МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
БАШКИРСКИЙ ИНСТИТУТ ТЕХНОЛОГИЙ И УПРАВЛЕНИЯ (ФИЛИАЛ)
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕХНОЛОГИЙ И УПРАВЛЕНИЯ ИМЕНИ К.Г. РАЗУМОВСКОГО (ПЕРВЫЙ КАЗАЧИЙ УНИВЕРСИТЕТ)»
(БИТУ (филиал) ФГБОУ ВО «МГУТУ им. К.Г. Разумовского (ПКУ)»)

Кафедра «Информационные технологии и системы управления»

«Утверждаю»
Директор БИТУ (филиал)
ФГБОУ ВО «МГУТУ
им. К.Г. Разумовского (ПКУ)»
_____Е.В. Кузнецова
«06» февраля 2020 г.

Рабочая программа дисциплины

Б1.О.02.08 – Информационная безопасность

Направление подготовки 09.03.01 Информатика и вычислительная техника

Направленность (профиль) подготовки Программное обеспечение вычислительной техники и автоматизированных систем в пищевой промышленности и отраслях агропромышленного комплекса

Квалификация выпускника – бакалавр

Форма обучения очно-заочная

Мелеуз 2020 г.

Рабочая программа дисциплины **«Информационная безопасность»** разработана на основании федерального государственного образовательного стандарта высшего образования по направлению подготовки **09.03.01 Информатика и вычислительная техника**, утвержденного приказом Министерства образования и науки Российской Федерации от 19 сентября 2017г. №929 «Об утверждении федерального государственного образовательного стандарта высшего образования по направлению подготовки 09.03.01 Информатика и вычислительная техника», учебного плана по основной профессиональной образовательной программе высшего образования «**Программное обеспечение вычислительной техники и автоматизированных систем в пищевой промышленности и отраслях агропромышленного комплекса**».

Рабочая программа дисциплины разработана группой в составе:
к.т.н. Колязов К.А., к.п.н. Одинокова Е.В., к.ф.-м.н. Смирнов Д.Ю., к.п.н. Тучкина Л.К., к.п.н. Яшин Д.Д., ст. преподаватель Остапенко А.Е.

Руководитель основной профессиональной образовательной программы
кандидат физико-математических наук, доцент _____ Д.Ю. Смирнов
(подпись)

Рабочая программа дисциплины обсуждена и утверждена на заседании кафедры «Информационные технологии и системы управления»
Протокол № 7 от «05» февраля 2020 года

И.о. заведующего кафедрой
к.п.н., доцент _____ Е.В. Одинокова
(подпись)

Оглавление

1. Цели и задачи дисциплины

Цель – ознакомить обучающихся с правовыми основами защиты информации, организационными методами защиты информации, математическими методами, лежащими в основе защиты информации.

Задачи:

- ознакомления обучающихся с мерами и мероприятиями, обеспечивающими безопасность информации и информационных систем;
- рассмотреть основные подходы к защите информации;
- ознакомить обучающихся с наиболее широко применимыми видами технических и программных средств защиты информации.

2. Место дисциплины в структуре ОПОП

Дисциплина Б1.О.02.08 «Информационная безопасность» относится к дисциплинам по выбору вариативной части ОПОП по направлению **09.03.01 Информатика и вычислительная техника** (бакалавриат), профиль «**Автоматизированные системы обработки информации и управления**».

В качестве «входных» знаний дисциплины используются знания и умения, полученные обучающимися при изучении дисциплин: Программирование, Информационные технологии, Интернет-технологии.

Дисциплина может являться предшествующей при изучении дисциплин: Проектирование автоматизированных информационных систем для предприятий пищевой промышленности и отраслей агропромышленного комплекса, Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты.

3. Требования к результатам освоения дисциплины:

Процесс изучения дисциплины направлен на формирование следующих компетенций:

ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

Знать: правовые основы защиты информации и сведений, составляющих коммерческую и государственную тайну; международные стандарты информационного обмена; задачи и способы построения системы защиты данных; методологию проектирования защищенных информационных систем, методы и программные средства защиты данных; организационное обеспечение систем защиты информации; алгоритмы и стандарты криптографической защиты данных.

Уметь: оценивать степень защищенности информационных систем, в том числе сетей и операционных систем, осуществлять выбор программных средств защиты от несанкционированного доступа, осуществлять выбор аппаратных средств защиты от несанкционированного доступа, применять современные алгоритмы и программные средства защиты, в том числе обнаруживать сетевые атаки и противодействовать им.

Владеть: терминологией, принятой в профессиональном сообществе, математическими методами и алгоритмами, составляющими основу дисциплины, типовыми программными продуктами, позволяющими обеспечивать безопасность информации и информационных систем.

Код и описание компетенции	Планируемые результаты обучения по дисциплине
ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;	ОПК-3.1 Знает принципы информационной и библиографической культуры, методы и средства решения стандартных задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
	ОПК-3.2 Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
	ОПК-3.3 Владеет методами поиска и анализа информации для подготовки документов, обзоров, рефератов, докладов, публикаций, на основе информационной и библиографической культуры с учетом соблюдения авторского права и требований информационной безопасности

4. Объем дисциплины и виды учебной работы (разделяется по формам обучения)

Очно-заочная форма обучения

Вид учебной работы	Всего часов / зач. ед.	Семестры
		8
Аудиторные занятия (контактная работа)	**32**	32
В том числе:		
Лекции	**8**	8
Практические занятия (ПЗ)	**12**	12
Семинары (С)		
Лабораторные работы (ЛР)	**12**	12
Самостоятельная работа	**76**	76
Вид промежуточной аттестации:		экзамен
Контроль	**36**	36
Общая трудоемкость (часов)	**144**	144
зачетных единиц	**4**	4

для обучающихся по индивидуальному учебному плану количество часов контактной и самостоятельной работы устанавливается индивидуальным учебным планом[1].

