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

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

Согласовано:
Председатель УМК института
/ Р.А. Гильмутдинова

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Криптографические методы защиты информации
(Б1.В.1.ДВ.08.02 дисциплина по выбору)

программа специалитета

Специальность
10.05.05 Безопасность информационных технологий в правоохранительной сфере

Специализация
Технология защиты информации в правоохранительной сфере

Квалификация
Специалист по защите информации

Разработчик (составитель) / А.Б. Пушкарёв

Для приема: 2014 г.

Уфа 2018

Составитель / составители: А.Б. Пушкарёв

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

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры управления информационной безопасностью, протокол № ___ от «____» _____ 201 _ г.

Заведующий кафедрой _____/ А.С. Исмагилова/

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

Заведующий кафедрой _____/ А.С. Исмагилова/

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

Заведующий кафедрой _____/ А.С. Исмагилова/

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

Заведующий кафедрой _____/ А.С. Исмагилова/

Список документов и материалов

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы....4
2. Цель и место дисциплины в структуре образовательной программы....6
3. Содержание рабочей программы (объем дисциплины, типы и виды учебных занятий, учебно-методическое обеспечение самостоятельной работы обучающихся)....6
4. Фонд оценочных средств по дисциплине....6
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 7
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 8
4.3 Рейтинг-план дисциплины 16
5. Учебно-методическое и информационное обеспечение дисциплины....16
5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины 16
5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины 17
6.Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине....17
Приложение 1....20
Приложение 2....24

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

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

Результаты обучения		Формируемая компетенция (с указанием кода)	Примечание
Знания	1. Знать сущность и структуру психологии группы, динамические процессы в межличностных отношениях, механизмы межгруппового взаимодействий, структуру психологии группы, динамические процессы в межличностных отношениях, механизмы межгруппового взаимодействий, основные психические процессы, свойства и состояния личности, факторы, негативно влияющие на психическое здоровье сотрудников, признаки стрессового напряжения и «эмоционального выгорания»	ОК-6: Способность проявлять психологическую устойчивость в сложных и экстремальных условиях, применять методы эмоциональной и когнитивной регуляции для оптимизации собственной деятельности и психологического состояния	
	2. Знать политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации, понятие системы управления, основные виды структур, принципы системного подхода к анализу структур	ПК-3: Способность организовывать и проводить мероприятия по контролю за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, проводить анализ эффективности системы защиты информации	
	3. Знать особенности защиты государственной тайны, состояние законодательной базы и стандарты в области защиты государственной тайны	ПК-30: Способность планировать проведение работ по комплексной защите информации и сведений, составляющих государственную тайну, на объекте информатизации	
Умения	1. Уметь анализировать факторы, влияющие на развитие и формирование личности и ее профессиональных способностей, формировать цели и задачи личностного и профессионального роста,	ОК-6: Способность проявлять психологическую устойчивость в сложных и экстремальных условиях, применять методы эмоциональной и когнитивной регуляции для оптимизации собственной деятельности и психологического состояния	

	осознавать и осмыслять различные проявления психики человека,оценивать, анализировать, критически осмысливать ситуацию, поведение людей с точки зрения психологии		
	2. Уметь реализовывать на практике принципы политики безопасности, использовать методы количественного представления информации и основные закономерности ее преобразования в каналах при выполнении комплекса мер по информационной безопасности	ПК-3: Способность организовывать и проводить мероприятия по контролю за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, проводить анализ эффективности системы защиты информации	
	3. Уметь обосновывать организационно-технические мероприятия по защите государственной тайны, ориентироваться в нормативно-правовых актах, регламентирующих сферу защиты государственной тайны, планировать внедрение и внедрять компоненты систем предприятия, обеспечивающих безопасность государственной тайны	ПК-30: Способность планировать проведение работ по комплексной защите информации и сведений, составляющих государственную тайну, на объекте информатизации	
Владения (навыки / опыт деятельности)	1. Владеть элементами саморефлексии в жизни и профессиональной деятельности, категориальным и методологическим аппаратом психологического анализа ситуации, методами саморегуляции и технологиями снятия эмоционального напряжения, профессионального мышления, профессиональной наблюдательности	ОК-6: Способность проявлять психологическую устойчивость в сложных и экстремальных условиях, применять методы эмоциональной и когнитивной регуляции для оптимизации собственной деятельности и психологического состояния	
	2. Владеть навыками анализа, обработки и интерпретации результатов решения прикладных задач управления; навыками	ПК-3: Способность организовывать и проводить мероприятия по контролю за обеспечением защиты информации, в том числе	

	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	сведений, составляющих государственную тайну, проводить анализ эффективности системы защиты информации	
	3. Владеть навыками обоснования, выбора, реализации и контроля результатов управленческого решения, 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-30: Способность планировать проведение работ по комплексной защите информации и сведений, составляющих государственную тайну, на объекте информатизации	

2. Цель и место дисциплины в структуре образовательной программы

Дисциплина «Криптографические методы защиты информации» относится к дисциплинам базовой части образовательной программы.

