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

Актуализировано:
на заседании кафедры
протокол от «07»июня 2018 г. №10
Зав. кафедрой /А.С. Исмагилова

Согласовано:
Председатель УМК института
/Р.А. Гильмутдинова

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Программно-аппаратные средства защиты информации

Б1.Б.15 базовая

программа бакалавриата

Направление подготовки
10.03.01 Информационная безопасность

Профиль подготовки
Организация и технология защиты информации

Квалификация
бакалавр

Разработчики (составители)
ст. преподаватель /И.В. Салов
к.б.н., доцент /Ф.Т. Байрушин/

Для приема: 2017 г.

Уфа 2018 г.

Составители: И.В.Салов, Ф.Т. Байрушин

Рабочая программа дисциплины актуализирована на заседании кафедры управления информационной безопасностью протокол от «07»июня 2018 г. №10

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 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	Знать понятие и методы саморазвития, самообучения и самовоспитания личности, компоненты образовательной деятельности (мотивационный, процессуальный, организационный, оценочный), типовые алгоритмы самообразования, требования к компетентности специалиста и его развитию, требования к повышению квалификации и мастерства в профессиональной среде	ОК-8: Способность к самоорганизации и самообразованию	
	Знать аппаратные средства вычислительной техники; операционные системы персональных ЭВМ; основы администрирования вычислительных сетей; системы управления БД, эксплуатационные и технико-экономические характеристики программных и технических средств защиты информации и обеспечения информационной безопасности, типы технических и программно-аппаратных средств обработки и защиты информации, основные направления политик защиты информации на предприятии (организации)	ПК-1:Способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	
	Знать основы систем и языков программирования, инструментальные средства для обработки данных, средства разработки программного обеспечения, технологии создания программ сложной структуры	ПК-2: Способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	
	Знать политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и	ПК-13: Способность принимать участие в формировании, организовывать 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	поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	
Умения	Уметь самостоятельно ставить самообразовательные задачи, планировать и реализовывать собственную образовательную траекторию, анализировать и выбирать формы и методы повышения квалификации и мастерства в зависимости от собственных потребностей и образовательной траектории	ОК-8: Способность к самоорганизации и самообразованию	
	Уметь формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе, осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты, выполнять работы по установке, конфигурированию и эксплуатации технических и программных средств обеспечения информационной безопасности и защиты информации	ПК-1:Способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	
	Уметь использовать существующие пакеты прикладных программ для решения поставленной задачи, реализовать и отлаживать пакеты прикладных программ, решать задачи проектирования программных систем с помощью различных методов	ПК-2: Способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	
	Уметь реализовывать на практике принципы политики безопасности, использовать закономерности преобразования данных в каналах при выполнении комплекса мер по информационной безопасности, обосновывать организационно-	ПК-13: Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению	

	технические мероприятия по защите информации, использовать возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации	информационной безопасности, управлять процессом их реализации	
Владения (навыки / опыт деятельности)	Владеть методами самоанализа, анализом и оценкой эффективности программы и результатов самообразования, способами управления своими знаниями для обеспечения своей конкурентоспособности, методами организации собственного обучения	ОК-8: Способность к самоорганизации и самообразованию	
	Владеть методами оценки, тестирования. настройки на применение средств программно-технического обеспечения защиты информации	ПК-1:Способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	
	Владеть навыками применения инструментальных средств для создания программ различного назначения, навыками создания системного, прикладного ПО для решения профессиональных задач	ПК-2: Способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	
	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-	ПК-13: Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	

	коммуникационных технологий, навыками внедрения, адаптации и настройки средств защиты прикладных ИС		

2. Место дисциплины в структуре образовательной программы

Дисциплина «Программно-аппаратные средства защиты информации» относится к дисциплинам базовой части образовательной программы.

Дисциплина изучается на 3-емкурсе в 6 семестре.

Цель изучения дисциплины: формирование у бакалавров целостного представления об программно-аппаратных средствах защиты информации. Для освоения дисциплины необходимы компетенции, сформированные в рамках изучения следующих дисциплин:

Математика,

Математический анализ,

Дискретная математика,

Основы информационной безопасности,

Средства вычислительной техники,

Аппаратные средства вычислительной техники.

Эти дисциплины направлены на формирование компетенций ОК-8, ПК-1, ПК-2, ПК-13.

3. Содержание рабочей программы (объем дисциплины, типы и виды учебных занятий, учебно-методическое обеспечение самостоятельной работы обучающихся)

Содержание рабочей программы представлено в Приложении 1.

4. Фонд оценочных средств по дисциплине

4.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

ОК-8: Способность к самоорганизации и самообразованию

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 понятие и методы саморазвития, самообучения и самовоспитания личности	Не знает	Имеет фрагментарные знания о методах саморазвития, самообучения и самовоспитания личности	В целом знает методы саморазвития, самообучения и самовоспитания личности	Демонстрирует целостные знания о методах саморазвития, самообучения и самовоспитания личности
	Знать компоненты образовательной деятельности (мотивационный, процессуальный, организационный, оценочный)	Не знает	Имеет фрагментарные знания о компонентах образовательной деятельности (мотивационный, процессуальный, организационный, оценочный)	В целом знает компоненты образовательной деятельности (мотивационный, процессуальный, организационный, оценочный)	Демонстрирует целостные знания о компонентах образовательной деятельности (мотивационный, процессуальный, организационный, оценочный)

