МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ

«БРАТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Базовая кафедра менеджмента и информационных технологий

УТВЕРЖДАЮ:
Проректор по учебной работе
_____Е.И. Луковникова
«_____» _____ 201 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Б1.Б.19

НАПРАВЛЕНИЕ ПОДГОТОВКИ

09.03.03 Прикладная информатика

ПРОФИЛЬ ПОДГОТОВКИ

Прикладная информатика в экономике

Программа академического бакалавриата

Квалификация (степень) выпускника: бакалавр

СОДЕРЖАНИЕ ПРОГРАММЫ **Стр.**

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 организационно-управленческому видам профессиональной деятельности выпускника в соответствии с компетенциями и видами деятельности, указанными в учебном плане.

Цель дисциплины

Овладение основами теоретических и практических знаний в области методов и способов обеспечения сохранности, целостности и безопасности информационных ресурсов.

Задачи дисциплины

Задачами изучения дисциплины является формирование у обучающихся систематизированных знаний в области криптографии и шифрования.

Задачи изучения дисциплины направлены на формирование следующих компетенций

Код компетенции	Содержание компетенций	Перечень планируемых результатов обучения по дисциплине
1	2	3
ОК-4	Способность использовать основы правовых знаний в различных сферах деятельности	**знать:** основы правовых знаний **уметь:** использовать основы правовых знаний в различных сферах деятельности **владеть:** навыками использования основ правовых знаний в различных сферах деятельности
ПК-12	Способность проводить тестирование компонентов программного обеспечения информационных систем	**знать:** основы настройки параметров информационных систем в области информационной безопасности (далее – ИБ) и тестирования результатов настройки; **уметь:** вести техническую документацию в области ИБ; **владеть:** навыками технического сопровождения информационных систем в области ИБ в процессе их эксплуатации
ПК-15	Способность осуществлять тестирование компонентов информационных систем по заданным сценариям	**знать:** основы тестирования компонентов информационных систем в области ИБ по заданным сценариям; **уметь:** принимать участие в экспертном тестировании информационных систем в области ИБ на этапе опытной эксплуатации; **владеть:** информационным обеспечением прикладных процессов в области ИБ
ПК-18	Способность принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью	**знать:** методы координации работ по созданию, адаптации и сопровождению информационных систем в области ИБ; **уметь:** управлять техническим сопровождением информационной системы в процессе ее

		эксплуатации с целью обеспечения ИБ; **владеть:** навыками управления ИБ информационных систем

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Информационная безопасность» относится к базовой части.

Дисциплина «Информационная безопасность» базируется на знаниях, полученных при изучении учебных дисциплин «Информатика и программирование», «Информационные системы и технологии», «Компьютерный практикум».

Основываясь на изучении перечисленных дисциплин, дисциплина «Информационная безопасность» представляет основу для изучения следующих дисциплин: «Разработка программных приложений», «Управление информационными ресурсами», «Программная инженерия», «Управление информационными системами».

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*						*Курсовая работа (проект), контрольная работа, реферат, РГР*	*Вид промежуточной аттестации*
			Всего часов (с экз.)	*Аудиторных часов*	*Лекции*	*Лабораторные работы*	*Практические занятия*	*Самостоятельная работа*		
1	2	3	4	5	6	7	8	9	10	11
Очная	3	6	144	54	36	18	–	54	–	экзамен
Заочная	2	–	144	17	5	–	12	118	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 интерактивной, активной, инновационной формах, (час.)*	*Распределение по семестрам, час*
			6
1	2	3	4
I. Контактная работа обучающихся с преподавателем (всего)	54	12	54
Лекции (Лк)	36	6	36
Лабораторные работы (ЛР)	18	6	18
Групповые консультации	+	–	+
II.Самостоятельная работа обучающихся (СР)	54	–	54
Подготовка к лабораторным работам	27	–	27

Подготовка к экзамену в течение семестра		27	–	27
III. Промежуточная аттестация	экзамен	36	–	36
Общая трудоемкость дисциплины:	час.	144	–	144
	зач. ед.	4	–	4

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Распределение разделов дисциплины по видам учебных занятий

- для очной формы обучения:

