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

31 мая 20 21 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.06 Информационная безопасность

Закреплена за кафедрой **Информатики, математики и физики**

Учебный план b090302_21_ИСиТ.plx
Направление: 09.03.02 Информационные системы и технологии

Квалификация **Бакалавр**

Форма обучения **очная**

Общая трудоемкость **4 ЗЕТ**

Виды контроля в семестрах:
Зачет 8

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	8 (4.2)		Итого	
Недель	9			
Вид занятий	УП	РП	УП	РП
Лекции	18	18	18	18
Лабораторные	45	45	45	45
В том числе инт.	12	12	12	12
Итого ауд.	63	63	63	63
Контактная работа	63	63	63	63
Сам. работа	54	54	54	54
Часы на контроль	27	27	27	27
Итого	144	144	144	144

Программу составил(и):
к.т.н., доц., Фигура К.Н. _____

Рабочая программа дисциплины

Информационная безопасность

разработана в соответствии с ФГОС:

Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 09.03.02 Информационные системы и технологии (приказ Минобрнауки России от 19.09.2017 г. № 926)

составлена на основании учебного плана:

Направление: 09.03.02 Информационные системы и технологии
утвержденного приказом ректора от 01.03.2021 протокол № 80.

Рабочая программа одобрена на заседании кафедры

Информатики, математики и физики

Протокол от 16.04. 2021 г. № 9

Срок действия программы: 2021-2025 уч.г.

Зав. кафедрой Горохов Д.Б.

Председатель МКФ

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

Ответственный за реализацию ОПОП _____ Д.Б. Горохов
(подпись) (ФИО)

Директор библиотеки Сошт Сотник Л.П.
(подпись) (ФИО)

№ регистрации 222
(методический отдел)

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	Получение устойчивых знаний и навыков по построению защищенных информационных систем. Усвоение основных принципов по аудиту информационной безопасности информационных систем, обнаружению и устранению потенциальных уязвимостей.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП	
Цикл (раздел) ООП:	Б1.В.06
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Архитектура корпоративных информационных систем
2.1.2	Проектирование информационных систем
2.1.3	Системное администрирование
2.1.4	Методы и технологии разработки клиент-серверных приложений
2.1.5	Серверные технологии
2.1.6	Сетевое администрирование
2.1.7	Web-программирование
2.1.8	Программирование
2.1.9	Базы данных
2.1.10	Технологии программирования
2.1.11	Инфокоммуникационные системы и сети
2.1.12	Архитектура ЭВМ
2.1.13	Информационные и автоматизированные системы
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	Основы процессов внедрения информационных систем

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
ПК-5: Способность управлять безопасностью сетевых устройств и программного обеспечения, проводить контроль производительности сетевой инфраструктуры инфокоммуникационной системы	
Индикатор 1	ПК-5.1 Выполняет работы по управлению безопасностью сетевых устройств и программного обеспечения администрируемой сети.
Индикатор 2	ПК-5.2 Осуществляет контроль производительности сетевой инфраструктуры инфокоммуникационной системы с использованием штатных и внешних программно-аппаратных средств контроля.

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	базовые направления обеспечения информационной безопасности предприятия; современные программные средства, в том числе отечественного производства, при решении задач обеспечения необходимого уровня информационной безопасности;
3.1.2	технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации.
3.2	**Уметь:**
3.2.1	разрабатывать способы защиты информации, и меры противодействия несанкционированному доступу к источникам конфиденциальной информации;
3.2.2	использовать современные ИТ и программные средства, при анализе защищенности ИС предприятия.
3.3	**Владеть:**
3.3.1	методологией построения средств противодействия угрозам;
3.3.2	методами и приемами разработки концептуальных моделей информационной безопасности предприятия.

