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации, состояние законодательной базы и стандарты в области информационной безопасности	ПК-1: способностью 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.	Контроль-тестирование, экзамен
	Знать правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации, правовые основы организации защиты государственной тайны и конфиденциальной	ПК-4: Способность участвовать в аттестационных испытаниях и аттестации объектов, помещений, технических средств и систем, а также сертификационных программных средств на предмет соответствия требованиям защиты информации	Контроль-тестирование, экзамен

	информации, системы организации бумажного и электронного конфиденциального делопроизводства		
	Знать подходы обоснования затрат на информационную безопасность, методы и модели установления зависимости между затратами на защиту информации и уровнем защищенности	ПК-28: Способность выполнять предварительный технико-экономический анализ и обоснование проектных решений по созданию систем обеспечения безопасности информации и защиты государственной тайны	Контроль-тестирование, экзамен
	Знать основы построения и функционирования комплексов программно-аппаратной защиты информации на предприятии (организации, учреждении), наиболее распространенные методы и средства несанкционированного доступа к информации, методы и средства противодействия несанкционированному доступу к информации, современные возможности и тенденции применения комплексов программно-аппаратной защиты для совершенствования экономической деятельности	ПСК-1: Способность участвовать в разработке аппаратных и программных средств в составе автоматизированных систем, связанных с обеспечением информационной безопасности	Контроль-тестирование, экзамен
	Знать нормативно-правовые документы по обеспечению информационной безопасности в нашей стране и за рубежом	ПСК-3: Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности	Контроль-тестирование, экзамен
Умения	Уметь проводить мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств обработки и защиты	ОПК-2: Способность проводить мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств обработки и защиты информации	Контроль-тестирование, экзамен

	информации		
	Уметь реализовывать на практике принципы политики безопасности, использовать закономерности преобразования данных в каналах при выполнении комплекса мер по информационной безопасности, обосновывать организационно-технические мероприятия по защите информации, использовать возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации	ПК-1: способностью 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.	
	Уметь выбирать тип необходимых средств для выявления наличия электронных средств перехвата информации,применять на практике методы локальной и комплексной автоматизации процессов обработки документов в документационной службе,разрабатывать организационно-распорядительные документы по вопросам защиты информации	ПК-4: Способность участвовать в аттестационных испытаниях и аттестации объектов, помещений, технических средств и систем, а также сертификационных программных средств на предмет соответствия требованиям защиты информации	Контроль-тестирование, экзамен
	Уметь оценивать эффективность управленческих решений и анализировать экономические показатели деятельности подразделения,самостоятельно находить нужную информацию по тематике и выбирать необходимые для организации информационные	ПК-28: Способность выполнять предварительный технико-экономический анализ и обоснование проектных решений по созданию систем обеспечения безопасности информации и защиты государственной тайны	Контроль-тестирование, экзамен

	ресурсы и источники знаний в электронной среде,использовать основные методики оценки совокупной стоимости владения для подсистемы информационной безопасности,определять зависимость между затратами на ИБ и уровнем защищенности		
	Уметь находить рациональное сочетание технических, методологических и человеческих средств в реализации функционала комплекса программно-аппаратной защиты,контролировать ход разработки проекта и осуществлять приемку комплекса,принимать обоснованные решения по приобретению технических средств защиты информации в зависимости от экономического состояния, информационных потоков, и других факторов деятельности предприятия (организации, учреждения)	ПСК-1: Способность участвовать в разработке аппаратных и программных средств в составе автоматизированных систем, связанных с обеспечением информационной безопасности	Контроль-тестирование, экзамен
	Уметьинтерпретировать и обобщать данные, формулировать выводы и рекомендации,применять на практике методы обработки данных,разрабатывать и реализовывать решения, направленные на поддержку социально-значимых проектов и развитие компьютерного творчества	ПСК-3: Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности	Контроль-тестирование, экзамен
Владения (навыки /	Владеть навыками проведения мероприятий	ОПК-2: Способность проводить мероприятия по охране труда и	Контроль-тестировани

опыт деятельности)	по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств обработки и защиты информации	технике безопасности в процессе эксплуатации и технического обслуживания средств обработки и защиты информации	е, экзамен
	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, навыками организации комплекса мероприятий по защите информации в процессах автоматизированной обработки информации, навыками выявления и устранения угроз информационной безопасности, навыками эксплуатации современного электронного оборудования и информационно-коммуникационных технологий, навыками внедрения, адаптации и настройки средств защиты прикладных ИС	ПК-1: способностью 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.	Контроль-тестирование, экзамен
	Владеть навыками работы с нормативными правовыми актами и навыками лицензирования в области защиты информации,методами сбора и анализа исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по	ПК-4: Способность участвовать в аттестационных испытаниях и аттестации объектов, помещений, технических средств и систем, а также сертификационных программных средств на предмет соответствия требованиям защиты информации	Контроль-тестирование, экзамен

	показателям информационной безопасности		
	Владеть навыками определения затрат компании на ИБ,навыками обоснования проектных решений по созданию систем обеспечения безопасности информации и защиты государственной тайны	ПК-28: Способность выполнять предварительный технико-экономический анализ и обоснование проектных решений по созданию систем обеспечения безопасности информации и защиты государственной тайны	Контроль-тестирование, экзамен
	Владеть навыками нахождения и пресечения с помощью комплекса программно-аппаратных средств реальных и потенциальных каналов утечки информации на предприятии (организации, учреждении)	ПСК-1: Способность участвовать в разработке аппаратных и программных средств в составе автоматизированных систем, связанных с обеспечением информационной безопасности	Контроль-тестирование, экзамен
	Владетьинтерпретации и обобщения результатов, формулирования рекомендаций и принятия решений,методологией и навыками решения научных и практических задач	ПСК-3: Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности	Контроль-тестирование, экзамен

2. Место дисциплины в структуре образовательной программы

Дисциплина «Техническая защита информации» относится к дисциплинам базовой частиобразовательной программы.

Дисциплина изучается на 4-емкурсе в 7 семестре.

Цель изучения дисциплины: формирование у специалистов целостного представления о технической защите информации.

Для освоения дисциплины необходимы компетенции, сформированные в рамках изучения следующих дисциплин:

Введение в специальность,

Математика,

Программно-аппаратная защита информации,

Теория информационной безопасности и методология защиты информации,

Информационная безопасность в правоохранительной сфере,

Экономика защиты информации.

Эти дисциплины направлены на формирование компетенций ОПК-2, ПК-1, ПК-4, ПК-28, ПСК-1, ПСК-3.

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

ОПК-2: Способность проводить мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств обработки и защиты информации.