№ раз-дела и темы	*Наименование раздела и тема дисциплины*	*Трудоем-кость, (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.	**Международные стандарты информационного обмена и угрозы информационной безопасности (далее – ИБ)**	**18**	**6**	–	**12**
1.1.	Международные стандарты информационного обмена	6	2	–	4
1.2.	Понятие и классификация угроз ИБ	6	2	–	4
1.3.	Виды противников или «нарушителей» ИБ	6	2	–	4
2.	**Три вида возможных нарушений безопасности информационной системы**	**12**	**4**	–	**8**
2.1.	Анализ способов нарушений ИБ	6	2	–	4
2.2.	Виды компьютерных вирусов	6	2	–	4
3.	**Основные положения теории информационной безопасности**	**14**	**6**	**–**	**8**
3.1.	Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы	8	4	–	4
3.2.	Модели безопасности и их применение	6	2	–	4
4.	**Основные технологии построения защищенных экономических информационных систем**	**64**	**20**	**18**	**26**
4.1.	Место ИБ экономических систем в национальной безопасности страны	6	2	–	4
4.2.	Концепция ИБ	8	4	–	4
4.3.	Методы криптографии	40	10	16	14
4.4.	Защита и разработка защищенных информационных систем	10	4	2	4
	ИТОГО	**108**	**36**	**18**	**54**

- для заочной формы обучения:

№ раз-дела и темы	*Наименование раздела и тема дисциплины*	*Трудоем-кость, (час.)*	*Виды учебных занятий, включая самостоятельную работу обучающихся и трудоемкость, (час.)*		
			учебные занятия		*самостоятельная работа обучающихся*
			лекции	*практические занятия*	
1	2	3	4	5	6
1.	**Международные стандарты информационного обмена и угрозы информационной безопасности (далее – ИБ)**	**22**	**1,5**	–	**20,5**
1.1.	Международные стандарты информационного обмена	6,5	0,5	–	6
1.2.	Понятие и классификация угроз ИБ	8	0,5	–	7,5
1.3.	Виды противников или «нарушителей» ИБ	7,5	0,5	–	7
2.	**Три вида возможных нарушений безопасности информационной системы**	**19**	**1**	–	**18**
2.1.	Анализ способов нарушений ИБ	9,5	0,5	–	9
2.2.	Виды компьютерных вирусов	9,5	0,5	–	9
3.	**Основные положения теории информационной безопасности**	**21**	**1**	**–**	**20**
3.1.	Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы	10,5	0,5	–	10
3.2.	Модели безопасности и их применение	10,5	0,5	–	10
4.	**Основные технологии построения защищенных экономических информационных систем**	**73**	**1,5**	**12**	**59,5**
4.1.	Место ИБ экономических систем в национальной безопасности страны. Концепция ИБ	10	0,5	–	9,5
4.2.	Методы криптографии	42,5	0,5	10	32
4.3.	Защита и разработка защищенных информационных систем	20,5	0,5	2	18
	ИТОГО	**135**	**5**	**12**	**118**

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, инновационной формах, (час.)*
1	2	3	4
1.	**Международные стандарты информационного обмена и угрозы информационной безопасности (далее – ИБ)**		–
1.1.	Международные стандарты информационного обмена	Рассматриваются международный стандарт информационного обмена UDDI, протоколы WSDL и SOAP, понятие «электронного государства», структура стандартов и методик информационного обмена	–
1.2.	Понятие и классификация угроз ИБ	Дается понятие и классификация угроз ИБ по различным признакам: по аспекту ИБ, компонентам информационных систем, на которые угрозы нацелены, способу осуществления, расположению источника угроз. Рассматриваются формальные модели атак и угроз	Лекция-диспут (2 часа)
1.3.	Виды противников или «нарушителей» ИБ	Анализируются виды противников или «нарушителей» ИБ в зависимости от мотивов, целей и методов действия	Лекция-диспут (2 часа)
2.	**Три вида возможных нарушений безопасности информационной системы**		–
2.1.	Анализ способов нарушений ИБ	Анализируются три основных вида возможных нарушений безопасности информационных ресурсов и систем (нарушение доступности, целостности и конфиденциальности) и поддерживающей инфраструктуры. Рассматриваются конкретные примеры нарушений (информационные войны, компьютерные преступления, взлом парольной защиты, вредоносное программное обеспечение, шпионские программные закладки). Дается понятие несанкционированного доступа к информации, его цели и методы реализации	Лекция-диспут (2 часа)
2.2.	Виды компьютерных вирусов	Рассматриваются основные виды компьютерных вирусов: макровирусы, полиморфные и скрытые вирусы, «троянские кони», «черви», враждебные апплеты Java, механизм и последствия их вредоносного действия	-