Дисциплина изучается на 4-м курсе в 7 семестре.

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

Правовая защита информации,

Программно-аппаратная защита информации,

Эти дисциплины направлены на формирование компетенций ОК-6, ПК-3, ПК-30.

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-6: Способность проявлять психологическую устойчивость в сложных и экстремальных условиях, применять методы эмоциональной и когнитивной регуляции для оптимизации собственной деятельности и психологического состояния.

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения	
		«Не зачтено»	«Зачтено»
Первый этап (уровень)	основные психические процессы, свойства и состояния личности	Не знает	Знает основные психические процессы, свойства и состояния личности
Второй этап (уровень)	осознавать и осмыслять различные проявления психики человека	Не умеет	Умеет осознавать и осмыслять различные проявления психики человека
Третий этап (уровень)	методами саморегуляции и технологиями снятия эмоционального напряжения.	Не владеет	Владеет методами саморегуляции и технологиями снятия эмоционального напряжения

ПК-3. Способность организовывать и проводить мероприятия по контролю за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, проводить анализ эффективности системы защиты информации.

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения	
		Не зачтено	Зачтено
Первый этап (уровень)	Знать: подходы обоснования затрат на информационную безопасность; методы и модели установления зависимости между затратами на защиту информации и уровнем защищенности, нормативно-правовые документы по обеспечению информационной безопасности в нашей стране и за рубежом; стандарты построения систем информационной безопасности и стандарты оценки степени защиты систем информационной безопасности объектов; методики анализа рисков информационных систем	Фрагментарные представления о подходах к обоснованию затрат на информационную безопасность, Имеет фрагментарные знания о нормативно-правовых документах по обеспечению информационной безопасности в нашей стране и за рубежом; стандартах построения систем информационной безопасности и стандартах оценки степени защиты систем информационной безопасности объектов; методиках анализа рисков информационных систем	Сформированные представления о подходах к обоснованию затрат на информационную безопасность; методах и моделях установления зависимости между затратами на защиту информации и уровнем защищенности, свободное знание нормативно-правовые документов по обеспечению информационной безопасности в нашей стране и за рубежом; стандартов построения систем информационной безопасности и стандартов оценки степени защиты систем информационной безопасности объектов; методик анализа рисков информационных систем
Второй этап (уровень)	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, интерпретировать 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	Слабо выраженные способности к работе с данными, использованию основных методик оценки совокупной стоимости владения для подсистемы информационной безопасности; определению зависимости между затратами на ИБ и уровнем защищенности; слабые умения интерпретировать 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	Умеет оценивать эффективность управленческих решений и анализировать экономические показатели деятельности подразделения; самостоятельно находить нужную информацию; использовать основные методики оценки совокупной стоимости владения для подсистемы информационной безопасности; определять зависимость между затратами на ИБ и уровнем защищенности, способен уверенно интерпретировать 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

Третий этап (уровень)	Владеть: навыками определения затрат компании на ИБ, навыками интерпретации и обобщения результатов, формулирования рекомендаций и принятия решений, методологией и навыками решения научных и практических задач	Фрагментарные навыки определения затрат компании на ИБ, слабые навыки интерпретации и обобщения результатов, формулирования рекомендаций и принятия решений, методологией и навыками решения научных и практических задач	Успешное и систематическое применение навыков определения затрат компании на ИБ, уверенные навыки интерпретации и обобщения результатов, формулирования рекомендаций и принятия решений, методологией и навыками решения научных и практических задач

ПК-30. Способность планировать проведение работ по комплексной защите информации и сведений, составляющих государственную тайну, на объекте информатизации

