

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ МОСКОВСКИЙ
ГОСУДАРСТВЕННЫЙ СТРОИТЕЛЬНЫЙ УНИВЕРСИТЕТ»

РАБОЧАЯ ПРОГРАММА

Шифр	Наименование дисциплины
Б1.Б.22	Защита информации

Код направления подготовки	09.03.02
Направление подготовки	Информационные системы и технологии
Наименование ОПОП	Системотехника и информационные технологии проектирования и управления в строительстве (Академический бакалавриат)
Год начала реализации ОПОП	2017
Уровень образования	Бакалавриат
Форма обучения	Очная
Год разработки/обновления	2016

Разработчики:

должность	ученая степень, учёное звание	ФИО
доцент	К.т.н	Шилова Л.А.

Рабочая программа рассмотрена и одобрена на заседании кафедры (структурного подразделения) «ИСТАС», Протокол № 9 от 29.09.2016

Заведующий кафедрой
(руководитель структурного подразделения)

 / Гинзбург А.В./
Подпись, ФИО

Рабочая программа утверждена методической комиссией, Протокол № 1 от 17.10.16

Председатель (зам. председателя)
методической комиссии

 / Кузина О.Н./
Подпись, ФИО

Согласовано:

ЦОСП

 / Кузнецова С.В./
дата _____ Подпись, ФИО

1. Цель освоения дисциплины

Целью освоения дисциплины «*Защита информации*» является формирование компетенций обучающегося в области изучения основных принципов разработки систем информационной безопасности, в том числе основ криптографии, как одного из элементов обеспечения защиты информации.

Программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по направлению подготовки Информационные системы и технологии (уровень образования - бакалавриат).

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

Компетенция по ФГОС	Код компетенции по ФГОС	Основные показатели оценивания (показатели достижения результата)	Код показателя оценивания
Понимание и значения информации в развитии современного информационного общества, соблюдение основных требований к информационной безопасности, в том числе защите государственной тайны	ОПК-4.	Знать понятие информации и основные понятия информатики. Основные способы хранения, обработки, защиты информации.	З1
		Уметь производить определенные операции над информацией. Применять различные средства защиты информации	У1
		Иметь навыки использования двоичной системы счисления для кодирования числовых данных и выполнений арифметических действий над ними. Элементами математической логики. Основными методами защиты информации	Н1
Способность оценивать надежность и качество функционирования объекта проектирования	ПК- 6	Знать методы, модели и современные инструментальные средства исследования для оценки и обеспечения надежности и качества информационных систем, основы разработки средств обнаружения, локализации, и восстановления отказавших элементов информационных систем.	З2
		Уметь разрабатывать и исследовать по критериям надежности избыточные информационные структуры, разрабатывать математические модели надежности информационных систем, разрабатывать средства обнаружения, локализации и восстановления отказавших элементов информационных систем.	У2
		Иметь навыки использования инструментальных средств обработки информации.	Н2
Способность обеспечивать безопасность и целостность данных информационных систем и технологий	ПК-31	Знать принципы защиты информации и обеспечения информационной безопасности, об основных угрозах информационной безопасности и их источниках; понятия конфиденциальной информации, персональных данных и государственной тайны.	З3
		Уметь выбирать методы и средства построения систем защиты информации.	У3

Компетенция по ФГОС	Код компетенции по ФГОС	Основные показатели оценивания (показатели достижения результата)	Код показателя оценивания
		Иметь навыки использования средств защиты информации для обеспечения заданных свойств информационной безопасности.	НЗ

3. Указание места дисциплины (модуля) в структуре образовательной программы

Дисциплина «*Защита информации*» относится к базовой части Блока 1 «Дисциплины/модули» основной профессиональной образовательной программы по направлению подготовки 09.03.02 «Информационные системы и технологии» (уровень образования бакалавриат), профиль «Системотехника и информационные технологии проектирования и управления в строительстве». Дисциплина является обязательной к изучению.

Изучение дисциплины «*Защита информации*» основано на знаниях, умениях и навыках, полученных при изучении обучающимися следующих дисциплин:

- «Операционные системы»,
- «Программирование на языке высокого уровня»,
- «Сети и телекоммуникации».

Для освоения дисциплины «*Защита информации*» обучающийся должен:

знать:

основы булевой алгебры,
основы организации и работы сетей;

уметь:

создавать программы на любом актуальном языке программирования,

владеть:

навыками работы с компьютером и компьютерными сетями.

Дисциплина «*Защита информации*» является завершающей дисциплиной теоретического курса основной образовательной программы бакалавров.

4. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины составляет 4 зачетных единиц, 144 академических часов.