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
Первый этап (уровень)	Знать способы проведения мероприятий по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств обработки и защиты информации	Не знает	Имеет фрагментарные знания о способах проведения мероприятий по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств обработки и защиты информации	В целом знает основные понятия способов проведения мероприятий по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств обработки и защиты информации	Демонстрирует целостные знания о способах проведения мероприятий по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств обработки и защиты информации
Второй этап (уровень)	Уметь проводить мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств обработки и защиты информации	Не умеет	Умеет проводить мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств обработки и защиты информации, но допускает значительные ошибки	Умеет проводить мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств обработки и защиты информации, но допускает незначительные ошибки	Умеет проводить мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств обработки и защиты информации
Третий этап (уровень)	Владеть навыками проведения мероприятий по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств обработки и защиты информации	Не владеет	Недостаточно владеет навыками проведения мероприятий по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств обработки и защиты информации	Владеет отдельными навыками проведения мероприятий по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств обработки и защиты информации	Способен использовать навыки навыками проведения мероприятий по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств обработки 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

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

	компетенций)				
Первый этап (уровень)	Знать политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации	Не знает	Имеет фрагментарные знания о политиках, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации	Знает основы политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации	Знает основы политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации
	Знать общеметодологические принципы теории информационной безопасности	Не знает	Имеет фрагментарные знания о общеметодологических принципах теории информационной безопасности	Знает основные общеметодологические принципы теории информационной безопасности	Знает общеметодологические принципы теории информационной безопасности
	Знать возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации	Не знает	Имеет фрагментарные знания о возможностях и особенностях организационных, аппаратных и программных средств безопасности и защиты информации	Знает основные возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации	Знает возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации
	Знать состояние законодательной базы и стандарты в области информационной безопасности	Не знает	Имеет фрагментарные знания о состоянии законодательной базы и стандартов в области информационной безопасности	Знает основные новости знания о состоянии законодательной базы и стандартов в области информационной безопасности	Знает состояние законодательной базы и стандарты в области информационной безопасности
Второй этап (уровень)	Уметь реализовывать на практике принципы политики безопасности	Не умеет	Допускает значительные ошибки при реализации на практике принципов политики безопасности	Допускает незначительные ошибки при реализации на практике принципов политики безопасности	Имеет навыки реализации на практике принципов политики безопасности
	Уметь использовать закономерности преобразования данных в каналах при выполнении комплекса мер по информационной безопасности	Не умеет	Допускает значительные ошибки при использовании закономерности преобразования данных в каналах при выполнении комплекса мер по информационной безопасности	Допускает незначительные ошибки при использовании закономерности преобразования данных в каналах при выполнении комплекса мер по информационной безопасности	Имеет навыки использования закономерности преобразования данных в каналах при выполнении комплекса мер по информационной безопасности
	Уметь обосновывать организационно-технические мероприятия по защите информации	Не умеет	Допускает значительные ошибки при обосновании организационно-технических мероприятий по защите информации	Допускает незначительные ошибки при обосновании организационно-технических мероприятий по защите информации	Имеет навыки обоснования организационно-технических мероприятий по защите информации
	Уметь использовать возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации	Не умеет	Допускает значительные ошибки при использовании возможностей и особенностей организационных, аппаратных и программных средств безопасности и защиты информации	Допускает незначительные ошибки при использовании возможностей и особенностей организационных, аппаратных и программных средств безопасности и защиты информации	Имеет навыки использования возможностей и особенностей организационных, аппаратных и программных средств безопасности и защиты информации
Третий этап (уровень)	Владеть навыками анализа, обработки и интерпретации результатов решения прикладных задач управления	Не владеет	Недостаточно владеет навыками анализа, обработки и интерпретации результатов решения прикладных задач управления	Владеет отдельными навыками анализа, обработки и интерпретации результатов решения прикладных задач управления	Владеет навыками анализа, обработки и интерпретации результатов решения прикладных задач управления
	Владеть навыками	Не владеет	Недостаточно	Владеет отдельными	Владеет навыками

	формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью		владеет навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью	навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью	формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью
	Владеть навыками организации комплекса мероприятий по защите информации в процессах автоматизированной обработки информации	Не владеет	Недостаточно владеет навыками организации комплекса мероприятий по защите информации в процессах автоматизированной обработки информации	Владеет отдельными навыками организации комплекса мероприятий по защите информации в процессах автоматизированной обработки информации	Владеет навыками организации комплекса мероприятий по защите информации в процессах автоматизированной обработки информации
	Владеть навыками выявления и устранения угроз информационной безопасности	Не владеет	Недостаточно владеет навыками выявления и устранения угроз информационной безопасности	Владеет отдельными навыками выявления и устранения угроз информационной безопасности	Владеет навыками выявления и устранения угроз информационной безопасности
	Владеть навыками эксплуатации современного электронного оборудования и информационно-коммуникационных технологий	Не владеет	Недостаточно владеет навыками эксплуатации современного электронного оборудования и информационно-коммуникационных технологий	Владеет отдельными навыками эксплуатации современного электронного оборудования и информационно-коммуникационных технологий	Владеет навыками эксплуатации современного электронного оборудования и информационно-коммуникационных технологий
	Владеть навыками внедрения, адаптации и настройки средств защиты прикладных ИС	Не владеет	Недостаточно владеет навыками внедрения, адаптации и настройки средств защиты прикладных ИС	Владеет отдельными навыками внедрения, адаптации и настройки средств защиты прикладных ИС	Владеет навыками внедрения, адаптации и настройки средств защиты прикладных ИС

ПК-4: Способность участвовать в аттестационных испытаниях и аттестации объектов, помещений, технических средств и систем, а также сертификационных программных средств на предмет соответствия требованиям защиты информации.

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
Первый этап (уровень)	Знать правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации	Не знает	Имеет фрагментарные знания о правовых нормах и стандартах по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации	Знает основные правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации	Знает правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации
	Знать правовые основы организации защиты государственной тайны и конфиденциальной информации, системы организации бумажного и электронного конфиденциального делопроизводства	Не знает	Имеет фрагментарные знания о правовых основах организации защиты государственной тайны и конфиденциальной информации, системы организации бумажного и электронного конфиденциального делопроизводства	Знает основные правовые основы организации защиты государственной тайны и конфиденциальной информации, системы организации бумажного и электронного конфиденциального делопроизводства	Знает правовые основы организации защиты государственной тайны и конфиденциальной информации, системы организации бумажного и электронного конфиденциального делопроизводства
Второй этап (уровень)	Уметь выбирать тип необходимых средств для выявления	Не умеет	Допускает значительные ошибки при выборе	Допускает незначительные ошибки при выборе	Имеет навыки выбора типа необходимых средств

	наличия электронных средств перехвата информации		типа необходимых средств для выявления наличия электронных средств перехвата информации	типа необходимых средств для выявления наличия электронных средств перехвата информации	для выявления наличия электронных средств перехвата информации
	Уметь применять на практике методы локальной и комплексной автоматизации процессов обработки документов в документационной службе	Не умеет	Допускает значительные ошибки при применении на практике методов локальной и комплексной автоматизации процессов обработки документов в документационной службе	Допускает незначительные ошибки при применении на практике методов локальной и комплексной автоматизации процессов обработки документов в документационной службе	Умеет применять на практике методы локальной и комплексной автоматизации процессов обработки документов в документационной службе
	Уметь разрабатывать организационно-распорядительные документы по вопросам защиты информации	Не умеет	Допускает значительные ошибки при разработке организационно-распорядительных документов по вопросам защиты информации	Допускает незначительные ошибки при разработке организационно-распорядительных документов по вопросам защиты информации	Имеет навыки работы по разработке организационно-распорядительных документов по вопросам защиты информации
Третий этап (уровень)	Владеть навыками работы с нормативными правовыми актами и навыками лицензирования в области защиты информации	Не владеет	Недостаточно владеет навыками работы с нормативными правовыми актами и навыками лицензирования в области защиты информации	Владеет отдельными навыками работы с нормативными правовыми актами и навыками лицензирования в области защиты информации	Владеет навыками работы с нормативными правовыми актами и навыками лицензирования в области защиты информации
	Владеть методами сбора и анализа исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности	Не владеет	Недостаточно владеетметодами сбора и анализа исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности	Владеет отдельными методами сбора и анализа исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности	Владеетметодами сбора и анализа исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности

ПК-28: Способность выполнять предварительный технико-экономический анализ и обоснование проектных решений по созданию систем обеспечения безопасности информации и защиты государственной тайны.