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения	
		Не зачтено	Зачтено
Первый этап (уровень)	Знать: особенности защиты государственной тайны, состояние законодательной базы и стандарты в области защиты государственной тайны	Имеет фрагментарные знания об особенностях защиты государственной тайны, состояние законодательной базы и стандарты в области защиты государственной тайны	Демонстрирует целостность знаний особенностей защиты государственной тайны, состояние законодательной базы и стандарты в области защиты государственной тайны
Второй этап (уровень)	Уметь: обосновывать организационно-технические мероприятия по защите государственной тайны, ориентироваться в нормативно-правовых актах, регламентирующих сферу защиты государственной тайны, планировать внедрение и внедрять компоненты систем предприятия, обеспечивающих безопасность государственной тайны	Не умеет обосновывать организационно-технические мероприятия по защите государственной тайны, ориентироваться в нормативно-правовых актах, регламентирующих сферу защиты государственной тайны, планировать внедрение и внедрять компоненты систем предприятия, обеспечивающих безопасность государственной тайны	Умеет эффективно обосновывать организационно-технические мероприятия по защите государственной тайны, ориентироваться в нормативно-правовых актах, регламентирующих сферу защиты государственной тайны, планировать внедрение и внедрять компоненты систем предприятия, обеспечивающих безопасность государственной тайны
Третий этап (уровень)	Владеть: обоснования, выбора, реализации и контроля результатов управленческого решения, выявления и устранения угроз информационной безопасности, эксплуатации современного электронного оборудования и информационно-коммуникационных технологий, внедрения, адаптации и настройки средств защиты прикладных ИС	Не способен обосновать выбор, реализации и контроля результатов управленческого решения, выявления и устранения угроз информационной безопасности, эксплуатации современного электронного оборудования и информационно-коммуникационных технологий, внедрения, адаптации и настройки средств защиты прикладных ИС	Владеет методиками обоснования, выбора, реализации и контроля результатов управленческого решения, выявления и устранения угроз информационной безопасности, эксплуатации современного электронного оборудования и информационно-коммуникационных технологий, внедрения, адаптации и настройки средств защиты прикладных ИС

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

Шкала оценивания для зачета:

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

не зачтено – от 0 до 59 рейтинговых баллов.

4.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и опыта деятельности, характеризующих этапы формирования компетенций

Этапы освоения	Результаты обучения	Компетенция	Оценочные средства
1-й этап Знания	Знать сущность и структуру психологии	ОК-6: Способность проявлять	Тестирование, практическая работа

	группы, динамические процессы в межличностных отношениях, механизмы межгруппового взаимодействий, структуру психологии группы, динамические процессы в межличностных отношениях, механизмы межгруппового взаимодействий, основные психические процессы, свойства и состояния личности, факторы, негативно влияющие на психическое здоровье сотрудников, признаки стрессового напряжения и «эмоционального выгорания»	психологическую устойчивость в сложных и экстремальных условиях, применять методы эмоциональной и когнитивной регуляции для оптимизации собственной деятельности и психологического состояния	
	Знать политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации, понятие системы управления, основные виды структур, принципы системного подхода к анализу структур	ПК-3: Способность организовывать и проводить мероприятия по контролю за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, проводить анализ эффективности системы защиты информации	Тестирование, практическая работа
	Знать особенности защиты государственной тайны, состояние законодательной базы и стандарты в области защиты государственной тайны	ПК-30: Способность планировать проведение работ по комплексной защите информации и сведений, составляющих государственную тайну, на объекте информатизации	Тестирование, практическая работа
2-й этап Умения	Уметь анализировать факторы, влияющие на развитие и формирование личности и ее профессиональных способностей, формировать цели и задачи личностного и профессионального роста, осознавать и осмыслять различные проявления психики человека,	ОК-6: Способность проявлять психологическую устойчивость в сложных и экстремальных условиях, применять методы эмоциональной и когнитивной регуляции для оптимизации собственной деятельности и психологического состояния	Тестирование, практическая работа

	оценивать, анализировать, критически осмысливать ситуацию, поведение людей с точки зрения психологии		
	Уметь реализовывать на практике принципы политики безопасности, использовать методы количественного представления информации и основные закономерности ее преобразования в каналах при выполнении комплекса мер по информационной безопасности	ПК-3: Способность организовывать и проводить мероприятия по контролю за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, проводить анализ эффективности системы защиты информации	Тестирование, практическая работа
	Уметь обосновывать организационно-технические мероприятия по защите государственной тайны, ориентироваться в нормативно-правовых актах, регламентирующих сферу защиты государственной тайны, планировать внедрение и внедрять компоненты систем предприятия, обеспечивающих безопасность государственной тайны	ПК-30: Способность планировать проведение работ по комплексной защите информации и сведений, составляющих государственную тайну, на объекте информатизации	Тестирование, практическая работа
3-й этап Владения навыками	Владеть элементами саморефлексии в жизни и профессиональной деятельности, категориальным и методологическим аппаратом психологического анализа ситуации, методами саморегуляции и технологиями снятия эмоционального напряжения, профессионального мышления, профессиональной наблюдательности	ОК-6: Способность проявлять психологическую устойчивость в сложных и экстремальных условиях, применять методы эмоциональной и когнитивной регуляции для оптимизации собственной деятельности и психологического состояния	Тестирование, практическая 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	ПК-3: Способность организовывать и проводить мероприятия по контролю за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, проводить анализ эффективности системы защиты информации	Тестирование, практическая работа
	Владеть навыками обоснования, выбора, реализации и контроля результатов управленческого решения, 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-30: Способность планировать проведение работ по комплексной защите информации и сведений, составляющих государственную тайну, на объекте информатизации	Тестирование, практическая работа