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. Основные понятия и принципы информационной безопасности**						

1.1	Лек	Основные понятия в области безопасности автоматизированных систем	8	2	ПК-5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2	0	ПК-5.1, ПК-5.2
1.2	Лек	Угрозы безопасности автоматизированных систем	8	2	ПК-5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2	0	ПК-5.1, ПК-5.2
1.3	Ср	Основные понятия в области безопасности автоматизированных систем	8	4	ПК-5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2	0	ПК-5.1, ПК-5.2
1.4	Ср	Угрозы безопасности автоматизированных систем	8	4	ПК-5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2	0	ПК-5.1, ПК-5.2
1.5	Зачёт	Подготовка к зачету	8	2	ПК-5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2	0	ПК-5.1, ПК-5.2
1.6	Зачёт		8	4	ПК-5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2	0	ПК-5.1, ПК-5.2
	Раздел	**Раздел 2. Правовые основы обеспечения безопасности автоматизированных систем**						
2.1	Лек	Правовые основы обеспечения безопасности автоматизированных систем	8	2	ПК-5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2	0	ПК-5.1, ПК-5.2
2.2	Ср	Правовые основы обеспечения безопасности автоматизированных систем	8	6	ПК-5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2	0	ПК-5.1, ПК-5.2
2.3	Зачёт	Подготовка к зачету	8	1	ПК-5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2	0	ПК-5.1, ПК-5.2
2.4	Зачёт		8	2	ПК-5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2	0	ПК-5.1, ПК-5.2

	Раздел	**Раздел 3. Обеспечение безопасности информационных систем**						
3.1	Лек	Технологии аутентификации, авторизации и управления доступом	8	2	ПК-5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2	0	ПК-5.1, ПК-5.2
3.2	Лаб	Получение паролей с помощью специальных программных средств	8	4	ПК-5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2	0	ПК-5.1, ПК-5.2
3.3	Ср	Технологии аутентификации, авторизации и управления доступом	8	8	ПК-5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2	0	ПК-5.1, ПК-5.2
3.4	Лек	Технология безопасности на основе анализа трафика	8	2	ПК-5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2	2	Лекция-дискуссия, ПК-5.1, ПК-5.2
3.5	Лаб	Фильтрация трафика маршрутизатором (на примере маршрутизаторов Cisco)	8	2	ПК-5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2	2	case-study (анализ конкретных ситуаций, ситуационный анализ), ПК-5.1, ПК-5.2
3.6	Лаб	Настройка файервола (в программном пакете Cisco packet tracer)	8	2	ПК-5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2	2	case-study (анализ конкретных ситуаций, ситуационный анализ), ПК-5.1, ПК-5.2
3.7	Лаб	Технология трансляции сетевых адресов (NAT)	8	2	ПК-5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2	2	case-study (анализ конкретных ситуаций, ситуационный анализ), ПК-5.1, ПК-5.2
3.8	Лаб	Настройка системы обнаружения вторжений (IPS) в пакете Cisco Packet Tracer	8	8	ПК-5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2	0	ПК-5.1, ПК-5.2
3.9	Ср	Технология безопасности на основе анализа сетевого трафика	8	8	ПК-5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2	0	ПК-5.1, ПК-5.2

3.10	Ср	Настройка файервола	8	4	ПК-5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2	0	ПК-5.1, ПК-5.2
3.11	Ср	Настройка системы обнаружения вторжений	8	4	ПК-5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2	0	ПК-5.1, ПК-5.2
3.12	Лаб	Туннелирование трафика (технология сетей VPN) в программном пакете Cisco Packet Tracer	8	8	ПК-5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2	0	ПК-5.1, ПК-5.2
3.13	Ср	Туннелирование трафика (технология сетей VPN)в программном пакете Cisco Packet Tracer	8	4	ПК-5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2	0	ПК-5.1, ПК-5.2
3.14	Зачёт	Подготовка к зачету	8	2	ПК-5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2	0	ПК-5.1, ПК-5.2
3.15	Зачёт		8	8	ПК-5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2	0	ПК-5.1, ПК-5.2
	Раздел	**Раздел 4. Основы криптографии**						
4.1	Лаб	Шифр Цезаря	8	2	ПК-5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2	0	ПК-5.1, ПК-5.2
4.2	Лаб	Шифрование с помощью перестановочного шифра	8	2	ПК-5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2	0	ПК-5.1, ПК-5.2
4.3	Лаб	Аффиное шифрование с помощью модульной арифметики	8	2	ПК-5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2	0	ПК-5.1, ПК-5.2
4.4	Лаб	Подстановочный шифр	8	2	ПК-5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2	0	ПК-5.1, ПК-5.2