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
Первый этап (уровень)	Знать подходы обоснования затрат на информационную безопасность	Не знает	Имеет фрагментарные знания о подходах обоснования затрат на информационную безопасность	Знает основы подходов обоснования затрат на информационную безопасность	Знает подходы обоснования затрат на информационную безопасность
	Знать методы и модели установления зависимости между затратами на защиту информации и уровнем защищенности	Не знает	Имеет фрагментарные знания ометодах и моделях установления зависимости между затратами на защиту информации и уровнем защищенности	Знает основные методы и модели установления зависимости между затратами на защиту информации и уровнем защищенности	Знает методы и модели установления зависимости между затратами на защиту информации и уровнем защищенности
Второй этап (уровень)	Уметь оценивать эффективность управленческих решений и	Не умеет	Допускает значительные ошибки при оценке эффективности	Допускает незначительные ошибки при оценке эффективности	Умеет оценивать эффективность управленческих решений и

	анализировать экономические показатели деятельности подразделения		управленческих решений и анализе экономических показателей деятельности подразделения	управленческих решений и анализе экономических показателей деятельности подразделения	анализировать экономические показатели деятельности подразделения
	Уметь самостоятельно находить нужную информацию по тематике и выбирать необходимые для организации информационные ресурсы и источники знаний в электронной среде	Не умеет	Допускает значительные ошибки при самостоятельном нахождении нужной информации по тематике и выборе необходимых для организации информационных ресурсов и источников знаний в электронной среде	Допускает незначительные ошибки при самостоятельном нахождении нужной информации по тематике и выборе необходимых для организации информационных ресурсов и источников знаний в электронной среде	Умеет самостоятельно находить нужную информацию по тематике и выбирать необходимые для организации информационные ресурсы и источники знаний в электронной среде
	Уметь использовать основные методики оценки совокупной стоимости владения для подсистемы информационной безопасности	Не умеет	Допускает значительные ошибки при использовании основных методик оценки совокупной стоимости владения для подсистемы информационной безопасности	Допускает незначительные ошибки при использовании основных методик оценки совокупной стоимости владения для подсистемы информационной безопасности	Умеет использовать основные методики оценки совокупной стоимости владения для подсистемы информационной безопасности
	Уметь определять зависимость между затратами на ИБ и уровнем защищенности	Не умеет	Допускает значительные ошибки при определении зависимости между затратами на ИБ и уровнем защищенности	Допускает незначительные ошибки при определении зависимости между затратами на ИБ и уровнем защищенности	Умеет определять зависимость между затратами на ИБ и уровнем защищенности
Третий этап (уровень)	Владеть навыками определения затрат компании на ИБ	Не владеет	Недостаточно владеет навыками определения затрат компании на ИБ	Владеет отдельными навыками определения затрат компании на ИБ	Владеет навыками определения затрат компании на ИБ
	Владеть навыками обоснования проектных решений по созданию систем обеспечения безопасности информации и защиты государственной тайны	Не владеет	Недостаточно владеет навыками обоснования проектных решений по созданию систем обеспечения безопасности информации и защиты государственной тайны	Владеет отдельными навыками обоснования проектных решений по созданию систем обеспечения безопасности информации и защиты государственной тайны	Владеет навыками обоснования проектных решений по созданию систем обеспечения безопасности информации и защиты государственной тайны

ПСК-1: Способность участвовать в разработке аппаратных и программных средств в составе автоматизированных систем, связанных с обеспечением информационной безопасности.

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
Первый этап (уровень)	Знать основы построения и функционирования комплексов программно-аппаратной защиты информации на предприятии (организации, учреждении)	Не знает	Имеет фрагментарные знания оосновах построения и функционирования комплексов программно-аппаратной защиты информации на предприятии (организации, учреждении)	Знает некоторые элементы основ построения и функционирования комплексов программно-аппаратной защиты информации на предприятии (организации, учреждении)	Знает основы построения и функционирования комплексов программно-аппаратной защиты информации на предприятии (организации, учреждении)
	Знать наиболее распространенные методы и средства несанкционированного доступа к информации, методы	Не знает	Имеет фрагментарные знания онаиболее распространенных методах и средствах несанкционированно	Знает основные некоторые распространенные методы и средства несанкционированного доступа к	Знает наиболее распространенные методы и средства несанкционированного доступа к информации, методы

	и средства противодействия несанкционированному доступу к информации		го доступа к информации, методы и средства противодействия несанкционированному доступу к информации	информации, методы и средства противодействия несанкционированному доступу к информации	и средства противодействия несанкционированному доступу к информации
	Знать современные возможности и тенденции применения комплексов программно-аппаратной защиты для совершенствования экономической деятельности	Не знает	Имеет фрагментарные знания о современных возможностях и тенденциях применения комплексов программно-аппаратной защиты для совершенствования экономической деятельности	Знает основные современные возможности и тенденции применения комплексов программно-аппаратной защиты для совершенствования экономической деятельности	Знает современные возможности и тенденции применения комплексов программно-аппаратной защиты для совершенствования экономической деятельности
Второй этап (уровень)	Уметь находить рациональное сочетание технических, методологических и человеческих средств в реализации функционала комплекса программно-аппаратной защиты	Не умеет	Допускает значительные ошибки при нахождении рационального сочетания технических, методологических и человеческих средств в реализации функционала комплекса программно-аппаратной защиты	Допускает незначительные ошибки при нахождении рационального сочетания технических, методологических и человеческих средств в реализации функционала комплекса программно-аппаратной защиты	Имеет навыки нахождения рационального сочетания технических, методологических и человеческих средств в реализации функционала комплекса программно-аппаратной защиты
	Уметь контролировать ход разработки проекта и осуществлять приемку комплекса	Не умеет	Допускает значительные ошибки при контроле хода разработки проекта и осуществлении приемки комплекса	Допускает незначительные ошибки при контроле хода разработки проекта и осуществлении приемки комплекса	Имеет навыки контроля хода разработки проекта и осуществления приемки комплекса
	Уметь принимать обоснованные решения по приобретению технических средств защиты информации в зависимости от экономического состояния, информационных потоков, и других факторов деятельности предприятия (организации, учреждения)	Не умеет	Допускает значительные ошибки при принятии обоснованных решений по приобретению технических средств защиты информации в зависимости от экономического состояния, информационных потоков, и других факторов деятельности предприятия (организации, учреждения)	Допускает незначительные ошибки при принятии обоснованных решений по приобретению технических средств защиты информации в зависимости от экономического состояния, информационных потоков, и других факторов деятельности предприятия (организации, учреждения)	Умеет принимать обоснованные решения по приобретению технических средств защиты информации в зависимости от экономического состояния, информационных потоков, и других факторов деятельности предприятия (организации, учреждения)
Третий этап (уровень)	Владеть навыками нахождения и пресечения с помощью комплекса программно-аппаратных средств реальных и потенциальных каналов утечки информации на предприятии (организации, учреждении)	Не владеет	Недостаточно владеет навыками нахождения и пресечения с помощью комплекса программно-аппаратных средств реальных и потенциальных каналов утечки информации на предприятии (организации, учреждении)	Владеет отдельными навыками нахождения и пресечения с помощью комплекса программно-аппаратных средств реальных и потенциальных каналов утечки информации на предприятии (организации, учреждении)	Владеет навыками нахождения и пресечения с помощью комплекса программно-аппаратных средств реальных и потенциальных каналов утечки информации на предприятии (организации, учреждении)