(1 зачетная единица соответствует 36 академическим часам)

Структура дисциплины:

Форма обучения - очная

№ п/п	Наименование раздела дисциплины (модуля)	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)			Формы текущего контроля успеваемости (по неделям семестра) Форма промежуточной аттестации
				Контактная работа с обучающимися		Самостоятельная работа	
				Лекции	Практико-ориентированные занятия		

					Лабораторный практикум	Практические занятия	Групповые занятия - комп. практикумы	в период теор. обучения	в сессию	(по семестрам)
1	Основные составляющие информационной безопасности	8	1-3	4		2	2	10	4	
2	Законодательный уровень информационной безопасности	8	3-4	4		2	2	10	4	Устный опрос
3	Административный уровень информационной безопасности	8	5-6	4		2	2	10	4	
4	Процедурный уровень информационной безопасности	8	6-7	4		2	2	10	4	
5	Основные программно-технические меры обеспечения информационной безопасности	8	7-11	4		2	2	19	4	Контрольная работа
6	Системный подход к обеспечению информационной безопасности	8	11-12	4		2	2	10	7	
	Итого:	8		24		12	12	69	27	Экзамен

5. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

5.1. Содержание лекционных занятий

№ п/п	Наименование раздела дисциплины (модуля)	Тема и содержание занятия	Кол-во акад. часов
1	Основные составляющие информационной безопасности	Понятие информационной безопасности Анализ угроз информационной безопасности Комплексный поиск возможных методов доступа	4
2	Законодательный уровень информационной безопасности	Обзор законодательных актов в области информационной безопасности Стандарты и спецификации в области информационной безопасности	4
3	Административный уровень информационной безопасности	Содержание административного уровня информационной безопасности Политика безопасности. Понятие и основные положения Программа безопасности. Синхронизация программы безопасности с жизненным циклом систем Управление рисками при разработке системы информационной безопасности	4
4	Процедурный уровень информационной	Управление персоналом организации Физическая защита на процедурном уровне	4

	безопасности	Поддержание работоспособности Реагирование на нарушение режима безопасности Планирование восстановительных работ	
5	Основные программно-технические меры обеспечения информационной безопасности	Сервисы информационной безопасности Идентификация и аутентификация Управление доступом Протоколирование и аудит Контроль целостности Методы обеспечения безотказности Экранирование Анализ защищенности Туннелирование Криптографические методы защиты Управление системами безопасности	4
6	Системный подход к обеспечению информационной безопасности	Особенности современных информационных систем, существенные с точки зрения безопасности. Архитектурная безопасность.	4
		Итого	24

5.2. Лабораторный практикум

Лабораторный практикум не предусмотрен Учебным планом

5.3. Перечень практических занятий

№ п/п	Наименование раздела дисциплины	Тема и содержание занятия	Кол-во акад. часов
1	Основные составляющие информационной безопасности	Классификация методов шифрования информации. Классификация шифров	2
2	Законодательный уровень информационной безопасности	Блочные шифры. Шифры замены Блочные шифры. Шифры перестановки Блочные составные шифры. DES. ГОСТ 28147-89 Поточные шифры. Гаммирование. Требования, предъявляемые к гамме	2
3	Административный уровень информационной безопасности	Принципы асимметричного шифрования. RSA Шифр Эль-Гамала Шифр на основе укладки ранца Шифр на основе эллиптических кривых	2
4	Процедурный уровень информационной безопасности	Шифрование	2
5	Основные программно-технические меры обеспечения информационной безопасности	Виды электронной цифровой подписи. Алгоритм формирования	2
6	Системный подход к обеспечению информационной безопасности	Изучение программ, реализующих криптографические алгоритмы	2
		Итого	12

5.4. Групповые занятия – компьютерные практикумы

№ п/п	Наименование раздела дисциплины (модуля)	Тема и содержание группового занятия – компьютерного практикума	Кол-во акад. часов
-------	--	---	--------------------

1	Основные составляющие информационной безопасности	Классификация методов шифрования информации. Классификация шифров	2
2	Законодательный уровень информационной безопасности	Блочные шифры. Шифры замены Блочные шифры. Шифры перестановки Блочные составные шифры. DES. ГОСТ 28147-89 Поточные шифры. Гаммирование. Требования, предъявляемые к гамме	2
3	Административный уровень информационной безопасности	Принципы асимметричного шифрования. RSA Шифр Эль-Гамала Шифр на основе укладки ранца Шифр на основе эллиптических кривых	2
4	Процедурный уровень информационной безопасности	Шифрование	2
5	Основные программно-технические меры обеспечения информационной безопасности	Виды электронной цифровой подписи. Алгоритм формирования	2
6	Системный подход к обеспечению информационной безопасности	Изучение программ, реализующих криптографические алгоритмы	2
		Итого	12