Типовые вопросы для зачета:

1. Виды криптосистем.
2. Задачи, решаемые методами криптографии.
3. Виды информации, подлежащие закрытию, их модели и свойства.
4. Частотные характеристики открытых сообщений.
5. Критерии на открытый текст.
6. Особенности нетекстовых сообщений.
7. Классификация шифров.
8. Классификация шифров по области применения.
9. Кодирование.
10. Классификация шифров по особенностям алгоритма шифрования.
11. Классификация шифров по количеству символов сообщения.
12. Этапы криптографии.
13. Шифры наивной криптографии.

14. Шифр Цезаря.
15. Полибианский квадрат.
16. Шифр «Решетка».
17. Шифр Виженера.
18. Шифр Плейфера.
19. Шифр Хилла.
20. Шифр Вернама.
21. Шифр Хагелина.
22. Машина шифрования Enigma.
23. Блочные и поточные шифры.
24. Лавинный эффект.
25. Поточные шифры.
26. Избыточность информации.
27. Ненадежность шифра и расстояние единственности.
28. Модель криптоаналитика.
29. Классификация блочных шифров.
30. Режим шифрования.
31. Режим простой замены ECB.
32. Режим шифрования с зацеплением CBC.
33. Режим обратной связи по шифротексту CFB.
34. Режим шифрования с обратной связью по выходу OFB (гаммирование или внутренняя обратная связь).
35. Сцепление блоков шифротекста с распространением ошибки (PCBC).
36. Counter mode (CTR) режим счетчика.
37. Режим счётчик с аутентификацией Галуа (Galois/Counter Mode GCM).
38. Аутентифицированное шифрование с присоединёнными данными (AEAD-режим блочного шифрования).
39. Ячейка Фестеля.
40. Сеть Фейстеля.
41. Алгоритм Blowfish.
42. Шифр DES.
43. ГОСТ 28147–89 Системы обработки информации.
44. Защита криптографическая.
45. Алгоритм криптографического преобразования.
46. Шифр AES.
47. Процедура расширения ключа.
48. Шифр IDEA.
49. Многократное шифрование блоков.
50. Атаки на блочные шифры.
51. Режимы использования блочных шифров.
52. Классификация поточных шифров.
53. Синхронные поточные шифры.
54. Самосинхронизирующиеся (асинхронные поточные шифры АПШ) поточные шифры.
55. Генерация случайных и псевдослучайных последовательностей.
56. Криптографически безопасные псевдослучайные последовательности.
57. Настоящие случайные последовательности.
58. Детерминированные генераторы простых случайных чисел.
59. Анализ генераторов псевдослучайных чисел.
60. Регистр сдвига с линейной обратной связью (РСЛОС, англ.
61. Linearfeedbackshiftregister, LFSR).
62. Линейная сложность.