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

Этап (уровень) освоения	Планируемые результаты обучения	Критерии оценивания результатов обучения			
		2 («Не	3	4 («Хорошо»)	5 («Отлично»)

компетенции	(показатели достижения заданного уровня освоения компетенций)	удовлетворительно»)	(«Удовлетворительно»)		
Первый этап (уровень)	Знать нормативно-правовые документы по обеспечению информационной безопасности в нашей стране и за рубежом	Не знает	Имеет фрагментарные знания о нормативно-правовых документах по обеспечению информационной безопасности в нашей стране и за рубежом	Знает основные нормативно-правовые документы по обеспечению информационной безопасности в нашей стране и за рубежом	Знает нормативно-правовые документы по обеспечению информационной безопасности в нашей стране и за рубежом
	Знать стандарты построения систем информационной безопасности и стандарты оценки степени защиты систем информационной безопасности объектов	Не знает	Имеет фрагментарные знания о стандартах построения систем информационной безопасности и стандартах оценки степени защиты систем информационной безопасности объектов	Знает основные стандарты построения систем информационной безопасности и стандарты оценки степени защиты систем информационной безопасности объектов	Знает стандарты построения систем информационной безопасности и стандарты оценки степени защиты систем информационной безопасности объектов
	Знать методики анализа рисков информационных систем	Не знает	Имеет фрагментарные знания о методиках анализа рисков информационных систем	Знает основныеметодики анализа рисков информационных систем	Знает методики анализа рисков информационных систем
Второй этап (уровень)	Уметь интерпретировать и обобщать данные, формулировать выводы и рекомендации	Не умеет	Допускает значительные ошибки при интерпретации и обобщении данных, формулировании выводов и рекомендаций	Допускает незначительные ошибки при интерпретации и обобщении данных, формулировании выводов и рекомендаций	Имеет навыки интерпретации и обобщения данных, формулирования выводов и рекомендаций
	Уметь применять на практике методы обработки данных	Не умеет	Допускает значительные ошибки при применении на практике методов обработки данных	Допускает незначительные ошибки при применении на практике методов обработки данных	Умеет применять на практике методы обработки данных
	Уметь разрабатывать и реализовывать решения, направленные на поддержку социально-значимых проектов и развитие компьютерного творчества	Не умеет	Допускает значительные ошибки при разработке и реализации решений, направленных на поддержку социально-значимых проектов и развитие компьютерного творчества	Допускает незначительные ошибки при разработке и реализации решений, направленных на поддержку социально-значимых проектов и развитие компьютерного творчества	Имеет навыки работы по разработке и реализации решений, направленных на поддержку социально-значимых проектов и развитие компьютерного творчества
Третий этап (уровень)	Владеть навыками интерпретации и обобщения результатов, формулирования рекомендаций и принятия решений	Не владеет	Недостаточно владеет навыками интерпретации и обобщения результатов, формулирования рекомендаций и принятия решений	Владеет отдельными навыками интерпретации и обобщения результатов, формулирования рекомендаций и принятия решений	Владеет навыками интерпретации и обобщения результатов, формулирования рекомендаций и принятия решений
	Владеть методологией и навыками решения научных и практических задач	Не владеет	Недостаточно владеетметодологией и навыками решения научных и практических задач	Владеет отдельными методами и навыками решения научных и практических задач	Владеетметодами и навыками решения научных и практических задач

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

Шкалы оцениваниядля экзамена:

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 освоения	Результаты обучения	Компетенция	Оценочные средства
1-й этап Знания	Знать способы проведения мероприятий по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств обработки и защиты информации	ОПК-2: Способность проводить мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств обработки и защиты информации	Практическая работа, тестирование
	Знать политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации, общеметодологические принципы теории информационной безопасности, возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации, состояние законодательной базы и стандарты в области информационной безопасности	ПК-1: способностью 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.	Практическая работа, тестирование
	Знать правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации, правовые основы организации защиты государственной тайны и конфиденциальной информации, системы организации бумажного и	ПК-4: Способность участвовать в аттестационных испытаниях и аттестации объектов, помещений, технических средств и систем, а также сертификационных программных средств на предмет соответствия	Практическая работа, тестирование

	электронного конфиденциального делопроизводства	требованиям защиты информации	
	Знать подходы обоснования затрат на информационную безопасность, методы и модели установления зависимости между затратами на защиту информации и уровнем защищенности	ПК-28: Способность выполнять предварительный технико-экономический анализ и обоснование проектных решений по созданию систем обеспечения безопасности информации и защиты государственной тайны	Практическая работа, тестирование
	Знать основы построения и функционирования комплексов программно-аппаратной защиты информации на предприятии (организации, учреждении), наиболее распространенные методы и средства несанкционированного доступа к информации, методы и средства противодействия несанкционированному доступу к информации, современные возможности и тенденции применения комплексов программно-аппаратной защиты для совершенствования экономической деятельности	ПСК-1: Способность участвовать в разработке аппаратных и программных средств в составе автоматизированных систем, связанных с обеспечением информационной безопасности	Практическая работа, тестирование
	Знать нормативно-правовые документы по обеспечению информационной безопасности в нашей стране и за рубежом	ПСК-3: Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности	Практическая работа, тестирование
2-й этап Умения	Уметь проводить мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств обработки и защиты информации	ОПК-2: Способность проводить мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств обработки и защиты информации	Практическая работа, тестирование
	Уметь реализовывать на практике принципы политики безопасности, использовать закономерности преобразования данных в каналах при выполнении комплекса мер по информационной безопасности,	ПК-1: способностью формировать и реализовывать комплекс мер по обеспечению безопасности информации,	Практическая работа, тестирование

	обосновывать организационно-технические мероприятия по защите информации, использовать возможности и особенности организационных, аппаратных и программных средств безопасности и защиты 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.	
	Уметь выбирать тип необходимых средств для выявления наличия электронных средств перехвата информации,применять на практике методы локальной и комплексной автоматизации процессов обработки документов в документационной службе,разрабатывать организационно-распорядительные документы по вопросам защиты информации	ПК-4: Способность участвовать в аттестационных испытаниях и аттестации объектов, помещений, технических средств и систем, а также сертификационных программных средств на предмет соответствия требованиям защиты информации	Практическая работа, тестирование
	Уметь оценивать эффективность управленческих решений и анализировать экономические показатели деятельности подразделения,самостоятельно находить нужную информацию по тематике и выбирать необходимые для организации информационные ресурсы и источники знаний в электронной среде,использовать основные методики оценки совокупной стоимости владения для подсистемы информационной безопасности,определять зависимость между затратами на ИБ и уровнем защищенности	ПК-28: Способность выполнять предварительный технико-экономический анализ и обоснование проектных решений по созданию систем обеспечения безопасности информации и защиты государственной тайны	Практическая работа, тестирование
	Уметь находить рациональное сочетание технических, методологических и человеческих средств в реализации функционала комплекса программно-аппаратной защиты,контролировать ход разработки проекта и осуществлять приемку комплекса,принимать обоснованные решения по приобретению технических средств защиты информации в зависимости от экономического состояния,	ПСК-1: Способность участвовать в разработке аппаратных и программных средств в составе автоматизированных систем, связанных с обеспечением информационной безопасности	Практическая работа, тестирование

