

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ

«БРАТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Кафедра информатики и прикладной математики

УТВЕРЖДАЮ:

Проректор по учебной работе

_____ Е.И. Луковникова

«_____» _____ 201__ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ

Б1.В.ДВ.11.02

НАПРАВЛЕНИЕ ПОДГОТОВКИ

09.03.02 Информационные системы и технологии

ПРОФИЛЬ ПОДГОТОВКИ

Информационные системы и технологии

Программа академического бакалавриата

Квалификация (степень) выпускника: бакалавр

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	3
2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	5
3. РАСПРЕДЕЛЕНИЕ ОБЪЕМА ДИСЦИПЛИНЫ	5
3.1 Распределение объёма дисциплины по формам обучения.....	5
3.2 Распределение объёма дисциплины по видам учебных занятий и трудоемкости	5
4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ	6
4.1 Распределение разделов дисциплины по видам учебных занятий	6
4.2 Содержание дисциплины, структурированное по разделам и темам	7
4.3 Лабораторные работы.....	8
4.4 Семинары / практические занятия.....	8
4.5. Контрольные мероприятия: курсовой проект (курсовая работа), контрольная работа, РГР, реферат.....	8
5. МАТРИЦА СООТНЕСЕНИЯ РАЗДЕЛОВ УЧЕБНОЙ ДИСЦИПЛИНЫ К ФОРМИРУЕМЫМ В НИХ КОМПЕТЕНЦИЯМ И ОЦЕНКЕ РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ	10
6. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ	11
7. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ.....	11
8. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО – ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ» НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ	12
9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ.....	12
9.1. Методические указания для обучающихся по выполнению лабораторных работ	13
9.2. Методические указания по выполнению контрольной работы	18
10. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ	20
11. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ	21
Приложение 1. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине.....	22
Приложение 2. Аннотация рабочей программы дисциплины	27
Приложение 3. Протокол о дополнениях и изменениях в рабочей программе	28

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Вид деятельности выпускника

Дисциплина охватывает круг вопросов, относящихся к производственно-технологическому и сервисно-эксплуатационному видам профессиональной деятельности выпускника в соответствии с компетенциями и видами деятельности, указанными в учебном плане.

Цель дисциплины

Формирование у обучающихся знаний в области основ информационной безопасности и навыков практического обеспечения защиты информации и безопасного использования программных и аппаратных средств в сетях и системах связи.

Задачи дисциплины

Заложить методически правильные основы знаний, необходимые будущим специалистам по инфокоммуникационным технологиям и системам связи в области информационной безопасности.

Код компетенции	Содержание компетенций	Перечень планируемых результатов обучения по дисциплине
1	2	3
ПК-16	способность проводить подготовку документации по менеджменту качества информационных технологий	знать: методологию оценки качества информационных технологий (ИТ); уметь: оценивать качество представленного программного решения с использованием современных методик; владеть: методиками организации работ по оценке качества и надежности информационных систем и технологий (ИСИТ) .
ПК-30	способность поддерживать работоспособность информационных систем и технологий в заданных функциональных характеристиках и соответствии критериям качества	знать: параметры нормального и аварийного режимов работы компонентов ИС; уметь: использовать технологии восстановления данных ИС после сбоев; владеть: навыками оценки последствий программных и аппаратных сбоев;
ПК-31	способность обеспечивать безопасность и целостность данных информационных систем и технологий	знать: основные понятия, связанные с целостностью данных в ИС; уметь: реализовывать требования к целостности данных на этапе проектирования базы данных ИС; владеть: навыками применения средств обеспечения целостности данных на уровне системы управления базами данных.

1	2	3
ОПК-6	способность выбирать и оценивать способ реализации информационных систем и устройств (программно-, аппаратно- или программно-аппаратно-) для решения поставленной задачи	<p>знать:</p> <ul style="list-style-type: none"> – основные модели данных; – современные реляционные СУБД; – методы и средства проектирования структуры реляционной базы данных ИС; <p>уметь:</p> <ul style="list-style-type: none"> – проектировать компоненты ИС на основе современных концептуальных моделей; – реализовывать проект ИС средствами современной среды разработки; <p>владеть:</p> <ul style="list-style-type: none"> – навыками разработки различных объектов базы данных; – навыками разработки компонентов эргономичного пользовательского интерфейса.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина Б1.В.ДВ.11.02 «Безопасность информационных систем» относится к элективным дисциплинам.

Дисциплина «Безопасность информационных систем» базируется на знаниях, полученных при изучении дисциплин «Управление данными», «Методы и средства проектирования информационных систем и технологий» и «Инструментальные средства информационных систем».

Дисциплина «Безопасность информационных систем» представляет основу для преддипломной практики и подготовки к государственной итоговой аттестации.

Такое системное междисциплинарное изучение направлено на достижение требуемого ФГОС уровня подготовки по квалификации бакалавр.

3. РАСПРЕДЕЛЕНИЕ ОБЪЕМА ДИСЦИПЛИНЫ

3.1. Распределение объема дисциплины по формам обучения

Форма обучения	Курс	Семестр	Трудоемкость дисциплины в часах						Контрольная работа	Вид промежуточной аттестации
			Всего часов (с экз.)	Аудиторных часов	Лекции	Лабораторные работы	Семинары Практические занятия	Самостоятельная работа		
1	2	3	4	5	6	7	8	9	10	11
Очная	4	8	180	55	33	22	-	89	кр	экзамен
Заочная	5	-	180	18	8	10	-	153	кр	экзамен
Заочная (ускоренное обучение)	-	-	-	-	-	-	-	-	-	-
Очно-заочная	-	-	-	-	-	-	-	-	-	-

3.2. Распределение объема дисциплины по видам учебных занятий и трудоемкости

Вид учебных занятий	Трудо- емкость (час.)	в т.ч. в интерак- тивной, активной, инновационной формах, (час.)	Распределение по семестрам, час
			8
1	2	3	4
I. Контактная работа обучающихся с преподавателем (всего)	55	37	55
Лекции (Лк)	33	33	33
Лабораторные работы (ЛР)	22	4	22
Контрольная работа	+	-	+
Групповые консультации	+	-	+
II. Самостоятельная работа обучающихся (СР)	89	-	89
Подготовка к лабораторным работам	29	-	29
Выполнение контрольной работы	30	-	30
Подготовка к экзамену в течение семестра	30	-	30
III. Промежуточная аттестация экзамен	36	-	36
Общая трудоемкость дисциплины .. час.	180	-	180
зач. ед.	5	-	5

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Распределение разделов дисциплины по видам учебных занятий

- для очной формы обучения:

