Федеральное государственное бюджетное образовательное учреждение
высшего образования
Московский государственный университет имени М.В. Ломоносова
Высшая школа управления и инноваций

УТВЕРЖДАЮ
и.о.декана
/В.В.Печковская /
«12» февраля 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

МАГИСТРАТУРА

27.04.05 "ИННОВАТИКА"

Форма обучения:

очная, очно-заочная

Рабочая программа рассмотрена и одобрена
Советом факультета

(протокол № 2, 12 февраля 2019 г.)

Москва 2019

Рабочая программа дисциплины (модуля) разработана в соответствии с самостоятельно установленным МГУ образовательным стандартом (ОС МГУ) для реализуемых основных профессиональных образовательных программ высшего образования по направлению подготовки / специальности 27.04.05 «Инноватика» (программы магистратуры) в редакции приказа МГУ от 30 декабря 2016 г.

Год (годы) приема на обучение: 2017, 2018, 2019.

I. Цели и задачи учебной дисциплины

Целью изучения дисциплины «Информационная безопасность и защита информации» является формирование у студентов системы знаний в области информационной безопасности и применения на практике методов и средств защиты информации.

Задачами дисциплины являются:

- формирование умения обеспечить защиту информации и объектов информатизации;
- формирование умения составлять заявительную документацию в надзорные государственные органы инфокоммуникационной отрасли;
- формирование навыков выполнения работ в области технического регулирования, сертификации технических средств, систем, процессов, оборудования и материалов;
- формирование навыков обеспечения защиты объектов интеллектуальной собственности, результатов исследований и разработок как коммерческой тайны предприятия.

В результате изучения данного курса, обучающиеся получат представление о сущности и значении информации в развитии современного информационного общества, научатся осознавать опасности и угрозы, возникающие в этом процессе, а также соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны.

II. Место дисциплины в структуре ОПОП ВО

Дисциплина «Информационная безопасность и защита информации» относится к профессиональному блоку вариативной части (дисциплины по выбору студента) учебного плана программы магистратуры 27.04.05. «Инноватика».

Изучение дисциплины базируется на знаниях и умениях, полученных обучающимися в процессе изучения гуманитарных, социальных и экономических дисциплин программы бакалавриата: «Математика», «Системный анализ и теория принятия решений», «Методы исследования в менеджменте», а также дисциплин программы магистратуры: «Правовая среда бизнеса и интеллектуальное право» и «Системный анализ и теория принятия решений» программы магистратуры.

Для успешного освоения дисциплины обучающийся должен:

Знать:

- фундаментальные положения теории информационного кодирования;
- теоретические основы системного анализа;
- основные проблемы современной философии и подходов к их решению;

Уметь:

- использовать междисциплинарные системные связи наук;
- анализировать и оценивать философские проблемы при решении социальных и профессиональных задач;
- применять математический инструментарий к решению социальных и профессиональных проблем.

Владеть:

- навыками математической формализации экономических и социальных процессов;
- навыками выбора наиболее актуальных направлений научных исследований, ставить задачи исследования и определять способы решения поставленных задач;

- самостоятельно приобретать и использовать в практической деятельности новые знания и умения в различных сферах деятельности.

Знания, навыки и умения, полученные при изучении дисциплины «Информационная безопасность и защита информации» обеспечивают успешное освоение дисциплин «Технологический аудит», «Системный инжиниринг» и необходимы для прохождения преддипломной практики, осуществления научно-исследовательской работы и написания выпускной квалификационной работы (магистерской диссертации). Изучается на 2 курсе (3 семестр).

III.Требования к результатам освоения дисциплины

УК-1. Способность формулировать научно обоснованные гипотезы, создавать теоретические модели явлений и процессов, применять методологию научного познания в профессиональной деятельности
УК-2. Готовность к саморазвитию, самореализации, использованию творческого потенциала
УК-3. Готовность действовать в нестандартных ситуациях, нести социальную и этическую ответственность за принятые решения
ОПК-3. Способность решать профессиональные задачи на основе философии, математических методов и моделей для управления инновациями, компьютерных технологий в инновационной сфере
ОПК-4. Способность к абстрактному мышлению, анализу, синтезу
ПК-10. Способность критически анализировать современные проблемы инноватики с учётом экономического, социального, экологического и технологического аспектов жизнедеятельности человека

Специализированные профессиональные компетенции:

- Способность обеспечить защиту информации и объектов информатизации.
- Умение обеспечить защиту объектов интеллектуальной собственности и результатов исследований и разработок как коммерческой тайны предприятия.
- Умение составлять заявительную документацию в надзорные государственные органы инфокоммуникационной отрасли.