1	2	3	4
3.	**Основные положения теории информационной безопасности**		
3.1.	Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы	Рассматриваются базовые отечественные и зарубежные стандарты информационной безопасности компьютерных систем и технологий, федеральные законы и постановления Правительства Российской Федерации, а также основные характеристики стандартов в области ИБ: универсальность, гибкость, гарантированность, реализуемость, актуальность	–
3.2.	Модели безопасности и их применение	Изучаются наиболее распространенные модели безопасности (модель Биба, модель Гогена-Мезегера, Сазерлендская модель защиты, модель Кларка-Вильсона) и их применение на практике	–
4.	**Основные технологии построения защищенных экономических информационных систем**		–
4.1.	Место ИБ экономических систем в национальной безопасности страны	Рассматривается место ИБ экономических систем в национальной безопасности страны на примере способов защиты банковских и платежных систем: использование стойких схем аутентификации, современных систем электронного перевода денежных средств, банковских криптографических протоколов и интеллектуальных карточек	–
4.2.	Концепция ИБ	Дается понятие концепции ИБ и этапы ее разработки, рассматривается создание стратегии безопасности информации и архитектуры системы защиты информации, политики ИБ	–
4.3.	Методы криптографии	Рассматриваются симметричные и асимметричные методы криптографического преобразования информации, понятие абсолютно стойкого шифра, требования, предъявляемые к современным криптографическим системам защиты информации, а также классические методы криптоанализа	–
4.4.	Защита и разработка защищенных информационных систем	Дается понятие защиты информационных систем от несанкционированного использования, рассматриваются основные вида контроля доступа, основанные на владении физическим ключом, личностных характеристиках пользователя, обладании специфической информацией (парольная защита). Рассматриваются примеры реализации защищенных информационных систем на законодательном, административном, процедурном и программно-техническом уровнях	-

4.3. Лабораторные работы

№ п/п	*Номер раздела дисциплины*	*Наименование тем лабораторных работ*	*Объем, (час.)*	*Вид занятия в интерактивной, активной, инновационной формах, (час.)*
1	**4.**	Шифрование текстовой информации случайной перестановкой символов	2	–
2		Шифрование текстовой информации заменой символов	4	–
3		Шифрование текстовой информации случайными сдвигами символов	2	–
4		Шифрование текстовой информации сдвигами по паролю символов	4	Разбор конкретных ситуаций (3 часа)
5		Шифрование текстовой информации заменой части символов	4	Разбор конкретных ситуаций (3 часа)
6		Установка парольной защиты, учетных записей и разграничение прав доступа в клиентских приложениях	2	–
		ИТОГО	**18**	**6**

4.4. Контрольные мероприятия: контрольная работа.

Контрольные мероприятия в рамках данной дисциплины предусмотрены только для заочной формы обучения.

Цель: закрепление теоретических знаний и формирование практических навыков работы в области информационной безопасности с использованием современных средств вычислительной техники и прикладных программ, информационных систем и технологий.

Основная тематика: основные вопросы информационной безопасности в соответствии с вариантом, выдаваемым преподавателем.

Структура: введение, теоретическая часть, практическая часть, заключение, список использованных источников.

Рекомендуемый объем: 12-15 страниц в компьютерном исполнении, оформляемых в соответствии со стандартом ФГБОУ ВО «БрГУ».

Выдача задания, прием и защита контрольной работы проводится в соответствии с календарным учебным графиком.

Оценка	Критерии оценки контрольной работы
зачтено	Оценка «зачтено» за работу выставляется, если в ней: - используется научная, учебная, методическая литература по проблеме; - верно применены полученные знания на практике при решении конкретных задач; - оформление соответствует предъявляемым требованиям (выдержаны орфография, стиль изложения материала, имеются цитаты, ссылки и т.д.); - обучающийся четко и аргументированно отвечает на вопросы по анализируемой теме.

Не зачтено	Оценка «не зачтено» выставляется, если: - библиография ограничена; - обучающийся плохо защищает работу; - оформление не соответствует требованиям.