№ раз- дела и те- мы	Наименование раздела и тема дисциплины	Трудо- ем- кость, (час.)	Виды учебных занятий, включая самостоятельную работу обучаю- щихся и трудоемкость; (час.)		
			учебные занятия		самостоя- тельная работа обучаю- щихся
			лекции	лабораторные работы	
1	2	3	4	5	6
1.	Основы информационной безопасности.	48	11	8	29
1.1.	Понятие информационной безопасности.	23	5	4	14
1.2.	Наиболее распространенные угрозы информационной безопасности.	25	6	4	15
2.	Уровни информационной безопасности.	48	12	6	30
2.1.	Законодательный уровень информационной безопасности.	27	6	6	15
2.2.	Административный и процедурный уровни информационной безопасности.	21	6	-	15
3.	Основные программно-технические меры информационной безопасности сетей и систем.	48	10	8	30

3.1	Идентификация и аутентификация, управление доступом. Протоколирование и аудит, шифрование, контроль целостности.	19	4	4	15
3.2	Программно-технические средства защиты информации в сетях и системах связи.	25	6	4	15
ИТОГО		144	33	22	89

- для заочной формы обучения:

№ раздела и темы	Наименование раздела и тема дисциплины	Трудоемкость, (час.)	Виды учебных занятий, включая самостоятельную работу обучающихся и трудоемкость; (час.)		
			учебные занятия		самостоятельная работа обучающихся
			лекции	лабораторные работы	
1	2	3	4	5	6
1.	Основы информационной безопасности.	56	2	4	50
1.1.	Понятие информационной безопасности.	27	-	2	25
1.2.	Наиболее распространенные угрозы информационной безопасности.	29	2	2	25
2.	Уровни информационной безопасности.	58	4	4	50
2.1.	Законодательный уровень информационной безопасности.	29	2	2	25
2.2.	Административный и процедурный уровни информационной безопасности.	29	2	2	25
3.	Основные программно-технические меры информационной безопасности сетей и систем.	57	2	2	53
3.1	Идентификация и аутентификация, управление доступом. Протоколирование и аудит, шифрование, контроль целостности.	29	2	2	25
3.2	Программно-технические средства защиты информации в сетях и системах связи.	28	-	-	28
ИТОГО		171	8	10	153

4.2. Содержание дисциплины, структурированное по разделам и темам

№ раздела и темы	Наименование раздела и темы дисциплины	Содержание лекционных занятий	Вид занятия в интерактивной, активной,

			<i>инновационной формах, (час.)</i>
<i>1</i>	<i>2</i>	<i>3</i>	<i>4</i>
1.	Основы информационной безопасности.		
1.1.	Понятие информационной безопасности.	Понятие и основные составляющие информационной безопасности. Важность и сложность проблемы информационной безопасности.	Лекция-дискуссия, (5 час.)
1.2.	Наиболее распространенные угрозы информационной безопасности.	Основные определения и критерии классификации угроз. Наиболее распространенные угрозы доступности. Вредоносное программное обеспечение. Угрозы целостности. Угрозы конфиденциальности.	Лекция-дискуссия, (6 час.)
2.	Уровни информационной безопасности.		
2.1.	Законодательный уровень информационной безопасности.	Что такое законодательный уровень информационной безопасности и почему он важен. Обзор российского законодательства в области информационной безопасности. Обзор зарубежного законодательства в области информационной безопасности.	Лекция-дискуссия, (6 час.)
2.2.	Административный и процедурный уровни информационной безопасности.	Политика безопасности. Программа безопасности. Синхронизация программы безопасности с жизненным циклом инфокоммуникационных систем. Управление рисками. Основные классы мер процедурного уровня. Управление персоналом. Физическая защита. Поддержание работоспособности. Реагирование на нарушения режима безопасности. Планирование восстановительных работ.	Лекция-дискуссия, (6 час.)
3.	Основные программно-технические меры информационной безопасности сетей и систем.		
3.1	Идентификация и аутентификация, управление доступом. Протоколирование и аудит, шифрование, контроль целостности.	Основные понятия программно-технического уровня информационной безопасности. Особенности современных информационных систем, существенные с точки зрения безопасности. Архитектурная безопасность. Основные понятия об идентификации и аутентификации. Парольная аутентификация. Идентификация/аутентификация с помощью биометрических данных. Управление доступом. Ролевое управление доступом. Основные понятия протоколирования и аудита. Активный аудит. Симметричное и асимметричное шифрование. Контроль целостности: хэш-функции и электронно-цифровая подпись.	Лекция-дискуссия, (4 час.)
3.2	Программно-технические средства защиты информации в	Экранирование: основные понятия и архитектурные аспекты. Классификация межсетевых экранов. Анализ защищенности. Основные понятия доступности. Основы мер обеспечения высокой доступности. Отказоустойчивость	Лекция-дискуссия, (6 час.)

	сетях и системах связи.	и зона риска. Обеспечение обслуживаемости.	
--	-------------------------	--	--

4.3. Лабораторные работы

<i>№ п/п</i>	<i>Номер раздела дисциплины</i>	<i>Наименование лабораторной работы</i>	<i>Объем (час.)</i>	<i>Вид занятия в интерактивной, активной, инновационной формах, (час.)</i>
1.	1.	Основы теории вероятности	4	-
2.	1.	Характеристики простейшего потока	4	-
3.	2.	Основные показатели надежности восстанавливаемых элементов информационных систем	6	-
4.	3.	Основные характеристики надежности восстанавливаемых элементов информационных систем	4	Работа в малых группах (4 часа)-
5.	3.	Математические модели надежности	2	-
6.	3.	Надежность сложных информационных систем	2	-
ИТОГО			22	4

4.4. Семинары / практические занятия

Учебным планом не предусмотрены.

4.5. Контрольные мероприятия: контрольная работа

Цель работы: научиться применять полученные знания при расчете надежности информационных систем, приобретение навыков работы с учебной, научной и справочной литературой, и закрепление практических знаний по дисциплине

Структура работы:

- титульный лист;
- содержание;
- введение;
- основные разделы работы;
- заключение;
- список использованных источников.

Основная тематика: расчет показателей надежности информационной системы.

Рекомендуемый объем: контрольная работа выполняется в виде пояснительной записки объемом 10-15 страниц, оформляется в строгом соответствии со стандартом ФГБОУ ВО «БрГУ».

Выдача заданий на контрольную работу производится в соответствии с графиком учебного процесса.