5.5. Самостоятельная работа

№ п/п	Наименование раздела дисциплины	Виды самостоятельной работы	Кол-во акад. часов	
			в период теор. обучения	в сессию
1	Основные составляющие информационной безопасности	Самостоятельное изучение отдельных тем раздела.	10	4
2	Законодательный уровень информационной безопасности	Самостоятельное изучение отдельных тем раздела.	10	4
3	Административный уровень информационной безопасности	Самостоятельное изучение отдельных тем раздела.	10	4
4	Процедурный уровень информационной безопасности	Самостоятельное изучение отдельных тем раздела.	10	4
5	Основные программно-технические меры обеспечения информационной безопасности	Самостоятельное изучение отдельных тем раздела. Подготовка к контрольной работе.	19	4
6	Системный подход к обеспечению информационной безопасности	Самостоятельное изучение отдельных тем раздела.	10	7
		Подготовка к экзамену и его сдача		27
		Итого	69	27

6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

Основные принципы организации самостоятельной работы обучающихся изложены в Положении об организации самостоятельной работы обучающихся (НИУ МГСУ).

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

Фонд оценочных средств по дисциплине (модулю) для проведения промежуточной аттестации, а также текущего контроля обучающихся является Приложением 1 к рабочей программе дисциплины (модуля).

Оценочные материалы для проведения промежуточной аттестации, а также текущего контроля по дисциплине (модуля) хранятся на кафедре, ответственной за преподавание данной дисциплины.

8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

Для освоения дисциплины обучающийся может использовать:

- учебно-методическую литературу, имеющуюся в НТБ НИУ МГСУ,
- учебную литературу, размещённую в Электронных библиотечных системах ЭБС АСВ и IPRbooks,
- методическую литературу, размещённую в ЭБС НИУ МГСУ.

Перечень используемой литературы ежегодно обновляется с учётом уровня развития науки и техники и представлен в Приложении 2 к рабочей программе дисциплины.

9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет»), необходимых для освоения дисциплины (модуля)

Наименование ресурса сети «Интернет»	Электронный адрес ресурса
«Российское образование» - федеральный портал	http://www.edu.ru/index.php
Научная электронная библиотека	http://elibrary.ru/defaultx.asp?
Электронная библиотечная система IPRbooks	http://www.iprbookshop.ru/
Федеральная университетская компьютерная сеть России	http://www.runnet.ru/
Информационная система "Единое окно доступа к образовательным ресурсам"	http://window.edu.ru/
Научно-технический журнал по строительству и архитектуре «Вестник МГСУ»	http://www.vestnikmgsu.ru/
Научно-техническая библиотека НИУ МГСУ	http://www.mgsu.ru/resources/Biblioteka/
Раздел «Кафедры» на официальном сайте НИУ МГСУ	http://www.mgsu.ru/universityabout/Struktura/Kafedri/

10. Методические указания для обучающихся по освоению дисциплины (модуля)

Перечень тем по разделам дисциплины (модуля) для самостоятельного изучения обучающимися приведён в таблице.

№ п/п	Наименование раздела дисциплины (модуля)	Темы для самостоятельного изучения (в период теоретического обучения)
-------	--	---

1	Основные составляющие информационной безопасности	Угрозы информационной безопасности. Оценка степени защищённости домашних информационных ресурсов (ПК, ноутбук, роутер, телефон, планшетный компьютер). Средства поиска и устранения «заражения» компьютерной системы. Выбор подходящего для самостоятельного использования средства защиты Средства анализа состояния компьютерной сети. Проверка домашней вычислительной техники на предмет сетевой безопасности
2	Законодательный уровень информационной безопасности	Анализ законодательной базы информационной безопасности. Знакомство с основными положениями законов. Изучение стандартов и спецификаций в области информационной безопасности
3	Административный уровень информационной безопасности	Основные разделы политики безопасности. Составление примерной программы безопасности. Анализ рисков информационной безопасности
4	Процедурный уровень информационной безопасности	Управление персоналом организации. Основные меры по обеспечению информационной безопасности. Физическая защита на процедурном уровне. Поддержание работоспособности. Комплекс мер. Реагирование на нарушение режима безопасности
5	Основные программно-технические меры обеспечения информационной безопасности	Состав основных сервисов информационной безопасности Криптографические методы защиты.
6	Системный подход к обеспечению информационной безопасности	Применение системного подхода к проектированию комплексного решения в сфере информационной безопасности.

Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю) приведён в п.6.

Организация учебной работы обучающихся на аудиторных занятиях осуществляется в соответствии с п. 4.