	Знать типовые алгоритмы самообразования	Не знает	Имеет фрагментарные знания о типовых алгоритмах самообразования	В целом знает типовые алгоритмы самообразования	Демонстрирует целостные знания о типовых алгоритмах самообразования
	Знать требования к компетентности специалиста и его развитию, требования к повышению квалификации и мастерства в профессиональной среде	Не знает	Имеет фрагментарные знания о требованиях к компетентности специалиста и его развитию, требованиях к повышению квалификации и мастерства в профессиональной среде	В целом знает требования к компетентности специалиста и его развитию, требования к повышению квалификации и мастерства в профессиональной среде	Демонстрирует целостные знания о требованиях к компетентности специалиста и его развитию, требованиях к повышению квалификации и мастерства в профессиональной среде
Второй этап (уровень)	Уметь самостоятельно ставить самообразовательные задачи	Не умеет	Умеет самостоятельно ставить самообразовательные задачи, но допускает значительные ошибки	Умеет самостоятельно ставить самообразовательные задачи, но допускает незначительные ошибки	Умеет самостоятельно ставить самообразовательные задачи
	Уметь планировать и реализовывать собственную образовательную траекторию	Не умеет	Умеет планировать и реализовывать собственную образовательную траекторию, но допускает значительные ошибки	Умеет планировать и реализовывать собственную образовательную траекторию, но допускает незначительные ошибки	Умеет планировать и реализовывать собственную образовательную траекторию
	Уметь анализировать и выбирать формы и методы повышения квалификации и мастерства в зависимости от собственных потребностей и образовательной траектории	Не умеет	Умеет анализировать и выбирать формы и методы повышения квалификации и мастерства в зависимости от собственных потребностей и образовательной траектории, но допускает значительные ошибки	Умеет анализировать и выбирать формы и методы повышения квалификации и мастерства в зависимости от собственных потребностей и образовательной траектории, но допускает незначительные ошибки	Умеет анализировать и выбирать формы и методы повышения квалификации и мастерства в зависимости от собственных потребностей и образовательной траектории
Третий этап (уровень)	Владеть методами самоанализа	Не владеет	Недостаточно владеет методами самоанализа	Владеет отдельными методами самоанализа	Способен использовать методы самоанализа
	Владеть анализом и оценкой эффективности программы и результатов самообразования	Не владеет	Недостаточно владеет анализом и оценкой эффективности программы и результатов самообразования	Владеет отдельными методами анализа и оценкой эффективности программы и результатов самообразования	Способен использовать анализ и оценку эффективности программы и результатов самообразования
	Владеть способами управления своими знаниями для обеспечения своей конкурентоспособности	Не владеет	Недостаточно владеет способами управления своими знаниями для обеспечения своей конкурентоспособности	Владеет отдельными способами управления своими знаниями для обеспечения своей конкурентоспособности	Способен использовать способы управления своими знаниями для обеспечения своей конкурентоспособности
	Владеть методами организации собственного обучения	Не владеет	Недостаточно владеет методами организации собственного обучения	Владеет отдельными методами организации собственного обучения	Способен использовать методы организации собственного обучения

ПК-1: Способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств 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 аппаратные средства вычислительной техники; операционные системы персональных ЭВМ; основы администрирования вычислительных сетей; системы управления БД	Не знает	Имеет фрагментарные знания о аппаратных средствах вычислительной техники; операционных системах персональных ЭВМ; основах администрирования вычислительных сетей; системы управления БД	Знает основы аппаратных средств вычислительной техники; операционных систем персональных ЭВМ, администрирования вычислительных сетей; системы	Знает аппаратные средства вычислительной техники; операционные системы персональных ЭВМ, администрирования вычислительных сетей; системы управления БД
	Знать эксплуатационные и технико-экономические характеристики программных и технических средств защиты информации и обеспечения информационной безопасности	Не знает	Имеет фрагментарные знания о эксплуатационных и технико-экономических характеристиках программных и технических средств защиты информации и обеспечения информационной безопасности	Знает основы эксплуатационных и технико-экономических характеристик программных и технических средств защиты информации и обеспечения информационной безопасности	Знает эксплуатационные и технико-экономические характеристики программных и технических средств защиты информации и обеспечения информационной безопасности
	Знать типы технических и программно-аппаратных средств обработки и защиты информации	Не знает	Имеет фрагментарные знания о типах технических и программно-аппаратных средств обработки и защиты информации	Знает основные типы технических и программно-аппаратных средств обработки и защиты информации	Знает типы технических и программно-аппаратных средств обработки и защиты информации
	Знать основные направления политик защиты информации на предприятии (организации)	Не знает	Имеет фрагментарные знания о основных направлениях политик защиты информации на предприятии (организации)	Знает некоторые основные направления политик защиты информации на предприятии (организации)	Знает основные направления политик защиты информации на предприятии (организации)
Второй этап (уровень)	Уметь формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе	Не умеет	Допускает значительные ошибки при формулировании и настройке политик безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе	Допускает незначительные ошибки при формулировании и настройке политик безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе	Имеет навыки формулировании и настройки политик безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе
	Уметь осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты	Не умеет	Допускает значительные ошибки при осуществлении мер противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты	Допускает незначительные ошибки при осуществлении мер противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты	Имеет навыки осуществления мер противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты
	Уметь выполнять работы по установке, конфигурированию и эксплуатации технических и программных средств обеспечения информационной безопасности и защиты информации	Не умеет	Допускает значительные ошибки при выполнении работ по установке, конфигурированию и эксплуатации технических и программных средств обеспечения информационной безопасности и защиты информации	Допускает незначительные ошибки при выполнении работ по установке, конфигурированию и эксплуатации технических и программных средств обеспечения информационной безопасности и защиты информации	Имеет навыки выполнения работ по установке, конфигурированию и эксплуатации технических и программных средств обеспечения информационной безопасности и защиты информации

Третий этап (уровень)	Владеть методами оценки, тестирования, настройки на применение средств программно-технического обеспечения защиты информации	Не владеет	Недостаточно владеет методами оценки, тестирования, настройки на применение средств программно-технического обеспечения защиты информации	Владеет отдельными методами оценки, тестирования, настройки на применение средств программно-технического обеспечения защиты информации	Владеет методами оценки, тестирования, настройки на применение средств программно-технического обеспечения защиты информации

ПК-2: Способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач.