[1] для обучающихся по индивидуальному учебному плану - учебному плану, обеспечивающему освоение соответствующей образовательной программы на основе индивидуализации ее содержания с учетом особенностей и образовательных потребностей конкретного обучающегося (в том числе при ускоренном обучении, для обучающихся с ограниченными возможностями здоровья и инвалидов, для лиц, зачисленных для продолжения обучения в соответствии с частью 5 статьи 5 Федерального закона от 05.05.2014 №84-ФЗ «Об особенностях правового регулирования отношений в сфере образования в связи с принятием в Российскую Федерацию Республики Крым и образованием в составе Российской Федерации

Дисциплина реализуется посредством проведения учебных занятий (включая проведение текущего контроля успеваемости и промежуточной аттестации обучающихся). В соответствии с рабочей программой и тематическим планом изучение дисциплины проходит в форме контактной работы обучающихся с преподавателем и самостоятельной работы обучающихся. При реализации дисциплины предусмотрена аудиторная контактная работа и внеаудиторная контактная работа посредством электронной информационно-образовательной среды. Учебный процесс в аудитории осуществляется в форме лекций и практических занятий. В лекциях раскрываются основные темы изучаемого курса, которые входят в рабочую программу. На практических занятиях более подробно изучается программный материал в плоскости отработки практических умений и навыков и усвоения тем. Внеаудиторная контактная работа включает в себя проведение текущего контроля успеваемости (тестирование) в электронной информационно-образовательной среде.

5. Содержание дисциплины

5.1. Содержание разделов и тем дисциплины

Тема 1. Общие вопросы информационной безопасности (ОПК-3)

Основные понятия и определения. Понятия информация, информатизация, информационная система, информационная безопасность. Понятия автора и собственника информации, взаимодействие субъектов в информационном обмене. Защита информации, тайна, средства защиты информации.

Тема 2. Государственная система информационной безопасности (ОПК-3)

Структура государственной системы информационной безопасности. Структура законодательной базы по вопросам информационной безопасности. Лицензирование и сертификация в области защиты информации. Место информационной безопасности экономических систем в национальной безопасности страны, опасности страны.

Тема 3. Угрозы безопасности (ОПК-3)

Понятие угрозы. Виды противников или «нарушителей». Классификация угроз информационной безопасности. Виды угроз. Основные нарушения Характер происхождения угроз (умышленные и естественные факторы). Источники угроз. Предпосылки появления угроз. Классы каналов несанкционированного получения информации.

Тема 4. Теоретические основы методов защиты информационных систем (ОПК-3)

Основные положения теории информационной безопасности информационных систем. Модели безопасности и их применение. Формальные модели безопасности. Дискреционная модель Харрисона-Руззо-Ульмана. Типизированная матрица доступа. Модель распространения прав доступа Take-Grant. Мандатная модель БеллаЛаПадулы. Ролевая политика безопасности. Ограничения на области применения формальных моделей.

Тема 5. Методы защиты средств вычислительной техники (ОПК-3)

Использование защищенных компьютерных систем. Аппаратные и программные средства для защиты компьютерных систем от НСД. Средства операционной системы. Средства резервирования данных. Проверка целостности. Способы и средства восстановления работоспособности.

Тема 6. Основы криптографии (ОПК-3)

Методы криптографии. Симметричное и асимметричное шифрование. Алгоритмы шифрования. Электронно-цифровая подпись. Алгоритмы электронно-цифровой подписи.

новых субъектов - Республики Крым и города федерального значения Севастополя и о внесении изменений в Федеральный закон «Об образовании в Российской Федерации»).

Хеширование. Имитовставки. Криптографические генераторы случайных чисел. Способы распространения ключей. Обеспечиваемая шифром степень защиты. Криптанализ и атаки на криптосистемы.

Тема 7. Алгоритмы и привязки программного обеспечения к аппаратному окружению (ОПК-3)

Индивидуальные параметры вычислительной системы. Блок проверки аппаратного окружения. Дискета как средство привязки. Технология HASP, эмуляторы. Временные метки и запись в реестр. Обеспечение требуемого количества запусков (trial version). Технология spyware. Виды распространения программного обеспечения. Шифрование и запутывание исполняемого кода.

Тема 8. Алгоритмы безопасности в компьютерных сетях (ОПК-3)

Межсетевые экраны. Проектирование МЭ. Снифферы. Эксплоиты. Атаки на сервера. Атаки на рабочие станции. Атака типа «отказ в обслуживании». Протоколирование. Сетевые защищенные протоколы.

5.2 Разделы дисциплины и междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами

№ п/п	Наименование обеспечиваемых (последующих) дисциплин	№ разделов и тем данной дисциплины, необходимых для изучения обеспечиваемых (последующих) дисциплин							
1.	Проектирование автоматизированных информационных систем	1	2	3	4	5	6	7	8
2.	Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	1	2	3	4	5	6	7	8

5.3. Разделы и темы дисциплины и виды занятий

№ п/п	Наименование темы	Виды занятий в часах				
		Лекции	Прак. занятия	Лаб. работы	СРС	Всего
1.	Общие вопросы информационный безопасности	1	2	2	9	14
2.	Государственная система информационной безопасности	1	1	1	10	13
3.	Угрозы безопасности	1	1	1	10	13
4.	Теоретические основы методов защиты информационных систем	1	1	1	10	13
5.	Методы защиты средств вычислительной техники	1	1	1	10	13
6.	Основы криптографии	1	2	2	9	14
7.	Алгоритмы и привязки программного обеспечения к аппаратному окружению	1	2	2	9	14
8.	Алгоритмы безопасности в компьютерных сетях	1	2	2	9	14

* часы занятий, проводимые в активной и интерактивной формах

Формы учебных занятий с использованием активных и интерактивных технологий обучения

№	Наименование разделов (тем), *в которых используются активные и/или интерактивные образовательные технологии*	Образовательные технологии
1.	Общие вопросы информационный безопасности	Лекция-визуализация
2.	Государственная система информационной безопасности	Лекция-визуализация
3.	Угрозы безопасности	Лекция-визуализация
4.	Теоретические основы методов защиты информационных систем	Лекция-визуализация
5.	Методы защиты средств вычислительной техники	Лекция-визуализация
6.	Основы криптографии	Лекция-визуализация
7.	Алгоритмы и привязки программного обеспечения к аппаратному окружению	Лекция-визуализация
8.	Алгоритмы безопасности в компьютерных сетях	Лекция-визуализация