4.5	Лаб	Шифр Виженера	8	2	ПК-5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2	0	ПК-5.1, ПК-5.2
4.6	Лаб	Одноразовые шифроблокноты	8	2	ПК-5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2	0	ПК-5.1, ПК-5.2
4.7	Лаб	Шифрование с открытым ключом	8	4	ПК-5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2	2	case-study (анализ конкретных ситуаций, ситуационный анализ), ПК-5.1, ПК-5.2
4.8	Зачёт	Подготовка к зачету	8	2	ПК-5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2	0	ПК-5.1, ПК-5.2
4.9	Зачёт		8	8	ПК-5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2	0	ПК-5.1, ПК-5.2
	Раздел	**Раздел 5. Аудит информационной безопасности**						
5.1	Лек	Методология тестирования на проникновение	8	2	ПК-5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2	2	Лекция-дискуссия, ПК-5.1, ПК-5.2
5.2	Лек	Получение отпечатка исследуемой системы и сбор информации	8	2	ПК-5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2	0	ПК-5.1, ПК-5.2
5.3	Лек	Методы сканирования и уклонения	8	2	ПК-5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2	0	ПК-5.1, ПК-5.2
5.4	Лек	Сканирование уязвимостей	8	2	ПК-5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2	0	ПК-5.1, ПК-5.2
5.5	Лаб	Сканирование системы и поиск уязвимостей	8	3	ПК-5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2	0	ПК-5.1, ПК-5.2

5.6	Ср	Аудит информационной безопасности	8	4	ПК-5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2	0	ПК-5.1, ПК-5.2
5.7	Зачёт	Подготовка к зачету	8	1	ПК-5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2	0	ПК-5.1, ПК-5.2
5.8	Зачёт		8	5	ПК-5	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2	0	ПК-5.1, ПК-5.2

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Образовательные технологии с использованием интерактивных методов обучения (круглый стол (дискуссия, дебаты), семинар - исследование, семинар «Пресс – антипресс», мозговой штурм (брейнсторм, мозговая атака), деловые, имитационные, операционные и ролевые игры, case-study (анализ конкретных ситуаций, ситуационный анализ), мастер класс, дидактические игры)

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 дистанционного обучения (получение образовательных услуг без посещения университета, с помощью современных систем телекомму-никации (электронная почта, Интернет и др.))

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

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

Задания для лабораторных работ

Лабораторная работа №1 Получение паролей с помощью специальных программных средств
Изучить методы получения паролей с помощью специальных программных средств

Лабораторная работа №2 Фильтрация трафика маршрутизатором (на примере маршрутизаторов Cisco)
Изучить методы фильтрации трафика маршрутизатором (на примере маршрутизаторов Cisco)

Лабораторная работа №3 Настройка файервола (в программном пакете Cisco packet tracer)
Изучить настройку файервола (в программном пакете Cisco packet tracer)

Лабораторная работа №4 Технология трансляции сетевых адресов (NAT)
Изучить технологию трансляции сетевых адресов (NAT)

Лабораторная работа №5 Настройка системы обнаружения вторжений (IPS) в пакете Cisco Packet Tracer
Изучить настройку системы обнаружения вторжений (IPS) в пакете Cisco Packet Tracer

Лабораторная работа №6 Туннелирование трафика (технология сетей VPN) в программном пакете Cisco Packet Tracer
Изучить туннелирование трафика (технология сетей VPN) в программном пакете Cisco Packet Tracer

Лабораторная работа №7 Шифр Цезаря
Изучить шифр Цезаря

Лабораторная работа №8 Шифрование с помощью перестановочного шифра
Изучить шифрование с помощью перестановочного шифра

Лабораторная работа №9 Аффиное шифрование с помощью модульной арифметики
Изучить аффиное шифрование с помощью модульной арифметики

Лабораторная работа №10 Подстановочный шифр
Изучить подстановочный шифр

Лабораторная работа №11 Шифр Виженера
Изучить шифр Виженера

Лабораторная работа №12 Одноразовые шифроблокноты
Изучить одноразовые шифроблокноты

Лабораторная работа №13 Шифрование с открытым ключом
Изучить шифрование с открытым ключом

Лабораторная работа №14 Сканирование системы и поиск уязвимостей
Изучить методы сканирования системы и поиска уязвимостей

6.2. Темы письменных работ

Учебным планом не предусмотрено

6.3. Фонд оценочных средств

Вопросы к зачету

Раздел №1 Основные понятия и принципы информационной безопасности
1. Определение безопасности автоматизированных систем;
2. Информация и информационные ресурсы;
3. Субъекты информационных отношений, их безопасность;
4. Цель защиты автоматизированной системы и циркулирующей в ней информации;
5. Уязвимость основных структурно-функциональных элементов распределенных автоматизированных систем;
6. Угрозы безопасности информации, автоматизированных систем и субъектов информационных отношений;
7. Классификация угроз безопасности;
8. Классификация каналов проникновения в автоматизированную систему и утечки информации;
9. Защищаемая информация;
10. Лицензирование;