Оценка	Критерии оценки контрольной работы
зачтено	соответствие требованиям по структурному содержанию и объему работы; правильность выполнения задания, сопровождающегося рисунками, таблицами, диаграммами; правильность решения практических заданий, самостоятельность выполнения; отсутствие стилистических ошибок; уверенное владение материалом при устной защите.
не зачтено	несоответствие требованиям по структурному содержанию и объему работы; неправильность выполнения задания, сопровождающегося рисунками, таблицами, диаграммами; наличие ошибок в выполнении практических заданий; отсутствие самостоятельности выполнения; наличие стилистических ошибок;

	отсутствие владения материалом при устной защите.
--	---

5. МАТРИЦА СООТНЕСЕНИЯ РАЗДЕЛОВ УЧЕБНОЙ ДИСЦИПЛИНЫ К ФОРМИРУЕМЫМ В НИХ КОМПЕТЕНЦИЯМ И ОЦЕНКЕ РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

<i>Компетенции</i> <i>№, наименование разделов дисциплины</i>	<i>Кол-во часов</i>	<i>Компетенции</i>				Σ <i>комп.</i>	<i>t_{ср}, час</i>	<i>Вид учебной работы</i>	<i>Оценка результатов</i>
		<i>ОПК</i>	<i>ПК</i>						
		<i>6</i>	<i>16</i>	<i>30</i>	<i>31</i>				
1	2	3	4	5	6	7	8	9	10
1. Основы информационной безопасности.	48	+	-	-	-	1	48	ЛК, ЛР, СРС	экзамен
2. Уровни информационной безопасности.	48	-	-	+	-	1	48	ЛК, ЛР, СРС	экзамен, кр
3. Основные программно-технические меры информационной безопасности сетей и систем.	48	-	+	-	+	2	24	ЛК, ЛР, СРС	экзамен
<i>всего часов</i>	144	48	48	48	48	4	36		

6. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

1. Кияев, В. Безопасность информационных систем : курс / В. Кияев, О. Граничин. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 192 с. : ил. ; То же [Электронный ресурс]. - URL:<http://biblioclub.ru/index.php?page=book&id=429032> (06.12.2017).

7. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

№	Наименование издания	Вид занятия (Лк, ЛР, кр)	Количество экземпляров в библиотеке, шт.	Обеспеченность, (экз./чел.)
1	2	3	4	5
Основная литература				
1.	Голиков, А.М. Защита информации в инфокоммуникационных системах и сетях : учебное пособие / А.М. Голиков ; Министерство образования и науки Российской Федерации, Томский Государственный Университет Систем Управления и Радиоэлектроники (ТУСУР). - Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. - 284 с. : схем., табл., ил. - Библиогр. в кн. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=480637 (06.12.2017).	Лк, ЛР, кр, СРС	ЭР	1
2.	Петренко, В.И. Защита персональных данных в информационных системах : учебное пособие / В.И. Петренко ; Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет». - Ставрополь : СКФУ, 2016. - 201 с. : схем. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=459205 (06.12.2017).	Лк, ЛР, кр	ЭР	1
Дополнительная литература				
3.	Комплексное обеспечение информационной безопасности автоматизированных систем : лабораторный практикум / Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет» ; авт.-сост. М.А. Лапина, Д.М. Марков и др. - Ставрополь : СКФУ, 2016. - 242 с. : ил. - Библиогр. в кн. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=458012 (06.12.2017).	Лк, ЛР, кр, СРС	ЭР	1
4.	Организация безопасной работы информационных систем : учебное пособие / Ю.Ю. Громов,	Лк, ЛР, СРС	ЭР	1

	<p>Ю.Ф. Мартемьянов, Ю.К. Букурако и др. ; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Тамбовский государственный технический университет». - Тамбов : Издательство ФГБОУ ВПО «ТГТУ», 2014. - 132 с. : ил. - Библиогр. в кн. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=277794 (06.12.2017).</p>			
--	---	--	--	--

8. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО - ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ» НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1. Электронный каталог библиотеки БрГУ http://irbis.brstu.ru/CGI/irbis64r_15/cgiirbis_64.exe?LNG=&C21COM=F&I21DBN=BOOK&P21DBN=BOOK&S21CNR=&Z21ID=.
2. Электронная библиотека БрГУ <http://ecat.brstu.ru/catalog> .
3. Электронно-библиотечная система «Университетская библиотека online» <http://biblioclub.ru> .
4. Электронно-библиотечная система «Издательство «Лань» <http://e.lanbook.com> .
5. Информационная система "Единое окно доступа к образовательным ресурсам" <http://window.edu.ru> .
6. Научная электронная библиотека eLIBRARY.RU <http://elibrary.ru> .
7. Университетская информационная система РОССИЯ (УИС РОССИЯ) <https://uisrussia.msu.ru/>.
8. Национальная электронная библиотека НЭБ <http://xn--90ax2c.xn--p1ai/how-to-search/>.
9. Научная электронная библиотека «КИБЕРЛЕНИНКА» // Электронный ресурс [Режим доступа: свободный] <http://cyberleninka.ru/>.

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Вид учебных занятий	Организация деятельности обучающихся
Лекции	<p>Написание конспекта лекций: кратко, последовательно фиксировать основные положения, выводы, формулировки, обобщения; пометить важные мысли, выделять ключевые слова, термины. Проверка терминов с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удастся разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, практическом занятии.</p>
Лабораторные работы	<p>Работа с конспектом лекций, обобщение, систематизация, углубление и конкретизация полученных теоретических знаний, выработка способности и готовности их использования на практике. Развитие интеллектуальных умений, подготовка ответов к контрольным вопросам, работа с основной и дополнительной литературой, необходимой для освоения дисциплины, выполнение заданий, решение задач, активное участие в интерактивной, активной, инновационной формах обучения, составление письменных отчетов.</p>
Самостоятельная работа обучающихся	<p><i>Подготовка к лабораторным работам.</i> Проработка основной и дополнительной литературы, терминов, сведений, формул требующихся для запоминания и являющихся основополагающими в разделе. Конспектирование прочитанных литературных источников. Проработка материалов по изучаемому вопросу, с использованием на рекомендуемых ресурсах информационно-телекоммуникационной</p>

	<p>сети «Интернет». Выполнение заданий преподавателя, необходимых для подготовки к участию в интерактивной, активной, инновационных формах обучения по изучаемой теме.</p> <p><i>Подготовка к экзамену.</i> При подготовке к экзамену необходимо ориентироваться на конспекты лекций, рекомендуемую литературу, использовать рекомендуемые ресурсы информационно-телекоммуникационной сети «Интернет».</p>
--	--

9.1. Методические указания для обучающихся по выполнению лабораторных работ

Лабораторная работа № 1. Основы теории вероятности

Цель работы:

- вспомнить основные понятия и формулы теории вероятности;
- рассчитать вероятность наступления отказа как случайного события по основным формулам теории вероятности.

Задание:

1. В партии из 100 деталей отдел технического контроля обнаружил 5 нестандартных деталей. Чему равна относительная частота нестандартных деталей.
2. Среднее число вызовов, поступающих на АТС в одну минуту, равно 4. Найти вероятность того, что за 4 минуты поступит: а) 3 вызова; б) менее 3 вызовов; в) не менее 3 вызовов.
3. Производится 8 выстрелов с вероятностями попадания в цель, равными: $P_1 = 0,8$, $P_2 = 0,2$, $P_3 = 0,3$, $P_4 = 0,4$, $P_5 = 0,7$, $P_6 = 0,1$, $P_7 = 0,4$, $P_8 = 0,6$. Найти математическое ожидание общего числа попаданий.
4. Куб, все грани которого окрашены, распилили на 100 кубиков одинакового размера, которые затем перемешаны. Найти вероятность того, что наугад извлеченный кубик имеет 3 окрашенных грани.