6. Перечень лабораторных и практических работ

№ п/п	№ раздела и темы дисциплины	Наименование лабораторных работ	Трудоемкость (час.)	Оценочные средства	Формируемые компетенции
1	Тема 1	Криптографические методы защиты	4	Устный опрос, отчёт по лабораторной работе	ОПК-3
2	Тема 2	Шифрование методом IDEA	2	Устный опрос, отчёт по лабораторной работе	ОПК-3
3	Тема 3	Шифрование методом RC6	2	Устный опрос, отчёт по лабораторной работе	ОПК-3
4	Тема 4	Шифрование методом SAFER K-64	2	Устный опрос, отчёт по лабораторной работе	ОПК-3
5	Тема 5	Криптосистема Эль-Гамаля	4	Устный опрос, отчёт по лабораторной работе	ОПК-3
6	Тема 6	Шифрование методом Вернам	4	Устный опрос, отчёт по лабораторной работе	ОПК-3
7	Тема 7	Шифрование методом аналитических преобразований	4	Устный опрос, отчёт по лабораторной работе	ОПК-3
8	Тема 8	Сокрытие информации методом стеганографии	4	Устный опрос, отчёт по лабораторной работе	ОПК-3

6.1. План самостоятельной работы студентов

№ п/п	Тема	Вид самостоятельной работы	Задание	Рекомендуемая литература	Количество часов
1.	Общие вопросы информационный безопасности	Подготовка к лабораторным работам Подготовка к зачету	Проработать теоретический материал к зачету, оформить отчёт по лабораторной работе	Осн. №1-4, доп. №1-5	9
2.	Государственная система информационной безопасности	Подготовка к лабораторным работам Подготовка к зачету	Проработать теоретический материал к зачету, оформить отчёт по лабораторной работе	Осн. №1-4, доп. №1-5	10
3.	Угрозы безопасности	Подготовка к лабораторным работам Подготовка к зачету	Проработать теоретический материал к зачету, оформить отчёт по лабораторной работе	Осн. №1-4, доп. №1-5	10
4.	Теоретические основы методов защиты информационных систем	Подготовка к лабораторным работам Подготовка к зачету	Проработать теоретический материал к зачету, оформить отчёт по лабораторной работе	Осн. №1-4, доп. №1-5	10
5.	Методы защиты средств вычислительной техники	Подготовка к лабораторным работам Подготовка к зачету	Проработать теоретический материал к зачету, оформить отчёт по лабораторной работе	Осн. №1-4, доп. №1-5	10
6.	Основы криптографии	Подготовка к лабораторным работам Подготовка к зачету	Проработать теоретический материал к зачету, оформить отчёт по лабораторной работе	Осн. №1-4, доп. №1-5	9

7.	Алгоритмы и привязки программного обеспечения к аппаратному окружению	Подготовка к лабораторным работам Подготовка к зачету	Проработать теоретический материал к зачету, оформить отчёт по лабораторной работе	Осн. №1-4, доп. №1-5	9
8.	Алгоритмы безопасности в компьютерных сетях	Подготовка к лабораторным работам Подготовка к зачету	Проработать теоретический материал к зачету, оформить отчёт по лабораторной работе	Осн. №1-4, доп. №1-5	9

6.2. Методические указания по организации самостоятельной работы студентов

Для успешного обучения обучающийся должен готовиться к лекции, которая является важнейшей формой организации учебного процесса. Лекция:

- знакомит с новым учебным материалом,
- разъясняет учебные элементы, трудные для понимания,
- систематизирует учебный материал,
- ориентирует в учебном процессе.

Подготовка к лекции заключается в следующем:

- внимательно прочитайте материал предыдущей лекции,
- выясните тему предстоящей лекции (по тематическому плану, по информации лектора),
- ознакомьтесь с учебным материалом по учебнику и учебным пособиям,
- постарайтесь определить место изучаемой темы в своей профессиональной подготовке,
- запишите возможные вопросы, которые вы зададите лектору на лекции.

Подготовка к лабораторным работам:

- внимательно прочитайте материал лекций, относящихся к данному семинарскому занятию, ознакомьтесь с учебным материалом по учебнику и учебным пособиям,
- выпишите основные термины,
- в соответствии с методическим рекомендациями подготовьте первую часть отчёта по лабораторной работе – цель, задание, краткие теоретические сведения,
- определите, какие учебные элементы остались для вас неясными и постарайтесь получить на них ответ заранее (до лабораторной работы) во время текущих консультаций преподавателя,
- продумайте алгоритм или методику выполнения задания лабораторной работы.

Подготовка к промежуточной аттестации. К промежуточной аттестации необходимо готовиться целенаправленно, регулярно, систематически и с первых дней обучения по данной дисциплине. Попытки освоить дисциплину в период зачётно-экзаменационной сессии, как правило, показывают не удовлетворительные результаты.

В самом начале учебного курса познакомьтесь с рабочей программой дисциплины и другой учебно-методической документацией, включающими:

- перечень знаний и умений, которыми обучающийся должен владеть;
- тематические планы лекций и практических занятий;

- контрольные мероприятия;
- учебники, учебные пособия, а также электронные ресурсы;
- перечень вопросов (вопросов к зачету).

После этого у вас должно сформироваться чёткое представление об объеме и характере знаний и умений, которыми надо будет овладеть по дисциплине. Систематическое выполнение учебной работы на лекциях и практических занятиях позволит успешно освоить дисциплину и создать хорошую базу для прохождения промежуточной аттестации.

Методические указания по подготовке к материалам лекций

Освоить теоретический материал, найти ответы на представленные вопросы, используя конспекты лекций и предлагаемую литературу. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопросы и обратиться на текущей консультации или на ближайшей лекции за помощью к преподавателю. Каждую неделю рекомендуется отводить время для повторения пройденного материала, проверяя свои знания, умения и навыки по представленным вопросам.