63. Нелинейные регистры сдвига с обратной связью.
64. Нелинейная комбинация генераторов.
65. Линейное и предварительное шифрование.
66. Шифр A5.
67. Гаммирование.
68. Шифр RC 4.
69. Атаки на поточные шифры.
70. Характеристики имитостойкости.
71. Методы обеспечения имитостойкости шифров.
72. Совершенная имитостойкость.
73. Связь между имитостойкостью по Симмонсу и секретностью по Шеннону.
74. Понятие кода аутентификации и его свойства имитостойкости и секретности.
75. Назначение и конструкция кодов аутентификации и защитных контрольных сумм.
76. Требования к хэш-функциям.
77. Криптографическая стойкость хэш-функций.
78. Коллизии.
79. Применение хэш-функций.
80. Подходы к проектированию хэш-функций.
81. Алгоритмы выработки хэш-функций.
82. Хэш-функции на основе блочного шифра.
83. Ключевые хэш-функции.
84. Стандарт на хэш-функции: ГОСТ Р 34.11-94
85. Алгоритм SHA.
86. Криптография открытого ключа.
87. Понятие односторонней функции и односторонней функции с "лазейкой".
88. Проблемы факторизации целых чисел и логарифмирования в конечных полях.
89. Криптосистема Диффи-Хэллмана.
90. Криптосистемы RSA, Эль-Гамаля, Рабина, Гольдвассер-Микали, Блюма-Гольдвассер.
91. Рюкзачные шифры.
92. Классификация криптографических протоколов.
93. Классификация криптографических протоколов по характеру разрешения спорных вопросов.
94. Классификация криптографических протоколов по типу используемых криптографических примитивов.
95. Классификация криптографических протоколов по числу участников.
96. Классификация криптографических протоколов по числу передаваемых сообщений.
97. Классификация криптографических протоколов по функциональному (целевому) назначению.
98. Классификация криптографических протоколов по сложности.
99. Классификация криптографических протоколов по области применения.
100. Криптографические примитивы.
101. Криптографические примитивы с секретном ключом.
102. Криптографические примитивы с открытым ключом.
103. Управление криптографическими ключами.
104. Генерация ключей.
105. Накопление ключей.
106. Цели управления ключами.
107. Политика безопасности управления ключами.

108. Сроки действия ключей.
109. Жизненный цикл ключей.
110. Управление ключами, основанное на системах с открытым ключом.
111. Протокол обмена секретным ключом.
112. Использование сертификатов.
113. Протокол распределения ключей.
114. Временные данные.
115. Разновидности временных данных Симметричные протоколы.
116. Однопроходовый key transport.
117. Challenge Response.
118. Authenticated Key Exchange Protocol.
119. Протокол Шамира.
120. Протоколы, использующие центр сертификации (доверенный центр) или сервер.
121. Лягушка с открытым ртом.
122. Протокол Нидхема-Шрёдера на симметричных ключах.
123. Протокол Kerberos.
124. The Kerberos Ticket.
125. Протокол Отвея-Рииса.
126. Алгоритм DASS.
127. Асимметричные протоколы.
128. Протокол Нидхема-Шрёдера на ассиметричных ключах.
129. Электронная подпись.
130. Алгоритм X.509.
131. Хэш функция.
132. Однонаправленные хэш-функции.
133. Алгоритм MD4.
134. Алгоритм MD5.
135. Алгоритм MD2.
136. Алгоритм безопасного хэширования (Secure Hash Algorithm, SHA).
137. Алгоритм RIPE-MD.
138. Алгоритм HAVAL.
139. Однонаправленные хэш-функции, использующие симметричные блочные алгоритмы.
140. Стандарт хэш–функций ГОСТ Р 34.11-2012.

Критериями оценивания являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения модулей (разделов дисциплины), перечисленных в рейтинг-плане дисциплины (для зачета: текущий контроль – максимум 50 баллов; рубежный контроль – максимум 50 баллов, поощрительные баллы – максимум 10).

Шкалы оценивания:

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

не зачтено – от 0 до 59 рейтинговых баллов).

Тестирование

Задание №1 (***Образец***)

Какую задачу не решает криптография:

а) обеспечения нарушения целостности информации;

б) Обеспечения конфиденциальности;

в) Обеспечения целостности данных;

г) Обеспечения аутентификации;

д) Невозможности отказа от авторства.

Задание №2

Криптосистема это:

а) Система расшифровки зашифрованной информации без предназначенного для такой расшифровки ключа и сам процесс такой расшифровки;

б) Завершенная комплексная модель, способная производить двусторонние криптопреобразования над данными произвольного объёма и подтверждать время отправки сообщения, обладающая механизмом преобразования паролей и ключей и системой транспортного кодирования;

в) Метод записи чисел, представление чисел с помощью письменных знаков;

г) Система измерения, сбора, анализа, представления и интерпретации информации о посетителях веб-сайтов с целью их улучшения и оптимизации;

Задание №3

Согласно правилу Керкхоффа, надежность традиционного шифрования определяет:

а) Простота алгоритма шифрования;

б) Секретность алгоритма шифрования;

в) Секретность ключа;

г) Сложность вычисления односторонней функции.

Задание №4

Шифр Цезаря является:

а) Поточным подстановочным(замена) шифром;

б) Детерминированный аддитивным шифром;

в) Блочным шифром с гаммированием;

г) Нестойким блочным шифром.

Задание № 5

Шифр Хилла это:

а) Полиграммный шифр подстановки, основанный на линейной алгебре с использованием матриц;

б) Аддитивный шифр, основанный на сложности нахождения логарифма в поле;

в) Симметричный шифр, основанный на сложности разложения заданного числа на простые сомножители;

г) Полиграммный шифр простой перестановки, основанный на использовании эллиптических кривых.