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 систем и языков программирования	Не знает	Имеет фрагментарные знания о основах систем и языков программирования	Знает элементы основ систем и языков программирования	Знает основы систем и языков программирования
	Знать инструментальные средства для обработки данных	Не знает	Имеет фрагментарные знания о инструментальных средствах для обработки данных	Знает основы инструментальных средств для обработки данных	Знает инструментальные средства для обработки данных
	Знать средства разработки программного обеспечения	Не знает	Имеет фрагментарные знания о средствах разработки программного обеспечения	Знает основные средства разработки программного обеспечения	Знает средства разработки программного обеспечения
	Знать технологии создания программ сложной структуры	Не знает	Имеет фрагментарные знания о технологиях создания программ сложной структуры	Знает некоторые технологии создания программ сложной структуры	Знает технологии создания программ сложной структуры
Второй этап (уровень)	Уметь использовать существующие пакеты прикладных программ для решения поставленной задачи	Не умеет	Допускает значительные ошибки при использовании существующих пакетов прикладных программ для решения поставленной задачи	Допускает незначительные ошибки при использовании существующих пакетов прикладных программ для решения поставленной задачи	Имеет навыки использования существующих пакетов прикладных программ для решения поставленной задачи
	Уметь реализовать и отлаживать пакеты прикладных программ	Не умеет	Допускает значительные ошибки при реализации и отладке пакетов прикладных программ	Допускает незначительные ошибки при реализации и отладке пакетов прикладных программ	Имеет навыки реализации и отладки пакетов прикладных программ
	Уметь решать задачи проектирования программных систем с помощью различных методов	Не умеет	Допускает значительные ошибки при решении задач проектирования программных систем с помощью различных методов	Допускает незначительные ошибки при решении задач проектирования программных систем с помощью различных методов	Имеет навыки выполнения работ по решению задач проектирования программных систем с помощью различных методов
Третий этап (уровень)	Владеть навыками применения инструментальных средств для создания программ различного назначения	Не владеет	Недостаточно владеет навыками применения инструментальных средств для создания программ различного назначения	Владеет отдельными навыками применения инструментальных средств для создания программ различного назначения	Владеет навыками применения инструментальных средств для создания программ различного назначения
	Владеть навыками создания системного, прикладного ПО для решения профессиональных	Не владеет	Недостаточно владеет навыками создания системного, прикладного ПО для решения	Владеет отдельными навыками создания системного, прикладного ПО для решения	Владеет навыками создания системного, прикладного ПО для решения профессиональных

	задач		профессиональных задач	профессиональных задач	задач

ПК-13: Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации.

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 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 основные политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации	Знает 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	Знает состояние основных элементов 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	Умеет применять на 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 работы по обоснованию организационно-технических мероприятий по защите информации
	Уметь использовать возможности и особенности организационных,	Не умеет	Допускает значительные ошибки при использовании	Допускает незначительные ошибки при использовании	Имеет навыки использования возможности и особенности

	аппаратных и программных средств безопасности и защиты информации		возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации	возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации	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 формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью	Не владеет	Недостаточно владеет навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью	Владеет отдельными 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
	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

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 понятие и методы саморазвития, самообучения и самовоспитания личности, компоненты образовательной деятельности (мотивационный, процессуальный, организационный, оценочный),	ОК-8: Способность к самоорганизации и самообразованию	тестирование, практическое задание, контрольная работа, лабораторная работа

	типовые алгоритмы самообразования, требования к компетентности специалиста и его развитию, требования к повышению квалификации и мастерства в профессиональной среде		
	Знать аппаратные средства вычислительной техники; операционные системы персональных ЭВМ; основы администрирования вычислительных сетей; системы управления БД, эксплуатационные и технико-экономические характеристики программных и технических средств защиты информации и обеспечения информационной безопасности, типы технических и программно-аппаратных средств обработки и защиты информации, основные направления политик защиты информации на предприятии (организации)	ПК-1:Способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	тестирование, практическое задание, контрольная работа, лабораторная работа
	Знать основы систем и языков программирования, инструментальные средства для обработки данных, средства разработки программного обеспечения, технологии создания программ сложной структуры	ПК-2: Способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	тестирование, практическое задание, контрольная работа, лабораторная работа
	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-13: Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	тестирование, практическое задание, контрольная работа, лабораторная работа

2-й этап Умения	Уметь самостоятельно ставить самообразовательные задачи, планировать и реализовывать собственную образовательную траекторию, анализировать и выбирать формы и методы повышения квалификации и мастерства в зависимости от собственных потребностей и образовательной траектории	ОК-8: Способность к самоорганизации и самообразованию	тестирование, практическое задание, контрольная работа, лабораторная работа
	Уметь формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе, осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты, выполнять работы по установке, конфигурированию и эксплуатации технических и программных средств обеспечения информационной безопасности и защиты информации	ПК-1:Способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	тестирование, практическое задание, контрольная работа, лабораторная работа
	Уметь использовать существующие пакеты прикладных программ для решения поставленной задачи, реализовать и отлаживать пакеты прикладных программ, решать задачи проектирования программных систем с помощью различных методов	ПК-2: Способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	тестирование, практическое задание, контрольная работа, лабораторная работа
	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	ПК-13: Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	тестирование, практическое задание, контрольная работа, лабораторная работа

	средств безопасности и защиты информации		
3-й этап Владения навыками	Владеть методами самоанализа, анализом и оценкой эффективности программы и результатов самообразования, способами управления своими знаниями для обеспечения своей конкурентоспособности, методами организации собственного обучения	ОК-8: Способность к самоорганизации и самообразованию	тестирование, практическое задание, контрольная работа, лабораторная работа
	Владеть методами оценки, тестирования. настройки на применение средств программно-технического обеспечения защиты информации	ПК-1:Способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	тестирование, практическое задание, контрольная работа, лабораторная работа
	Владеть навыками применения инструментальных средств для создания программ различного назначения, навыками создания системного, прикладного ПО для решения профессиональных задач	ПК-2: Способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	тестирование, практическое задание, контрольная работа, лабораторная работа
	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-	ПК-13: Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	тестирование, практическое задание, контрольная работа, лабораторная работа

	коммуникационных технологий, навыками внедрения, адаптации и настройки средств защиты прикладных ИС		

4.3 Рейтинг-план дисциплины

Рейтинг–план дисциплины представлен в приложении 2.