В результате изучения дисциплины студент должен:

Знать:

- сущность и значение информации в развитии современного информационного общества;
- основные виды опасностей и угроз, возникающие в процессе хранения и передачи информации;
- основные требования информационной безопасности, в том числе защиты государственной тайны.

Уметь:

- решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением инфокоммуникационных технологий;
- решать нестандартные задачи в сфере защиты информации с учетом основных требований информационной безопасности.

Владеть:

- техническими средствами и методами защиты информации;
- методами применения криптографических средств защиты информации;

– программно-аппаратными средствами и методами обеспечения информационной безопасности.

Иметь опыт использования инструментов обеспечения информационной безопасности организации.

Формат обучения: очная, очно-заочная.

IV. Формы контроля

Контроль за освоением дисциплины осуществляется в каждом дисциплинарном разделе отдельно.

Рубежный контроль: контрольная работа по отдельным разделам дисциплины.

Итоговая аттестация в 3 семестре – зачет.

Результаты текущего контроля и итоговой аттестации формируют рейтинговую оценку работы обучающегося. Распределение баллов по отдельным видам работ в процессе освоения дисциплины «Информационная безопасность и защита информации» осуществляется в соответствии с Приложением 1.

V. Объём дисциплины и виды учебной работы

Объем курса – 108 часов, 3 зачетные единицы, в том числе 24 часов – аудиторная нагрузка, из которых 12 часов – лекции, 12 часов – семинары, 84 часа – самостоятельная работа студентов. Изучается на 2 курсе (3 семестр), итоговая форма отчетности – зачет.

Вид учебной работы	Всего часов
Контактные занятия (всего)	24
В том числе:	-
Лекции	12
Практические занятия (ПЗ)	-
Семинары (С)	12
Лабораторные работы (ЛР)	-
Самостоятельная работа (всего)	84
В том числе:	-
Домашние задания	20
Реферат	33
Подготовка к опросу	10
Подготовка к тестированию	7
Подготовка к контрольной работе	10
Вид промежуточной аттестации Зачет	4
Общая трудоемкость (часы) Зачетные единицы	108 4

VI. Структура и содержание дисциплины

п/п	Раздел	Содержание (темы)
1	**Введение в информационную безопасность**	Информационная безопасность. Основные понятия. Модели информационной безопасности. Виды

		защищаемой информации. Использование баз данных для нахождения и изучения нормативных документов в области информационной безопасности.
2	**Правовое обеспечение информационной безопасности**	Основные нормативно-правовые акты в области информационной безопасности. Правовые особенности обеспечения безопасности конфиденциальной информации и государственной тайны.
3	**Организационное обеспечение информационной безопасности**	Основные стандарты в области обеспечения информационной безопасности. Политика безопасности. Экономическая безопасность предприятия.
4	**Технические средства и методы защиты информации**	Инженерная защита объектов. Защита информации от утечки по техническим каналам.
5	**Программно-аппаратные средства и методы обеспечения информационной безопасности**	Основные виды сетевых и компьютерных угроз. Средства и методы защиты от сетевых компьютерных угроз. Создание удостоверяющего центра, генерация открытых и секретных ключей, создание сертификатов открытых ключей, создание электронной подписи, проверка электронной подписи. Использование средств стеганографии для защиты файлов. Изучение настроек средств антивирусной защиты информации.
6	**Криптографические методы защиты информации**	Симметричные и ассиметричные системы шифрования. Цифровые подписи (Электронные подписи). Инфраструктура открытых ключей. Криптографические протоколы. Создание зашифрованных файлов и криптоконтейнеров и их расшифрование. Создание защищенного канала связи средствами виртуальной частной сети.

