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

Утверждено:
на заседании кафедры
протокол №9 от 24.04.2020
Зав. кафедрой / А.С. Исмагилова

Согласовано:
Председатель УМК института
/Р.А. Гильмутдинова

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Криптографические методы защиты информации

Б1.В.16 (базовая)

программа бакалавриата

Направление подготовки
10.03.01 Информационная безопасность

Профиль подготовки
Организация и технология защиты информации

Квалификация
бакалавр

Разработчик (составитель) / А.Б. Пушкарёв

Для приема: 2020 г.

Уфа 2020 г.

Составитель: А.Б. Пушкарёв

Рабочая программа дисциплины утверждена на заседании кафедры управления информационной безопасностью
протокол № 9 от 24.04.2020

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

Заведующий кафедрой

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

Заведующий кафедрой

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

Заведующий кафедрой

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

Заведующий кафедрой

Список документов и материалов

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 основные понятия и методы математического анализа, теории вероятностей и математической статистики, математической логики и теории алгоритмов, теории информации и кодирования, математические методы обработки экспериментальных данных	ОПК-2: Способность применять соответствующий математический аппарат для решения профессиональных задач	
	2. 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	
	3. 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	ПК-4: Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	

	защиты информации, состояние законодательной базы и стандарты в области информационной безопасности		
Умения	1. Уметь использовать математические методы и модели для решения прикладных задач	ОПК-2: Способность применять соответствующий математический аппарат для решения профессиональных задач	
	2. 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	
	3. Уметь реализовывать на практике принципы политики безопасности, использовать закономерности преобразования данных в каналах при выполнении комплекса мер по информационной безопасности, обосновывать организационно-технические мероприятия по защите информации, использовать возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации	ПК-4: Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	
Владения (навыки / опыт деятельности)	1. Владеть основными методами исследования функций и навыками формулирования и решения простейших задач об	ОПК-2: Способность применять соответствующий математический аппарат для решения профессиональных задач	

	отыскании экстремума функции, навыками анализа алгебраических и геометрических объектов		
	2. 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	
	3. Владеть навыками анализа, обработки и интерпретации результатов решения прикладных задач управления, навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью, навыками организации комплекса мероприятий по защите информации в процессах автоматизированной обработки информации, навыками выявления и устранения угроз информационной безопасности, навыками эксплуатации современного электронного оборудования и информационно-коммуникационных технологий, навыками внедрения, адаптации и настройки средств защиты прикладных ИС	ПК-4: Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	

2. Цель и место дисциплины в структуре образовательной программы

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

Дисциплина изучается на 3-ем курсе в 6 семестре.

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

Математика,

Математический анализ,

Теория вероятностей и математическая статистика,

Дискретная математика,

Аппаратные средства вычислительной техники,

Программно-аппаратные средства защиты информации.

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

Содержание рабочей программы представлено в Приложении 1.

4. Фонд оценочных средств по дисциплине

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

ОПК-2: Способность применять соответствующий математический аппарат для решения профессиональных задач.

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения			
		2 («Неудовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
Первый этап (уровень)	Знать основные понятия и методы математического анализа, теории вероятностей и математической статистики, математической логики и теории алгоритмов	Не знает	Имеет фрагментарные знания оосновных понятиях и методах математического анализа, теории вероятностей и математической статистики, математической логики и теории алгоритмов	В целом знает основные понятия и методы математического анализа, теории вероятностей и математической статистики, математической логики и теории алгоритмов	Демонстрирует целостные знания оосновных понятиях и методах математического анализа, теории вероятностей и математической статистики, математической логики и теории алгоритмов
	Знать методы теории информации и кодирования	Не знает	Имеет фрагментарные знания о методах теории информации и кодирования	В целом знает методы теории информации и кодирования	Демонстрирует целостные знания о методах теории информации и кодирования

