МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ

"БРАТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ"

УТВЕРЖДАЮ

Проректор по учебной работе

_____ Е.И.Луковникова

18 сентября 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.12 Основы информационной безопасности сетей и систем

Закреплена за кафедрой **Управления в технических системах**

Учебный план b110302_21_МТС.plx
Направление: 11.03.02 Инфокоммуникационные технологии и системы связи

Квалификация **Бакалавр**

Форма обучения **очная**

Общая трудоемкость **5 ЗЕТ**

Виды контроля в семестрах:
Контрольная работа 8, Экзамен 8

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	8 (4.2)		Итого	
Недель	12			
Вид занятий	УП	РП	УП	РП
Лекции	36	36	36	36
Лабораторные	24	24	24	24
Практические	24	24	24	24
В том числе инт.	14	14	14	14
Итого ауд.	84	84	84	84
Контактная работа	84	84	84	84
Сам. работа	60	60	60	60
Часы на контроль	36	36	36	36
Итого	180	180	180	180

Программу составил(и):
к.т.н., ст.пр., Ульянов А.Д. _____

Рабочая программа дисциплины

Основы информационной безопасности сетей и систем

разработана в соответствии с ФГОС:

Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 11.03.02 Инфокоммуникационные технологии и системы связи (приказ Минобрнауки России от 19.09.2017 г. № 930)

составлена на основании учебного плана:

Направление: 11.03.02 Инфокоммуникационные технологии и системы связи
утвержденного приказом ректора от 01.03.2021 протокол № 80.

Рабочая программа одобрена на заседании кафедры

Управления в технических системах

Протокол от 09 апреля 2021 г. № 9

Срок действия программы: 2021 - 2025 уч.г.

Зав. кафедрой Игнатьев И.В. _____

Председатель МКФ

старший преподаватель Латушкина С.В. №8 20 апреля 2021 г. _____

Ответственный за реализацию ОПОП _____ Игнатьев И.В.
(подпись) (ФИО)

Директор библиотеки _____ Сотник Ф.Ф.
(подпись) (ФИО)

№ регистрации 339
(методический отдел)

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	Формирование у обучаемых знаний в области основ информационной безопасности и навыков практического обеспечения защиты информации и безопасного использования про граммных и аппаратных средств в сетях и системах связи.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП	
Цикл (раздел) ООП:	Б1.В.12
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Информатика
2.1.2	Информационные технологии телекоммуникаций
2.1.3	Направляющие среды электросвязи
2.1.4	Сетевые технологии высокоскоростной передачи данных
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Выполнение и защита выпускной квалификационной работы
2.2.2	Производственная (преддипломная) практика

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
ПК-6: Способен оценивать параметры безопасности и защиты программного обеспечения и сетевых устройств администрируемой сети с помощью специальных средств управления безопасностью	
Индикатор 1	ПК-6.1. Знает архитектуру, протоколы и общие принципы функционирования аппаратных, программных и программно¬аппаратных средств администрируемой сети
Индикатор 2	ПК-6.2. Знает основные принципы, протоколы и программные криптографические средства обеспечения информационной безопасности сетевых устройств
Индикатор 3	ПК-6.3. Умеет применять программные, аппаратные и программно-аппаратные средствазащиты сетевых устройств от несанкционированного доступа
Индикатор 4	ПК-6.4. Пользоваться нормативно¬технической документацией в области обеспечения информационной безопасности инфокоммуникационных технологий
Индикатор 5	ПК-6.5. Владеет навыками и средствами установки и управления специализированными программными средствами защиты сетевых устройств администрируемой сети от несанкционированного доступа

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	Основы цифровой вычислительной техники, структуры и функционирование локальных вычислительных сетей и глобальной сети Интернет.
3.2	**Уметь:**
3.2.1	Оценивать основные проблемы, связанные с эксплуатацией и внедрением новой телекоммуникационной техники.
3.3	**Владеть:**
3.3.1	Навыками отладки с использованием соответствующих отладочных средств программного обеспечения сигнальных процессов и микроконтроллеров.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Вид занятия	Наименование разделов и тем	Семестр / Курс	Часов	Компетен-ции	Литература	Инте ракт.	Примечание
	Раздел	**Раздел 1. Введение в информационную безопасность**						
1.1	Лек	Понятие информационной безопасности	8	1	ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1	1	Лекция беседа, ПК-6.1. ПК-6.2. ПК-6.3. ПК-6.4. ПК-6.5
1.2	Лек	Основные составляющие информационной безопасности	8	2	ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1	1	Лекция беседа, ПК-6.1. ПК-6.2. ПК-6.3. ПК-6.4. ПК-6.5