Тематическое содержание разделов и вопросы для самопроверки

Раздел №1. Введение в информационные технологии

Перечень изучаемых элементов содержания

- Понятие информации как продукта информационной технологии.
- Виды информации. Количественные характеристики информации.
- Информационный ресурс и его составляющие.
- Итология. Предмет, методы и роль итологии.
- Организационная структура в области стандартизации ИТ.
- Понятие новой информационной технологии.
- Информационные технологии как система.
- Классификация информационных технологий.
- Этапы эволюции информационных технологий.

Вопросы для самопроверки

1. Рассмотреть закон о государственной тайне
2. Рассмотреть вопрос лицензировании отдельных видов деятельности
3. Изучить дифференциальное кодирование, манчестерский код.
4. Изучить дискретизация и модуляция сигналов, теорема Котельникова.
5. Изучить физическая природа тока и условия его появления.
6. Изучить преимущества и недостатки цифровой передачи данных перед аналоговой.
7. Изучить ВЧ навязывание и методы защиты от него
8. Изучить работы Ван Эйка (Wim van Eck) по перехвату изображений с мониторов
9. Изучить работы Маркуса Куна(Markus G. Kuhn) на тему перехвата изображений с ЖК экранов
10. Ознакомиться с биографией Норберта Винера
11. Ознакомиться с биографией Клода Шенона
12. Рассмотреть парадокс дней рождений
13. Рассмотреть теорему Байеса
14. Изучить основные различия между понятиями кольцо и поле
15. Изучить Алгоритм Евклида
16. Изучить Тест Ферма
17. Изучить Решето Эратосфена
18. Рассмотреть возможность применения дифференциального криптоанализа и

встречи посередине для алгоритмов симметричного шифрования с различной структурой

19. Изучить области применения ассиметричного шифрования в современном мире, рассмотреть, что отличает реальные реализации RSA от предложенного на лекции примитива
20. Изучить особенности постановки задачи выбора криптографических средств защиты информации и административные особенности применения этих средств в рамках ИС организации.
21. Рассмотреть подходы к криптоанализу и особенности программной реализации некоторых криптоаналитических алгоритмов.
22. Рассмотреть приёмы эффективной реализации симметричных шифров.
23. Изучить атаки типа SQL-injection и методы защиты от них
24. Изучить атаки типа XSS и методы защиты от них
25. Изучить атаки типа CSRF и методы защиты от них
26. Рассмотреть средства анализа сетевой активности.

Перечень вопросов к лабораторным работам

Лабораторная работа № 1. Тема: «Криптографические методы защиты».

Список вопросов:

1. Какие методы защиты информации называют криптографическими?
2. Какие группы (классы) криптографических алгоритмов Вам известны?
3. Какие криптографические методы появились первыми?

Лабораторная работа № 2. Тема: «Шифрование методом IDEA»

Список вопросов:

1. В чём заключается метод IDEA?
2. Как выглядит алгоритм его реализации?
3. В чём заключаются достоинства и недостатки метода?
4. Каковы области применения метода?

Лабораторная работа № 3. Тема: «Шифрование методом RC6»

Список вопросов:

1. В чём заключается метод RC6?
2. Как выглядит алгоритм его реализации?
3. В чём заключаются достоинства и недостатки метода?
4. Каковы области применения метода?

Лабораторная работа № 4. Тема: «Шифрование методом SAFER K-64»

Список вопросов:

1. В чём заключается метод SAFER K-64?
2. Как выглядит алгоритм его реализации?
3. В чём заключаются достоинства и недостатки метода?
4. Каковы области применения метода?

Лабораторная работа № 5. Тема: «Криптосистема Эль-Гамаля»

Список вопросов:

1. В чём заключается метод Эль-Гамаля?
2. Как выглядит алгоритм его реализации?
3. В чём заключаются достоинства и недостатки метода?
4. Каковы области применения метода?

Лабораторная работа № 6. Тема: «Шифрование методом Вернам»

Список вопросов:

1. В чём заключается метод Вернам?
2. Как выглядит алгоритм его реализации?
3. В чём заключаются достоинства и недостатки метода?

4. Каковы области применения метода?

Лабораторная работа № 7. Тема: «Шифрование методом аналитических преобразований»

Список вопросов:

1. В чём заключается метод преобразований?
2. Как выглядит алгоритм его реализации?
3. В чём заключаются достоинства и недостатки метода?
4. Каковы области применения метода?

Лабораторная работа № 8. Тема: «Сокрытие информации методом стеганографии»

Список вопросов:

1. В чём заключается метод стеганографии?
2. Как выглядит алгоритм его реализации?
3. В чём заключаются достоинства и недостатки метода?
4. Каковы области применения метода?

7. Примерная тематика курсовых работ (проектов) (при наличии)

Не предусмотрены.

8. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература *(указывается литература, изданная за последние пять лет)*

1. Информационная безопасность и защита информации: учеб. пособие / Баранова Е.К., Бабаш А.В. — 4-е изд., перераб. и доп. — М. : РИОР: ИНФРА-М, 2019. — 322 с. — (Высшее образование). // http://znanium.com/bookread2.php?book=1009606
2. Информационная безопасность компьютерных систем и сетей : учеб. пособие / В.Ф. Шаньгин. — М.: ИД «ФОРУМ»: ИНФРА-М, 2017. — 416 с. — (Профессиональное образование). // http://znanium.com/bookread2.php?book=775200
3. Информационная безопасность предприятия : учеб. пособие / Н.В. Гришина. — 2-е изд., доп. — М.: ФОРУМ: ИНФРА-М, 2017. — 239 с.: ил. — (Высшее образование: Бакалавриат). // http://znanium.com/bookread2.php?book=612572
4. Информационная безопасность: Учебное пособие / Ковалев Д.В., Богданова Е.А. - Ростов-на-Дону:Южный федеральный университет, 2016. - 74 с. // http://znanium.com/bookread2.php?book=997105

б) дополнительная литература:

1. Бирюков, А. А. Информационная безопасность: защита и нападение / А.А. Бирюков. - 2-е изд., перераб. и доп. - Москва: ДМК Пресс, 2017. - 434 с. // http://znanium.com/bookread2.php?book=1028060

2. Зашита информации: учеб. пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 3-е изд. - М.: РИОР: ИНФРА-М, 2019. - 400 с. - (Высшее образование). //http://znanium.com/bookread2.php?book=1018901