Разделы дисциплин и виды занятий (ак. часы)

п/п	Наименование раздела дисциплины	Лекция	Практи-ческие занятия	Лабора-торные занятия	Семинар	СРС	Формы текущего контроля
1	**Введение в информационную безопасность**	**2**	**-**	**-**	**2**	**10**	**Задание Опрос КР**
2	**Правовое обеспечение информационной безопасности**	**2**	**-**	**-**	**2**	**10**	**Реферат Опрос КР**

3	**Организационное обеспечение информационной безопасности**	**2**	**-**	**-**	**2**	**10**	**Задание Тест КР**
4	**Технические средства и методы защиты информации**	**2**	**-**	**-**	**2**	**10**	**Задание Тест КР**
5	**Программно-аппаратные средства и методы обеспечения информационной безопасности**	**2**	**-**	**-**	**2**	**20**	**Задание Тест КР**
6	**Криптографические методы защиты информации**	**2**	**-**	**-**	**2**	**20**	**Задание Тест КР**
	Промежуточная аттестация (зачет)					**4**	
	Итого	**12**	**-**	**-**	**12**	**84**	

Разделы дисциплины и междисциплинарные связи

№ п/п	**Наименование обеспечиваемых (последующих) дисциплин**	**№ № разделов данной дисциплины, необходимых для изучения обеспечиваемых (последующих) дисциплин**					
		1	**2**	**3**	**4**	**5**	**6**
1.	**Технологический аудит**	-	+	-	+	+	-
2.	**Системный инжиниринг**	+	+	-	+	+	+

VII. Образовательные технологии

В процессе освоения дисциплины «Информационная безопасность и защита информации» используются следующие образовательные технологии:

1. Стандартные методы обучения:

- лекции;
- семинары;
- письменные или устные домашние задания;
- консультации преподавателей;
- самостоятельная работа студентов, в которую входит освоение теоретического материала, подготовка к семинарам, выполнение указанных выше письменных работ.

2. Методы обучения с применением интерактивных форм образовательных технологий:

- интерактивные лекции;
- анализ деловых ситуаций на основе кейс-метода и имитационных моделей;
- круглые столы;
- обсуждение подготовленных студентами рефераты;
- групповые дискуссии и проекты;

– обсуждение результатов работы студенческих исследовательских групп.

VIII. Учебно-методическое, информационное и материально-техническое обеспечение дисциплины

Учебно-методическое и информационное обеспечение дисциплины

а) Основная литература:

1. Бабаш, А.В. Информационная безопасность (+ CD-ROM) [Текст] / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. – М.: КноРус, 2013. – 136 с.
2. Васильков, А.В. Безопасность и управление доступом в информационных системах [Текст] / А.В. Васильков, И.А. Васильков. – М.: Форум, 2015. - 368 с.
3. Гафнер, В. В. Информационная безопасность [Текст] / В.В. Гафнер. – М.: Феникс, 2014. – 336 с.
4. Степанов, Е.А. Информационная безопасность и защита информации: учебное пособие [Текст] / Е.А. Степанов, И.К. Корнеев. – М.: ИНФРА-М, 2017. – 304 с.
5. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей [Текст] / В.Ф. Шаньгин. – М.: Форум, Инфра-М, 2017. – 416 с.

б) Дополнительная литература:

1. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. – М.: Наука, 2015. – 552 с.
2. Безопасность России. Правовые, социально-экономические и научно-технические аспекты. Основы информационно-психологической безопасности: моногр. – М.: Международный гуманитарный фонд «Знание», 2014. – 416 с.
3. Рассел, Джесси Honeypot (информационная безопасность) [Текст] / Джесси Рассел. – М.: VSD, 2013. – 686 с.
4. Сальная, Л.К. Английский язык для специалистов в области информационной безопасности [Текст] / Л.К. Сальная, А.К. Шилов, Ю.А. Королева. – М.: Гелиос АРВ, 2016. – 208 с.
5. Федоров, А.В. Информационная безопасность в мировом политическом процессе [Текст] / А.В. Федоров. – М.: МГИМО-Университет, 2017. – 220 с.
6. Чипига, А.Ф. Информационная безопасность автоматизированных систем [Текст] / А.Ф. Чипига. – М.: Гелиос АРВ, 2013. – 336 с.
7. Шаньгин, Владимир Федорович Информационная безопасность и защита информации [Текст] / Шаньгин Владимир Федорович. – М.: ДМК Пресс, 2017. – 249 с.
8. Ярочкин, В. Безопасность информационных систем [Текст] / В. Ярочкин. – М.: Ось-89, 2016. – 320 с.
8. Ярочкин, В.И. Информационная безопасность [Текст] / В.И. Ярочкин. – М.: Академический проект, 2014. – 544 с.