Порядок выполнения:

1. Ознакомиться с приведенными преподавателем теоретическими сведениями и примерами.
2. Решить задачи в соответствии с вариантом задания.
3. Оформить отчет по итогам выполнения работы.

Форма отчетности:

Отчет по лабораторной работе, скрепленный титульным листом. Отчет должен содержать название работы, цель, задание и результат выполнения задания.

Рекомендации по выполнению заданий и подготовке к лабораторной работе

При подготовке и выполнении лабораторной работы рекомендуется использовать материал лекций соответствующих разделов и литературу, предложенную для изучения данной дисциплины.

Рекомендуемые источники

1. Библиотека Братского государственного университета // Электронный ресурс [Режим доступа: свободный] <http://library.brstu.ru/>
2. Электронно-библиотечная система «Университетская библиотека online» // Электронный ресурс <http://biblioclub.ru/>

Основная литература

Источники 1-2, указанные в разделе 7.

Дополнительная литература

Источники 3-4, указанные в разделе 7.

Контрольные вопросы для самопроверки:

1. Дайте определение различных видов событий.
2. Дайте определение классической и статистической вероятности.

3. В чем отличие вероятности от относительной частоты?
4. Назовите основные формулы комбинаторики.
5. Какой вид примет формула Пуассона при нахождении вероятности на интервале времени?
6. Что понимают под математическим ожиданием?

Лабораторная работа № 2. Характеристики простейшего потока

Цель работы: научиться определять характеристики простейшего потока с производственным сценарием..

Задание:

1. Определить интенсивность отказов некоторого устройства, если за t часов для такого же типа устройств в среднем происходит n отказов.

Исходные данные к задаче 1

Вариант	1	2	3	4	5	6	7	8	9	10
t	500	700	1000	800	500	700	600	500	2000	500
n	1	2	5	4	1	3	3	1	8	2

1. На автоматическую телефонную станцию поступает простейший поток вызовов с интенсивностью, равной λ (вызовов в мин). Найти вероятность того, что за t минут: а) не придет ни одного вызова; б) придет ровно n вызовов; в) придет хотя бы n вызовов.

Исходные данные к задаче 2

Вариант	1	2	3	4	5	6	7	8	9	10
λ	0,8	0,65	0,7	0,2	0,8	0,3	0,9	0,6	0,5	0,4
t	2	2	2	3	3	3	4	4	4	5
n	1	2	3	1	2	3	1	2	3	1

Порядок выполнения:

1. Ознакомиться с приведенными преподавателем теоретическими сведениями и примерами.
2. Решить задачи в соответствии с вариантом задания.
3. Оформить отчет по итогам выполнения работы.

Форма отчетности:

Отчет по лабораторной работе, скрепленный титульным листом. Отчет должен содержать название работы, цель, задание и результат выполнения задания.

Рекомендации по выполнению заданий и подготовке к лабораторной работе

При подготовке и выполнении лабораторной работы рекомендуется использовать материал лекций соответствующих разделов и литературу, предложенную для изучения данной дисциплины.

Рекомендуемые источники

1. Библиотека Братского государственного университета // Электронный ресурс [Режим доступа: свободный] <http://library.brstu.ru/>
2. Электронно-библиотечная система «Университетская библиотека online» // Электронный ресурс <http://biblioclub.ru/>

Основная литература

Источники 1-2, указанные в разделе 7.

Дополнительная литература

Источники 3-4, указанные в разделе 7.

Контрольные вопросы для самопроверки:

1. Какое состояние технического устройства называется работоспособным?
2. Что такое отказ?
3. Какой поток называется простейшим?

4. Каковы свойства простейшего потока и их характеристики.
5. Определите среднее число событий, наступающих в простейшем потоке и связь среднего числа событий с интенсивностью.

Лабораторная работа № 3. Основные показатели надежности невосстанавливаемых элементов информационных систем

Цель работы: научиться определять основные характеристики надежности невосстанавливаемых элементов информационных систем.

Задание: В течение t_2 часов наблюдали за N_0 видеоадаптерами. Определить статистическую вероятность безотказной работы этих устройств ($P(t_1)$, $P(t_2)$, $P(t_2/t_1)$), если в течение указанного срока зарегистрировано n отказов, причем n_1 из них произошли в первые t_1 часов.

Исходные данные к задаче:

Вариант	t_1	t_2	N_0	n	n_1
1	2000	400	480	52	12
2	2200	420	550	60	17
3	1800	380	400	48	19
4	1500	300	370	44	13
5	2100	410	520	55	23
6	1400	250	320	40	11
7	1900	450	490	57	21
8	3000	600	580	68	36
9	3500	650	600	70	38
10	3600	700	610	75	43

Порядок выполнения:

1. Ознакомиться с приведенными преподавателем теоретическими сведениями и примерами.
2. Решить задачи в соответствии с вариантом задания.
3. Оформить отчет по итогам выполнения работы.

Форма отчетности:

Отчет по лабораторной работе, скрепленный титульным листом. Отчет должен содержать название работы, цель, задание и результат выполнения задания.

Рекомендации по выполнению заданий и подготовке к лабораторной работе

При подготовке и выполнении лабораторной работы рекомендуется использовать материал лекций соответствующих разделов и литературу, предложенную для изучения данной дисциплины.

Рекомендуемые источники

1. Библиотека Братского государственного университета // Электронный ресурс [Режим доступа: свободный] <http://library.brstu.ru/>
2. Электронно-библиотечная система «Университетская библиотека online» // Электронный ресурс <http://biblioclub.ru/>

Основная литература

Источники 1-2, указанные в разделе 7.

Дополнительная литература

Источники 3-4, указанные в разделе 7.

Контрольные вопросы для самопроверки:

1. Дать определение:
 - вероятности безотказной работы;
 - вероятности безотказной работы на некотором интервале времени;
 - вероятности отказов;
 - интенсивности отказов;

- плотности вероятности отказов;
 - какие характерные участки имеет кривая интенсивности отказов невосстанавливаемых технических устройств?
2. каково среднее время безотказной работы?
 3. какова зависимость между $a(t)$ и $p(t)$, $p(t)$ и $\lambda(t)$, $a(t)$ и $\lambda(t)$, $T_{ср}$ и $\lambda(t)$?
 4. как зависят $p(t)$, $a(t)$ и $T_{ср}$ от $\lambda(t)$ при $\lambda(t) = \lambda = \text{const}$?

Лабораторная работа № 4. Основные характеристики надежности восстанавливаемых элементов информационных систем

Цель работы: научиться определять основные характеристики надежности восстанавливаемых элементов информационных систем.