Раздел №2 Правовые основы обеспечения безопасности автоматизированных систем
11. Сертификация средств защиты информации и аттестация объектов информатизации;
12. Специальные требования и рекомендации по технической защите конфиденциальной информации;
13. Юридическая значимость электронных документов с электронной подписью;
14. Ответственность за нарушения в сфере защиты информации;
15. Структура государственной системы защиты информации;

Раздел №3 Обеспечение безопасности информационных систем
11. Сертификация средств защиты информации и аттестация объектов информатизации;
12. Специальные требования и рекомендации по технической защите конфиденциальной информации;
13. Юридическая значимость электронных документов с электронной подписью;
14. Ответственность за нарушения в сфере защиты информации;
15. Структура государственной системы защиты информации;
16. Организация защиты информации в системах и средствах информатизации и связи;
17. Технология управления безопасностью информации и ресурсов в автоматизированной системе;
18. Политика безопасности организации;
19. Мероприятия по созданию и обеспечению функционирования комплексной системы защиты;

Раздел №4 Основы криптографии
20. Понятие криптографии;
21. Криптография с открытым ключом;

Раздел №5 Аудит информационной безопасности
22. Назначение и методы сканирования портов;
23. Методы поиска уязвимостей;
24. Эксплуатация уязвимостей;
25. Получение отпечатка системы и методы сбора информации.

6.4. Перечень видов оценочных средств

Задания для лабораторных работ.
Отчеты по лабораторным работам.
Вопросы к зачету

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)					
7.1. Рекомендуемая литература					
7.1.1. Основная литература					
	Авторы,	Заглавие	Издательство, год	Кол-во	Эл. адрес
Л1.1	Моргунов А. В.	Информационная безопасность: учебно-методическое пособие	Новосибирск: Новосибирский государственный технический университет, 2019	1	http://biblioclub.ru/index.php?page=book&id=576726
Л1.2	Котов Ю. А.	Криптографические методы защиты информации: шифры: учебное пособие	Новосибирск: Новосибирский государственный технический университет, 2016	1	http://biblioclub.ru/index.php?page=book&id=576379
Л1.3	Котов Ю. А.	Криптографические методы защиты информации: стандартные шифры. Шифры с открытым ключом: учебное пособие	Новосибирск: Новосибирский государственный технический университет, 2017	1	http://biblioclub.ru/index.php?page=book&id=574782
Л1.4	Кубашева Е. С., Малашкевич И. А., Чекулаева Е. Н.	Информатика и вычислительная техника. Информационная безопасность автоматизированных систем: учебно-методическое пособие	Йошкар-Ола: Поволжский государственный технологический университет, 2019	1	http://biblioclub.ru/index.php?page=book&id=562246
Л1.5	Кирпичников А. П., Хайбуллина З. М.	Криптографические методы защиты компьютерной информации: учебное пособие	Казань: Казанский научно-исследовательский технологический университет (КНИТУ), 2016	1	http://biblioclub.ru/index.php?page=book&id=560536
7.1.2. Дополнительная литература					
	Авторы,	Заглавие	Издательство, год	Кол-во	Эл. адрес
Л2.1	Дронов В. Ю., Анюшин В. В.	Информационная безопасность банковской деятельности: учебно-методическое пособие	Новосибирск: Новосибирский государственный технический университет, 2016	1	http://biblioclub.ru/index.php?page=book&id=575372
Л2.2	Басыня Е. А.	Системное администрирование и информационная безопасность: учебное пособие	Новосибирск: Новосибирский государственный технический университет, 2018	1	http://biblioclub.ru/index.php?page=book&id=575325
Л2.3	Ковалев Д. В., Богданова Е. А.	Информационная безопасность: учебное пособие	Ростов-на-Дону: Южный федеральный университет, 2016	1	http://biblioclub.ru/index.php?page=book&id=493175
7.1.3. Методические разработки					
	Авторы,	Заглавие	Издательство, год	Кол-во	Эл. адрес
Л3.1	Ищейнов В. Я.	Информационная безопасность и защита информации: теория и практика: учебное пособие	Москва|Берлин: Директ-Медиа, 2020	1	http://biblioclub.ru/index.php?page=book&id=571485
7.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"					