	Знать математические методы обработки экспериментальных данных	Не знает	Имеет фрагментарные знания о математических методах обработки экспериментальных данных	В целом знает математические методы обработки экспериментальных данных	Демонстрирует целостные знания о математических методах обработки экспериментальных данных
Второй этап (уровень)	Уметь использовать математические методы и модели для решения прикладных задач	Не умеет	Умеет использовать математические методы и модели для решения прикладных задач, но допускает значительные ошибки	Умеет использовать математические методы и модели для решения прикладных задач, но допускает незначительные ошибки	Умеет использовать математические методы и модели для решения прикладных задач
Третий этап (уровень)	Владеть основными методами исследования функций и навыками формулирования и решения простейших задач об отыскании экстремума функции	Не владеет	Недостаточно владеет основными методами исследования функций и навыками формулирования и решения простейших задач об отыскании экстремума функции	Владеет отдельными элементами основных методов исследования функций и навыков формулирования и решения простейших задач об отыскании экстремума функции	Способен использовать основные методы исследования функций и навыки формулирования и решения простейших задач об отыскании экстремума функции
	Владеть навыками анализа алгебраических и геометрических объектов	Не владеет	Недостаточно владеет навыками анализа алгебраических и геометрических объектов	Владеет отдельными элементамианализа алгебраических и геометрических объектов	Способен использовать навыки анализа алгебраических и геометрических объектов

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 оаппаратных средствах вычислительной техники; операционных системах персональных ЭВМ; основах администрирования вычислительных сетей; системах управления БД	Знает основы аппаратных средств вычислительной техники; операционных систем персональных ЭВМ; администрировани я вычислительных сетей; систем управления БД	Знает аппаратные средства вычислительной техники; операционные системы персональных ЭВМ; основы 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 оэксплуатационных и технико-экономических характеристиках программных и технических средств защиты информации и обеспечения информационной безопасности	Знает основные понятия эксплуатационных и технико-экономических характеристиках 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 отипах 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 оосновных направлениях политик защиты информации на предприятии (организации)	Знает некоторые элементы основных направлений 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 формулировке и настройке политик безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе	Допускает незначительные ошибки при формулировке и настройке политик безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе	Имеет навыки формулировки 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, конфигурировани ю 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-4: Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты.

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 ообщеметодологических 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 овозможностях 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 осостоянии законодательной базы и стандартов в области информационной безопасности	Знает основные элементы состояния 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 закономерностей преобразования данных в каналах при выполнении комплекса мер по информационной	Допускает незначительные ошибки при использовании закономерностей преобразования данных в каналах при выполнении комплекса мер по	Умеет использовать закономерности преобразования данных в каналах при выполнении комплекса мер по информационной безопасности

			безопасности	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, аппаратных и программных средств безопасности и защиты информации	Не умеет	Допускает значительные ошибки при использовании возможностей и особенностей организационных, аппаратных и программных средств безопасности и защиты информации	Допускает незначительные ошибки при использовании возможностей и особенностей организационных, аппаратных и программных средств безопасности и защиты информации	Имеет навыки работы по использования возможностей и особенностей организационных, аппаратных и программных средств безопасности и защиты информации
Третий этап (уровень)	Владеть навыками анализа, обработки и интерпретации результатов решения прикладных задач управления	Не владеет	Недостаточно владеет навыками анализа, обработки и интерпретации результатов решения прикладных задач управления	Владеет отдельными навыками анализа, обработки и интерпретации результатов решения прикладных задач управления	Владеет навыками анализа, обработки и интерпретации результатов решения прикладных задач управления
	Владеть навыками 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

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

Шкалы оценивания для экзамена:

от 45 до 59 баллов – «удовлетворительно»;

от 60 до 79 баллов – «хорошо»;

от 80 баллов – «отлично».

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

Этапы освоения	Результаты обучения	Компетенция	Оценочные средства
1-й этап Знания	Знать основные понятия и методы математического анализа, теории вероятностей и математической статистики, математической логики и теории алгоритмов, теории информации и кодирования, математические методы обработки экспериментальных данных	ОПК-2: Способность применять соответствующий математический аппарат для решения профессиональных задач	Контрольная работа, тестирование, практическая работа, тестирование
	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	Контрольная работа, тестирование, практическая работа, тестирование
	Знать политики, стратегии и технологии информационной безопасности и защиты	ПК-4: Способность участвовать в работах по реализации политики информационной	Контрольная работа, тестирование, практическая работа, тестирование