Задание: Производилось наблюдение за работой трех экземпляров однотипной аппаратуры. За период наблюдения было зафиксировано по первому экземпляру аппаратуры N1 отказов, по второму и третьему – N2 и N3 отказов соответственно. Нарботка первого экземпляра составила T1 часов, второго – T2 и третьего – T3 часов. Требуется определить наработку аппаратуры на отказ, если допустить, что восстановления проходили мгновенно.

Исходные данные к задаче

Вариант	N1	N2	N3	T1	T2	T3
1	6	11	8	181	329	245
2	5	10	9	156	300	221
3	4	9	7	136	298	235
4	7	13	10	174	346	278
5	6	15	9	123	389	287
6	8	19	11	179	453	321
7	9	18	17	176	299	219
8	3	17	15	163	285	310
9	5	12	16	190	292	385
10	8	14	13	179	312	250

Порядок выполнения:

1. Ознакомиться с приведенными преподавателем теоретическими сведениями и примерами.
2. Решить задачи в соответствии с вариантом задания.
3. Оформить отчет по итогам выполнения работы.

Форма отчетности:

Отчет по лабораторной работе, скрепленный титульным листом. Отчет должен содержать название работы, цель, задание и результат выполнения задания.

Рекомендации по выполнению заданий и подготовке к лабораторной работе

При подготовке и выполнении лабораторной работы рекомендуется использовать материал лекций соответствующих разделов и литературу, предложенную для изучения данной дисциплины.

Рекомендуемые источники

1. Библиотека Братского государственного университета // Электронный ресурс [Режим доступа: свободный] <http://library.brstu.ru/>
2. Электронно-библиотечная система «Университетская библиотека online» // Электронный ресурс <http://biblioclub.ru/>

Основная литература

Источники 1-2, указанные в разделе 7.

Дополнительная литература

Источники 3-4, указанные в разделе 7.

Контрольные вопросы для самопроверки:

1. Какие элементы называются восстанавливаемыми?

2. Дать определение параметра потока отказов.
3. Что значит наработка на отказ?
4. Коэффициент готовности и коэффициент вынужденного простоя. Как связываются эти коэффициенты?
5. Как определяется вероятность заставить систему в исправном состоянии?
6. В каких случаях критериями надежности восстанавливаемых систем могут быть критерии надежности невозстанавливаемых систем?

Лабораторная работа № 5. Математические модели надежности

Цель работы: определение основных характеристик надежности по выбранным математическим моделям.

Задание: Вероятность безотказной работы автоматической линии изготовления цилиндров автомобильного двигателя в течение времени t , ч, равна P . Требуется рассчитать интенсивность отказов и частоту отказов линии для момента времени t , ч, при условии, что $\lambda = \text{const}$.

Исходные данные к задаче

Вариант	t	P
1	110	0,8
2	95	0,68
3	140	0,7
4	170	0,6
5	110	0,715
6	90	0,55
7	100	0,85
8	140	0,65
9	130	0,75
10	120	0,58

Порядок выполнения:

1. Ознакомиться с приведенными преподавателем теоретическими сведениями и примерами.
2. Решить задачи в соответствии с вариантом задания.
3. Оформить отчет по итогам выполнения работы.

Форма отчетности:

Отчет по лабораторной работе, скрепленный титульным листом. Отчет должен содержать название работы, цель, задание и результат выполнения задания.

Рекомендации по выполнению заданий и подготовке к лабораторной работе

При подготовке и выполнении лабораторной работы рекомендуется использовать материал лекций соответствующих разделов и литературу, предложенную для изучения данной дисциплины.

Рекомендуемые источники

1. Библиотека Братского государственного университета // Электронный ресурс [Режим доступа: свободный] <http://library.brstu.ru/>
2. Электронно-библиотечная система «Университетская библиотека online» // Электронный ресурс <http://biblioclub.ru/>

Основная литература

Источники 1-2, указанные в разделе 7.

Дополнительная литература

Источники 3-4, указанные в разделе 7.

Контрольные вопросы для самопроверки:

1. Как рассчитываются показатели надежности при распределении Вейбулла?

2. Как параметр δ в распределении Вейбулла влияет на интенсивность?
3. Какой закон распределения справедлив при $\lambda = \text{const}$?
4. Чему равна вероятность безотказной работы на интервале, превышающем среднее время, при экспоненциальном распределении?
5. Что является характерным признаком распределения Рэлея? 6. Чем характеризуется нормальный закон распределения?

Лабораторная работа № 6. Надежность сложных информационных систем.

Цель работы: научиться составлять структурную схему надежности и определять надёжность системы.

Задание: Определить вероятность безотказной работы системы, структурная схема надежности которой задается преподавателем.

Вероятности безотказной работы элементов равны: $p_1 = 0,998$; $p_2 = 0,5p_1$; $p_3 = p_1$; $p_4 = 0,75p_1$; $p_5 = p_4^2$.

Порядок выполнения:

1. Ознакомиться с приведенными преподавателем теоретическими сведениями и примерами.
2. Решить задачи в соответствии с вариантом задания.
3. Оформить отчет по итогам выполнения работы.

Форма отчетности:

Отчет по лабораторной работе, скрепленный титульным листом. Отчет должен содержать название работы, цель, задание и результат выполнения задания.

Задания для самостоятельной работы:

Рекомендации по выполнению заданий и подготовке к лабораторной работе

При подготовке и выполнении лабораторной работы рекомендуется использовать материал лекций соответствующих разделов и литературу, предложенную для изучения данной дисциплины.

Рекомендуемые источники

1. Библиотека Братского государственного университета // Электронный ресурс [Режим доступа: свободный] <http://library.brstu.ru/>
2. Электронно-библиотечная система «Университетская библиотека online» // Электронный ресурс <http://biblioclub.ru/>

Основная литература

Источники 1-2, указанные в разделе 7.

Дополнительная литература

Источники 3-4, указанные в разделе 7.

Контрольные вопросы для самопроверки:

1. Что такое структурная схема надежности?
2. Что такое структурная схема надежности с последовательным соединением элементов?
3. Что такое структурная схема надежности с параллельным соединением элементов?
4. Как определяется надежность системы при последовательном соединении элементов.
5. Как определяется надежность системы при параллельном соединении элементов?

9.2. Методические указания по выполнению контрольной работы

Порядок выполнения контрольной работы.

При выполнении контрольной работы обучающийся должен:
- совершенствовать теоретические знания по дисциплине «Качество и надежность информационных систем»;

- продемонстрировать способность обобщать, систематизировать и анализировать информацию, необходимую для проведения исследования и решения поставленных задач;
- совершенствовать навыки работы с учебной, научной, справочной и правовой литературой.

Пояснительная записка контрольной работы должна содержать:

- титульный лист; • задание;
- содержание;
- введение (1-2 страницы);
- основную часть (7-10 страниц);
- заключение (1 страница);
- список использованных источников.