	информационных потоков, и других факторов деятельности предприятия (организации, учреждения)		
	Уметьинтерпретировать и обобщать данные, формулировать выводы и рекомендации,применять на практике методы обработки данных,разрабатывать и реализовывать решения, направленные на поддержку социально-значимых проектов и развитие компьютерного творчества	ПСК-3: Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности	Практическая работа, тестирование
3-й этап Владения навыками	Владеть навыками проведения мероприятий по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств обработки и защиты информации	ОПК-2: Способность проводить мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств обработки и защиты информации	Практическая работа, тестирование
	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, навыками организации комплекса мероприятий по защите информации в процессах автоматизированной обработки информации, навыками выявления и устранения угроз информационной безопасности, навыками эксплуатации современного электронного оборудования и информационно-коммуникационных технологий, навыками внедрения, адаптации и настройки средств защиты прикладных ИС	ПК-1: способностью 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.	Практическая работа, тестирование
	Владеть навыками работы с нормативными правовыми актами и навыками лицензирования в области защиты информации,методами сбора и анализа исходных данных для проектирования систем защиты	ПК-4: Способность участвовать в аттестационных испытаниях и аттестации объектов, помещений, технических средств и систем, а также	Практическая работа, тестирование

	информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности	сертификационных программных средств на предмет соответствия требованиям защиты информации	
	Владеть навыками определения затрат компании на ИБ,навыками обоснования проектных решений по созданию систем обеспечения безопасности информации и защиты государственной тайны	ПК-28: Способность выполнять предварительный технико-экономический анализ и обоснование проектных решений по созданию систем обеспечения безопасности информации и защиты государственной тайны	Практическая работа, тестирование
	Владеть навыками нахождения и пресечения с помощью комплекса программно-аппаратных средств реальных и потенциальных каналов утечки информации на предприятии (организации, учреждении)	ПСК-1: Способность участвовать в разработке аппаратных и программных средств в составе автоматизированных систем, связанных с обеспечением информационной безопасности	Практическая работа, тестирование
	Владетьинтерпретации и обобщения результатов, формулирования рекомендаций и принятия решений,методологией и навыками решения научных и практических задач	ПСК-3: Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности	Практическая работа, тестирование

Экзамен

Типовые материалы к экзамену

1. Источники конфиденциальной информации.
2. Организационные каналы обмена и передачи информации.
3. Виды информации.
4. Понятие тайны.
5. Свойства информации.
6. Классификация носителей информации.
7. Цели защиты информации.
8. Виды технических каналов утечки информации
9. Электромагнитный канал утечки информации
10. Индукционный канал утечки информации
11. Характеристика звука
12. Понятие волны
13. Звукопоглощающие материалы
14. Звукоизоляция помещений.

15. Маскировка звуковых сигналов.
16. Звуковое поле в помещении
17. Разборчивость речи.
18. Микрофоны и их характеристики
19. Виброакустический канал утечки информации
20. Оптикоэлектронный канал утечки информации
21. Параметрический канал утечки информации
22. Технические каналы утечки видовой информации
23. Технические каналы утечки информации. Структура и классификация.
24. Задачи систем защиты информации.
25. Технические каналы утечки информации. Основные характеристики.
26. Технические каналы утечки информации при передаче ее по каналам связи.
27. Технические каналы утечки речевой информации
28. Контроль и прослушивание телефонных линий связи.
29. Демаскирующие признаки объектов. Общие положения.
30. Демаскирующие признаков в видимом диапазоне электромагнитного спектра.
31. Понятие демаскирующих признаков в ИК диапазоне. Основные понятия и положения.
32. Технические характеристики радиосигналов.
33. Технические признаки радиоизлучений.
34. Демаскирующие признаки РЭС. Характеристики. Основные положения.
35. Системы технической защиты.
36. Способы технической защиты
37. Концепция и методы инженерно-технической защиты информации
38. Понятие экранирования. Основные положения
39. Виды экранирования
40. Экранирование проводов и катушек индуктивности.
41. Экранированные помещения
42. Безопасность ВОЛС
43. Заземление технических средств. Понятия, определения и виды.
44. Фильтрация информационных сигналов.
45. Виды помехоподавляющих фильтров
46. Методика выбора типа фильтров.
47. Типовые схемы фильтров
48. Система пространственного зашумления.
49. Способы предотвращения утечки информации через ПЭМИН ПК
50. Особенности слаботочных линий связи и сетей как каналов утечки информации.
51. Скрытие и защита от утечки информации по акустическому и виброакустическому каналам.
52. Анализаторы линий и устройства контроля проводных линий
53. Криптографические методы защиты информации.
54. Способы защиты информации с помощью программного обеспечения
55. Способы защиты информации с помощью USB-ключа
56. Способы защиты информации с помощью технологии Proximity и смарт-карт
57. Устройства быстрого уничтожения информации на жестких дисках.
58. Защита конфиденциальной информации от несанкционированного доступа в автоматизированных системах
59. Цели и задачи технического контроля эффективности мер защиты информации.
60. Контроль защищенности информации на объекте ВТ от утечки по каналу ПЭМИ
61. Аттестационный контроль защищенности от РПЭМИН.
62. Технический контроль защищенности от РПЭМИН.
63. Эксплуатационный контроль защищенности от РПЭМИН.
64. Методы испытаний. Общие положения.

65. Методы испытаний. Аппаратура и оборудование.
66. Методы испытаний. Измерения напряжения ПЭМИН
67. Методы испытаний. Измерения напряженности поля
68. Методы контроля защищенности помещений генераторов технических средств
69. Технический контроль акустической защищенности выделенного помещения. Общие положения
70. Технический контроль акустической защищенности выделенного помещения. Подготовительный этап контроля
71. Технический контроль акустической защищенности выделенного помещения. Акустический и виброакустический контроль
72. Технический контроль акустической защищенности выделенного помещения. Контроль технических средств и систем
73. Аттестация объектов информатизации. Основные положения
74. Организационная структура системы аттестации объектов информатизации в РБ
75. Аттестация объектов информатизации. Мероприятия по выявлению и оценке свойств каналов утечки
76. Аттестация объектов информатизации. Специальные проверки
77. Аттестация объектов информатизации. Специальные обследования
78. Специальные исследования. Основные понятия.
79. Физический смысл задачи специальных исследований
80. Специальные исследования в области акустики и виброакустики
81. Специальные исследования в области акустоэлектрических преобразований
82. Специальные исследования в области защиты цифровой информации.
83. Общие сведения по оценке безопасности объектов
84. Оценка эффективности защиты акустической (речевой) информации.
85. Оценка экранирования электромагнитных волн
86. Оценка эффективности систем защиты программного обеспечения
87. Сущность и задачи комплексной системы защиты информации
88. Модель представления комплексной системы информационной безопасности.
89.

Структура экзаменационного билета.
Экзаменационный билет включает в себя два теоретических вопроса и одну задачу.
Примерные вопросы для экзамена:
1. Теоретический вопрос.
2.Теоретический вопрос.

Образец экзаменационного билета

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

Специальность10.05.05«Безопасность информационных технологий в правоохранительной сфере»

Дисциплина Техническая защита информации

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Организационные каналы обмена и передачи информации.
2. Электромагнитный канал утечки информации.