	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	безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	
2-й этап Умения	Уметь использовать математические методы и модели для решения прикладных задач	ОПК-2: Способность применять соответствующий математический аппарат для решения профессиональных задач	Контрольная работа, тестирование, практическая работа, тестирование
	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	Контрольная работа, тестирование, практическая работа, тестирование

	Уметь реализовывать на практике принципы политики безопасности, использовать закономерности преобразования данных в каналах при выполнении комплекса мер по информационной безопасности, обосновывать организационно-технические мероприятия по защите информации, использовать возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации	ПК-4: Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Контрольная работа, тестирование, практическая работа, тестирование
3-й этап Владения навыками	Владеть основными методами исследования функций и навыками формулирования и решения простейших задач об отыскании экстремума функции, навыками анализа алгебраических и геометрических объектов	ОПК-2: Способность применять соответствующий математический аппарат для решения профессиональных задач	Контрольная работа, тестирование, практическая работа, тестирование
	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	Контрольная работа, тестирование, практическая работа, тестирование

	Владеть навыками анализа, обработки и интерпретации результатов решения прикладных задач управления, навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью, навыками организации комплекса мероприятий по защите информации в процессах автоматизированной обработки информации, навыками выявления и устранения угроз информационной безопасности, навыками эксплуатации современного электронного оборудования и информационно-коммуникационных технологий, навыками внедрения, адаптации и настройки средств защиты прикладных ИС	ПК-4: Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Контрольная работа, тестирование, практическая работа, тестирование

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.

Типовые материалы к экзамену

1. Криптографическая защита информации на основе применения асимметричных алгоритмов шифрования.
2. Односторонняя функция с потайным входом (англ. trapdoorfunction).
3. Протокол Диффи-Хелмана.
4. Протокол ГОСТ Р 34.10-2001.
5. Протокол Эль-Гамаля.
6. Протокол Фиата-Шамира.

7. Алгоритм Фейге-Фиата-Шамира.
8. Алгоритм RSA.
9. Алгоритм Меркла-Хеллмана для электронных подписей.
10. Электронно-цифровая подпись и протоколы.
11. Ключевая информация ЭЦП.

Структура экзаменационного билета.

Экзаменационный билет включает в себя два теоретических вопроса и одну задачу.

Примерные вопросы для экзамена:

1. Теоретический вопрос.

2.Теоретический вопрос.

Образец экзаменационного билета

Федеральное государственное бюджетное образовательное учреждение высшего образования

«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Институт истории и государственного управления

Направление 10.03.01«Информационная безопасность»

Дисциплина Криптографические методы защиты информации

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 2

1. Ключевая информация ЭЦП.
2. Односторонняя функция с потайным входом (англ. trapdoorfunction).

Зав. кафедрой
управления информационной безопасностью А.С.Исмагилова

Кафедра управления информационной безопасностью

Критерии оценивания результатов экзамена для ОФО:

Критерии и методика оценивания (в баллах):

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

- 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. 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***)

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 и методика оценивания:
Один тестовый вопрос (25 вопросов).
- 0,4 балл выставляется студенту, если ответ правильный;
- 0 баллов выставляется студенту, если ответ неправильный.

Лабораторное задание
Проектирование и оптимизация логических элементов

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 и методика оценивания:
- 1 балл выставляется студенту, если работа выполнена с ошибками;
- 3 балла выставляется студенту, если работа выполнена, но без оптимизации схемы;
– 5 баллов выставляется студенту, если работа выполнена с оптимизацией схемы.

Защита лабораторной работы

Проводится в форме устного опроса после выполнения работы.

Критерии и методика оценивания:
- 0 баллов выставляется студенту, если он не владеет содержанием работы;
- 1 балл выставляется студенту, если он частично владеет содержанием работы;
- 3 балла выставляется студенту, если он владеет содержанием работы, но не может объяснить полученные результаты;
– 5 баллов выставляется студенту, если он владеет содержанием работы, может объяснить полученные результаты.

Творческое задание (презентация, доклад)

Выполняется по результатам изучения темы дисциплины с целью дополнения практического материала.

Примеры тем творческих заданий
Кодирование и шифрование. Общие принципы и различия
«Наивная» криптография. Неизвестные страницы.
Проблемы выбора инициализирующего вектора.
Электронная подпись сегодня.