Во введении определяется актуальность расчета надежности ИС, формулируется проблема и круг вопросов, необходимых для её решения.

Основная часть содержит выполнение расчетов надежности по предложенной выше методике:

- анализ функционирования системы и составление структурно-логической схемы надежности;
- выбор и обоснование формул для расчета показателей надежности;
- расчет показателей надежности системы;
- графики зависимостей.

В заключении необходимо сделать вывод о надежности ИС и предложить способы повышения надежности.

Основные требования к оформлению пояснительной записки:

- отчет выполняется на листах бумаги формата А4 печатным способом;
- шрифт Times New Roman 14 пт;
- поля: верхнее – 2 см, нижнее – 2 см, левое – 2,5 см, правое – 1,5 см;
- интервал междустрочный 1,5;
- нумерация страниц справа в нижней части страницы.

Список использованных источников должен включать в себя перечень законодательных и нормативных правовых актов, литературных и других источников, действительно использованных при выполнении контрольной работы, и состоять не менее чем из 10 позиций.

Приложения помещаются в пояснительную записку к контрольной работе при необходимости. Это может быть справочная информация, различные нормативные документы, а также законодательные акты (либо их фрагменты), которые, по мнению автора контрольной работы, необходимы для иллюстрации или аргументации положений контрольной работы.

Выполнение контрольной работы должно начинаться с подбора и глубокого изучения литературных источников по теме работы. Ориентиром в этой части работы может служить список рекомендуемой литературы, приведенный ниже. Данный список содержит перечень основных литературных источников, имеющихся в университетской библиотеке.

Важнейшим требованием, предъявляемым к контрольной работе, является самостоятельный характер ее выполнения. Оформление пояснительной записки контрольной работы должно осуществляться в строгом соответствии со стандартом ФГБОУ ВО «БрГУ» «Оформление пояснительной записки учебной работы» СМК СПб 1.4-01-2005.

Пояснительная записка должна быть выполнена аккуратно, без исправлений.

Тематика контрольных работ:

Расчет показателей надежности информационной системы

Цель работы: научиться применять полученные знания при расчете надежности информационных систем.

Задание:

Схема локальной информационной системы изображена на рисунке 1.

Функционирование ИС:

- режим работы в течение года – с понедельника по субботу, с 8.00 до 20.00;

- в группе А обязательно должны функционировать все 5 компьютеров по количеству работающих пользователей;
- в группе В работают 5 пользователей, но 2 компьютера могут простаивать, не влияя на работу систему;
- вся информация и базы данных расположены на сервере, в серверной группе установлено 2 резервных компьютера, которые подключены по схеме основного общего резервирования;
- E-mail сервер должен работать 10 % от общего времени.

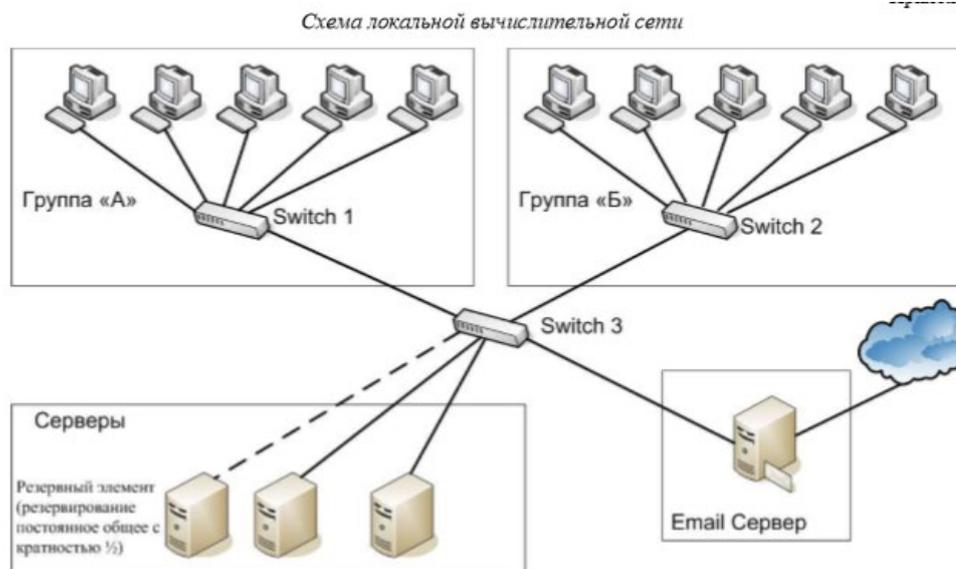


Рис. 1 – Структура ЛВС ИС

Исходные данные для расчета:

- интенсивность отказа компьютеров в группе А $\lambda_1 = 0,0007$ 1/час;
- интенсивность отказа компьютеров в группе В $\lambda_2 = 0,006$ 1/час;
- интенсивность отказа серверов $\lambda_3 = 0,000003$ 1/час;
- интенсивность отказа кабеля $\lambda_4 = 0,00000004$ 1/час;
- интенсивность отказа ПО на компьютере в рабочих группах $\lambda_5 = 0,006$ 1/час, вероятность отказа ПО сервера считать нулевой;
- интенсивность отказа коммуникационных устройств $\lambda_6 = 0,0000008$ 1/час;
- расчет проводить для нормального периода эксплуатации.

Найти среднее время безотказной работы ИС и рассчитать вероятность безотказной работы ИС в момент времени $T_{ср}$. Определить вероятность нахождения объекта в работоспособном состоянии через 6 месяцев работы, если рассматривать систему как единый объект с интенсивностью отказа системы, полученной при расчете и интенсивностью восстановления $\mu = \text{const} = 0,66$ 1/час.

10. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

ИКТ преподаватель использует для выполнения лабораторных работ по всем темам следующие информационные технологии: ОС Windows 7 Professional, Microsoft Office 2010 Russian Academic OPEN no Level, Kaspersky Security.

При осуществлении образовательного процесса по дисциплине применяются инновационные технологии обучения, активные и интерактивные формы проведения занятий, указанные в разделах 3.2, 4.2.