Зав. кафедрой управления информационной безопасностью А.С.Исмагилова

Критерии и методика оценивания (в баллах):

- 25-30 баллов выставляется студенту, если студент дал полные, развернутые ответы на все теоретические вопросы билета, продемонстрировал знание функциональных возможностей, терминологии, основных элементов, умение применять теоретические знания при выполнении практических заданий. Студент без затруднений ответил на все дополнительные вопросы. Практическая часть работы выполнена полностью без неточностей и ошибок;

- 17-24 баллов выставляется студенту, если студент раскрыл в основном теоретические вопросы, однако допущены неточности в определении основных понятий. При ответе на дополнительные вопросы допущены небольшие неточности. При выполнении практической части работы допущены несущественные ошибки;

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

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

Перевод оценки из 100-балльной в четырехбалльную 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.

Тестирование

Задание №1 (***Образец***)

К рекомендуемым методам и способам защиты информации в информационных системах относятся:

а) методы и способы устранения конкурентов;

б) методы и способы защиты информации от несанкционированного доступа;

в) методы и способы сокрытия информации от внутренних нарушителей;

г) методы и способы защиты информации от утечки по техническим каналам.

Задание №2

Сопротивления заземляющих проводников, а также земляных шин должны быть:

а) более 8 Ом;

б) более 6 Ом;

в) не более 6 Ом;

г) не более 8 Ом;

д) более 4 Ом;

е) не более 4 Ом.

Задание №3

В целях устранения акустических каналов утечки информации система вентиляции:

а) не должна быть связана с системой вентиляции других помещений и иметь общий забор и выброс воздуха;

б) не должна быть связана с системой вентиляции других помещений и иметь свой отдельный забор и выброс воздуха;

в) должна удаляться в защищаемом помещении;

г) должна быть связана с системой вентиляции других помещений и иметь свой отдельный забор и выброс воздуха.

Задание №4

Требования по защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах определяются:

а) Приказом ФСТЭК России от 05 февраля 2010 г. № 58;

б) Приказом ФСТЭК России от 18 февраля 2013 г. № 21;

в) Приказом ФСТЭК России от 11 февраля 2013 г. № 17;

г) Приказом ФСТЭК России от 20 июля 2012 г. № 89.

Задание № 5

Генератор шума «Гном-3» может использоваться для:

а) виброакустического зашумления защищаемых помещений;

б) акустического зашумления защищаемых помещений;

в) создания маскирующих электромагнитных помех в посторонних проводниках и соединительных линиях технических средств;

г) создания маскирующих электромагнитных помех в ограждающих конструкциях.

Критерии оценки тестовых заданий

Структура работы	Критерии оценки	Распределение баллов
Один вопрос теста (25 вопросов в варианте)	Неправильный ответ / Правильный ответ	0/0,6 0/15

Темы практических работ

1) Виброакустические технические каналы утечки речевой информации.
2) Технические каналы утечки видовой информации. Способы скрытого видеонаблюдения и съемки.
3) Защита конфиденциальной информации от несанкционированного доступа в автоматизированных системах.
4) Порядок проведения контроля защищенности выделенных помещений от утечки акустической речевой информации.

Типовая практическая работа

Модуль 2. Скрытие и защита информации от утечки по техническим каналам

Тема: Порядок проведения контроля защищенности выделенных помещений от утечки акустической речевой информации.

Цель: Практическое ознакомление с оформлением Протокола инструментально-расчётной оценки защищённости защищаемого помещения от утечки речевой информации.

Задание:

1) Заполните Протокол инструментально-расчётной оценки защищённости защищаемого помещения от утечки речевой информации. В качестве защищаемого помещения выбрана аудитория, в которой проводятся практические занятия.

Порядок выполнения:

1) Подготовить план–схему защищаемого помещения.

2) Подготовить описание ограждающих конструкций и элементов технических систем защищаемого помещения
3) Подготовьте описание применяемых мер и средств защиты.
4) Перечислите нормативные и методические документы, используемые при оценке защищённости.
5) По имеющимся замерам полностью заполнить таблицу:

iНомер октавной полосы	Измеренный уровень дБL_{c1i} акустического сигнала в защищаемом помещении	Измеренный уровень $L_{ші}$, дБакустического шума в контрольной точке	ического ого шума вУровень измеренного очке	$L_{(с+ш)i}$ - $L_{ші}$Расчётное значение	ого сигнала вРасчётный уровень	Октавные уровни в контрольной чке
Контрольная точка № 1						
1	70	16	28			
2	70	23	28			
3	70	13	23			
4	70	26	27			
5	70	18	21			

6) Вынести заключение о выполняемости/не выполняемости требований по защите информации.

Критерии оценки практической работы

Структура работы	Критерии оценки	Распределение баллов
Модуль 1. Классификация программного обеспечения Модуль 2. Основы операционных систем	работа выполнена с ошибками/ работа выполнена, но без оптимизации / работа выполнена с оптимизацией схемы	0/3/5

Темы лабораторных работ

1) Технические каналы утечки речевой информации.
2) Портативный комплект для обнаружения средств съема информации и выявления каналов ее утечки «Пиранья».
3) Система охранно-тревожной сигнализации. Система контроля и управления доступом. Телевизионные системы. Система пожарной сигнализации.
4) Порядок проведения контроля защищенности выделенных помещений от утечки акустической речевой информации.

Типовая лабораторная работа

Модуль 1. Технические каналы утечки информации

Тема: Портативный комплект для обнаружения средств съема информации и выявления каналов ее утечки «Пиранья».

Цель: Практическое ознакомление с многофункциональным поисковым прибором ST031 «Пиранья».

Задание:

Порядок выполнения:

1) По техническому описанию прибора и настоящему пособию изучить устройство, технические характеристики, инструкцию по эксплуатации прибора ST031 «Пиранья» и меры безопасности при работе с ним.
2) Руководствуясь инструкцией по эксплуатации, подготовить прибор к работе, произвести проверку его работоспособности, настройку и юстировку.
3) Обеспечить удаление из помещения, где проводятся занятия, мощных помеховых объектов, отключить сотовые телефоны.
4) Провести проверку работоспособности прибора ST031 во всех основных режимах работу, или только в режимах указанных преподавателем. Зафиксировать характеристики тестовых сигналов, излучаемых КУ.
5) Провести обследование помещения в одном из режимов, указанном преподавателем, при обнаружении посторонних сигналов провести их идентификацию и определить характеристики. По возможности установить источник этих излучений и его примерное местоположение.

Критерии оценки лабораторной работы

Структура работы	Критерии оценки	Распределение баллов
Модуль 1. Классификация программного обеспечения Модуль 2. Основы операционных систем	работа выполнена с ошибками/ работа выполнена, но без ответов на дополнительные вопросы / работа выполнена с дополнительными вопросами.	0/3/5

4.3 Рейтинг-план дисциплины

(при необходимости)

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. Скрипник Д. А. Общие вопросы технической защиты информации: Учебная литература для ВУЗов [Электронный ресурс/ Москва: Национальный Открытый Университет «ИНТУИТ», 2016.- 425 стр. Режим доступа //http://http://biblioclub.ru/index.php?page=book_red&id=429070&sr=1
2. Голиков А. М. Защита информации от утечки по техническим каналам: учебное пособие[Электронный ресурс]Томский государственный университет систем управления и радиоэлектроники, 2015. -256с.Режим доступа //http:/http://biblioclub.ru/index.php?page=book_red&id=480636&sr=1

Дополнительная литература

3. Блохин А.В. Электротехника: учебник [Электронный ресурс]/А.В. Блохин.:

Екатеринбург.: УГТУ, 2014.184с. .Режим доступа //http://biblioclub.ru/book/275798/