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)

11.1. Перечень информационных технологий, используемых при осуществлении образовательного процесса

№ п/п	Наименование раздела дисциплины	Информационные технологии
1	Основные составляющие информационной безопасности	Проверка домашних заданий и консультирование посредством электронной почты. Использование слайд-презентаций, графических объектов, видео-, аудиоматериалов при проведении лекционных, практических занятий.
2	Законодательный уровень информационной безопасности	Проверка домашних заданий и консультирование посредством электронной почты. Использование слайд-презентаций, графических объектов, видео-, аудиоматериалов при проведении лекционных, практических занятий.
3	Административный уровень информационной безопасности	Проверка домашних заданий и консультирование посредством электронной почты. Использование слайд-презентаций, графических объектов, видео-, аудиоматериалов при проведении лекционных, практических занятий.
4	Процедурный уровень информационной безопасности	Проверка домашних заданий и консультирование посредством электронной почты. Использование слайд-презентаций, графических объектов, видео-, аудиоматериалов при проведении лекционных, практических занятий.

5	Основные программно-технические меры обеспечения информационной безопасности	Проверка домашних заданий и консультирование посредством электронной почты. Использование слайд-презентаций, графических объектов, видео-, аудиоматериалов при проведении лекционных, практических занятий.
6	Системный подход к обеспечению информационной безопасности	Проверка домашних заданий и консультирование посредством электронной почты. Использование слайд-презентаций, графических объектов, видео-, аудиоматериалов при проведении лекционных, практических занятий.

11.2. Перечень программного обеспечения, используемого при осуществлении образовательного процесса

При освоении дисциплины используется лицензионное и открытое программное обеспечение, указанное в Приложении 3 к рабочей программе.

11.3. Перечень информационных справочных систем

Информационно-библиотечные системы

Наименование ИБС	Электронный адрес ресурса
Научная электронная библиотека	http://elibrary.ru/defaultx.asp?
Электронная библиотечная система IPRbooks	http://www.iprbookshop.ru/
Научно-техническая библиотека НИУ МГСУ	http://www.mgsu.ru/resources/Biblioteka/

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю):

Учебные занятия по дисциплине проводятся в оборудованных учебных кабинетах, оснащенных соответствующим оборудованием и программным обеспечением. Перечень материально-технического обеспечения дисциплины (модуля) приведён в Приложении 4 к рабочей программе.

Шифр	Наименование дисциплины
Б1.Б.22	Защита информации

Код направления подготовки	09.03.02
Направление подготовки	Информационные системы и технологии
Наименование ОПОП	Системотехника и информационные технологии проектирования и управления в строительстве (Академический бакалавриат)
Год начала реализации ОПОП	2017
Уровень образования	Бакалавриат
Форма обучения	Очная
Год разработки/обновления	2016

Фонд оценочных средств для проведения промежуточной аттестации и текущего контроля обучающихся по дисциплине (модулю)

1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Формирование компетенций при изучении дисциплины (модуля) происходит поэтапно, по мере освоения обучающимися разделов дисциплины (модуля).

Код компетенции по ФГОС	Этапы формирования компетенций (разделы теоретического обучения)					
	1	2	3	4	5	6
ОПК-4	+	+	+	+	+	+
ПК-6		+	+	+	+	+
ПК-31			+	+	+	+

2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Оценивание формирования компетенций осуществляется посредством прохождения обучающимися форм промежуточной аттестации и текущего контроля.

Оценивание формирования компетенций производится на основе показателей оценивания, указанных в п.2. рабочей программы.

2.1. Описание показателей и форм оценивания компетенций

Формами оценивания компетенций являются мероприятия промежуточной аттестации и текущего контроля по дисциплине (модулю), указанные в учебном плане и в п.4 рабочей программы.

Взаимосвязь форм и показателей оценивания компетенций приведена в таблице.

Код компетенции по ФГОС	Показатели освоения (Код показателя оценивания)	Формы оценивания			Обеспеченность оценивания компетенции
		Текущий контроль		Промежуточная аттестация	
		Устный опрос	Контрольная работа		
1	2		3	4	5
ОПК-4	З1	+	+	+	+
	У1			+	+
	Н1		+	+	+
ПК-6	З2	+	+	+	+
	У2		+	+	+
	Н2		+	+	+
ПК-31	З3	+	+	+	+
	У3			+	+
	Н3			+	+
ИТОГО		+	+	+	+

2.2. Описание шкалы и критериев оценивания

При проведении промежуточной аттестации в форме экзамена используется четырёх балльная шкала оценивания:

Уровень освоения	Оценка
Минимальный	«2» (неудовлетворительно)
Пороговый	«3» (удовлетворительно)
Углубленный	«4» (хорошо)
Продвинутый	«5» (отлично)