1.3	Лек	Важность и сложность проблемы информационной безопасности	8	1	ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1	1	Лекция беседа, ПК-6.1. ПК-6.2. ПК-6.3. ПК-6.4. ПК-6.5
1.4	Лек	Основные определения и критерии классификации угроз	8	2	ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1	1	Лекция беседа, ПК-6.1. ПК-6.2. ПК-6.3. ПК-6.4. ПК-6.5
1.5	Лек	Некоторые примеры угроз доступности	8	1	ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-6.1. ПК-6.2. ПК-6.3. ПК-6.4. ПК-6.5
1.6	Лек	Вредоносное программное обеспечение	8	2	ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-6.1. ПК-6.2. ПК-6.3. ПК-6.4. ПК-6.5
1.7	Лек	Основные угрозы целостности	8	1	ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-6.1. ПК-6.2. ПК-6.3. ПК-6.4. ПК-6.5
1.8	Лек	Основные угрозы конфиденциальности	8	2	ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-6.1. ПК-6.2. ПК-6.3. ПК-6.4. ПК-6.5
1.9	Ср	Подготовка к экзамену	8	20	ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-6.1. ПК-6.2. ПК-6.3. ПК-6.4. ПК-6.5
1.10	Экзамен		8	10	ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-6.1. ПК-6.2. ПК-6.3. ПК-6.4. ПК-6.5
	Раздел	**Раздел 2. Уровни информационной безопасности**						
2.1	Лек	Законодательный уровень информационной безопасности	8	1	ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-6.1. ПК-6.2. ПК-6.3. ПК-6.4. ПК-6.5
2.2	Лек	Обзор российского законодательства в области информационной безопасности	8	2	ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-6.1. ПК-6.2. ПК-6.3. ПК-6.4. ПК-6.5
2.3	Лек	Обзор зарубежного законодательства в области информационной безопасности	8	1	ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-6.1. ПК-6.2. ПК-6.3. ПК-6.4. ПК-6.5
2.4	Лек	Административный уровень информационной безопасности	8	1	ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-6.1. ПК-6.2. ПК-6.3. ПК-6.4. ПК-6.5
2.5	Лек	Политика безопасности	8	1	ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-6.1. ПК-6.2. ПК-6.3. ПК-6.4. ПК-6.5
2.6	Лек	Программа безопасности	8	1	ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-6.1. ПК-6.2. ПК-6.3. ПК-6.4. ПК-6.5
2.7	Лек	Синхронизация программы безопасности с жизненным циклом систем	8	1	ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-6.1. ПК-6.2. ПК-6.3. ПК-6.4. ПК-6.5

2.8	Лек	Процедурный уровень информационной безопасности	8	1	ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-6.1. ПК-6.2. ПК-6.3. ПК-6.4. ПК-6.5
2.9	Лек	Управление персоналом	8	1	ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-6.1. ПК-6.2. ПК-6.3. ПК-6.4. ПК-6.5
2.10	Лек	Физическая защита	8	1	ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-6.1. ПК-6.2. ПК-6.3. ПК-6.4. ПК-6.5
2.11	Лек	Поддержание работоспособности	8	1	ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-6.1. ПК-6.2. ПК-6.3. ПК-6.4. ПК-6.5
2.12	Лек	Реагирование на нарушения режима безопасности	8	1	ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-6.1. ПК-6.2. ПК-6.3. ПК-6.4. ПК-6.5
2.13	Лек	Планирование восстановительных работ	8	1	ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-6.1. ПК-6.2. ПК-6.3. ПК-6.4. ПК-6.5
2.14	Ср	Подготовка к экзамену	8	20	ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-6.1. ПК-6.2. ПК-6.3. ПК-6.4. ПК-6.5
2.15	Экзамен		8	10	ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-6.1. ПК-6.2. ПК-6.3. ПК-6.4. ПК-6.5
	Раздел	**Раздел 3. Основные программно-технические меры информационной безопасности сетей и систем**						
3.1	Лек	Основные понятия программно-технического уровня информационной безопасности	8	1	ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-6.1. ПК-6.2. ПК-6.3. ПК-6.4. ПК-6.5
3.2	Лек	Особенности современных информационных систем, существенные с точки зрения безопасности	8	1	ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-6.1. ПК-6.2. ПК-6.3. ПК-6.4. ПК-6.5
3.3	Лек	Идентификация и аутентификация	8	1	ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-6.1. ПК-6.2. ПК-6.3. ПК-6.4. ПК-6.5
3.4	Лек	Архитектурная безопасность	8	1	ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-6.1. ПК-6.2. ПК-6.3. ПК-6.4. ПК-6.5
3.5	Лек	Управление доступом	8	0,5	ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-6.1. ПК-6.2. ПК-6.3. ПК-6.4. ПК-6.5
3.6	Лек	Протоколирование и аудит	8	0,5	ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-6.1. ПК-6.2. ПК-6.3. ПК-6.4. ПК-6.5
3.7	Лек	Активный аудит	8	0,5	ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-6.1. ПК-6.2. ПК-6.3. ПК-6.4. ПК-6.5