3. Информационная безопасность конструкций ЭВМ и систем: учеб. пособие / Е.В. Глинская, Н.В. Чичварин. — М.: ИНФРА-М, 2018. — 118 с. - (Высшее образование: Бакалавриат). // http://znanium.com/bookread2.php?book=925825

4. Комплексная защита информации в корпоративных системах: учеб. пособие / В.Ф. Шаньгин. — М.: ИД «ФОРУМ» : ИНФРА-М, 2018. — 592 с. — (Высшее образование: Бакалавриат). // http://znanium.com/bookread2.php?book=937502

5. Криптографическая защита информации: учеб. пособие / С.О. Крамаров, О.Ю. Митясова, С.В. Соколов [и др.]; под ред. проф. С.О. Крамарова. — М.: РИОР : ИНФРА-М, 2018. — 321 с. — (Высшее образование). // http://znanium.com/bookread2.php?book=901659

в) программное обеспечение

1. Microsoft Windows
2. Microsoft Word
3. Microsoft Excel
4. Microsoft Power Point

г) полнотекстовые базы данных

1. http://znanium.com/ ООО электронно-библиотечная система "ЗНАНИУМ"
2. https://rucont.ru/ ООО "Национальный цифровой ресурс «РУКОНТ»
3. http://biblioclub.ru/ ЭБС «Университетская библиотека онлайн»

9. Материально-техническое обеспечение дисциплины:

Наименование специальных помещений и помещений для самостоятельной работы

Лаборатория Информационных технологий Учебная аудитория для проведения занятий лекционного типа; занятий лабораторного и практического типа; для курсового проектирования (выполнения курсовых работ); для проведения групповых и индивидуальных консультаций; для текущего контроля и промежуточной аттестации.

Оснащенность специальных помещений и помещений для самостоятельной работы

Рабочие места обучающихся; Рабочее место преподавателя; Ноутбук; Проектор переносной; Экран переносной; Классная доска; 20 рабочих мест обучающихся оснащенные ПЭВМ с подключением к сети интернет и обеспечением доступа в электронную информационно-образовательную среду Университета.

10. Образовательные технологии

При реализации учебной дисциплины «Информационная безопасность» применяются различные образовательные технологии, в том числе технологии электронного обучения, используют в учебном процессе активные и интерактивные формы учебных занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

Учебные часы дисциплины «Информационная безопасность» предусматривают классическую контактную работу преподавателя с обучающимся в аудитории и контактную работу посредством электронной информационно-образовательной среды в синхронном и асинхронном режиме (вне аудитории) посредством применения возможностей компьютерных технологий (электронная почта, электронный учебник, тестирование, видеофильм, презентация и др.)

Активные методы обучения – методы, стимулирующие познавательную деятельность обучающихся, строятся в основном на диалоге, который предполагает свободный обмен мнениями о путях разрешения той или иной проблемы, они характеризуются высоким уровнем активности обучающихся. Именно такое обучение сейчас общепринято считать «наилучшей практикой обучения». Исследования показывают, что именно на активных занятиях – если они ориентированы на достижение конкретных целей и хорошо организованы – учащиеся часто усваивают материал наиболее полно и с пользой для себя. Фраза «наиболее полно и с пользой для себя» означает, что учащиеся думают о том, что они изучают, применяют это в ситуациях реальной жизни или для дальнейшего обучения и могут продолжать учиться самостоятельно.

По дисциплине « Информационная безопасность» проводятся:

- *лекция-визуализация* – передача информации посредством графического представления в образной форме (слайды, видео-слайды, плакаты и т.д.). Подготовка данной лекции преподавателем состоит в том, чтобы изменить, переконструировать учебную информацию по теме лекционного занятия в визуальную форму для представления через технические средства обучения (ноутбук, акустические системы,

экран, мультимедийный проектор) или вручную (схемы, рисунки, чертежи и т.п.). Лекцию-визуализацию рекомендуется проводить по темам, ключевым для данного предмета, раздела. При подготовке наглядных материалов следует соблюдать требования и правила, предъявляемые к представлению информации.

11. Оценочные средства (ОС):

Оценочные средства по дисциплине разработаны в соответствии с положением о балльно-рейтинговой системе оценки успеваемости студентов ФГБОУ ВО «МГУТУ им. К.Г. Разумовского (Первый казачий университет)».

Общее количество баллов за виды учебной деятельности студента, предусмотренные основной образовательной программой освоения дисциплины, должно составлять не менее 60 баллов (зачетный балл) для прохождения промежуточной аттестации.

Критерии оценки текущих занятий

- ✓ посещение студентом одного занятия – 1 балл;
- ✓ выполнение заданий для самостоятельной работы – от 1 до 3 баллов за каждый пункт задания;
- ✓ активная работа на практическом занятии – от 1 до 3 баллов

Критерии оценки тестовых заданий:

- ✓ каждое правильно выполненное задание – 1 балл

БАЛЛЬНО-РЕЙТИНГОВАЯ СИСТЕМА

Максимальная сумма рейтинговых баллов, которая может быть начислена студенту по учебной дисциплине, составляет 100 рейтинговых

Форма промежуточной аттестации	Количество баллов		
	Текущий контроль	Рубежный контроль	Сумма баллов
Зачет с оценкой	30-70	20-30	60-100

Рейтинг студента в семестре по дисциплине складывается из рейтинговых баллов, которыми преподаватель в течение семестра оценивает посещение учебных занятий, его текущую работу на занятиях и самостоятельную работу, результаты текущих контрольных работ, тестов, устных опросов, премиальных и штрафных баллов.

Рубежный рейтинг студента по дисциплине складывается из оценки в рейтинговых баллах ответа на экзамене.

Преподаватель, осуществляющий проведение практических занятий, доводит до сведения студентов на первом занятии информацию о формировании рейтинга студента и рубежного рейтинга.

По окончании семестра каждому студенту выставляется его Рейтинговая оценка текущей успеваемости, которая является оценкой посещаемости занятий, активности на занятиях, качества самостоятельной работы.