Критерии оценки тестовых заданий

Структура работы	Критерии оценки	Распределение баллов
Один вопрос теста Весь тест (25 вопросов в варианте)	Неправильный ответ / Правильный ответ	0/1,2 0/30

Темы практических работ

Цель проведения лабораторных работы – практическое освоение материала дисциплины.

1) Алгоритмы наивной криптографии.
2) Алгоритмы блочных шифров.
3) Алгоритмы поточных шифров.
4) Хэш–функции.
5) Криптосистемы открытого ключа.
6) Управление криптографическими ключами.
7) Протоколы распределения ключей
8) Электронная подпись.

Типовая практическая работа

Модуль 1. Симметричные шифры.

Тема: Классификация шифров. Полибианский квадрат.

Цель: Практические навыки при шифровании и расшифровывании алгоритмами наивной криптографии.

Задание: Расшифруйте слово 34124142364326462463 с использованием модифицированного квадрата Полибия.

	1	2	3	4	5	6
1	А	Б	В	Г	Д	Е
2	Ё	Ж	З	И	Й	К
3	Л	М	Н	О	П	Р
4	С	Т	У	Ф	Х	Ц
5	Ч	Ш	Щ	Ъ	Ы	Ь
6	Э	Ю	Я	-	-	-

Критерии оценки практической работы

Структура работы	Критерии оценки	Распределение баллов
Одно практическое 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	0/3/5

4.3 Рейтинг-план дисциплины

Рейтинг-план дисциплины представлен в приложении 2.

5. Учебно-методическое и информационное обеспечение дисциплины

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

Основная литература

1. Фороузан, Б.А. Математика криптографии и теория шифрования / Б.А. Фороузан. - 2-е изд., испр. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 511 с. : ил., схем. - (Основы информационных технологий). - Библиогр. в кн. - ISBN 978-5-9963-0242-0 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=428998 (20.04.2019).

2. Кнауб, Л.В. Теоретико-численные методы в криптографии : учебное пособие / Л.В. Кнауб, Е.А. Новиков, Ю.А. Шитов ; Министерство образования и науки Российской Федерации, Сибирский Федеральный университет. - Красноярск : Сибирский федеральный

университет, 2011. - 160 с. - ISBN 978-5-7638-2113-7 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=229582 (20.04.2019).

Дополнительная литература

3. Петренко, В.И. Теоретические основы защиты информации : учебное пособие / В.И. Петренко ; Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет». - Ставрополь : СКФУ, 2015. - 222 с. : ил. - Библиогр.: с. 214-215 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=458204 (20.04.2019).
4. Аверченков, В.И. Аудит информационной безопасности : учебное пособие для вузов / В.И. Аверченков. - 3-е изд., стер. - Москва : Издательство «Флинта», 2016. - 269 с. - Библиогр. в кн. - ISBN 978-5-9765-1256-6 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=93245 (20.04.2019).

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

1. Электронная библиотечная система «Университетская библиотека онлайн» – https://biblioclub.ru.
2. Электронная библиотечная система издательства «Лань» – https://e.lanbook.com/
3. Электронный каталог Библиотеки БашГУ – http://www.bashlib.ru/catalogi/
4. Сайт ФСТЭК России – www.fstec.ru
5. Сайт ФСБ России – www.fsb.ru
6. Портал по вопросам информационной безопасности – www.itsec.ru
7. Наиболее обширная электронная база учебников и методических материалов на сайте информационной системы «Единое окно доступа к образовательным ресурсам» – http://window.edu.ru/;
8. Новая электронная библиотека – www.newlibrary.ru;
9. Федеральный портал российского образования – www. edu.ru;
10. Научная электронная библиотека – www.elibrary.ru;
11. Правовая система «КонсультантПлюс» – http://www.consultant.ru/.
12. 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.
13. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные.
14. Система централизованного тестирования БашГУ (Moodle). GNU General Public License.