Перечень лицензионного программного обеспечения

MS Office

Перечень профессиональных баз данных и информационных справочных систем

1. ЭБС «Юрайт» [раздел «ВАША ПОДПИСКА: учебники и учебные пособия издательства «Юрайт»]: сайт. – URL: https://www.biblio-online.ru/catalog/
2. ЭБС издательства «Лань» [учебные, научные издания, первоисточники, художественные произведения различных издательств; журналы] : сайт. – URL: http://e.lanbook.com
3. http://nbmgu.ru/ – Научная библиотека МГУ имени М.В. Ломоносова
4. http://rucont.ru – Электронно-библиотечная система РУКОНТ
5. http://www.book.ru – Электронно-библиотечная система BOOK.ru

6. http://www.iprbookshop.ru – Электронно-библиотечная система IPRbooks

Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. http://www.olap.ru – информационный портал, посвященный технологиям интерактивной аналитической обработки
2. http://neiroset.ru – Информационный портал «Нейросеть.ру»

Рекомендуемые обучающие, справочно-информационные, контролирующие и прочие компьютерные программы, используемые при изучении дисциплины

№ п/п	Название рекомендуемых по разделам и темам программы технических и компьютерных средств обучения	Номера тем
2.	MS Excel	4, 5, 6
3.	PowerPoint	1, 2, 3

Методические указания для обучающихся по освоению дисциплины

В процессе изучения курса обучающиеся обязаны соблюдать дисциплину, вовремя приходить на занятия, делать домашние задания, осуществлять подготовку к семинарам и контрольным работам, проявлять активность на занятиях.

При этом важное значение имеет самостоятельная работа, которая направлена на формирование у учащегося умений и навыков правильного оформления конспекта и работы с ним, работы с литературой и электронными источниками информации, её анализа, синтеза и обобщения. Для проведения самостоятельной работы обучающимся предоставляется список учебно-методической литературы.

Материально-техническое обеспечение дисциплины

Для проведения образовательного процесса необходима аудитория, оборудованная компьютерами и проектором, необходимыми для демонстрации презентаций и использования программного обеспечения для решения математических задач. Обязательное программное обеспечение – MS Office.

IX. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Темы курсовых работ

Курсовая работа по дисциплине « Информационная безопасность и защита информации» не предусмотрена.

Темы рефератов

1. Проведение анализа информационной системы. Выявление угроз и уязвимостей, каналов утечки информации
2. Построение системы защиты информации в информационной системе.
3. Разработка или подбор алгоритмов для использования в реальных информационных системах.
4. Программирование привязки ПО к аппаратному обеспечению.
5. Настройка межсетевых экранов.
6. Взлом систем защиты.
7. Исследование алгоритмов вирусов и антивирусов.
8. Классификация информации. Виды данных и носителей.
9. Ценность информации. Цена информации.

10. Количество и качество информации.
11. Виды защищаемой информации.
12. Демаскирующие признаки объектов защиты.
13. Классификация источников и носителей информации.
14. Мероприятия по управлению доступом к информации.
15. Функциональные источники сигналов. Опасный сигнал.
16. Основные средства и системы, содержащие потенциальные источники опасных сигналов.
17. Вспомогательные средства и системы, содержащие потенциальные источники опасных сигналов.
18. Виды паразитных связей и наводок, характерные для любых радиоэлектронных средств и проводов, соединяющих их кабелей.
19. Виды угроз безопасности информации.
20. Основные принципы добывания информации.
21. Процедура идентификации, как основа процесса обнаружения объекта.
22. Методы синтеза информации.
23. Методы несанкционированного доступа к информации.
24. Основными способами привлечения сотрудников государственных и коммерческих структур, имеющих доступ к интересующей информации.
25. Способы наблюдения с использованием технических средств.
26. Каналы утечки информации. Технические каналы утечки
27. Классификация технических каналов утечки по физической природе носителя.
28. Классификация технических каналов утечки по информативности.
29. Классификация технических каналов утечки по времени функционирования.
30. Классификация технических каналов утечки по структуре.
31. Наблюдение в оптическом диапазоне и применяемые для этого средства. Характеристики таких средств.
32. Перехват электромагнитных излучений.
33. Акустическое подслушивание. Эффекты, возникающие при подслушивании.
34. Понятия скрытия информации, виды скрытий. Информационный портрет.
35. Противодействие наблюдению. Способы маскировки.
36. Способы и средства противодействия подслушиванию.
37. Нейтрализация закладных устройств.
38. Состав инженерной защиты и технической охраны объектов.
39. Инженерные конструкции и сооружения для защиты информации. Их классификация.
40. Средства идентификации личности.
41. Классификация датчиков охранной сигнализации.
42. Классификация извещателей.
43. Телевизионные системы наблюдения.
44. Основные средства системы видеоконтроля.
45. Защита личности как носителя информации.
46. Системный подход к защите информации.
47. Параметры системы защиты информации.
48. Этапы проектирования системы защиты информации.
49. Потенциальные каналы утечки информации.
50. Этапы разработки мер по предотвращению угроз утечки информации.