Экзамен

Структура экзаменационного билета

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

Экзаменационные материалы

1. Основные понятия и определения в области создания ПАСОИБ.
2. Нормативно-правовая база создания ПАСОИБ.
3. Анализ угроз информационной безопасности.
4. Анализ сетевых угроз информационной безопасности.
5. Классификация ПАСОИБ.
6. Функциональные возможности ПАСОИБ.
7. Принципы разработки ПАСОИБ.
8. Концепция диспетчера доступа.
9. Основные этапы проектирования ПАСОИБ.
10. Классификация функциональных требований по защите информации и данных.
11. Принципы действия и технологические особенности программно-аппаратных средств, реализующих отдельные функциональные требования по защите информации и данных и их взаимодействие с общесистемными компонентами вычислительных систем.
12. Методы обеспечения идентификации и аутентификации.
13. Методы криптографической защиты.
14. Методы и средства хранения ключевой информации.
15. Методы и средства ограничения доступа к компонентам вычислительных систем.
16. Характеристика методов и средства привязки программного обеспечения к аппаратному кружению и физическим носителям.
17. Методы аудита безопасности.
18. Методы обеспечения доступа к системе защиты и управления безопасностью.
19. Методы обеспечения целостности системы защиты.
20. Классификация аппаратных компонентов средств защиты программ.
21. Классификация программных компонентов средств защиты программ.
22. Структура программного обеспечения.
23. Способы встраивания средств защиты в программное обеспечение.
24. Способы определения факта незаконного использования программ.
25. Способы защиты программ от незаконного использования.
26. Способы изучения кода программ.
27. Способы защиты программ от изучения кода.
28. Основные принципы обеспечения безопасности программ.
29. Изолированная программная среда.
30. Классификация программно-аппаратных средств защиты от

несанкционированного доступа к информации, хранимой в ПЭВМ.

31. Характеристики программно-аппаратных средств защиты от несанкционированного доступа к информации, хранимой в ПЭВМ.
32. Понятие электронного замка.
33. Принципы построения и функционирования электронных замков.
34. Механизмы контроля аппаратной конфигурации ПЭВМ.
35. Общие принципы разграничения доступа пользователей к устройствам ПЭВМ.
36. Основные принципы криптографической защиты информации.
37. Классификация программно-аппаратных средств защиты информации в сетях передачи данных.
38. Принципы построения и функционирования межсетевых экранов в сетях передачи данных.
39. Программно-аппаратные средства межсетевого экранирования.
40. Основные принципы защиты информации при передаче по каналам связи.
41. Программно-аппаратные средства защиты информации при передаче по каналам связи.
42. Основные принципы разграничения доступа к сетевым ресурсам.
43. Основные принципы обнаружения сетевых атак.
44. Программно-аппаратные средства обнаружения сетевых атак.
45. Основные принципы защиты от сетевых атак.
46. Программно-аппаратные средства защиты от сетевых атак.
47. Основные принципы управления безопасностью сети.
48. Программно-аппаратные средства управления безопасностью сети.
49. Обзор штатных средств сетевого оборудования, предназначенных для защиты информации при передаче по каналам связи.
50. Способы применения штатных средств сетевого оборудования, предназначенных для защиты информации при передаче по каналам связи.
51. Основные требования к информационной безопасности.
52. Задачи сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности.
53. Технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности.
54. Классификация требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности.
55. Проверка ОИ на базе вычислительной техники.
56. Электронный документ (ЭД). Понятие ЭД. Типы ЭД.
57. Виды информации в КС. Информационные потоки в КС. Понятие исполняемого модуля.
58. Уязвимость компьютерных систем. Понятие доступа, субъект и объект доступа.
59. Понятие несанкционированного доступа (НСД), классы и виды НСД. Несанкционированное копирование программ как особый вид НСД.
60. Понятие злоумышленника; злоумышленник в криптографии и при решении проблем компьютерной безопасности (КБ).
61. Политика безопасности в компьютерных системах. Оценка защищенности.
62. Способы защиты конфиденциальности, целостности и доступности в КС.
63. Руководящие документы Гостехкомиссии по оценке защищенности от НСД.
64. Понятие идентификации пользователя. Задача идентификации пользователя. Понятие протокола идентификации. Локальная и удаленная идентификация. Идентифицирующая информация (понятие, способы

хранения, связь с ключевыми системами).