Студент допускается к мероприятиям промежуточной аттестации, если его рейтинговая оценка текущей успеваемости (без учета премиальных рейтинговых баллов) не менее 30 рейтинговых баллов.

Студенты, не набравшие минимальных рейтинговых баллов по учебной дисциплине проходят процедуру добора баллов.

Максимальная рейтинговая оценка текущей успеваемости студента за семестр по результатам текущей работы и текущего контроля знаний (без учета премиальных баллов) составляет: 70 рейтинговых баллов для дисциплин, заканчивающихся зачетом с оценкой.

Ответ студента может быть максимально оценен на экзамене в 30 рейтинговых баллов.

Студент, по желанию, может сдать зачет с оценкой в формате «автомат», если его рейтинг за семестр, с учетом премиальных баллов, составил не менее:

– 60 рейтинговых баллов с выставлением оценки «удовлетворительно»;
– 70 рейтинговых баллов с выставлением оценки «хорошо»;
– 90 рейтинговых баллов с выставлением оценки «отлично».

Рейтинговая оценка по дисциплине и соответствующая аттестационная оценка по шкале «зачтено», «удовлетворительно», «хорошо», «отлично» при использовании формата «автомат», проставляется экзаменатором в зачетную книжку и зачетно-экзаменационную ведомость только в день проведения экзамена согласно расписанию группы, в которой обучается студент.

Для приведения рейтинговой оценки к аттестационной (пятибалльный формат) используется следующая шкала:

Аттестационная оценка по дисциплине	Рейтинг студента по дисциплине (включая премиальные баллы)
«отлично»	90- 100 баллов
«хорошо»	70 - 89 баллов
«удовлетворительно»	60 - 69 баллов
«неудовлетворительно»	менее 60 баллов

Рубежный рейтинг по дисциплине у студента на экзамене менее чем в 20 рейтинговых баллов считается неудовлетворительным (независимо от рейтинга студента в семестре). В этом случае в зачетно-экзаменационную ведомость в графе «Аттестационная оценка» проставляется «неудовлетворительно».

Преподавателю предоставляется право начислять студентам премиальные баллы за активность (участие в научных конференциях, конкурсах, олимпиадах, активная работа на аудиторных занятиях, публикации статей, работа со школьниками, выполнение заданий повышенной сложности, изготовление наглядных пособий и т.д.) в количестве, не превышающем 20 рейтинговых баллов за семестр. Премиальные баллы не входят в сумму рейтинга текущей успеваемости студента, а прибавляются к ним.

11.1. Оценочные средства для входного контроля

Типовые тестовые задания

1. *Заражение компьютерными вирусами может произойти в процессе:*
   a. работы с файлами
   b. форматирования дискеты
   c. выключения компьютера
   d. печати на принтере
2. *Для проверки на вирус жесткого диска необходимо иметь:*
   a. защищенную программу
   b. загрузочную программу
   c. файл с антивирусной программой
   d. дискету с антивирусной программой, защищенную от записи
3. *Программа, не являющаяся антивирусной:*
   a. AVP
   b. Defrag
   c. Norton Antivirus
   d. Dr Web
4. *Класс программ, не относящихся к антивирусным:*
   a. программы-фаги
   b. программы сканирования
   c. программы-ревизоры
   d. программы-детекторы
5. *Способ появления вируса на компьютере:*

a. перемещение с гибкого диска
b. при решении математической задачи
c. при подключении к компьютеру модема
d. самопроизвольно

6. *Заражению компьютерными вирусами могут подвергнуться:*
a. графические файлы
b. программы и документы
c. звуковые файлы
d. видеофайлы

7. *Для проверки на вирус жесткого диска необходимо иметь:*
a. защищенную программу
b. загрузочную программу
c. файл с антивирусной программой
d. дискету с антивирусной программой, защищенную от записи

8. *Заражение компьютерными вирусами может произойти в процессе:*
   a. работы с файлами
   b. форматирования дискеты
   c. выключения компьютера
   d. печати на принтере

9. *Для проверки на вирус жесткого диска необходимо иметь:*
   a. защищенную программу
   b. загрузочную программу
   c. файл с антивирусной программой
   d. дискету с антивирусной программой, защищенную от записи

10. *Программа, не являющаяся антивирусной:*
    a. AVP
    b. Defrag
    c. Norton Antivirus
    d. Dr Web

11. *Класс программ, не относящихся к антивирусным:*
    a. программы-фаги
    b. программы сканирования
    c. программы-ревизоры
    d. прогаммы-детекторы

11.2. Оценочные средства текущего контроля

Материалы для проведения текущего и промежуточного контроля знаний студентов

Полный комплект материалов для проведения текущего и промежуточного контроля знаний и шкалы оценивания компетенций находятся в приложении к рабочей программе (в ОС)

№ п\п	Вид контроля	Контролируемые темы (разделы)	Компетенции, компоненты которых контролируются
1.	**Устный опрос** - один из основных методов получения аудиторских доказательств, включающий беседу со всеми студентами.	Тема 1. Общие вопросы информационной безопасности. Тема 2. Государственная система информационной безопасности. Тема 3. Угрозы безопасности Тема 4. Теоретические основы методов защиты информационных	ОПК-3