Критериями оценивания уровня освоения компетенций являются:

Показатели оценивания	Критерии оценивания
Знания	Знание терминов и определений, понятий
	Знание основных закономерностей и соотношений, принципов
	Объём освоенного материала, усвоение всех дидактических единиц (разделов)
	Полнота ответов
	Правильность ответов
Умения	Чёткость изложения и интерпретации знаний
	Освоение методик - умение решать (типовые) практические задачи, выполнять (типовые) задания
	Умение использовать теоретические знания для выбора методики решения задач, выполнения заданий
	Умение проверять решение и анализировать результаты

	Умение качественно оформлять (презентовать) решение задач и выполнения заданий
Навыки	Навыки решения стандартных/нестандартных задач
	Быстрота выполнения трудовых действий Объем выполненных заданий
	Качество выполнения трудовых действий
	Самостоятельность планирования выполнения трудовых действий

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

3.1. Промежуточная аттестация

Промежуточная аттестация проводится в соответствии с Положением о текущем контроле и промежуточной аттестации обучающихся в НИУ МГСУ.

Перечень типовых вопросов/заданий для проведения экзамена в 8 семестре (очная форма обучения):

	Наименование раздела дисциплины	Вопросы / задания
1	Основные составляющие информационной безопасности	Понятие информационной безопасности Основные составляющие информационной безопасности Комплексный поиск возможных методов доступа - Терминалы защищенной информационной системы Комплексный поиск возможных методов доступа - Получение доступа на основе ошибок администратора и пользователей Комплексный поиск возможных методов доступа - Получение доступа на основе ошибок в реализации Комплексный поиск возможных методов доступа - Социальная психология и иные способы получения доступа
2	Законодательный уровень информационной безопасности	Законодательный уровень информационной безопасности. Законодательные акты в области информационной безопасности Стандарты и спецификации в области информационной безопасности - "Критерии оценки доверенных компьютерных систем" Стандарты и спецификации в области информационной безопасности – Руководящие документы Гостехкомиссии России
3	Административный уровень информационной безопасности	Административный уровень информационной безопасности Политика безопасности. Верхний уровень Политика безопасности. Средний уровень

		<p>Политика безопасности. Нижний уровень</p> <p>Программа безопасности</p> <p>Синхронизация программы безопасности с жизненным циклом систем – этап инициации</p> <p>Синхронизация программы безопасности с жизненным циклом систем – этап закупки</p> <p>Синхронизация программы безопасности с жизненным циклом систем – эксплуатация и выведение из эксплуатации</p> <p>Управление рисками. Подготовительные этапы</p> <p>Управление рисками. Основные этапы</p>
4	Процедурный уровень информационной безопасности	<p>Процедурный уровень информационной безопасности - управление персоналом</p> <p>Процедурный уровень информационной безопасности – физическая защита</p> <p>Процедурный уровень информационной безопасности - поддержание работоспособности</p> <p>Процедурный уровень информационной безопасности - реагирование на нарушения режима безопасности</p> <p>Процедурный уровень информационной безопасности – планирование восстановительных работ</p>
5	Основные программно-технические меры обеспечения информационной безопасности	<p>Программно-технический уровень информационной безопасности. Сервисы безопасности</p> <p>Идентификация и аутентификация - Парольная аутентификация</p> <p>Идентификация и аутентификация - Одноразовые пароли</p> <p>Идентификация и аутентификация - Идентификация/аутентификация с помощью биометрических данных</p> <p>Управление доступом</p> <p>Протоколирование и аудит</p> <p>Криптографические методы защиты</p> <p>Контроль целостности.</p> <p>Методы обеспечения безотказности</p> <p>Экранирование. Анализ защищенности.</p> <p>Туннелирование. Управление</p>
6	Системный подход к обеспечению информационной безопасности	<p>Системный подход к обеспечению информационной безопасности</p> <p>Особенности современных информационных систем, существенные с точки зрения безопасности</p> <p>Архитектурная безопасность</p>

3.2. Текущий контроль

Перечень проводимых мероприятий текущего контроля: контрольная работа

Контрольная работа содержит 3 задания на разработку алгоритмов шифрования.

Первое задание – блочный шифр симметричного шифрования (шифр Цезаря, лозунговый шифр, шифр Виженера, шифр Playfair, полибианский квадрат, простая одинарная перестановка, магический квадрат, блочная одинарная перестановка, двойная перестановка, табличная маршрутная перестановка, вертикальная перестановка).

Второе задание – поточный шифр симметричного шифрования (гаммирование по модулю N , гаммирование по модулю 2).