Критерии и методика оценивания:

Подготовленная и оформленная в соответствии с требованиями работа (презентация, доклад) оценивается преподавателем по следующим критериям:

- уровень эрудированности автора по изученной теме (знание автором состояния изучаемой проблематики, цитирование источников, в т.ч. НПА);
- логичность подачи материала, грамотность автора;
- соответствие работы всем стандартным требованиям к оформлению;
- знания и умения на уровне требований стандарта данной дисциплины: знание фактического материала, усвоение общих понятий и идей.
- 0 баллов выставляется студенту, если работа не соответствует критериям;
- 1 балл выставляется студенту, если работа частично соответствует критериям;
- 2 балла выставляется студенту, если работа соответствует критериям, но отсутствует логичность изложения информации;

– 3 балла выставляется студенту, если работа полностью соответствует критериям.

Контрольная работа

Вопросы контрольной работы:

1. Основные режимы, организующие обратную связь по шифротексту.
2. Назовите отличия симметричного и асимметричного шифрования.
3. Жизненный цикл ключа.
4. Абсолютно надежный шифр.
5. Мера избыточности информации.

Критерии и методика оценивания:

- 5 баллов выставляется студенту, если работа выполнена в полном объеме и изложена грамотным языком в определенной логической последовательности с точным использованием специализированной терминологии; показано уверенное владение нормативной базой;
- 3 балла выставляется студенту, если работа выполнена в полном объеме,

но имеет один из недостатков:

в работе допущены один-два недочета при освещении основного содержания ответа;

нет определенной логической последовательности, неточно используется специализированная терминология;

- 1 балл выставляется студенту, если работа выполнена неполно, не показано общее понимание вопроса, имелись затруднения или допущены ошибки в определении понятий, использовании терминологии, при знании теоретического материала выявлена недостаточная сформированность основных умений и навыков.

Задача

Использование шифра цезаря
http://log-lessons.ru/index.php/2010/11/zadacha-centr-tyazhesti-gruzopotokov/

Расшифруйте стихи А.С. Пушкина, (русский алфавит, Е и Ё считается одним символом)

Х шсхтгсхфзухщсчвщпрюълфвь
Кхщхйжщцчхшймамфгжлъь
Пхцвщ, швфхяпихсщчълфвь,
Пкмфпр, цзчзлхсшхйлчък,
Пштъюзр, ихкпохичмщзщмтг

Критерии и методика оценивания:

- 5 баллов выставляется студенту, если составлен правильный алгоритм решения задачи, в логическом рассуждении, в выборе формул и решении нет ошибок, получен верный ответ, задача решена рациональным способом, показано уверенное владение нормативной базой;

- 4 балла выставляется студенту, если составлен правильный алгоритм решения задачи, в логическом рассуждении и решении нет существенных ошибок; правильно сделан выбор формул для решения; есть объяснение решения, но задача решена нерациональным способом или допущено не более двух несущественных ошибок, получен верный ответ, нет определенной логической последовательности, неточно используется специализированная терминология;

- 3 балла выставляется студенту, если в логическом рассуждении нет существенных ошибок, но допущены существенные ошибки в выборе формул или в математических расчетах; задача решена не полностью или в общем виде;

- 2 балла выставляется студенту, если задача решена неправильно.

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. - М. : 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

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

Дополнительная литература

3. 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
4. Шишкин, В.В. МЕТОДИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. [Электронный ресурс] / В.В. Шишкин, Н.К. Юрков, Н.Ж. Мусин. — Электрон. дан. // Надежность и качество сложных систем. — 2013. — № 4. — С. 9-13. — Режим доступа: http://e.lanbook.com/journal/issue/298784 — Загл. с экрана.

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.