3.8	Лек	Шифрование	8	0,5	ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-6.1. ПК-6.2. ПК-6.3. ПК-6.4. ПК-6.5
3.9	Лек	Контроль целостности	8	0,5	ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-6.1. ПК-6.2. ПК-6.3. ПК-6.4. ПК-6.5
3.10	Лек	Экранирование	8	0,5	ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-6.1. ПК-6.2. ПК-6.3. ПК-6.4. ПК-6.5
3.11	Лек	Анализ защищенности	8	0,5	ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-6.1. ПК-6.2. ПК-6.3. ПК-6.4. ПК-6.5
3.12	Лек	Обеспечение высокой доступности	8	0,5	ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-6.1. ПК-6.2. ПК-6.3. ПК-6.4. ПК-6.5
3.13	Лек	Основы мер обеспечения высокой доступности	8	0,5	ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-6.1. ПК-6.2. ПК-6.3. ПК-6.4. ПК-6.5
3.14	Лек	Отказоустойчивость и зона риска	8	0,5	ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-6.1. ПК-6.2. ПК-6.3. ПК-6.4. ПК-6.5
3.15	Лек	Программное обеспечение промежуточного слоя	8	0,5	ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-6.1. ПК-6.2. ПК-6.3. ПК-6.4. ПК-6.5
3.16	Лек	Обеспечение обслуживаемости	8	0,5	ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-6.1. ПК-6.2. ПК-6.3. ПК-6.4. ПК-6.5
3.17	Лаб	Программирование арифметических алгоритмов	8	5	ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1	1	Работа в малых группах, ПК-6.1. ПК-6.2. ПК-6.3. ПК-6.4. ПК-6.5
3.18	Лаб	Программирование алгебраических алгоритмов	8	5	ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1	1	Работа в малых группах, ПК-6.1. ПК-6.2. ПК-6.3. ПК-6.4. ПК-6.5
3.19	Лаб	Защита от закладок при разработке программ	8	5	ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1	1	Работа в малых группах, ПК-6.1. ПК-6.2. ПК-6.3. ПК-6.4. ПК-6.5
3.20	Лаб	Программирование алгоритмов криптосистем с открытым ключом	8	5	ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1	1	Работа в малых группах, ПК-6.1. ПК-6.2. ПК-6.3. ПК-6.4. ПК-6.5

3.21	Лаб	Профилактика заражения вирусами компьютерных систем	8	4	ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1	2	Работа в малых группах, ПК-6.1. ПК-6.2. ПК-6.3. ПК-6.4. ПК-6.5
3.22	Пр	Криптографические методы защиты	8	4	ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1	1	Работа в малых группах, ПК-6.1. ПК-6.2. ПК-6.3. ПК-6.4. ПК-6.5
3.23	Пр	Шифрование методом IDEA	8	4	ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1	1	Работа в малых группах, ПК-6.1. ПК-6.2. ПК-6.3. ПК-6.4. ПК-6.5
3.24	Пр	Шифрование методом RC6	8	4	ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1	1	Работа в малых группах, ПК-6.1. ПК-6.2. ПК-6.3. ПК-6.4. ПК-6.5
3.25	Пр	Шифрование методом Джиффорда	8	4	ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1	1	Работа в малых группах, ПК-6.1. ПК-6.2. ПК-6.3. ПК-6.4. ПК-6.5
3.26	Пр	Шифрование методом аналитических преобразований	8	4	ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-6.1. ПК-6.2. ПК-6.3. ПК-6.4. ПК-6.5
3.27	Пр	Сокрытие информации методом стеганографии	8	4	ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-6.1. ПК-6.2. ПК-6.3. ПК-6.4. ПК-6.5
3.28	Контр.раб.	Информационная безопасность сетей и систем	8	6	ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-6.1. ПК-6.2. ПК-6.3. ПК-6.4. ПК-6.5
3.29	Ср	Подготовка к экзамену	8	20	ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-6.1. ПК-6.2. ПК-6.3. ПК-6.4. ПК-6.5
3.30	Экзамен		8	10	ПК-6	Л1.1 Л1.2Л2.1 Л2.2 Э1	0	ПК-6.1. ПК-6.2. ПК-6.3. ПК-6.4. ПК-6.5