Третье задание – либо блочные составные шифры симметричного шифрования (DES, ГОСТ 28147-89), либо шифры асимметричного шифрования (RSA, шифр Эль-Гамала, шифр на основе укладки ранца, шифр на основе эллиптических кривых).

Задания выполняются по вариантам. В работе требуется программная реализация заданного алгоритма. Необходимо выполнить полный цикл шифрования: зашифровать + расшифровать, с разнесением по времени данных процедур. Программа должна быть реализована на языках C#, C++, однако допускается выбор средств реализации в зависимости от желания студента. При оценке контрольной работы проверяется понимание принципов программной реализации алгоритма шифрования.

Вопросы для устного опроса:

Понятие информационной безопасности

Основные составляющие информационной безопасности

Комплексный поиск возможных методов доступа - Терминалы защищенной информационной системы

Комплексный поиск возможных методов доступа - Получение доступа на основе ошибок администратора и пользователей

Комплексный поиск возможных методов доступа - Получение доступа на основе ошибок в реализации

Комплексный поиск возможных методов доступа - Социальная психология и иные способы получения доступа

Законодательный уровень информационной безопасности. Законодательные акты в области информационной безопасности

Стандарты и спецификации в области информационной безопасности - "Критерии оценки доверенных компьютерных систем"

Стандарты и спецификации в области информационной безопасности – Руководящие документы Гостехкомиссии России

Административный уровень информационной безопасности.

4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедура промежуточной аттестации регламентируется с Положением о текущем контроле и промежуточной аттестации обучающихся в НИУ МГСУ.

4.1. Процедура оценивания при проведении промежуточной аттестации обучающихся по дисциплине (модулю) в форме экзамена/дифференцированного зачета

Промежуточная аттестация по дисциплине (модулю) проводится в форме экзамена в 8 семестре.

Используется четырёх балльная шкала оценивания освоения, указанная в п.2.2.

Используются критерии оценивания, указанные п.2.2.

Оценка выставляется преподавателем интегрально по всем показателям и критериям оценивания.

Код показателя оценивания	Оценка			
	«2» (неудовлетв.)	Пороговый уровень освоения	Углубленный уровень освоения	Продвинутый уровень освоения
		«3» (удовлетвор.)	«4» (хорошо)	«5» (отлично)
Знания З-1, З-2, З-3.	не знает терминов и определений	знает термины и определения, но допускает неточности формулировок	знает термины и определения	знает термины и определения, может сформулировать их самостоятельно
	не знает основные закономерности и соотношения, принципы построения знаний	знает основные закономерности, соотношения, принципы построения знаний	знает основные закономерности, соотношения, принципы построения знаний, способен их интерпретировать и использовать	знает основные закономерности, соотношения, принципы построения знаний, способен самостоятельно их получить и использовать
	не знает значительной части материала дисциплины	знает только основной материал дисциплины, не усвоил его деталей	знает материал дисциплины в запланированном объеме	обладает твердым и полным знанием материала дисциплины, владеет дополнительными знаниями
	Ответ не дан	дана только часть ответа на вопрос	ответ не полон, некоторые моменты в ответе не отражены	дан полный, развернутый ответ
	допускает грубые ошибки при изложении ответа на вопрос	В ответе имеются существенные ошибки	В ответе имеются несущественные неточности	Ответ верен
	Неверно излагает и интерпретирует знания. Изложение материала логически не выстроено. Не способен проиллюстрировать изложение поясняющими схемами, рисунками и примерами	Допускает неточности в изложении и интерпретации знаний. Имеются нарушения логической последовательности в изложении. Поясняющие рисунки, схемы выполнены не полно, не отражают материал.	Грамотно и по существу излагает материал. Логическая последовательность изложения не нарушена. Поясняющие рисунки, схемы и примеры корректны и понятны.	Логически, грамотно и точно излагает материал дисциплины, интерпретируя его самостоятельно, способен самостоятельно его анализировать и делать выводы. Поясняющие схемы, рисунки и примеры точны и раскрывают глубину полученных знаний.
Умения У1 У2 У3	Не умеет выполнять поставленные практические задания, выбрать типовой алгоритм решения	Умеет выполнять практические задания, но не всех типов. Способен решать задачи только по заданному алгоритму	Умеет выполнять типовые практические задания, предусмотренные программой	Умеет выполнять практические задания повышенной сложности
	Не может увязывать теорию с практикой, не может ответить на простые вопросы	Испытывает затруднения в применении теории при решении задач,	Правильно применяет полученные знания при выполнении заданий и	Умеет применять теоретическую базу дисциплины при выполнении