**11. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ
ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ**

<i>Вид занятия</i>	<i>Наименование аудитории</i>	<i>Перечень основного оборудования</i>	<i>№ ЛР</i>
1	2	3	4
Лк	Мультимедийный класс	Интерактивная доска SMART Board 680I, проектор Casio XJ-UT310WN. ПК: CPU 5000/RAM 2Gb/HDD; Монитор TFT 19 LG1953S-SF	-
ЛР	Дисплейный класс	8-ПК: P-IV (3,0 GHz/ 160Gb/1Gb/ DVD-ROM); 4-ПК: AMD Athlon 64 5GHz/250Gb/2Gb/DVD-RW, 2 ядра; Мониторы LCD 19Samsung 943 и TFT 19 LG1953S-SF; Акустическая система MSSSP-205B	ЛР №№ 1-6
кр	Дисплейный класс	8-ПК: P-IV (3,0 GHz/ 160Gb/1Gb/ DVD-ROM); 4-ПК: AMD Athlon 64 5GHz/250Gb/2Gb/DVD-RW, 2 ядра; Мониторы LCD 19Samsung 943 и TFT 19 LG1953S-SF; Акустическая система MSSSP-205B	-
СР	Читальный зал №1	Оборудование 10-ПК i5-2500/H67/4Gb (монитор TFT19 Samsung); принтер HP LaserJet P2055D	-

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ
ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ**

1. Описание фонда оценочных средств (паспорт)

№ компетенции	Элемент компетенции	Раздел	Тема	ФОС
ПК-16	способность проводить подготовку документации по менеджменту качества информационных технологий	3. Основные программно-технические меры информационной безопасности сетей и систем.	3.1. Идентификация и аутентификация, управление доступом. Протоколирование и аудит, шифрование, контроль целостности.	Экзаменационный билет
ПК-30	способность поддерживать работоспособность информационных систем и технологий в заданных функциональных характеристиках и соответствии критериям	2. Уровни информационной безопасности.	2.1. Понятие информационной безопасности. 2.2. Наиболее распространенные угрозы информационной безопасности.	
ПК-31	способность обеспечивать безопасность и целостность данных информационных систем и технологий	3. Основные программно-технические меры информационной безопасности сетей и систем.	3.2. Программно-технические средства защиты информации в сетях и системах связи.	
ОПК-6	способность выбирать и оценивать способ реализации информационных систем и устройств (программно-, аппаратно- или программно-аппаратно-) для решения поставленной задачи	1. Основы информационной безопасности.	1.1. Понятие информационной безопасности. 1.2. Наиболее распространенные угрозы информационной безопасности.	

2. Экзаменационные вопросы

№ п/п	Компетенции		ЭКЗАМЕНАЦИОННЫЕ ВОПРОСЫ	№ и наименование раздела
	Код	Определение		
1	2	3	4	5
1.	ПК-16	способность проводить подготовку документации по менеджменту качества информационных технологий	<p>1. Методы несимметричного шифрования. Использование несимметричного шифрования для обеспечения целостности данных.</p> <p>2. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.</p> <p>3. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности.</p> <p>4. Средства обеспечения информационной безопасности в ОС Windows'2000. Разграничение доступа к данным. Групповая политика.</p> <p>5. Применение файловой системы NTFS для обеспечения информационной безопасности в Windows NT/2000/XP. Списки контроля доступа к данным (ACL) их роль в разграничении доступа к данным.</p> <p>6. Основные этапы разработки защищенной системы: определение политики безопасности, проектирование модели ИС, разработка кода ИС, обеспечение гарантий соответствия реализации заданной политике безопасности.</p>	3. Основные программно-технические меры информационной безопасности сетей и систем.
2.	ПК-30	способность поддерживать работоспособность информационных систем и технологий в заданных функциональных характеристиках и соответствии критериям	<p>7. Понятие политики безопасности информационных систем. Назначение политики безопасности.</p> <p>8. Основные типы политики безопасности доступа к данным. Дискреционные и мандатные политики.</p> <p>9. Требования к системам криптографической защиты: криптографические требования, требования надежности, требования по защите от НСД, требования к средствам разработки.</p> <p>10. Законодательный уровень обеспечения информационной безопасности. Основные законодательные акты РФ в области защиты информации.</p> <p>11. Функции и назначение стандартов информационной безопасности. Примеры стандартов, их роль при</p>	2. Уровни информационной безопасности.

			<p>проектировании и разработке информационных систем.</p> <p>12. Критерии оценки безопасности компьютерных систем («Оранжевая книга»). Структура требований безопасности. Классы защищенности.</p> <p>13. Основные положения руководящих документов Гостехкомиссии России. Классификация автоматизированных систем по классам защищенности. Показатели защищенности средств вычислительной техники от несанкционированного доступа.</p> <p>14. Единые критерии безопасности информационных технологий. Понятие профиля защиты. Структура профиля защиты.</p> <p>15. Единые критерии безопасности информационных технологий. Проект защиты. Требования безопасности (функциональные требования и требования адекватности).</p>	
3.	ПК-31	способность обеспечивать безопасность и целостность данных информационных систем и технологий	<p>16. Причины нарушения безопасности информации при ее обработке криптографическими средствами.</p> <p>17. Понятие атаки на систему информационной безопасности. Особенности локальных атак.</p> <p>18. Распределенные информационные системы. Удаленные атаки на информационную систему.</p> <p>19. Каналы передачи данных. Утечка информации. Атаки на каналы передачи данных.</p> <p>20. Физические средства обеспечения информационной безопасности.</p> <p>21. Электронная почта. Проблемы обеспечения безопасности почтовых сервисов и их решения.</p> <p>22. Вирусы и методы борьбы с ними. Антивирусные программы и пакеты.</p>	3. Основные программно-технические меры информационной безопасности сетей и систем.
4.	ОП К-6	способность выбирать и оценивать способ реализации информационных систем и устройств (программно-, аппаратно- или программно-аппаратно-) для решения поставленной задачи	<p>23. Классификация угроз информационной безопасности автоматизированных систем по базовым признакам.</p> <p>24. Угроза нарушения конфиденциальности. Особенности и примеры реализации угрозы.</p> <p>25. Угроза нарушения целостности данных. Особенности и примеры реализации угрозы.</p> <p>26. Угроза отказа служб (угроза отказа в доступе). Особенности и примеры реализации угрозы.</p> <p>27. Угроза раскрытия параметров</p>	1. Основы информационной безопасности.

			системы. Особенности и примеры реализации угрозы.	
--	--	--	---	--

3. Описание показателей и критериев оценивания компетенций

Показатели	Оценка	Критерии
<p>Знать: (ПК-16): методологию оценки качества информационных технологий (ИТ); (ПК-30): параметры нормального и аварийного режимов работы компонентов ИС; (ПК-31): основные понятия, связанные с целостностью данных в ИС; (ОПК-6): – основные модели данных; – современные реляционные СУБД; – методы и средства проектирования структуры реляционной базы данных ИС.</p> <p>Уметь: (ПК-16): оценивать качество представленного программного решения с использованием современных методик; (ПК-30): использовать технологии восстановления данных ИС после сбоев; (ПК-31): реализовывать требования к целостности данных на этапе проектирования базы данных ИС; (ОПК-6): – проектировать компоненты ИС на основе современных концептуальных моделей; – реализовывать проект ИС средствами современной среды разработки.</p> <p>Владеть: (ПК-16): методиками организации работ по оценке качества и надежности информационных систем и технологий (ИСИТ); (ПК-30): навыками оценки последствий программных и аппаратных сбоев; (ПК-31): навыками применения средств обеспечения целостности данных на уровне системы управления базами данных; (ОПК-6):</p>	отлично	Оценка «отлично» выставляется в случае, если студент демонстрирует: – всестороннее систематическое знание программного материала; – правильное выполнение типовых заданий, направленных на применение программного материала; – правильное применение основных положений программного материала.
	хорошо	Оценка «хорошо» выставляется в случае, если студент демонстрирует: – недостаточно полное знание программного материала; – выполнение с несущественными ошибками типовых заданий, направленных на применение программного материала; – применение с несущественными ошибками основных положений программного материала.
	удовлетворительно	Оценка «удовлетворительно» выставляется в случае, если студент демонстрирует: – частичное знание программного материала; – частичное выполнение типовых заданий, направленных на применение программного материала; – частичное применение основных положений программного материала.
	неудовлетворительно	Оценка «неудовлетворительно» выставляется в случае, если студент демонстрирует: – существенные пробелы в знании программного материала; – принципиальные ошибки при выполнении типовых