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Традиционная (репродуктивная) технология (преподаватель знакомит обучающихся с порядком выполнения задания, наблюдает за выполнением и при необходимости корректирует работу обучающихся)

Образовательные технологии с использованием активных методов обучения (лекция – беседа, лекция – дискуссия, проблемная лекция, лекция-визуализация, лекция с заранее запланированными ошибками, лекция – пресс-конференция, лекция с разбором конкретных ситуаций, лекция-консультация, занятия с применением затрудняющих условий, методы группового решения творческих задач, метод развивающейся кооперации)

Технология компьютерного обучения(использование в учебном процессе компьютерных технологий и предоставляемых ими возможностях (электронные библиотеки, онлайн тесты, практические задания и т.д.))

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Контрольные вопросы и задания

Контрольные вопросы:
1. В чем главный принцип стенографии?
2. В каких «контейнерах» может быть спрятано зашифрованное сообщение?
3. Привести примеры стеганографии древних времён.
4. Дать определение аналитическим преобразованиям.
5. В каких случаях могут быть использованы аналитические преобразования?
6. К какой информации этот вид шифрования может быть применим?
7. Принцип действия метода шифрования Джиффорда?
8. Для каких целей использовался данный метода шифрования?
9. В каком году он был взломан?.
10. Что является входной информацией для шифра RC6?
11. Сколько нужно циклов шифрования для достаточной степени сокрытия информации?
12. На сколько блоков делиться входная информация?
13. Что является входной информацией для шифра IDEA?
14. Сколько нужно циклов шифрования для достаточной степени сокрытия информации?
15. На сколько блоков делиться входная информация?
16. Что такое шифрование?
17. Чем отличается открытый ключ от закрытого?
18. Дать определение стеганографии.

6.2. Темы письменных работ

Тема контрольной работы : Информационная безопасность сетей и систем.

Цель: Развить навыки студентов по использованию приобретённых знаний в ответах на конкретные вопросы.

Структура: Каждое индивидуальное задание предполагает ответ студента на десять вопросов по 5 темам:
- Основные понятия информационной безопасности.
- Правовое обеспечение защиты информации
- Организационное обеспечение защиты информации
- Инженерно-техническое обеспечение защиты информации
- Программно-аппаратные методы защиты информации

Основная тематика: Информационная безопасность сетей и систем.

Рекомендуемый объем: Пояснительная записка объемом 15 - 20 страниц должна содержать титульный лист, задание, ответ на заданные вопросы, список используемой литературы.

6.3. Фонд оценочных средств

Вопросы к экзамену:

Раздел 1. Введение в информационную безопасность
1. Понятие и основные составляющие информационной безопасности.
2. Важность и сложность проблемы информационной безопасности.
3. Основные определения и критерии классификации угроз.
4. Наиболее распространенные угрозы доступности.
5. Вредоносное программное обеспечение.
6. Угрозы целостности.
7. Угрозы конфиденциальности.

Раздел 2. Уровни информационной безопасности
8. Что такое законодательный уровень информационной безопасности и почему он важен.
9. Обзор российского законодательства в области информационной безопасности.
10. Обзор зарубежного законодательства в области информационной безопасности.
11. Политика безопасности.
12. Программа безопасности.
13. Синхронизация программы безопасности с жизненным циклом инфокоммуникационных систем.
14. Управление рисками.
15. Основные классы мер процедурного уровня.
16. Управление персоналом.
17. Физическая защита.
18. Поддержание работоспособности.
19. Реагирование на нарушения режима безопасности.
20. Планирование восстановительных работ.

Раздел 3. Основные программно-технические меры информационной безопасности сетей и систем
21. Основные понятия программно-технического уровня информационной безопасности.
22. Особенности современных информационных систем, существенные с точки зрения безопасности.
23. Архитектурная безопасность.
24. Основные понятия об идентификации и аутентификации.