	по выполнению заданий, не может обосновать выбор метода решения задач	при обосновании решения	обосновании решения. Грамотно обосновывает ход решения задач	практических заданий, предлагать собственный метод решения. Грамотно обосновывает ход решения задач.
	Допускает грубые ошибки при выполнении заданий, нарушающие логику решения	Допускает ошибки при выполнении заданий, нарушения логики решения. Испытывает затруднения с выводами	Допускает некоторые ошибки при выполнении заданий, не нарушающие логику решения. Делает выводы по результатам решения	Не допускает ошибок при выполнении заданий, правильно обосновывает принятое решение. Самостоятельно анализирует задания и решения
	Не способен проиллюстрировать решение поясняющими схемами, рисунками	Поясняющие рисунки и схемы содержат ошибки, оформлены небрежно	Поясняющие рисунки и схемы корректны и понятны.	Поясняющие рисунки и схемы верны и аккуратно оформлены
Навыки Н1 Н2 Н3	Не обладает навыками выполнения поставленных задач	Испытывает трудности при выполнении отдельных поставленных задач	Не испытывает затруднений при выполнении стандартных задач. Решение нестандартных задач представляет для него сложности.	Не испытывает затруднений при выполнении стандартных задач. Использует полученные навыки при решении сложных, нестандартных задач
	Не выполняет трудовые действия или выполняет очень медленно, не достигая поставленных задач	Выполняет трудовые действия медленно, с отставанием от установленного графика.	Выполняет трудовые действия, выполняет все поставленные задания.	Выполняет трудовые действия быстро, выполняя все поставленные задания.
	Выполняет трудовые действия некачественно	Выполняет трудовые действия с недостаточным качеством	Выполняет трудовые действия качественно	Выполняет трудовые действия качественно даже при выполнении сложных заданий
	Не может самостоятельно планировать и выполнять собственные трудовые действия	Выполняет трудовые действия только с помощью наставника	Самостоятельно выполняет трудовые действия с консультацией у наставника	Выполняет трудовые действия самостоятельно, без посторонней помощи

4.2. Процедура оценивания при проведении промежуточной аттестации обучающихся по дисциплине в форме Зачета

Промежуточная аттестация по дисциплине в форме зачёта не проводится.

4.3. Процедура оценивания при проведении промежуточной аттестации обучающихся по дисциплине в форме защиты курсовой работы/проекта

Промежуточная аттестация по дисциплине в форме защиты курсового проекта /курсовой работы не проводится.

Приложение 2 к рабочей программе

Шифр	Наименование дисциплины
<i>Б1.Б.22</i>	<i>Защита информации</i>

Код направления подготовки	09.03.02
Направление подготовки	Информационные системы и технологии
Наименование ОПОП	Системотехника и информационные технологии проектирования и управления в строительстве (Академический бакалавриат)
Год начала реализации ОПОП	2017
Уровень образования	Бакалавриат
Форма обучения	Очная
Год разработки/обновления	2016

Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

№ п/п	Наименование дисциплины (модуля) в соответствии с учебным планом	Автор, название, место издания, издательство, год издания учебной и учебно-методической литературы, количество страниц	Количество экземпляров печатных изданий в библиотеке НИУ МГСУ	Число обучающихся, одновременно изучающих дисциплину (модуль)
1	2	3	4	5
<i>Основная литература:</i>				
		НТБ НИУ МГСУ		
1	Защита информации	Жук А.П. Защита информации [Текст] : учебное пособие для студентов вузов, обучающихся по направлению подготовки 210700 - Инфокоммуникационные технологии и системы связи квалификации "бакалавр" и квалификации "магистр" / А. П. Жук [и др.]. - Москва : РИОР : ИНФРА-М, 2013. - 392 с.	15	60
		ЭБС АСВ		
2	Защита информации	Основы информационной безопасности [Электронный ресурс]/ Галатенко В.А.— Электрон.текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИИТГУИТ), 2016.— 266 с.	http://www.iprbookshop.ru/22424	60

3	Защита информации	Башлы П.Н. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие/ Башлы П.Н., Бабаш А.В., Баранова Е.К.— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2012.— 311 с.	http://www.iprbookshop.ru/10677	60
---	-------------------	--	---	----

Согласовано:

НТБ

24.10.16

дата



НТБ МГСУ

Подпись, ФИО

Приложение 3 к рабочей программе

Шифр	Наименование дисциплины
Б1.Б.22	Защита информации

Код направления подготовки	09.03.02
Направление подготовки	Информационные системы и технологии
Наименование ОПОП	Системотехника и информационные технологии проектирования и управления в строительстве (Академический бакалавриат)
Год начала реализации ОПОП	2017
Уровень образования	Бакалавриат
Форма обучения	Очная
Год разработки/обновления	2016