Вопросы для текущего контроля и самостоятельной работы студентов

1. Основные определения и критерии классификации угроз.

2. Угроза и их классификация.
3. Атака.
4. Окно опасности.
5. Наиболее распространенные угрозы доступности.
6. Угрозы доступности, классифицированные по компонентам ИС, на которые нацелены, угрозы.
7. Примеры угроз доступности.
8. Вредоносное программное обеспечение.
9. Грани вредоносного ПО.
10. Основные угрозы целостности.
11. Основные угрозы конфиденциальности.
12. Что такое законодательный уровень информационной безопасности и почему он важен?
13. Правовые акты общего назначения, затрагивающие вопросы информационной безопасности.
14. Закон «об информации, информатизации и защите информации» и устанавливаемые им основные определения.
15. Цели защиты информации согласно закону «об информации, информатизации и защите информации».
16. Закон "о лицензировании отдельных видов деятельности" и его определения.
17. Электронный документ, электронная цифровая подпись, владелец сертификата ключа подписи, средства электронной цифровой подписи, сертификат средств электронной цифровой подписи.
18. Закрытый ключ электронной цифровой подписи, открытый ключ электронной цифровой. подписи, сертификат ключа подписи, подтверждение подлинности электронной цифровой. подписи в электронном документе, информационная система общего пользования,
19. Корпоративная информационная система.
20. Особенности зарубежного законодательства в области информационной безопасности.
21. Текущее состояние российского законодательства в области информационной безопасности.
22. Оценочные стандарты и технические спецификации. Основные понятия.
23. Какими двумя основным критериям оценивается степень доверия?
24. Механизмы безопасности.
25. Классы безопасности.
26. Информационная безопасность распределенных систем. Рекомендации х.800.
27. Сервисы безопасности и исполняемые ими роли.
28. Сетевые механизмы безопасности.
29. Администрирование средств безопасности.
30. Стандарт iso/iec 15408 «критерии оценки безопасности информационных технологий» основные понятия.
31. Классы функциональных требований «оранжевой книги».
32. Требования доверия безопасности.
33. Европейские критерии информационной безопасности.
34. Интерпретация «оранжевой книги» для сетевых конфигураций.
35. Руководящие документы гостехкомиссии России в области информационной безопасности.

Пример теста для контроля знаний обучающихся

1. Создание помех для нормальной работы канала передачи связи, то есть нарушение работоспособности канала связи возникает:

а) со стороны злоумышленника;

б) со стороны законного отправителя сообщения;

в) со стороны законного получателя сообщения.

2. Какие алгоритмы используют один и тот же ключ для шифрования и дешифровки?
а) асимметричный;
б) **симметричный;**
в) правильного ответа нет.

3. Процесс нахождения открытого сообщения соответственно заданному закрытому при неизвестном криптографическом преобразовании называется:
а) шифрование;
б) дешифровка;
в) расшифровка.

4. В каких основных форматах существует симметричный алгоритм?
а) блока и строки;
б) потока и блока;
в) потока и данных

5. Открытым текстом в криптографии называют:
а) расшифрованный текст;
б) любое послание;
в) исходное послание.

6. Какой ключ известен только приемнику?
а) открытый;
б) закрытый.

7. Наука, занимающаяся защитой информации, путем преобразования этой информации это:
а) Криптография;
б) криптология;
в) криптоанализ.

8. В каких шифрах результат шифрования очередного блока зависит только от него самого и не зависит от других блоков шифруемого массива данных?
а) в потоковых;
б) в блочных.

9. Шифр, который заключается в перестановках структурных элементов шифруемого блока данных – битов, символов, цифр – это:
а) шифр функциональных преобразований;
б) шифр замен;
в) шифр перестановок.