4. Белоус А. И. , Ефименко С. А. , Турцевич А. С.Полупроводниковая силовая электроника - Москва: Техносфера, 2013.-228с. Режим доступа //https://biblioclub.ru/index.php?page=book_red&id=273783/

5. Рябов Б. А. , Малахов С. М., Хотунцев Ю. Л. Практикум по радиоэлектронике Москва: МПГУ, 2017.- 108 стр. Режим доступа //https: //biblioclub.ru/index.php? page=book_red&id=471195&sr=1

6. Голиков А. М. Защита информации в инфокоммуникационных системах и сетях: учебное пособие[Электронный ресурс]Томский государственный университет систем управления и радиоэлектроники, 2015. -256с.Режим доступа //http:/http://biblioclub.ru/index.php?page=book_red&id=480636&sr=1

7. Сердюк В. А. Организация и технологии защиты информации : обнаружение и предотвращение информационных атак в автоматизированных системах предприятий: учебное пособие[Электронный ресурс] Москва: Издательский дом Высшей школы экономики, 2015 .-574с. -Режим доступа http://biblioclub.ru/index.php? page=book_red&id=440285&sr=1

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

1. Справочная правовая система «КонсультантПлюс» – http://www.consultant-plus.ru.
2. Электронная библиотечная система «Университетская библиотека онлайн» – https:// biblioclub.ru.
3. Электронная библиотечная система издательства «Лань» – https://e.lanbook.com/
4. Электронный каталог Библиотеки БашГУ – http://www.bashlib.ru/catalogi/
5. www.fstec.ru –сайт ФСТЭК России
6. www.fsb.ru – сайт ФСБ России
7. http://window.edu.ru/– Наиболее обширная электронная база учебников и методических материалов на сайте информационной системы «Единое окно доступа к образовательным ресурсам»;
8. http://univertv.ru/video/matematika/ – Открытый образовательный видеопорталUniverTV.ru. Образовательные фильмы на различные темы. Лекции в ведущих российских и зарубежных вузах. Научная конференция или научно-популярная лекция по интересующему вопросу);
9. www.newlibrary.ru – Новая электронная библиотека;
10. www. edu.ru – Федеральный портал российского образования;
11. www.elibrary.ru – Научная электронная библиотека;
12. www.nehudlit.ru – Электронная библиотека учебных материалов.
13. Windows 8 Russian Russian OLP NL AcademicEdition и Windows Professional 8 Russian Upgrade OLP NL Academic Edition. Договор №104 от 17.06.2013 г. Лицензиибессрочные.
14. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензиибессрочные.
15. Система централизованного тестирования БашГУ (Moodle). GNUGeneralPublicLicense.

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

Наименование специальных помещений и помещений для самостоятельной работы	Вид занятия	Оснащенность специальных помещений и помещений для самостоятельной работы
1. *учебная аудитория для проведения занятий лекционного типа:* аудитория № 403 (гуманитарный корпус), аудитория № 405 (гуманитарный корпус), аудитория № 413 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 515 (гуманитарный корпус), аудитория № 516 (гуманитарный корпус). **2. *учебная аудитория для проведения лабораторных работ:*** компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус). **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	Лекции, практические работы, самостоятельные работы, групповой и индивидуальный опрос	**Аудитория № 403** Учебная мебель, доска, Мультимедийный-проектор Panasonic PT-LB78VE – 1 шт., Экран настенный ClassicNorma 244*183 – 1 шт., учебно-наглядные пособия. **Аудитория № 405** Учебная мебель, доска, вокальные радиомикрофоны AKGWMS 40 – 2шт., Интер-ая система со встроенным короткофокусным проекто-ром PrometheanActivBoard 387 RPOMOUNTEST -1 шт., Ком-ер встраиваемый в кафедру INTELCorei3-4150/DDr3 4 Gb/HDD, Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт., Настольный интерактивный дисплей , ActivPanel 21S – 1 шт. , Матричный коммутатор сигналов интерфейса HDMICMPRO 4H4H – 1 шт. , Мультимедиа-проектор PanasonicPT-EW640E - 1 шт., Двух-полосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W)(белый) -6 шт., Петличный радиомикрофон AKGWMS45 – 1 шт. , Терминал видео конференц-связи LifeSizeIcon 600 Camera 10xPhone 2ndGeneration – 1 шт., Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт. **Аудитория № 413** Учебная мебель, доска, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 6 шт., Микшер-усилитель 120Вт АРАРТ МА1225 – 1 шт. **Аудитория № 415** Учебная мебель, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 2 шт., Интерактивная доска SMART с проектором V25, Микшер-усилитель 120Вт АРАРТ МА1225 – 1 шт. **Аудитория № 416** Учебная мебель, доска, проектор Optoma Ex542 i- 1 шт., Экран настенный Dinon – 1 шт. **Аудитория № 418** Учебная мебель, доска, Экран настенный LumienMasterPikture 153*203 MatteWhiteFiberClas(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**

аудитория № 420 (гуманитарный корпус). **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). **5.*помещения для самостоятельной работы:*** читальный зал библиотеки аудитория 402 (гуманитарный корпус), аудитория № 613 (гуманитарный корпус). **6.*помещение для хранения и профилактического обслуживания учебного оборудования:***аудитория № 523 (гуманитарный корпус).		Учебная мебель, доска, терминал видео конференц-связи LifeSizeIcon 600-камера, интер-ая система со встроенным короткофокусным проектором PrometheanActivBoard 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/Thermaltake VL520B1N2E 220W/Win8Pro64, стол, трибуна, кресла секционные последующих рядов с пюпитром. **Аудитория № 516** Учебная мебель, доска, кресла секционные последующих рядов с пюпитром, мобильное мультимедийное оборудование: проектор ASK Proxima, ноутбук HP, экран. **Аудитория № 509** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 608** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 609** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 610** Учебная мебель, доска, учебно-наглядные пособия, LED Телевизор TCLL55P6 USBLACK – 1 шт., кронштейн для телевизора NBP 5 – 1 шт., Кабель HDMI (m)-HDH(m)ver14,10м. **Аудитория № 613** Учебная мебель, доска, моноблок стационарный – 15 шт. **Компьютерный класс аудитория № 420** Учебная мебель, моноблоки стационарные 15 шт. **Компьютерный класс аудитория № 404** Учебная мебель, компьютеры -15 штук. **Аудитория 402 читальный зал библиотеки** Учебная мебель, доска, компьютеры в комплекте (5 шт.): монитор Samsung, системный блок Asus, клавиатура, мышь, стеллажи, шкафы картотечные, комбинированные. **Аудитория № 523** Шкаф-стеллаж – 4 шт., стол-1 шт., стул – 2 шт.