<p>– навыками разработки различных объектов базы данных; навыками разработки компонентов эргономичного пользовательского интерфейса.</p>		<p>заданий, направленных на применение программного материала; – невозможность применения основных положений программного материала.</p>
---	--	---

4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и опыта деятельности

Цель и задачи дисциплины «Безопасность информационных систем» представлены в разделе 1 настоящей рабочей программы. Место дисциплины в структуре образовательной программы представлено в разделе 2 настоящей рабочей программы. Распределение объема дисциплины по формам обучения с указанием видов учебных занятий представлено в разделе 3 настоящей рабочей программы. Содержание дисциплины указано в разделе 4 настоящей рабочей программы.

Учебно-методические материалы для самостоятельной работы студентов по дисциплине находятся в свободном доступе в соответствии с разделом 6 настоящей рабочей программы.

При изучении дисциплины необходимо использовать литературу, указанную в разделе 7 настоящей рабочей программы, а также перечень ресурсов информационно-телекоммуникационной сети «Интернет», представленных в разделе 8 настоящей рабочей программы.

Консультации для студентов по дисциплине проводятся в соответствии с графиком проведения консультаций, представленном на стенде кафедры, за которой закреплена указанная дисциплина.

К экзамену допускаются студенты очной формы обучения, которые выполнили и оформили все лабораторные работы, предусмотренные в конкретном семестре, а также выполнили и защитили контрольную работу.

К экзамену допускаются студенты заочной формы обучения, которые выполнили и оформили все лабораторные работы, а также выполнили, оформили и защитили контрольную работу.

Методические указания по выполнению и оформлению лабораторных работ представлены в разделе 9.1. настоящей рабочей программы. Методические указания по выполнению, оформлению и защите контрольной работы представлены в разделе 9.2. настоящей рабочей программы.

Информационные технологии, используемые при освоении дисциплины, перечислены в разделе 10 настоящей рабочей программы.

Оценка знаний, умений, навыков осуществляется в процессе промежуточной аттестации обучающихся по дисциплине, которая осуществляется в виде экзамена (зачета). Для оценивания знаний, умений, навыков используются ФОС по дисциплине, содержащий экзаменационные билеты и типовые задания.

Экзамен проводится в письменной форме по выданному преподавателем заданию.

По итогам выполненного задания преподаватель оценивает уровень знаний, умений, навыков. Описание показателей и критериев оценивания компетенций, сформированных по итогам изучения дисциплины, представлено в разделе 3 Приложения 1 настоящей рабочей программы. Основными оценочными средствами при проведении промежуточной аттестации являются экзаменационные билеты, вопросы к зачету и типовые задания.

АННОТАЦИЯ рабочей программы дисциплины

Безопасность информационных систем

1. Цель и задачи дисциплины

Целью изучения дисциплины является: формирование у обучающихся знаний в области основ информационной безопасности и навыков практического обеспечения защиты информации и безопасного использования программных и аппаратных средств в сетях и системах связи.

Задачами изучения дисциплины являются: заложить методически правильные основы знаний, необходимые будущим специалистам по инфокоммуникационным технологиям и системам связи в области информационной безопасности.

2. Структура дисциплины

2.1 Распределение трудоемкости по отдельным видам учебных занятий, включая самостоятельную работу:

Лк- 33 час.; ЛР-22 час.; СР-89 час.

Общая трудоемкость дисциплины составляет 180 часов, 5 зачетных единиц.

2.2. Основные разделы дисциплины:

1 – Основы информационной безопасности.

2 – Уровни информационной безопасности.

3 – Основные программно-технические меры информационной безопасности сетей и систем.

2. Планируемые результаты обучения (перечень компетенций)

- ОПК-6 - способность выбирать и оценивать способ реализации информационных систем и устройств (программно-, аппаратно- или программно-аппаратно-) для решения поставленной задачи;

- ПК-16 - способность проводить подготовку документации по менеджменту качества информационных технологий;

- ПК-30 - способность поддерживать работоспособность информационных систем и технологий в заданных функциональных характеристиках и соответствии критериям;

- ПК-31 - способность обеспечивать безопасность и целостность данных информационных систем и технологий.

4. Вид промежуточной аттестации: экзамен, кр.

*Протокол о дополнениях и изменениях в рабочей программе
на 20__-20__ учебный год*

1. В рабочую программу по дисциплине вносятся следующие дополнения:

2. В рабочую программу по дисциплине вносятся следующие изменения:

Протокол заседания кафедры №____ от «__» _____ 20__ г.,
(разработчик)

Заведующий кафедрой _____
(подпись)

(Ф.И.О.)

Программа составлена в соответствии с федеральным государственным образовательным стандартом высшего образования по направлению подготовки 09.03.03 Информационные системы и технологии от «12» марта 2015 г. № 219

для набора 2015 года: и учебным планом ФГБОУ ВО «БрГУ» для очной формы обучения от «03» июля 2018 г. № 413.

для набора 2016 года: и учебным планом ФГБОУ ВО «БрГУ» для очной формы обучения от «16» сентября 2016 г. № 622, заочной формы обучения от «16» сентября 2016 г. № 622

для набора 2017 года: и учебным планом ФГБОУ ВО «БрГУ» для очной формы обучения от «06» марта 2017 г. № 125, заочной формы обучения от «06» марта 2017 г. № 125.

Программу составили:

Мельникова В.А., доцент каф. ИиПМ, к.т.н. _____

Рабочая программа рассмотрена и утверждена на заседании кафедры ИиПМ

от «19» декабря 2018 г., протокол № 5

И.о. заведующего кафедрой ИиПМ _____

А.С. Толстикова

СОГЛАСОВАНО:

Директор библиотеки _____

Т.Ф. Сотник

Рабочая программа одобрена методической комиссией ЕН факультета

от «20» декабря 2018 г., протокол № 4

Председатель методической комиссии факультета _____

М.А. Варданян

СОГЛАСОВАНО:

Начальник
учебно-методического управления _____

Г.П. Нежевец

Регистрационный № _____