		систем. Тема 5. Методы защиты средств вычислительной техники. Тема 6. Основы криптографии. Тема 7. Алгоритмы и привязки программного обеспечения к аппаратному окружению. Тема 8. Алгоритмы безопасности в компьютерных сетях.	
2.	**Собеседование** *(опрос по контрольным вопросам к лабораторным работам и лекциям)* - фронтальная форма контроля, представляющая собой ответы на вопросы преподавателя в устной форме	Тема 1. Общие вопросы информационной безопасности. Тема 2. Государственная система информационной безопасности. Тема 3. Угрозы безопасности Тема 4. Теоретические основы методов защиты информационных систем. Тема 5. Методы защиты средств вычислительной техники. Тема 6. Основы криптографии. Тема 7. Алгоритмы и привязки программного обеспечения к аппаратному окружению. Тема 8. Алгоритмы безопасности в компьютерных сетях.	ОПК-3
3.	**Отчет по лабораторным работам** - форма контроля, предусматривающая изложение и анализ знаниевых компонентов, методик исследования, этапов и результатов осуществления действий и операций по теме работе, представление и обоснование выводов по работе, факторный анализ результатов, формулирование предложений, ответы на вопросы преподавателя по теме работы. Отчет по лабораторной работе осуществляется ведущему преподавателю, предоставляется оформленная по установленному плану работы и представляет собой наглядную демонстрацию умений и	Тема 1. Общие вопросы информационной безопасности. Тема 2. Государственная система информационной безопасности. Тема 3. Угрозы безопасности Тема 4. Теоретические основы методов защиты информационных систем. Тема 5. Методы защиты средств вычислительной техники. Тема 6. Основы криптографии. Тема 7. Алгоритмы и привязки программного обеспечения к аппаратному окружению. Тема 8. Алгоритмы безопасности в компьютерных сетях. Представить оформленный отчет по результатам выполнения лабораторных работ (согласно типовой структуре лабораторной работы); объяснить знаниевые компоненты, этапы и результаты осуществления действий и операций по теме работе; продемонстрировать манипуляции на компьютере.	ОПК-3

	владений знаниями на компьютере, направленный на проверку уровня практических знаний, их соответствия нормам и стандартам.	**Типовая структура лабораторной работы** 1. Цель и задачи лабораторной работы 2. Результаты проведенной работы 3. Заключение по лабораторной работе. 4. Отчет проведенной работы в виде скриншотов	
4.	**Вопросы к зачёту** – вопросы для подготовки к промежуточной аттестации в виде устного ответа на вопрос	Тема 1. Общие вопросы информационной безопасности. Тема 2. Государственная система информационной безопасности. Тема 3. Угрозы безопасности Тема 4. Теоретические основы методов защиты информационных систем. Тема 5. Методы защиты средств вычислительной техники. Тема 6. Основы криптографии. Тема 7. Алгоритмы и привязки программного обеспечения к аппаратному окружению. Тема 8. Алгоритмы безопасности в компьютерных сетях.	ОПК-3

Примерные задания для устного опроса

№ раздела/тем	Внеаудиторная работа
1. Правовые основы информационной безопасности в Российской Федерации	Рассмотреть: 1. Закон о государственной тайне 2. О лицензировании отдельных видов деятельности
2.Физические основы передачи информации	Изучить: 1. Дифференциальное кодирование, манчестерский код. 2. Дискретизация и модуляция сигналов, теорема Котельникова. 3. Физическая природа тока и условия его появления. 4. Преимущества и недостатки цифровой передачи данных перед аналоговой.
3.Технические средства защиты информации	Изучить: 1. ВЧ навязывание и методы защиты от него 2. Работы Ван Эйка (Wim van Eck) по перехвату изображений с мониторов 3. Работы Маркуса Куна(Markus G. Kuhn) на тему перехвата изображений с ЖК экранов
4.История технологий шифрования	Ознакомиться с биографиями: 1. Норберта Винера 2. Клода Шенона
5.Модульная	Рассмотреть:

арифметика	1. Парадокс дней рождений 2. Теорему Байеса
6.Элементы коммутативной алгебры	Изучить основные различия между понятиями кольцо и поле
7.Элементы элементарной теории чисел	Изучить: 1. Алгоритм Евклида 2. Тест Ферма 3. Решето Эратосфена
8.Алгоритмы симметричного шифрования	Рассмотреть возможность применения дифференциального криптоанализа и встречи посередине для алгоритмов симметричного шифрования с различной структурой
9.Алгоритмы ассиметричного шифрования	Изучить области применения ассиметричного шифрования в современном мире, рассмотреть, что отличает реальные реализации RSA от предложенного на лекции примитива
10.Использование шифрования в системах защиты информации	Изучить особенности постановки задачи выбора криптографических средств защиты информации и административные особенности применения этих средств в рамках ИС организации.
11.Особенности программной реализации криптоаналитических алгоритмов	Рассмотреть подходы к криптоанализу и особенности программной реализации некоторых криптоаналитических алгоритмов.
12.Особенности программной реализации алгоритмов шифрования	Рассмотреть приёмы эффективной реализации симметричных шифров.
13.Уязвимости интернет страниц	Изучить атаки типа 1. SQL-injection 2. XSS 3. CSRF и методы защиты от них
14.Сетевая безопасность	Рассмотреть средства анализа сетевой активности.

Перечень вопросов к лабораторным работам

Лабораторная работа № 1. Тема: «Криптографические методы защиты».

Список вопросов:

1. Какие методы защиты информации называют криптографическими?
2. Какие группы (классы) криптографических алгоритмов Вам известны?
3. Какие криптографические методы появились первыми?

Лабораторная работа № 2. Тема: «Шифрование методом IDEA»

Список вопросов:

1. В чём заключается метод IDEA?
2. Как выглядит алгоритм его реализации?
3. В чём заключаются достоинства и недостатки метода?
4. Каковы области применения метода?

Лабораторная работа № 3. Тема: «Шифрование методом RC6»

Список вопросов:

1. В чём заключается метод RC6?
2. Как выглядит алгоритм его реализации?
3. В чём заключаются достоинства и недостатки метода?
4. Каковы области применения метода?

Лабораторная работа № 4. Тема: «Шифрование методом SAFER K-64»

Список вопросов:

1. В чём заключается метод SAFER K-64?
2. Как выглядит алгоритм его реализации?
3. В чём заключаются достоинства и недостатки метода?
4. Каковы области применения метода?

Лабораторная работа № 5. Тема: «Криптосистема Эль-Гамаля»

Список вопросов:

1. В чём заключается метод Эль-Гамаля?
2. Как выглядит алгоритм его реализации?
3. В чём заключаются достоинства и недостатки метода?
4. Каковы области применения метода?

Лабораторная работа № 6. Тема: «Шифрование методом Вернам»

Список вопросов:

1. В чём заключается метод Вернам?
2. Как выглядит алгоритм его реализации?
3. В чём заключаются достоинства и недостатки метода?
4. Каковы области применения метода?