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

Наименование специализированных аудиторий, кабинетов, лабораторий	Вид занятий	Наименование оборудования, программного обеспечения
1	2	3
1. *учебная аудитория для проведения занятий лекционного типа:* аудитория № 403 (гуманитарный корпус),	Лекции, практические занятия, групповые и индивидуальные	**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**

аудитория № 405 (гуманитарный корпус), аудитория № 413 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 515 (гуманитарный корпус), аудитория № 516 (гуманитарный корпус). **2. *учебная аудитория для проведения занятий семинарского типа:*** аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус). **3. *учебная аудитория для проведения групповых и индивидуальных консультаций:*** аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус), компьютерный класс аудитория № 404	консультации, текущий контроль, промежуточная аттестация	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. **Аудитория № 419** Учебная мебель, Проектор Optoma Ex542 i – 1 шт., Экран настенный Dinon – 1 шт. **Аудитория № 515** Учебная мебель, доска, терминал видео конференц-связи LifeSize Icon 600-камера, интер-ая система со встроенным короткофокусным проектором Promethean ActivBoard 387 RPO MOUNT EST, профес-сиональный LCD дисплей Flame 42ST, настольный интерактивный дисплей SMART Podium SP518 с ПО SMART Notebook, матричный коммутатор сигналов интерфейса HDMI CMPRO 4H4H, интер-ая напольная кафедра докладчика, ком-ер встраиваемый в кафедру IN-TEL Core i3-4150/DDr3 4 Gb/HDD 1TB/DVD-RW/ Therm altake VL520B1N2E 220W/Win8Pro64, стол, трибуна, кресла секционные последующих рядов с пюпитром. **Аудитория № 516** Учебная мебель, доска, кресла секционные последующих рядов с пюпитром, мобильное мультимедийное оборудование: проектор ASK Proxima, ноутбук HP, экран. **Аудитория № 509** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 608** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 609** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 610** Учебная мебель, доска, учебно-наглядные пособия, LED Телевизор TCLL55P6 USBLACK – 1 шт., кронштейн для

(гуманитарный корпус), компьютерный класс 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:***аудитория № 613 (гуманитарный корпус), читальный зал библиотеки аудитория 402 (гуманитарный корпус).		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

Приложение 1

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

Содержание рабочей программы
дисциплины **Криптографические методы защиты информации**
на 7 семестр ОФО

Вид работы	**Объем дисциплины**
Общая трудоемкость дисциплины (ЗЕТ / часов)	4 ЗЕТ / 144 часа
Учебных часов на контактную работу с преподавателем:	72,2
лекций	36
практических / семинарских	36
лабораторных	
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	0,2
Учебных часов на самостоятельную работу обучающихся (СР)	71,8
Учебных часов на подготовку к экзамену/зачету/дифференцированному зачету (Контроль)	

Форма(ы) контроля:
зачет 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	4	5	6	7	8	9	10
1	Симметричные шифры Тема: Виды криптосистем. Задачи, решаемые методами криптографии. Виды информации, подлежащие закрытию, их модели и свойства. Частотные характеристики открытых сообщений. Критерии на открытый текст. Особенности нетекстовых сообщений. Тема: Классификация шифров. Классификация шифров по области применения. Кодирование. Классификация шифров по особенностям алгоритма шифрования. Классификация шифров по количеству символов сообщения. Этапы криптографии. Шифры наивной криптографии. Шифр Цезаря. Полибианский квадрат. Шифр «Решетка». Шифр Виженера. Шифр Плейфера. Шифр Хилла. Шифр Вернама. Шифр Хагелина. Машина шифрования Enigma. Блочные и поточные шифры. Лавинный эффект. Поточные шифры. Тема: Избыточность информации. Ненадежность шифра и расстояние единственности. Модель криптоаналитика. Тема: Классификация блочных шифров. Режим шифрования. Режим простой замены ECB. Режим шифрования с зацеплением CBC. Режим обратной связи по шифротексту CFB. Режим шифрования с обратной связью по выходу OFB (гаммирование или внутренняя обратная связь). Сцепление блоков шифротекста с распространением ошибки (PCBC). Counter mode (CTR) режим счетчика. Режим счётчик с аутентификацией Галуа (Galois/Counter Mode GCM). Аутентифицированное шифрование с присоединёнными данными (AEAD-режим блочного шифрования). Тема: Ячейка Фестеля. Сеть Фейстеля. Алгоритм Blowfish. Тема: Шифр DES. ГОСТ 28147–89 Системы обработки информации.	2 2 2 2 2 2	4 6		3,9 4 4 4 4 4	1, 2, 3, 4	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Практическая работа, тестирование