65. Файл как объект доступа. Оценка надежности систем ограничения доступа – сведение к задаче оценки стойкости.
66. Организация доступа к файлам. Иерархический доступ к файлам. Понятие атрибутов доступа. Организация доступа к файлам различных ОС.
67. Защита сетевого файлового ресурса на примерах организации доступа в различных ОС.
68. Способы фиксации факторов доступа. Журналы доступа и критерии их информативности.
69. Выявление следов несанкционированного доступа к файлам, метод инициированного НСД.
70. Доступ данных со стороны процесса (понятие; отличия от доступа со стороны пользователя).
71. Построение программно-аппаратных комплексов шифрования.
72. Аппаратные и программно-аппаратные средства криптозащиты данных. Построение аппаратных компонент криптозащиты данных, специализированные СБИС как носителя алгоритма шифрования.
73. Защита алгоритма шифрования; принцип чувствительной области и принцип главного ключа.
74. Необходимые и достаточные функции аппаратного средства криптозащиты. Проектирование модулей криптопреобразований на основе сигнальных процессов.
75. Классификация защищаемых компонент ПЭВМ: отчуждаемые и неотчуждаемые компоненты ПЭВМ.
76. Процесс начальной загрузки ПЭВМ, взаимодействие аппаратной и программной частей. Механизмы расширения BIOS. Преимущества и недостатки программных и аппаратных средств.
77. Способы защиты информации на съемных дисках. Организация прозрачного режима шифрования.
78. Магнитные диски прямого доступа.
79. Магнитные и интеллектуальные карты.
80. Средство TouchMemory.
81. Способы изучения ПО: статистическое и динамическое изучение. Роль программной и аппаратной среды.
82. Временная надежность (невозможность обеспечения гарантированной надежности).
83. Задачи защиты от изучения и способы их решения.
84. Защита от отладки: итеративный программный замок.
85. Защита от отладки: принцип ловушек и избыточного кода.
86. Защита от дизассемблирования. Принцип внешней загрузки файлов.
87. Динамическая модификация программы. Защита от трассировки по прерываниям.
88. Способы ассоциирования защиты и программного обеспечения. Оценка надежности защиты от отладки.
89. Ключи на базе перепрограммируемой постоянной памяти.
90. Ключи на базе заказных чипов.
91. Примеры реализации ключей (Aktivator, HASP, Alladin и другие).
92. Ключи на базе микропроцессоров.
93. Модели взаимодействия прикладной программы и программы злоумышленника, компьютерные вирусы как особый класс РПВ, активная и пассивная защита, необходимые и достаточные условия недопущения разрушающего воздействия; понятие изолированной программной среды,

защита программ от изменения и контроль целостности.

94. Основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности; программно-аппаратные средства обеспечения информационной безопасности в типовых ОС, СУБД, вычислительных сетях.

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

Форма 1.4.-33

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ИНСТИТУТ ИСТОРИИ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

Направление 10.03.01 Информационная безопасность

Дисциплина Программно–аппаратные средства защиты информации

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Уязвимость компьютерных систем. Понятие доступа, субъект и объект доступа.
2. Классификация ПАСОИБ.

Зав. Кафедрой УИБ А.С. Исмагилова

Кафедра управления информационной безопасностью

Устанавливается следующая градация перевода оценки из многобалльной в четырехбалльную:

Экзамены:

- отлично – от 80 до 110 баллов (включая 10 поощрительных баллов),
- хорошо – от 60 до 79 баллов,
- удовлетворительно – от 45 до 59 баллов,
- неудовлетворительно – менее 45 баллов.

Критерии оценивания результатов экзамена для ОФО:
Критерии оценки (в баллах):

- 25-30 баллов выставляется студенту, если студент дал полные, развернутые ответы на все теоретические вопросы билета, продемонстрировал знание терминологии, основных понятий, умение применять теоретические знания при выполнении практических заданий. Студент без затруднений ответил на все дополнительные вопросы.

- 17-24 баллов выставляется студенту, если студент раскрыл в основном теоретические вопросы, однако допущены неточности в определении основных понятий. При ответе на дополнительные вопросы допущены небольшие неточности.

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

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

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***)

Незаконный сбор, присвоение и передача сведений составляющих коммерческую тайну, наносящий ее владельцу ущерб, - это...

а) политическая разведка;
б) промышленный шпионаж;
в) добросовестная конкуренция;
г) конфиденциальная информация;
д) правильного ответа нет.

Задание №2

Какая информация является охраняемой внутригосударственным законодательством или международными соглашениями как объект интеллектуальной собственности:

а) любая информация;
б) только открытая информация;
в) запатентованная информация;
г) закрываемая собственником информация;
д) коммерческая тайна.
е) Метод записи чисел, представление чисел с помощью письменных знаков;
ж) Система измерения, сбора, анализа, представления и интерпретации информации о посетителях веб-сайтов с целью их улучшения и оптимизации.

Задание №3

Кто может быть владельцем защищаемой информации

а) только государство и его структуры;
б) предприятия акционерные общества, фирмы;
в) общественные организации;
г) только вышеперечисленные;
д) кто угодно.

Задание №4

Какие сведения на территории РФ могут составлять коммерческую тайну

1) учредительные документы и устав предприятия;

2) сведенья о численности работающих, их заработной плате и условиях труда;

3) документы о платежеспособности, об уплате налогов, о финансово-хозяйственной деятельности;

4) другие;

5) любые.

Задание № 5

Какие секретные сведения входят в понятие «коммерческая тайна»?

1) связанные с производством;

2) связанные с планированием производства и сбытом продукции;

3) технические и технологические решения предприятия;

4) только первый и второй вариант ответа;

5) три первых варианта ответа.

Критерии оценки тестовых заданий

Структура работы	Критерии оценки	Распределение баллов
6 семестр Модуль 1. Основные принципы программно-аппаратных средств обеспечения информационной безопасности, Модуль 2. Программно-аппаратные средства защиты информации		
Один тестовый вопрос (всего в тесте 25 вопросов)	Не правильный ответ/	0/0,6
Тест (все 25 вопросов)	Правильный ответ	0/15

Темы лабораторных работ

Цель проведения лабораторных работы – практическое освоение материала дисциплины.

1) Применение антивирусных программы.
2) Использование программ шифрования дисков.
3) Установка и настройка СЗИ Dallas Lock 8.0.
4) Использование СЗИ Dallas Lock 8.0.

Типовая лабораторная работа

Модуль 1. Основные принципы программно-аппаратных средств обеспечения информационной безопасности.

Тема: Методы криптографической защиты..

Цель: Практическое использование программы сквозного шифрования дисков TrueCrypt 7.0.

Задание: Создать зашифрованный файловый контейнер. Защитить с помощью приложения TrueCrypt флеш-носитель паролем. Создать зашифрованный файловый контейнер.