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), компьютерный класс, аудитория 404 (гуманитарный корпус), аудитория 420 (гуманитарный корпус). **3. *учебная аудитория для проведения групповых и индивидуальных консультаций:*** аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус), компьютерный класс аудитория № 404	Лекции, практические занятия, лабораторные занятия, групповые и индивидуальные консультации, текущий контроль, промежуточная аттестация	**Аудитория № 403** Учебная мебель, доска, Мультимедийный-проектор Panasonic PT-LB78VE – 1 шт., Экран настенный Classic Norma 244*183 – 1 шт., учебно-наглядные пособия. **Аудитория № 405** Учебная мебель, доска, вокальные радиомикрофоны AKGWMS 40 – 2шт., Интер-ая система со встроенным короткофокусным проекто-ром PrometheanActivBoard 387 RPOMOUNTEST -1 шт., Ком-ер встраиваемый в кафедру INTELCorei3-4150/DDr3 4 Gb/HDD, Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт., Настольный интерактивный дисплей , ActivPanel 21S – 1 шт. , Матричный коммутатор сигналов интерфейса HDMICMPRO 4H4H – 1 шт. , Мультимедиа-проектор 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	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.

(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:*** читальный зал библиотеки аудитория 402 (гуманитарный корпус), аудитория № 613 (гуманитарный корпус). **6.*помещение для хранения и профилактического обслуживания учебного оборудования:*** аудитория № 523 (гуманитарный корпус).		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 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. **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 комплект инструментов для проведения работ по специальным проверкам 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

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 Криптографические методы защиты информации
на 6 семестр

Вид работы	Объем дисциплины
	Очная форма обучения
Общая трудоемкость дисциплины (ЗЕТ / часов)	4 ЗЕТ / 144 часа
Учебных часов на контактную работу с преподавателем:	49,2
лекций	16
практических / семинарских	–
лабораторных	32
Других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем)	1,2
Учебных часов на самостоятельную работу обучающихся, включая подготовку к экзамену	42 52,8

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		4	5	6	7	8	9	10
1	Симметричные шифры Криптографическая защита информации на основе применения асимметричных алгоритмов шифрования.		2	–	4	5	1, 2,	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Контрольная работа, тестирование, практическая работа, тестирование
2	Односторонняя функция с потайным входом		2		4	5	1, 2, 3	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет	Контрольная работа, тестирование, практическая работа, тестирование
3	Протокол Диффи-Хелмана. Протокол ГОСТ Р 34.10-2001		2		4	5	1, 2, 3	Самостоятельное изучение рекомендуемой основной и дополнительной	Контрольная работа, тестирование, практическая работа,

								литературы, интернет	тестирование
4	Протокол Эль-Гамаля. Протокол Фиата-Шамира.		2		4	5	1, 2, 3,4	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет	Контрольная работа, тестирование, практическая работа, тестирование
5	Асимметричные шифры Алгоритм Фейге-Фиата-Шамира. Алгоритм RSA.		2	–	4	7	1, 2, 3	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Контрольная работа, тестирование, практическая работа, тестирование
6	Алгоритм Меркла-Хеллмана для электронных подписей.		2		4	5	1, 2, 3,4	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Контрольная работа, тестирование, практическая работа, тестирование
7	Электронно-цифровая подпись и протоколы.		2		4	5	1, 2, 3,4	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Контрольная работа, тестирование, практическая работа, тестирование
8	Ключевая информация ЭЦП.		2		4	5	1, 2, 3	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Контрольная работа, тестирование, практическая работа, тестирование
	Всего		16		32	42			

Приложение 2

Рейтинг – план дисциплины

Криптографические методы защиты информации

Направление подготовки 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. Симметричные шифры				
Текущий контроль				20
1.Аудиторная работа	2	5	0	10
2.Выполнение лабораторных заданий	5	2	0	10
Рубежный контроль				
1.Письменная контрольная работа	5	1	0	5
2 Тестирование	10	1	0	10
Всего				
Модуль 2. Асимметричные шифры				
Текущий контроль				20
1.Аудиторная работа	2	5	0	10
2.Выполнение лабораторных заданий	5	2	0	10
Рубежный контроль				
1.Письменная контрольная работа	5	1	0	5
2. Тестирование	10	1	0	10
Всего				
Поощрительные баллы				
1.Выполнение индивидуального задания	10	1	0	10
Всего				10
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
1. Посещение лекционных занятий	-	-	-6	0
2. Посещение лабораторных занятий	-	-	-10	0
Итоговый контроль				
Экзамен				30