	Защита криптографическая. Алгоритм криптографического преобразования. Шифр AES. Процедура расширения ключа. Шифр IDEA. Многократное шифрование блоков. Атаки на блочные шифры. Режимы использования блочных шифров. Тема: Классификация поточных шифров. Синхронные поточные шифры. Самосинхронизирующиеся (асинхронные поточные шифры АПШ) поточные шифры. Генерация случайных и псевдослучайных последовательностей. Криптографически безопасные псевдослучайные последовательности. Настоящие случайные последовательности. Детерминированные генераторы простых случайных чисел. Анализ генераторов псевдослучайных чисел. Регистр сдвига с линейной обратной связью (РСЛОС, англ. Linearfeedbackshiftregister, LFSR). Линейная сложность. Нелинейные регистры сдвига с обратной связью. Нелинейная комбинация генераторов. Линейное и предварительное шифрование. Шифр A5. Гаммирование. Шифр RC 4. Атаки на поточные шифры. Тема: Характеристики имитостойкости. Методы обеспечения имитостойкости шифров. Совершенная имитостойкость. Связь между имитостойкостью по Симмонсу и секретностью по Шеннону. Понятие кода аутентификации и его свойства имитостойкости и секретности. Назначение и конструкция кодов аутентификации и защитных контрольных сумм. Тема: Требования к хэш-функциям. Криптографическая стойкость хэш-функций. Коллизии. Применение хэш-функций. Подходы к проектированию хэш-функций. Алгоритмы выработки хэш-функций. Хэш-функции на основе блочного шифра. Ключевые хэш-функции. Стандарты на хэш-функции: ГОСТ Р 34.11-94, SHA.	2 2 2	4 4		4 4 4			
2	Асимметричные шифры Тема: Криптография открытого ключа. Понятие односторонней функции и односторонней функции с "лазейкой". Проблемы факторизации целых чисел и логарифмирования в конечных полях. Тема: Криптосистема Диффи-Хэллмана. Криптосистемы RSA, Эль-Гамаля, Рабина, Гольдвассер-Микали, Блюма-Гольдвассер. Рюкзачные шифры. Тема: Классификация криптографических протоколов. Классификация криптографических протоколов по характеру разрешения спорных вопросов. Классификация криптографических протоколов по типу используемых криптографических примитивов. Классификация криптографических протоколов по числу участников. Классификация криптографических протоколов по числу передаваемых сообщений. Классификация криптографических протоколов по функциональному (целевому) назначению. Классификация криптографических протоколов по сложности. Классификация криптографических протоколов по	2 2 2	4		3,9 4 4	1, 2, 3, 4	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Практическая работа, тестирование

	области применения. Криптографические примитивы. Криптографические примитивы с секретном ключом. Криптографические примитивы с открытым ключом. Тема: Управление криптографическими ключами. Генерация ключей. Накопление ключей. Цели управления ключами. Политика безопасности управления ключами. Сроки действия ключей. Жизненный цикл ключей. Тема: Управление ключами, основанное на системах с открытым ключом. Протокол обмена секретным ключом. Использование сертификатов. Тема: Протокол распределения ключей. Временные данные. Разновидности временных данных Симметричные протоколы. Однопроходовый key transport. Challenge Response. Authenticated Key Exchange Protocol. Протокол Шамира. Протоколы, использующие центр сертификации (доверенный центр) или сервер. Лягушка с открытым ртом. Протокол Нидхема-Шрёдера на симметричных ключах. Протокол Kerberos. The Kerberos Ticket. Протокол Отвея-Рииса. Алгоритм DASS. Тема: Асимметричные протоколы. Протокол Нидхема-Шрёдера на ассиметричных ключах. Тема: Электронная подпись. X.509. Хэш функция. однонаправленные хэш-функции. MD4. MD5. MD2. Алгоритм безопасного хэширования (Secure Hash Algorithm, SHA). RIPE-MD. HAVAL. Тема: Однонаправленные хэш-функции, использующие симметричные блочные алгоритмы. ГОСТ Р 34.11-2012.	2 2 2 2 2 2	4 4 6 		4 4 4 4 4 4			
	Всего часов:	36	36		71,8			

Приложение 2

Рейтинг-план дисциплины
Криптографические методы защиты информации

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

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1. Симметричные шифры				
Текущий контроль				
1. Практическая работа	5	4	0	20
Рубежный контроль				
1. Тест	30	1	0	30
Всего		3	0	50
Модуль 2. Асимметричные шифры				
Текущий контроль				
1. Практическая работа	5	4	0	20
Рубежный контроль				
1. Тест	30	1	0	30
Всего		4	0	50
Поощрительные баллы				
1. Участие в студенческой олимпиаде по дисциплине	3	1	0	3
2.Публикация научной статьи	4	1	0	4
3.Участие в научно-практической конференции по профилю	3	1	0	3
Всего		3	0	10
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
1. Посещение лекционных занятий			0	-6
2. Посещение практических (семинарских, лабораторных занятий)			0	-10

Итоговый контроль				
1.Зачет				