10. Функция, предназначенная для выработки блока данных, используемого для модификации шифруемого блока, из инварианта и ключевого элемента называется:
а) функция шифрования шага преобразования;
б) инвариант стандартного шага шифрования.

11. Шифрование-это:
а) процесс создания алгоритмов шифрования;

б) процесс сжатия информации;
в) процесс криптографического преобразования информации к виду, когда ее смысл полностью теряется.

12. В каком случае построение цифровой подписи не требует наличия в системе третьего лица – арбитра, занимающегося аутентификацией?
а) при шифровании с помощью асимметричного алгоритма;
б) при шифровании с помощью симметричного алгоритма;
в) арбитр необходим всегда.

13. Можно ли отнести слабую аутентификацию к проблемам безопасности?
а) нет;
б) да;
в) в редких случаях.

14. Возможно ли расшифровывать информацию без знания ключа?
а) нет;
б) да;
в) в редких случаях.

15. Возможно ли вычислить закрытый ключ ассиметричного алгоритма, зная открытый?
а) нет;
б) да;
в) в редких случаях.

16. Характерная черта алгоритма Эль-Гамаля состоит в:
а) протоколе передачи подписанного сообщения, позволяющего подтверждать подлинность отправителя;
б) в точной своевременной передаче сообщения;
в) алгоритм не имеет особенностей и идентичен RSA.

17. Аутентификацией называют:
а) процесс регистрации в системе;
б) способ защиты системы;
в) процесс распознавания и проверки подлинности заявлений о себе пользователей и процессов.

18. Аутентификация бывает:
а) Статическая;
б) устойчивая;
в) постоянная;
г) все варианты правильные;
д) правильного варианта нет.

19. Стойкость ключа характеризуется
а) Длинной;
б) непредсказуемостью;
в) все варианты правильные;
г) правильного варианта нет.

20. Условие, при котором в распоряжении аналитика находиться возможность получить результат зашифровки для произвольно выбранного им зашифрованного сообщения размера n используется в анализе:

а) на основе произвольно выбранного шифротекста;
б) на основе произвольно выбранного открытого текста;
в) на основе только шифротекста.

21. Условие, при котором в распоряжении аналитика находится возможность получить результат зашифровки для произвольно выбранного им *массива открытых данных* размера n используется в анализе:

а) на основе произвольно выбранного шифротекста;
б) на основе произвольно выбранного открытого текста;
в) правильного ответа нет.

Вопросы к зачету

Зачёт проходит в форме контрольного задания и 2 вопросов, представляющих различные разделы дисциплины.

1. Государственные органы власти, обеспечивающие защиту информации в России.
2. Основные федеральные законы в области защиты информации.
3. Технология двухфакторной аутентификации.
4. Идентификация в вычислительной системе.
5. Циклические коды.
6. Недостатки систем хеширования.
7. Способы защиты информации.
8. Стратегии защиты информации.
9. Периметр охраняемой территории.
10. «Абсолютная» система защиты.
11. Понятие информационной безопасности
12. Что такое защита информации?
13. Основные составляющие информационной безопасности
14. Что понимается под доступностью?
15. Что понимают под целостностью информационных ресурсов?
16. Что такое конфиденциальность?
17. Важность и сложность проблемы информационной безопасности.
18. Сущность объектно-ориентированного подхода.
19. Инкапсуляция при объектно-ориентированном подходе.
20. Наследование при объектно-ориентированном подходе
21. Полиморфизм при объектно-ориентированном подходе
22. Грани объекта при объектно-ориентированном подходе
23. Уровень детализации при объектно-ориентированном подходе.
24. Компонент и контейнер компонент.
25. Применение объектно-ориентированного подхода к рассмотрению защищаемых систем.
26. Недостатки традиционного подхода к информационной безопасности с объектной точки зрения.

Примерные задачи к зачету

1. Используя алгоритмы двойной перестановки строк и столбцов выполнить шифрование следующих фраз (ключ выбирать самостоятельно, номер варианта выбрать по номеру в списке группы):

1. Он досрочно завалил экзамен.
2. Закон суров, но это закон.
3. Умному легче доказать, что он дурак.