Порядок выполнения:

1. Изучать «Инструкцию по использованию TrueCrypt 7.0»
2. Создать с помощью приложения TrueCrypt простой том (зашифрованный файловый контейнер). Описать свои действия. В качестве иллюстраций использовать скриншоты. Описать назначение простого тома приложения TrueCrypt.

3. Защитить с помощью приложения TrueCrypt флеш-носитель паролем. Описать свои действия. В качестве иллюстраций использовать скриншоты.
4. 3) Создать с помощью приложения TrueCrypt скрытый том (зашифрованный файловый контейнер). Описать свои действия. В качестве иллюстраций использовать скриншоты. Описать назначение зашифрованного тома приложения TrueCrypt.
5. 4) Описать назначение шифрования с помощью приложения TrueCrypt системного раздела.
6. Ответить на контрольные вопросы:
   a) Возможности ПО TrueCrypt.
   b) Какие еще программы с данными функциями еще известны.
   c) Какие алгоритмы шифрования используются в ПО TrueCrypt 7.0.
7. Защита лабораторной работы. Проводится в форме устного опроса после выполнения работы.

Критерии оценки лабораторной работы

Структура работы	Критерии оценки	Распределение баллов
Одно лабораторное задание	работа выполнена с ошибками и не получены ответы на все контрольные вопросы/ работа выполнена, но не получены ответы на все контрольные вопросы/ работа выполнена и получены ответы на все контрольные вопросы	0/3/7

Темы практических работ

1) Анализ угроз информационной безопасности.
2) Классификация ПАСОИБ.
3) Методы криптографической защиты.
4) Журналы регистрации событий на примере ОС Windows.
5) Программно-аппаратные средства защиты от несанкционированного доступа к информации, хранимой в ПЭВМ.
6) Система контроля и управления доступом (СКУД) на примере гуманитарного корпуса БашГУ.
7) Системы сигнализации на примере гуманитарного корпуса БашГУ.
8) Штатные средства сетевого оборудования, предназначенные для защиты информации при передаче по каналам связи.

Типовая практическая работа

Модуль 2. Программно-аппаратные средства защиты информации.

Тема: Журналы регистрации событий на примере ОС Windows.

Цель: Практическое ознакомление с системой журналирования, применяемой в ОС Windows.

Задание: Ознакомиться с системой журналирования ОС Windows.

Порядок выполнения:

1) Ознакомиться с системой журналирования ОС Windows.
2) Показать ключевые журналы ОС Windows.
3) Указать типичные проблемы, возникающие при обработке указанных журналов.
4) Перечислить типовые пути решения возникающих проблем.

Критерии оценки практической работы

Структура работы	Критерии оценки	Распределение баллов
6 семестр	работа выполнена неполно, не показано общее понимание вопроса, имелись затруднения или допущены ошибки в определении понятий, использовании терминологии /работа выполнена в полном объеме, но допущены один-два недочета при освещении основного содержания ответа, нет определенной логической последовательности, неточно используется специализированная терминология/ работа выполнена в полном объеме и изложена грамотным языком в определенной логической последовательности с точным использованием специализированной терминологии; показано уверенное владение прикладными программами	0/3/6

5. Учебно-методическое и информационное обеспечение дисциплины

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

Основная литература

1. Долозов, Н.Л. Программные средства защиты информации : конспект лекций / Н.Л. Долозов, Т.А. Гультяева ; Министерство образования и науки Российской Федерации, Новосибирский государственный технический университет. - Новосибирск : НГТУ, 2015. - 63 с. : схем., ил. - Библиогр. в кн. - ISBN 978-5-7782-2753-8; То же [Электронный ресурс]. - URL:http://biblioclub.ru/index.php?page=book&id=438307

2. Программно-аппаратные средства обеспечения информационной безопасности: учебное пособие для вузов / А.В. Душкин, О.М. Барсуков, К.В. Славнов, Е.В. Кравцов ; под ред. А.В. Душкина. - Москва : Горячая линия - Телеком, 2016. - 248 с. : схем., табл., ил. - Библиогр.: с. 234-235 - ISBN 978-5-9912-0470-5 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=483768 (07.04.2019).

Дополнительная литература

3. Волкова, Т.В. Основы проектирования компонентов автоматизированных систем : учебное пособие [Электронный ресурс]/ / Т.В. Волкова ; Министерство образования и науки Российской Федерации, Оренбургский Государственный Университет, Кафедра программного обеспечения вычислительной техники и автоматизированных систем. -

Оренбург : ОГУ, 2016. - 226 с. Режим доступа - URL: http://biblioclub.ru/index.php?page=book&id=471129 (13.01.2019).

4. Гухман, В.Б. Краткая история науки, техники и информатики : учебное пособие [Электронный ресурс]/ В.Б. Гухман. - Москва ; Берлин : Директ-Медиа, 2017. - 171с. [Электронный ресурс]/ URL: http://biblioclub.ru/index.php?page=book&id=474295 (13.01.2019).

5. Синицын, Ю.И. Сети и системы передачи информации : учебное пособие[Электронный ресурс]/ Ю.И. Синицын, Е. Ряполова, Р.Р. Галимов ; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего образования «Оренбургский государственный университет». - Оренбург : ОГУ, 2017. - 190 с. – Режим доступа : http://biblioclub.ru/index.php?page=book&id=485524 (13.01.2019).