Э1	Открытое образование - Информационная безопасность [Электронный ресурс]. – Режим доступа: https://openedu.ru/course/ITMOUniversity/INFSEC/. – Дата доступа: 01.05.2021.	https://openedu.ru/course/ITMOUniversity/INFSEC/
Э2	Введение в кибербезопасность [Электронный ресурс]. – Режим доступа: https://stepik.org/course/61595/promo. – Дата доступа: 01.05.2021.	https://stepik.org/course/61595/promo

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	ОС Linux
7.3.1.4	Python IDLE
7.3.1.5	Microsoft Windows (Win Pro 10)+
7.3.1.6	Anaconda

7.3.2 Перечень информационных справочных систем

7.3.2.1	Издательство "Лань" электронно-библиотечная система
7.3.2.2	«Университетская библиотека online»
7.3.2.3	Электронный каталог библиотеки БрГУ
7.3.2.4	Электронная библиотека БрГУ
7.3.2.5	Информационная система "Единое окно доступа к образовательным ресурсам"

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

3125	Дисплейный класс	Учебная мебель Комплект серверного оборудования для построения технической архитектуры комплекса терминальных решений в составе терминального сервера, терминальных рабочих мест и периферии в составе: терминальный сервер Dell PowerEdge RX740XD, монитор Samsung SM493 19’’, 15 тонких клиентов SmartClient Mini PC (Intel CPU J1900 1.99GHzx4, 4GB), монитор Forgame Liquid Crystal Dispay MK27FC 27’’ 1800R 1920x1080 144 Hz, вебкамера Logitech C920 PRO), МФУ Canon i-Sensys MF 421dw, доска интерактивная сенсорная Smart Board SB480.
3125	Дисплейный класс	Учебная мебель Комплект серверного оборудования для построения технической архитектуры комплекса терминальных решений в составе терминального сервера, терминальных рабочих мест и периферии в составе: терминальный сервер Dell PowerEdge RX740XD, монитор Samsung SM493 19’’, 15 тонких клиентов SmartClient Mini PC (Intel CPU J1900 1.99GHzx4, 4GB), монитор Forgame Liquid Crystal Dispay MK27FC 27’’ 1800R 1920x1080 144 Hz, вебкамера Logitech C920 PRO), МФУ Canon i-Sensys MF 421dw, доска интерактивная сенсорная Smart Board SB480.
1001	читальный зал №3	Учебная мебель. Оборудование 15- CPU 5000/RAM 2Gb/HDD (Монитор TFT 19 LG 1953S-SF);принтер HP LaserJet P3005
3125	Дисплейный класс	Учебная мебель Комплект серверного оборудования для построения технической архитектуры комплекса терминальных решений в составе терминального сервера, терминальных рабочих мест и периферии в составе: терминальный сервер Dell PowerEdge RX740XD, монитор Samsung SM493 19’’, 15 тонких клиентов SmartClient Mini PC (Intel CPU J1900 1.99GHzx4, 4GB), монитор Forgame Liquid Crystal Dispay MK27FC 27’’ 1800R 1920x1080 144 Hz, вебкамера Logitech C920 PRO), МФУ Canon i-Sensys MF 421dw, доска интерактивная сенсорная Smart Board SB480.

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

Работа на лекциях: ведение конспекта лекционного материала для успешного использования его при подготовке к зачету, закрепления и расширения теоретических знаний. После проработки лекционного материала обучающийся должен четко владеть следующими аспектами по каждой лекции:
- знать тему;
- четко представлять план лекции;
- уметь выделять основное, главное;
- усвоить значение примеров и иллюстраций.

Работа на лабораторных занятиях направлена на закрепление теоретических знаний и выработки навыков по их практическому применению.

Самостоятельная работа выполняет функцию закрепления, повторения изученного материала. Выполнение самостоятельной работы способствует углублению знаний и более успешному формированию умений и навыков,

связанных с изучением конкретных тем.
Характер самостоятельной работы: развитие способностей самостоятельно работать с информацией, используя учебную и научную литературу. Самостоятельная работа дисциплинирует обучающихся, развивает произвольное внимание и совершенствует навыки целесообразного восприятия.