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

Компетенции / *№, наименование разделов дисциплины*	*Кол-во часов*	*Компетенции*				*Σ комп.*	$t_{ср}$, *час*	*Вид учебных занятий*	*Оценка результатов*
		ОК	*ПК*						
		4	*12*	*15*	*18*				
1	2	3	4	5	6	7	8	9	10
1. Международные стандарты информационного обмена и угрозы информационной безопасности	18	+	+	+	+	4	4,5	Лк, СРС	экзамен
2. Три вида возможных нарушений безопасности информационной системы	12	+	+	+	+	4	3	Лк, СРС	экзамен
3. Основные положения теории информационной безопасности	14	+	+	+	+	4	3,5	Лк, СРС	экзамен
4. Основные технологии построения защищенных экономических информационных систем	64	+	+	+	+	4	16	Лк, ЛР, СРС	экзамен
всего часов	**108**	**27**	**27**	**27**	**27**	**4**	**27**		

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

1. Иванов М.Ю. Информационные технологии: методы криптографии: Учебное пособие / М.Ю. Иванов. – Братск: ГОУ ВПО «БрГУ», 2010. – 100 с.

2. Иванов М.Ю. Информационная безопасность: Методические указания к выполнению лабораторных работ / М.Ю. Иванов. – Братск: Изд-во БрГУ, 2014. – 44 с.

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

№	*Наименование издания*	*Вид занятия*	*Количество экземпляров в библиотеке*, шт.	*Обеспеченность*, (экз./ чел.)
1	2	3	4	5
	Основная литература			
1.	Прохорова О.В. Информационная безопасность и защита информации: Учебник / О.В. Прохорова. – Самара: Самарский госуд. арх.-строит. ун-т, 2014. – 113 с. http://biblioclub.ru/index.php?page=book_red&id=438331&sr=1	Лк, ПЗ, СР	1(ЭУ)	1
2	Ковалев, Д.В. Информационная безопасность : учебное пособие / Д.В. Ковалев, Е.А. Богданова ; Министерство образования и науки РФ, Южный федеральный университет. - Ростов-на-Дону : Издательство Южного федерального университета, 2016. - 74 с. http://biblioclub.ru/index.php?page=book&id=493175	Лк, ПЗ, СР	1(ЭУ)	1
	Дополнительная литература			
3.	Иванов М.Ю. Информационные технологии: методы криптографии: Учебное пособие / М.Ю. Иванов. – Братск: ГОУ ВПО «БрГУ», 2010. – 100 с.	Лк, ПЗ, СР	26	1
4.	Артемов А.В. Информационная безопасность: Курс лекций / А.В. Артемов. – Орел: МАБИВ, 2014. – 257 с. http://biblioclub.ru/index.php?page=book_red&id=428605&sr=1	Лк	1(ЭУ)	1
5.	Партыка Т.Л., Попов И.И. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. – М.: Форум; Инфра-М, 2014. – 432 с. – (Профессиональное образование).	Лк, ПЗ, СР	10	1
6.	Загинайлов Ю.Н. Теория информационной безопасности и методология защиты информации: Учебное пособие / Ю.Н. Загинайлов. – Москва-Берлин: DirectMedia, 2015. – 253 с. http://biblioclub.ru/index.php?page=book_red&id=276557&sr=1	Лк, ПЗ, СР	1(ЭУ)	1
7.	Нестеров С.А. Основы информационной безопасности: Учебное пособие / С.А. Нестеров. – СПб: Изд-во Политехнического ун-та, 2014. – 322 с. http://biblioclub.ru/index.php?page=book_red&id=363040&sr=1	Лк, ПЗ, СР	1(ЭУ)	1
8.	Иванов М.Ю. Информационная безопасность: Методические указания к выполнению лабораторных работ / М.Ю. Иванов. – Братск: Изд-во БрГУ, 2014. – 44 с.	ПЗ	25	1

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. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Вид учебных занятий	Организация деятельности обучающихся
1	**2**
Лекции	Написание конспекта лекций с выполнением требований кратко, последовательно и четко фиксировать основные положения, выводы, формулировки, обобщения; отмечать важные моменты, выделять ключевые слова, термины. Проверка терминов с помощью энциклопедий, словарей, справочников с выписыванием толкований. Конспект лекций позволяет обозначить вопросы, термины, материал, который вызывает трудности усвоения. В случае невозможности самостоятельно найти ответ в рекомендуемой литературе, необходимо сформулировать вопросы и задать их преподавателю на консультации или при выполнении лабораторных работ
Лабораторные работы	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 в лабораторных работах, решение задач, активное участие в интерактивной, активной, инновационной формах обучения, составление письменных отчетов
Самостоятельная работа обучающихся	*Подготовка к практическим занятиям.* Проработка основной и дополнительной литературы, терминов, сведений, требующихся для запоминания и являющихся основополагающими в теме / разделе. Конспектирование прочитанных литературных источников. Проработка материалов по изучаемому вопросу, с использованием на рекомендуемых ресурсов информационно-телекоммуникационной сети «Интернет». Выполнение заданий преподавателя, необходимых для подготовки к участию в интерактивной, активной, инновационных формах обучения по