6. Губарев, В.В. Введение в теоретическую информатику : учебное пособие / В.В. Губарев ; Министерство образования и науки Российской Федерации, Новосибирский государственный технический университет. - Новосибирск : НГТУ, 2014. - Ч. 1. - 420 с. : табл., граф., схем., ил. - Библиогр.: с. 452-457. - ISBN 978-5-7782-2477-3; То же [Электронный ресурс]. - URL:http://biblioclub.ru/index.php?page=book&id=436214

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

1. Справочная правовая система «КонсультантПлюс» – http://www.consultant-plus.ru.
2. Электронная библиотечная система «Университетская библиотека онлайн» – https://biblioclub.ru.
3. Электронная библиотечная система издательства «Лань» – https://e.lanbook.com/
4. Электронный каталог Библиотеки БашГУ – http://www.bashlib.ru/catalogi/
5. www.fstec.ru –сайт ФСТЭК России
6. www.fsb.ru – сайт ФСБ России
7. http://window.edu.ru/ – Наиболее обширная электронная база учебников и методических материалов на сайте информационной системы «Единое окно доступа к образовательным ресурсам»;
8. http://univertv.ru/video/matematika/ – Открытый образовательный видеопортал UniverTV.ru. Образовательные фильмы на различные темы. Лекции в ведущих российских и зарубежных вузах. Научная конференция или научно-популярная лекция по интересующему вопросу);
9. www.newlibrary.ru – Новая электронная библиотека;
10. www. edu.ru – Федеральный портал российского образования;
11. www.elibrary.ru – Научная электронная библиотека;
12. www.nehudlit.ru – Электронная библиотека учебных материалов.
13. Windows 8 Russian Russian OLP NL AcademicEdition и Windows Professional 8 Russian Upgrade OLP NL Academic Edition. Договор №104 от 17.06.2013 г. Лицензии бессрочные.
14. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные.
15. Система централизованного тестирования БашГУ (Moodle).GNU General Public License.
16. Kaspersky Endpoint Security для бизнеса. Договор №31806820398 от 17.09.2018 г. Лицензия стандартная, продление подписки на 1 год.
17. DallasLock 8.0-К (СЗИ НСД, СКН, МЭ, СОВ) (для обучения). Лицензии № 29096-8797-517, 29097-1369-650, 29099-7587-486, 29100-1081-462, 29098-2802-2020, бессрочные.

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

Наименование специализированных аудиторий, кабинетов, лабораторий	Вид занятий	Наименование оборудования, программного обеспечения
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*****:** Лаборатория полигон технической защиты информации № 508 (гуманитарный корпус), Лаборатория систем и сетей передачи данных, сетей и систем передачи информации, программно-аппаратных средств обеспечения информационной безопасности № 507 (гуманитарный корпус), компьютерный класс, аудитория 404 (гуманитарный корпус), аудитория 420 (гуманитарный корпус). **3.** ***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	**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 PanasonicPT-EW640E - 1 шт., Двух-полосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W)(белый) -6 шт., Петличный радиомикрофон AKGWMS45 – 1 шт. , Терминал видео конференц-связи LifeSizeIcon 600 Camera 10xPhone 2ndGeneration – 1 шт., Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт. **Аудитория № 413** Учебная мебель, доска, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 6 шт., Микшер-усилитель 120Вт APAPT MA1225 – 1 шт. **Аудитория № 415** Учебная мебель, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 2 шт., Интерактивная доска SMART с проектором V25, Микшер-усилитель 120Вт APAPT MA1225 – 1 шт. **Аудитория № 416** Учебная мебель, доска, проектор Optoma Ex542 i- 1 шт., Экран настенный Dinon – 1 шт. **Аудитория № 418** Учебная мебель, доска, Экран настенный Lumien Master Pikture 153*203 Matte White Fiber Clas(белый корпус) – 1 шт., Проектор Optoma Ex542 i - 1 шт.	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. Kaspersky Endpoint Security для бизнеса. Договор №31806820398 от 17.09.2018 г. Лицензия стандартная, продление подписки на 1 год. 5. DallasLock 8.0-К (СЗИ НСД, СКН, МЭ, СОВ) (для обучения). Лицензии № 29096-8797-517, 29097-1369-650, 29099-7587-486, 29100-1081-462, 29098-2802-2020, бессрочные.

(гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус). **4.** ***учебная аудитория для проведения групповых и индивидуальных консультаций:*** аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус), компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус). **5.** ***учебная аудитория для текущего контроля и промежуточной аттестации:*** аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус), компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус). **6.** ***помещения для самостоятельной***	**Аудитория № 419** Учебная мебель, Проектор Optoma Ex542 i – 1 шт., Экран настенный Dinon – 1 шт. **Аудитория № 515** Учебная мебель, доска, терминал видео конференц-связи LifeSize Icon 600-камера, интер-ая система со встроенным короткофокусным проектором Promethean ActivBoard 387 RPO MOUNT EST, профес-сиональный LCD дисплей Flame 42ST, настольный интерактивный дисплей SMART Podium SP518 с ПО SMART Notebook, матричный коммутатор сигналов интерфейса HDMI CMPRO 4H4H, интер-ая напольная кафедра докладчика, ком-ер встраиваемый в кафедру IN-TEL Core i3-4150/DDr3 4 Gb/HDD 1TB/DVD-RW/Therm altake VL520B1N2E 220W/Win8Pro64, стол, трибуна, кресла секционные последующих рядов с пюпитром. **Аудитория № 516** Учебная мебель, доска, кресла секционные последующих рядов с пюпитром, мобильное мультимедийное оборудование: проектор ASK Proxima, ноутбук HP, экран. **Аудитория № 509** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 510** 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	

работы: читальный зал библиотеки аудитория 402 (гуманитарный корпус), аудитория № 613 (гуманитарный корпус). **7.*помещение для хранения и профилактического обслуживания учебного оборудования:*** аудитория № 523 (гуманитарный корпус).	комплекте (5 шт.): монитор Samsung, системный блок Asus, клавиатура, мышь, стеллажи, шкафы картотечные, комбинированные. **Лаборатория систем и сетей передачи данных, сетей и систем передачи информации, программно-аппаратных средств обеспечения информационной безопасности № 507** Учебная мебель, учебно-наглядные пособия, аудиторная доска трехсекционная, плакаты с тематикой технические средства обработки информации, стенд "Устройство ПК". **Лаборатория полигон технической защиты информации № 508** Учебная мебель, учебно-наглядные пособия, аудиторная доска трехсекционная, плакаты с тематикой технической защиты информации, комплекс мониторинга WiFi сетей "Зодиак II", универсальный ком-плект инструментов для проведения работ по специальным провер-кам и специальным обследованиям Калейдоскоп-П2, многофункциональный поисковый прибор ST-031M "Пиранья", нелинейный локатор «Лорнет», анализатор электромагнитного поля "Кордон". **Аудитория № 523** Шкаф-стеллаж – 4 шт., стол-1 шт., стул – 2 шт.	