Перечень программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине

	Наименование раздела дисциплины	Тема	Наименование программного обеспечения	Тип лицензии
1	Основные составляющие информационной безопасности	Классификация методов шифрования информации. Классификация шифров	Microsoft Windows Microsoft Visual Studio	DreamSpark subscription
2	Законодательный уровень информационной безопасности	Блочные шифры. Шифры замены Блочные шифры. Шифры перестановки Блочные составные шифры. DES. ГОСТ 28147-89 Поточные шифры. Гаммирование. Требования, предъявляемые к гамме	Microsoft Windows Microsoft Visual Studio	DreamSpark subscription
3	Административный уровень информационной безопасности	Принципы асимметричного шифрования. RSA Шифр Эль-Гамала Шифр на основе укладки ранца Шифр на основе эллиптических кривых	Microsoft Windows Microsoft Visual Studio	DreamSpark subscription
4	Процедурный уровень информационной безопасности	Шифрование	Microsoft Windows Microsoft Visual Studio	DreamSpark subscription
5	Основные программно-технические меры обеспечения информационной безопасности	Виды электронной цифровой подписи. Алгоритм формирования	Microsoft Windows Microsoft Visual Studio	DreamSpark subscription
6	Системный подход к обеспечению информационной безопасности	Изучение программ, реализующих криптографические алгоритмы	Microsoft Windows Microsoft Visual Studio	DreamSpark subscription

Приложение 4 к рабочей программе

Шифр	Наименование дисциплины
<i>Б1.Б.22</i>	<i>Защита информации</i>
Код направления подготовки	09.03.02
Направление подготовки	Информационные системы и технологии
Наименование ОПОП	Системотехника и информационные технологии проектирования и управления в строительстве (Академический бакалавриат)
Год начала реализации ОПОП	2017
Уровень образования	Бакалавриат
Форма обучения	Очная
Год разработки/обновления	2016

Перечень материально-технического обеспечения по дисциплине (модулю):

№ п/п	Вид учебного занятия	Наименование оборудования	№ и наименование оборудованных учебных кабинетов, объектов для проведения практических занятий
1	2	3	4
1	Лекции	стационарные / мобильные (переносные) наборы демонстрационного мультимедийного оборудования (проектор, микрофон, экран, компьютер)	Учебные аудитории для проведения занятий лекционного типа (129337, г. Москва, ш. Ярославское, д.26, корп. 7, помещение 8 комн.14, 17, 63,64.)
2	Практические занятия	стационарные / мобильные (переносные) наборы демонстрационного мультимедийного оборудования (проектор, микрофон, экран, компьютер)	Учебная аудитория для проведения занятий семинарского типа (129337, г. Москва, ш. Ярославское, д.26, корп. 20, помещение 1, комн. 14, 15;)
3	Групповые занятия – компьютерные практикумы	Компьютерный класс: 26 персональных компьютеров с конфигурацией: 3,06 ГГц, HDD 500 Гб, RAM 4 Гб, Video RAM 512 Мб, DVD-R/RW, монитор 22 "", экран проекционный (Projecta ELPRO EL) (1 шт.); Компьютерный класс: 24 персональных компьютеров с конфигурацией: 3,06 ГГц, HDD 500 Гб, RAM 4 Гб, Video RAM 512 Мб, DVD-R/RW, монитор 22 "", экран проекционный (Projecta ELPRO EL) (1 шт.); Компьютерный класс: 27 персональных компьютеров с конфигурацией: 3,06 ГГц, HDD 500 Гб, RAM 4 Гб, Video RAM 512 Мб, DVD-R/RW, монитор 22 "", экран проекционный ELPRO EL 168*220 MW VID (1 шт.), проектор/тип №3 Epson (1 шт.); Компьютерный класс: 18 персональных компьютеров с конфигурацией: 3,06 ГГц, HDD 500 Гб, RAM 4 Гб, Video RAM 512 Мб, DVD-R/RW, монитор 22 "", экран проекционный Projecta Professional (2 шт.).	Аудитории / аудитория для проведения занятий семинарского типа в соответствии с перечнем аудиторного фонда (129337, г. Москва, ш. Ярославское, д.26, корп. 20, помещение 1, комн. 14,15,16,17.)

4	Самостоятельная работа	29 персональных компьютеров с конфигурацией: 1,6 ГГц, HDD 80 Гб, RAM 1 Гб, Video RAM 128 Мб, DVD-R/RW, монитор 17".	Помещение для самостоятельной работы обучающихся (129337, г. Москва, ш. Ярославское, д.26, корп. 2, помещение 6, комн. 5.)
---	------------------------	---	--