	изучаемой теме. *Подготовка к экзамену.* При подготовке к экзамену необходимо ориентироваться на конспекты лекций, рекомендуемую литературу, использовать рекомендуемые ресурсы информационно-телекоммуникационной сети «Интернет»

9.1. Методические указания для обучающихся по выполнению лабораторных работ

Лабораторная работа №1

Тема:

Шифрование текстовой информации случайной перестановкой символов.

Цель работы:

Приобретение практических навыков криптографического преобразования (шифрования) текстовой информации случайной перестановкой символов.

Задание:

1. Осуществить криптографическое преобразование (шифрование) текстовой информации случайной перестановкой символов с помощью интегрированной среды разработки программного обеспечения Turbo Pascal.

Порядок выполнения:

Разработать алгоритм шифрования с учетом возможностей интегрированной среды разработки программного обеспечения Turbo Pascal, написать программу для ЭВМ для шифрования и дешифрования текстовой информации случайной перестановкой символов, протестировать работу программы для ЭВМ на предмет корректного шифрования и дешифрования текстовой информации.

Форма отчетности:

Письменный отчет, отражающий:

1. этапы пошаговой разработки программы для ЭВМ, всех использованных процедур, функций и т.п., а также скриншоты, иллюстрирующие основные моменты выполнения задания по шифрованию текстовой информации случайной перестановкой символов;
2. выводы, сформулированные в результате выполнения задания.

Задания для самостоятельной работы:

1. проанализировать рекомендуемые источники информации, основную и дополнительную литературу по изучаемому вопросу с целью углубления, систематизации и расширения полученных знаний.
2. письменно ответить на контрольные вопросы для самопроверки.

Рекомендации по выполнению задания и подготовке к лабораторной работе:

Проработка основной и дополнительной литературы, терминов, сведений, требующихся для запоминания и являющихся основополагающими в данной теме. Краткое конспектирование наиболее важных литературных источников. Анализ материалов по изучаемому вопросу, с использованием рекомендуемых ресурсов информационно-телекоммуникационной сети «Интернет». Подготовка к обсуждению особенностей практического использования изученных способов и инструментов криптографического преобразования (шифрования) текстовой информации случайной перестановкой символов в результате выполнения задания.

Рекомендуемые источники:

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. Справочно-правовая система «КонсультантПлюс» www.consultant.ru

5. Научная электронная библиотека eLIBRARY.RU www.elibrary.ru/

6. Университетская информационная система РОССИЯ (УИС РОССИЯ) www.uisrussia.msu.ru

7. Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» http://www.consultant.ru/document/cons_doc_LAW_208191/

8. ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» http://www.internet-law.ru/gosts/gost/8419/

9. ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности» http://www.internet-law.ru/gosts/gost/54705/

10. ГОСТ Р ИСО/МЭК 15408-1-2012 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель» http://www.internet-law.ru/gosts/gost/54198/

11. ГОСТ Р ИСО/МЭК 15408-2-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности» http://www.internet-law.ru/gosts/gost/55439/

12. ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности» http://www.internet-law.ru/gosts/gost/55440/

13. ГОСТ Р ИСО/МЭК 18045-2013 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий» http://www.internet-law.ru/gosts/gost/55239/

14. Журнал «Информационная безопасность» http://www.itsec.ru/articles2/allpubliks

15. Журнал «Информация и безопасность» https://elibrary.ru/contents.asp?titleid=8748

16. Журнал «Вопросы кибербезопасности» http://cyberrus.com/

Основная литература

1. Прохорова О.В. Информационная безопасность и защита информации: Учебник / О.В. Прохорова. – Самара: Самарский госуд. арх.-строит. ун-т, 2014. – 113 с. http://biblioclub.ru/index.php?page=book_red&id=438331&sr=1

2. Ковалев, Д.В. Информационная безопасность : учебное пособие / Д.В. Ковалев, Е.А. Богданова ; Министерство образования и науки РФ, Южный федеральный университет. - Ростов-на-Дону : Издательство Южного федерального университета, 2016. - 74 с. http://biblioclub.ru/index.php?page=book&id=493175

Дополнительная литература

3. Иванов М.Ю. Информационная безопасность: Методические указания к выполнению лабораторных работ / М.Ю. Иванов. – Братск: Изд-во БрГУ, 2014. – 44 с.