25.	Парольная аутентификация.
26.	Идентификация/ аутентификация с помощью биометрических данных.
27.	Управление доступом.
28.	Ролевое управление доступом.
29.	Основные понятия протоколирования и аудита.
30.	Активный аудит.
31.	Симметричное и ассиметричное шифрование.
32.	Контроль целостности: хэш-функции и электронно-цифровая подпись.
33.	Экранирование: основные понятия и архитектурные аспекты.
34.	Классификация межсетевых экранов.
35.	Анализ защищенности.
36.	Основные понятия доступности.
37.	Основы мер обеспечения высокой доступности.
38.	Отказоустойчивость и зона риска.
39.	Обеспечение обслуживаемости.

6.4. Перечень видов оценочных средств

Отчеты по лабораторным работам, контрольная работа, экзаменацинные билеты

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1. Рекомендуемая литература

7.1.1. Основная литература

	Авторы,	Заглавие	Издательство,	Кол-во	Эл. адрес
Л1.1	Иванов М.Ю.	Информационные технологии: методы криптографии: учебное пособие	Братск: БрГУ, 2010	1	http://ecat.brstu.ru/catalog/Учебные%20и%20учебно-методические%20пособия/Информатика%20-%20Вычислительная%20техника%20-%20Программирование/Иванов%20М.Ю.%20Информационные%20технологии.Методы%20криптографии.2010.pdf
Л1.2	Нестеров С. А.	Основы информационной безопасности: учебное пособие	Санкт-Петербург: Издательство Политехническо го университета, 2014	1	http://biblioclub.ru/index.php?page=book&id=363040

7.1.2. Дополнительная литература

	Авторы,	Заглавие	Издательство,	Кол-во	Эл. адрес
Л2.1	Девянин П.Н.	Модели безопасности компьютерных систем. Управление доступом и информационными потоками: учебное пособие	Москва: Горячая линия-Телеком, 2012	5	
Л2.2	Малюк А.А., Пазизин С.В., Погожин Н.С.	Введение в защиту информации в автоматизированных системах: учебное пособие	Москва: Горячая линия-Телеком, 2011	5	

7.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Издательство "Лань" электронно-библиотечная система	http://e.lanbook.com

7.3.1 Перечень программного обеспечения

7.3.1.1	Microsoft Windows Professional 7 Russian Upgrade Academic OPEN No Level
7.3.1.2	Microsoft Office 2007 Russian Academic OPEN No Level
7.3.1.3	Microsoft Office Professional Plus 2010 Russian Academic OPEN 1 license No Level
7.3.1.4	Microsoft Windows (Win Pro 10)+

7.3.2 Перечень информационных справочных систем

7.3.2.1	Национальная электронная библиотека НЭБ
7.3.2.2	Университетская информационная система РОССИЯ (УИС РОССИЯ)
7.3.2.3	
7.3.2.4	Научная электронная библиотека eLIBRARY.RU
7.3.2.5	Информационная система "Единое окно доступа к образовательным ресурсам"

7.3.2.6	Электронная библиотека БрГУ
7.3.2.7	Электронный каталог библиотеки БрГУ
7.3.2.8	«Университетская библиотека online»
7.3.2.9	Издательство "Лань" электронно-библиотечная система

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

1230	Лаборатория УТС	Лабораторный комплекс «Локальные сети ЭВМ» .Телевизор LG 47. Учебная мебель

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Материал лекции учитывается при подготовке к лабораторным занятиям.
Для освоения обучающимися дисциплины и достижения запланированных результатов обучения. Учебным планом предусмотрены лекции, лабораторные работы, практические занятия, самостоятельная работа студента, выполнение контрольной работы, подготовка и сдача экзамена. В условиях рейтинговой системы контроля результаты текущего оценивания студента используются как показатель его текущего рейтинга.
Текущий контроль успеваемости осуществляется в течение семестра, в ходе повседневной учебной работы. Данный вид контроля стимулирует у обучающегося стремление к систематической самостоятельной работе по изучения дисциплины.
Обучающийся, пользуясь рабочей программой, основной и дополнительной литературой, сам организует процесс изучения дисциплины.
Самостоятельная работа способствует сознательному усвоению, углублению и расширению теоретических знаний; форматирует необходимые профессиональные умения и навыки и совершенствует имеющиеся; происходит более глубокое осмысление методов научного и творческого познания конкретной дисциплины.
Основными формами такой работы являются:
- конспектирование лекций и прочитанного источника;
- проработка материалов прослушанной лекции;
- самостоятельное изучение программных вопросов, указанных преподавателем на лекциях и выполнение домашних заданий;
- обзор и обобщение литературы по интересующему вопросу;
- подготовка к лабораторным занятиям, практическим занятиям, выполнение контрольной работы и экзамену.