Приложение 1

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

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ
дисциплины **Техническая защита информации** на 7 семестр

Вид работы	Объем дисциплины
	Очная форма обучения
Общая трудоемкость дисциплины (ЗЕТ / часов)	5 ЗЕТ / 180 часов
Учебных часов на контактную работу с преподавателем:	59,2
лекций	18
практических / семинарских	18
лабораторных	18
Других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем)	1,2
Учебных часов на самостоятельную работу обучающихся, включая подготовку к экзамену	77

Форма контроля:
Экзамен 7 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
1	Модуль 1. Технические каналы утечки информации Тема: Виды, источники и носители защищаемой информации. Классификация иностранной технической разведки. Возможности видов технической разведки. Основные этапы и процедуры добывания информации технической разведкой. Задачи систем защиты информации. Технические каналы утечки информации. Структура, классификация и основные характеристики. Технические каналы утечки информации, обрабатываемой ТСПИ.	2			8	Основная 1, 2 Дополнительная 3,4,5, 6, 7	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Практическая работа, тестирование
	Тема: Физическая природа побочных электромагнитных излучений. Основные уравнения электромагнитного поля. Элементарный электрический излучатель. Элементарный магнитный излучатель. Электромагнитные каналы утечки информации ТСПИ. Электрические каналы утечки информации. Наводки электромагнитных излучений ТСПИ. Параметрический канал утечки информации. Технические каналы утечки информации при передаче ее по каналам связи. Электрические линии связи. Средства передачи электрических сигналов. Виды проводных электрических линий связи и их параметры. Каналы утечки информации за счет паразитных связей. Опасные сигналы и их источники. Электрические каналы утечки информации. Контроль и прослушивание телефонных каналов связи.	2			8			

	Электромагнитные каналы утечки информации. Индукционный канал утечки информации.							
	Тема: Технические каналы утечки речевой информации. Краткие сведения по акустике. Звуковое поле. Линейные характеристики звукового поля. Энергетические характеристики звукового поля. Плоская волна. Сферическая волна. Акустические и электрические уровни. Звуковые сигналы. Маскировка звуковых сигналов. Понятность и разборчивость речи. Частотный диапазон и спектры. Звуковое поле в помещении. Звуковой фон в помещении. Характеристики помещения. Звукопоглощающие материалы и конструкции. Звукоизоляция помещений.	2			9			
	Тема: Акустические каналы утечки речевой информации. Микрофоны. Направленные микрофоны. Проводные системы, портативные диктофоны и электронные стетоскопы. Радиомикрофоны. Гидроакустические датчики. СВЧ- и ИК-передатчики. Виброакустические технические каналы утечки речевой информации. Акустоэлектрические каналы утечки речевой информации. Оптико-электронный технический канал утечки речевой информации. Параметрические технические каналы утечки речевой информации. Технические каналы утечки видовой информации. Способы скрытого видеонаблюдения и съемки Демаскирующие признаки объектов. Демаскирующие признаки объектов в видимом диапазоне электромагнитного спектра. Демаскирующие признаки объектов в инфракрасном диапазоне электромагнитного спектра. Демаскирующие признаки радиоэлектронных средств.	2	4	4	9			
	Тема: Индикаторы электромагнитного поля. Сканирующие радиоприемники. Анализаторы спектра, радиочастотомеры. Многофункциональные комплекты для выявления каналов утечки информации. Портативный комплект для обнаружения средств съема информации и выявления каналов ее утечки ПКУ-6М. Портативный комплект для обнаружения средств съема информации и выявления каналов ее утечки «Пиранья». Комплекс RS turbo. Комплексы измерения ПЭМИН. Нелинейные локаторы. Комплекс для измерения характеристик акустических сигналов «Спрут-7». Металлодетекторы. Портативная рентгенотелевизионная установка «НОРКА». Досмотровые эндоскопы.	2	6	6	8			

2	Модуль 2. Скрытие и защита информации от утечки по техническим каналам Тема: Концепция и методы инженерно-технической защиты информации. Экранирование электромагнитных волн. Электромагнитное экранирование и развязывающие цепи. Подавление емкостных паразитных связей. Подавление индуктивных паразитных связей. Экранирование проводов и катушек индуктивности. Экранированные помещения. Безопасность оптоволоконных кабельных систем. Заземление технических средств и подавление информационных сигналов в цепях заземления. Фильтрация информационных сигналов. Основные сведения о помехоподавляющих фильтрах. Выбор типа фильтра. Пространственное и линейное зашумление. Способы предотвращения утечки информации через ПЭМИН ПК.	2			9	Основная 1, 2 Дополнительная 3,4,5, 6, 7	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Практическая работа, тестирование
	Тема: Устройства контроля и защиты слаботочных линий и сети. Особенности слаботочных линий и сетей как каналов утечки информации. Рекомендуемые схемы подключения анализаторов к электросиловым и телефонным линиям в здании. Устройства контроля и защиты проводных линий от утечки информации. Скрытие и защита от утечки информации по акустическому и виброакустическому каналам. Скрытие речевой информации в телефонных системах с использованием криптографических методов. Защита конфиденциальной информации от несанкционированного доступа в автоматизированных системах. SecretNet 5.0. Электронный замок «Соболь». USB-ключ. Считыватели Proximity. Технология защиты информации на основе смарт-карт. Кейс «Тень». Устройство для быстрого уничтожения информации на жестких магнитных дисках «Стек-Н».	2			8			
	Тема: Категории объектов защиты. Особенности задач охраны различных типов объектов. Общие принципы обеспечения безопасности объектов. Система охранно-тревожной сигнализации. Система контроля и управления доступом. Телевизионные системы. Система пожарной сигнализации. Периметровая охрана. Тема: Мероприятия по выявлению и оценке свойств каналов утечки информации. Специальные проверки. Специальные обследования. Специальные исследования. Специальные исследования акустических и виброакустических каналов. Специальные исследования	2 2	4 4	4 4	9 9			

	акустоэлектрических преобразований. Специальные исследования технических средств и систем на возможность утечки информации за счет побочных электромагнитных излучений и наводок. Цели и задачи технического контроля эффективности мер защиты информации. Порядок проведения контроля защищенности информации на объекте ВТ от утечки по каналу ПЭМИ. Методы испытаний ПЭВМ. Порядок проведения контроля защищенности АС от НСД. Методы контроля побочных электромагнитных излучений генераторов технических средств. Порядок проведения контроля защищенности выделенных помещений от утечки акустической речевой информации. Подготовительный этап контроля. Акустический и виброакустический контроль. Методика контроля. Выбор контрольных точек и размещение элементов измерительных комплексов. Калибровка передающего измерительного комплекса. Размещение акустического излучателя передающего измерительного комплекса. Измерение отношений «сигнал/шум» в контрольных точках при инструментальном контроле рабочих помещений, не оборудованных системой звукоусиления. Измерение отношений «сигнал/шум» в контрольных точках при инструментальном контроле рабочих помещений, оборудованных системой звукоусиления. Контроль технических средств и систем на наличие акустоэлектрических преобразований. Подготовительный этап контроля. Методика контроля.							
Всего часов:		18	18	18	77			
		36	36		63			

Приложение 2

Рейтинг-план дисциплины

Техническая защита информации

Специальность 10.05.05 Безопасность информационных технологий в правоохранительной сфере курс 4, семестр7

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1. Технические каналы утечки информации.				
Текущий контроль				20
1. Практическая работа	5	2	0	10
2. Лабораторная работа	5	2	0	10
Рубежный контроль				
Тест	15	1	0	15
Всего		5	0	35
Модуль 2. Скрытие и защита информации от утечки по техническим каналам/				
Текущий контроль				20
1. Практическая работа	5	2	0	10
2. Лабораторная работа	5	2	0	10
Рубежный контроль				
Тест	15	1	0	15
Всего		5	0	35
Поощрительные баллы				
1. Участие в студенческой олимпиаде по дисциплине	3	1	0	3
2.Публикация научной статьи	4	1	0	4
3.Участие в научно-практической конференции по профилю	3	1	0	3
Всего		3	0	10
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
1. Посещение лекционных занятий			0	-6
2. Посещение практических (семинарских, лабораторных занятий)			0	-10

Итоговый контроль				
1.Экзамен	30	1	0	30