2. Используя алгоритмы двойной перестановки строк и столбцов выполнить дешифрование шифрограмм, приведенные в таблице 1 (номер варианта выбрать по последней цифре номера шифра). В шифротексте следует обратить внимание на наличие пробелов в тексте, длина текста по всем вариантам равняется 25 символам:

Таблица 1

Номер вар-та	Шифротекст	Ключ 1	Ключ 2
	В ОН, Т ОЭЗКНОА УОРСЗКНОА	КРУТО	СТУЖА
	ЗВАОЛИ ЛАН ОДОРОНЧСАЧТЕЗ	ВЕСНА	ОСЕНЬ
	ПАЙРДЕЕЖ М ЧЕДАТУМЬДУПОМ	ОСЕНЬ	ДОСУГ

Примеры контрольной работы

В 1

Используя шифр многоалфавитной замены шифровать фразу (исключив пробелы и знаки препинания), используя в качестве ключа «Ключ 1». Для шифрования использовать алфавит замены из таблицы.

В 2

Используя шифр многоалфавитной замены дешифровать фразу, используя «Ключ» (шифрограммы и ключи приведены в таблице).

Примеры домашнего задания

1. Используя алгоритм Диффи-Хелмана сгенерируйте ключ для симметричного алгоритма криптографии.

2. Сгенерировать открытый и закрытый ключи для алгоритма RSA. Передать открытый ключ следующему по списку студенту.

Таблица простых чисел в интервале [1; 200] приведена в таблице 2.

3. Выбрать последовательность цифр для шифрования. Выполнить шифрование последовательности цифр, используя свой закрытый ключ.

Передать шифрограмму адресату (следующему по списку студенту).

4. Произвести дешифрование полученного сообщения от другого студента, используя полученный от него открытый ключ.

Замечание: Некоторые простейшие ключи для алгоритма RSA представлены в таблице 4.

Таблица.2

Таблица простых чисел от 1 до 200

1	2	3	5	7	11	13	17	19	23
29	31	37	41	43	47	53	59	61	67

71	73	79	83	89	97	101	103	107	109
113	127	131	137	139	149	151	157	163	167
173	179	181	191	193	197	199			

Таблица 3

Последовательность цифр для шифрования

Варианты заданий (последняя цифра номера варианта)									
1	2	3	4	5	6	7	8	9	0
4 7 8 9 5 6	5 9 8 2 7 4	8 5 4 9 7 3	9 7 2 8 5 6	7 2 6 5 9 3	6 4 8 9 3 7	2 7 5 3 8 4	7 6 5 2 4 3	4 7 5 9 3 8	8 1 5 6 3 4

Таблица 4

Простейшие ключи для алгоритма RSA

№ пп	Открытый ключ	Закрытый ключ	№ пп	Открытый ключ	Закрытый ключ	№ пп	Открытый ключ	Закрытый ключ
1	(35,21)	(11,21)	8	(35,35)	(11,35)	15	(35,221)	(11,221)
2	(15,15)	(7,15)	9	(77,77)	(53,77)	16	(35,247)	(179,247)
3	(35,119)	(11,119)	10	(35,91)	(35,91)	17	(35,323)	(107,323)
4	(21,33)	(21,33)	11	(35,161)	(83,161)	18	(35,437)	(215,437)
5	(15,85)	(47,85)	12	(35,133)	(71,133)	19	(15,391)	(47,391)
6	(35,65)	(11,65)	13	(77,209)	(173,209)	20	(35,299)	(83,299)
7	(21,55)	(21,55)	14	(21,187)	(61,187)	21	(15,69)	(3,69)

Приложение 1.

СИСТЕМА РЕЙТИНГОВОЙ ОЦЕНКИ И КОНТРОЛЯ ЗНАНИЙ СТУДЕНТОВ

№ п/п	СТРУКТУРА	Баллы по каждому модулю
1.	Оценка за активное участие в учебном процессе и посещение занятий: Всех занятий Не менее 75% Не менее 50% Не менее 25% Итого:	 5 4 3 2 до 5
2.	устный опрос в форме собеседования (УО-1) письменный опрос в виде теста (ПР-1) письменная контрольная работа (ПР-2) письменная работа в форме реферата (ПР-4) Итого:	15 10 10 10 45
3.	Зачёт	50
	ВСЕГО:	100

Пересчет на 5 балльную систему

2 (неудовлетворительно)	3 (удовлетворительно)	4 (хорошо)	5 (отлично)
< 50	**50-64**	**65-84**	**85-100**

Язык преподавания: русский.

Автор программы: д.т.н., профессор, профессор Высшей школы управления и инноваций МГУ имени М.В. Ломоносова О.А. Косоруков.