Приложение 1

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ИНСТИТУТ ИСТОРИИ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ

дисциплины **Программно-аппаратные средства защиты информации** на 6 семестре ОФО

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (ЗЕТ / часов)	4 ЗЕТ / 144 часа
Учебных часов на контактную работу с преподавателем:	65,2
лекций	16
практических/ семинарских	32
лабораторных	16
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	1,2
Учебных часов на самостоятельную работу обучающихся, включая подготовку к экзамену	35 43,8

Форма контроля:
Экзамен 6 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. Основные принципы программно-аппаратных средств обеспечения информационной безопасности					Основная 1, 2 Дополнительная 3,4,5,6	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	тестирование, практическое задание, лабораторная работа
	Тема: Основные понятия и определения в области создания ПАСОИБ. Нормативно-правовая база создания ПАСОИБ. Анализ угроз информационной безопасности. Анализ сетевых угроз информационной безопасности. Классификация ПАСОИБ. Функциональные возможности ПАСОИБ. Принципы разработки ПАСОИБ. Концепция диспетчера доступа. Основные этапы проектирования ПАСОИБ.	2	2	0	4			
	Тема: Классификация функциональных требований по защите информации и данных. Принципы действия и технологические особенности программно-аппаратных средств, реализующих отдельные функциональные требования по защите информации и данных и их взаимодействие с общесистемными компонентами вычислительных систем. Методы обеспечения идентификации и аутентификации. Методы криптографической защиты. Методы и средства хранения ключевой информации.	2	6	4	4			
	Тема: Методы и средства ограничения доступа к компонентам вычислительных систем. Характеристика методов и средства привязки программного обеспечения к аппаратному кружению и физическим носителям.	2	4	0	4			
	Тема: Методы аудита безопасности. Методы обеспечения доступа к системе защиты и управления безопасностью. Методы обеспечения целостности системы защиты.	2	4	4	4			
2	Модуль 2. Программно-аппаратные средства					Основная 1, 2	Самостоятельное	тестирование,

	защиты информации Тема: Классификация аппаратных компонентов средств защиты программ. Классификация программных компонентов средств защиты программ. Структура программного обеспечения. Способы встраивания средств защиты в программное обеспечение. Способы определения факта незаконного использования программ. Способы защиты программ от незаконного использования. Способы изучения кода программ. Способы защиты программ от изучения кода. Основные принципы обеспечения безопасности программ. Изолированная программная среда. Классификация программно-аппаратных средств защиты от несанкционированного доступа к информации, хранимой в ПЭВМ. Характеристики программно-аппаратных средств защиты от несанкционированного доступа к информации, хранимой в ПЭВМ. Понятие электронного замка. Принципы построения и функционирования электронных замков. Механизмы контроля аппаратной конфигурации ПЭВМ. Общие принципы разграничения доступа пользователей к устройствам ПЭВМ. Основные принципы криптографической защиты информации.	2	4	4	6	Дополнительная 3,4,5,6	изучение рекомендуемой основной и дополнительной литературы	практическое задание, лабораторная работа
	Тема: Классификация программно-аппаратных средств защиты информации в сетях передачи данных. Принципы построения и функционирования межсетевых экранов в сетях передачи данных. Программно-аппаратные средства межсетевого экранирования. Основные принципы защиты информации при передаче по каналам связи. Программно-аппаратные средства защиты информации при передаче по каналам связи. Основные принципы разграничения доступа к сетевым ресурсам. Основные принципы обнаружения сетевых атак. Программно-аппаратные средства обнаружения сетевых атак. Основные принципы защиты от сетевых атак. Программно-аппаратные средства защиты от сетевых атак. Основные принципы управления безопасностью сети. Программно-аппаратные средства управления безопасностью сети. Обзор штатных средств сетевого оборудования, предназначенных для защиты информации при передаче по каналам связи. Способы применения штатных средств сетевого оборудования, предназначенных для защиты информации при передаче по каналам связи.	2	6	4	4			
	Тема: Основные требования к информационной безопасности. Задачи сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности. Технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности.	2	4	0	4			
	Тема: Классификация требований к программной и программно-	2	2	0	5			

	аппаратной реализации средств обеспечения информационной безопасности. Проверка ОИ на базе вычислительной техники.							
Всего:		16	32	16	35			

Приложение 2

Рейтинг-план дисциплины

Основы управления информационной безопасностью

Направление 10.03.01 Информационная безопасность курс 3, семестр 6

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1. Основные принципы программно-аппаратных средств обеспечения информационной безопасности				
Текущий контроль				20
1. Лабораторная работа	7	2	0	14
2. Практическая работа	6	1	0	5
Рубежный контроль				
Тест	15	1	0	15
Всего		3	0	35
Модуль 2. Программно-аппаратные средства защиты информации				
Текущий контроль				20
1. Лабораторная работа	7	2	0	14
2. Практическая работа	6	1	0	5
Рубежный контроль				
Тест	15	1	0	15
Всего		3	0	35
Поощрительные баллы				
1. Участие в студенческой олимпиаде по дисциплине	3	1	0	3
2.Публикация научной статьи	4	1	0	4
3.Участие в научно-практической конференции по профилю	3	1	0	3
Всего		3	0	10
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
1. Посещение лекционных занятий			0	-6
2. Посещение практических (семинарских, лабораторных занятий)			0	-10

Итоговый контроль				
1.Экзамен	30	1	0	30