Лабораторная работа № 7. Тема: «Шифрование методом аналитических преобразований»

Список вопросов:

1. В чём заключается метод преобразований?
2. Как выглядит алгоритм его реализации?
3. В чём заключаются достоинства и недостатки метода?
4. Каковы области применения метода?

Лабораторная работа № 8. Тема: «Сокрытие информации методом стеганографии»

Список вопросов:

1. В чём заключается метод стеганографии?
2. Как выглядит алгоритм его реализации?
3. В чём заключаются достоинства и недостатки метода?
4. Каковы области применения метода?

11.3. Оценочные средства для промежуточной аттестации (в форме зачёта с оценкой)

Код компетенции	**Содержание компетенции (части компетенции)**	**Результаты обучения**	**Уровни формирования компетенций**
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационн	Компетенции не сформированы. Знания современных инструментальных средств и технологий программирования, а также принципов и методов разработки компонентов аппаратно-программных комплексов и баз данных не сформированы.	Недостаточный уровень
		Компетенции сформированы. Сформированы базовые знания	Пороговый уровень

	ой и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	современных инструментальных средств и технологий программирования, а также принципов и методов разработки компонентов аппаратно-программных комплексов и баз данных. Демонстрируется низкий уровень сформированных навыков разработки компонентов аппаратно-программных комплексов и баз данных.	
		Компетенции сформированы. Имеются знания современных инструментальных средств и технологий программирования, а также принципов и методов разработки компонентов аппаратно-программных комплексов и баз данных. Демонстрируется высокий уровень сформированных навыков разработки компонентов аппаратно-программных комплексов и баз данных.	Продвинутый уровень
		Компетенции сформированы. Базовые знания современных инструментальных средств и технологий программирования, а также принципов и методов разработки компонентов аппаратно-программных комплексов и баз данных твердые аргументированные, всесторонние. Демонстрируется высокий уровень сформированных навыков разработки компонентов аппаратно-программных комплексов и баз данных при выполнении заданий практики.	Высокий уровень

Примерный перечень вопросов и заданий к зачету

1. Государственная политика в сфере обеспечения безопасности. Концепция национальной безопасности РФ.
2. Государственная политика в сфере обеспечения информационной безопасности. Доктрина информационной безопасности РФ.
3. Методы обеспечения информационной безопасности России.
4. Источники угроз информационной безопасности России.
5. Виды угроз информационной безопасности России.
6. Правовые методы обеспечения информационной безопасности России.
7. Права человека и информационная безопасность.
8. Ответственность за посягательство на информацию в сфере экономической деятельности.
9. Нормативно-правовые акты РФ по защите государственной тайны. Основные положения закона «О государственной тайне».
10. Роль ФАПСИ, ФСБ, ФСТЭК в обеспечении информационной безопасности России.
11. Определения ТСПИ и ТКУИ.
12. Способы перехвата информации передаваемой ТСПИ.
13. Достоинства и недостатки акустических закладок, в зависимости от их

принадлежности к определённому классу (классификация акустических закладок).
14. Методы выявления акустических закладок, в зависимости от класса
15. Шифр Цезаря, простой биграммной замены, самоключ Вижинера, квадраты Кардано.
16. Определение понятий код, номенклатор, открытый текст, шифры замены и перестановки, много- и одно- алфавитные шифры замены, криптоанализ, криптология.
17. Роль Джованни Порта, Этьена Базери, Блеза Виженера, Кергоффса, Клода Шенона, Уитфилда Диффи и Мартина Хеллмана в становлении крптографии.
18. Что означает формулировка числа a и b сравнимы по модулю N
19. Множество значений оператора mod N(т.е. понимать, что это за множество)
20. Какие свойства определяют группы и кольца
21. Образующая группы
22. Циклическая группа
23. Поле
24. Функция Эйлера и как вычислить её значение
25. Формулировка Малой теоремы Ферма
26. Алгоритм Евклида
27. Расширенный алгоритм Евклида
28. Формулировка китайской теоремы об остатках
29. Тест Ферма
30. Псевдопростые числа по определённому основанию
31. Решето Эратосфена
32. Теорема Котельникова-Найквиста
33. Принципы проводной передачи данных
34. Принципы беспроводной передачи данных
35. Симметричный алгоритм шифрования
36. Рассеивание и полнота
37. Режимы шифрования
38. Сеть Фейстеля и SP-блоки
39. Вычислительно необратимые функции
40. Какие существуют атаки на алгоритмы шифрования
41. Запас криптостойкости
42. Понятие раунда шифрования
43. Симметричный алгоритм шифрования
44. Рассеивание и полнота
45. Режимы шифрования
46. Определение длинны излучающей антенны
47. Высокочастотное навязывание и методы защиты от него
48. Сеть Фейстеля и SP-блоки
49. Вычислительно необратимые функции
50. Какие существуют атаки на алгоритмы шифрования
51. Запас криптостойкости
52. Понятие раунда шифрования
53. Понятие открытого и закрытого ключа
54. Что такое ассиметричное шифрование, и в каких областях оно используется
55. Алгоритм RSA
56. Виды и способы защиты от XSS атак
57. Виды и способы защиты от CSRF атак
58. Произведение Монтгомери

12. Организация образовательного процесса для лиц с ограниченными возможностями

Организация образовательного процесса для лиц с ограниченными возможностями осуществляется в соответствии с «Методическими рекомендациями по организации образовательного процесса для инвалидов и лиц с ограниченными возможностями здоровья в образовательных организациях высшего образования, в том числе оснащенности образовательного процесса» Министерства образования и науки РФ от 08.04.2014г. № АК-44/05вн.

В образовательном процессе используются социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе.

Студенты с ограниченными возможностями здоровья, в отличие от остальных студентов, имеют свои специфические особенности восприятия, переработки материала. Подбор и разработка учебных материалов производится с учетом индивидуальных особенностей.

Предусмотрена возможность обучения по индивидуальному графику, при составлении которого возможны различные варианты проведения занятий: в академической группе и индивидуально, на дому с использованием дистанционных образовательных технологий.

13. Лист регистрации изменений

№ п/п	Содержание изменения	Реквизиты документа об утверждении изменения	Дата введения изменения
1.			
2.			
3.			
4.			
5.			