4. Иванов М.Ю. Информационные технологии: методы криптографии: Учебное пособие / М.Ю. Иванов. – Братск: ГОУ ВПО «БрГУ», 2010. – 100 с.

5. Партыка Т.Л., Попов И.И. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. – М.: Форум; Инфра-М, 2014. – 432 с. – (Профессиональное образование).

6. Загинайлов Ю.Н. Теория информационной безопасности и методология защиты информации: Учебное пособие / Ю.Н. Загинайлов. – Москва-Берлин: DirectMedia, 2015. – 253 с. http://biblioclub.ru/index.php?page=book_red&id=276557&sr=1

7. Нестеров С.А. Основы информационной безопасности: Учебное пособие / С.А. Нестеров. – СПб: Изд-во Политехнического ун-та, 2014. – 322 с. http://biblioclub.ru/index.php?page=book_red&id=363040&sr=1

Контрольные вопросы для самопроверки:

1. Дайте определение понятиям «криптография», «криптоанализ», «шифрование», «шифр», «ключ».
2. Перечислите основные методы криптографии. В чем заключаются их достоинства и недостатки?
3. Опишите основные способы криптографических преобразований.
4. Дайте характеристику базовым симметричным криптоалгоритмам.
5. Опишите блочный метод шифрования информации. Перечислите требования, которым должна удовлетворять функция криптопреобразования стойкого блочного шифра.

Лабораторная работа №2

Тема:

Шифрование текстовой информации заменой символов.

Цель работы:

Приобретение практических навыков криптографического преобразования (шифрования) текстовой информации заменой символов.

Задание:

1. Осуществить криптографическое преобразование (шифрование) текстовой информации заменой символов с использованием шифра Цезаря с помощью интегрированной среды разработки программного обеспечения Turbo Pascal.

Порядок выполнения:

Разработать и математически обосновать алгоритм шифрования с учетом возможностей интегрированной среды разработки программного обеспечения Turbo Pascal, написать программу для ЭВМ для шифрования и дешифрования текстовой информации заменой символов с учетом требований шифра Цезаря, протестировать работу программы для ЭВМ на предмет корректного шифрования и дешифрования текстовой информации.

Форма отчетности:

Письменный отчет, отражающий:

1. этапы пошаговой разработки программы для ЭВМ, всех использованных процедур, функций и т.п., а также скриншоты, иллюстрирующие основные моменты выполнения задания по шифрованию текстовой информации заменой символов;
2. выводы, сформулированные в результате выполнения задания.

Задания для самостоятельной работы:

1. проанализировать рекомендуемые источники информации, основную и дополнительную литературу по изучаемому вопросу с целью углубления, систематизации и расширения полученных знаний.
2. письменно ответить на контрольные вопросы для самопроверки.

Рекомендации по выполнению задания и подготовке к лабораторной работе:

Проработка основной и дополнительной литературы, терминов, сведений, требующихся для запоминания и являющихся основополагающими в данной теме. Краткое конспектирование наиболее важных литературных источников. Анализ материалов по изучаемому вопросу, с использованием рекомендуемых ресурсов информационно-

телекоммуникационной сети «Интернет». Подготовка к обсуждению особенностей практического использования изученных способов и инструментов криптографического преобразования (шифрования) текстовой информации заменой символов в результате выполнения задания.

Рекомендуемые источники:

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. Справочно-правовая система «КонсультантПлюс» www.consultant.ru
5. Научная электронная библиотека eLIBRARY.RU www.elibrary.ru/
6. Университетская информационная система РОССИЯ (УИС РОССИЯ) www.uisrussia.msu.ru
7. Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» http://www.consultant.ru/document/cons_doc_LAW_208191/
8. ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» http://www.internet-law.ru/gosts/gost/8419/
9. ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности» http://www.internet-law.ru/gosts/gost/54705/
10. ГОСТ Р ИСО/МЭК 15408-1-2012 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель» http://www.internet-law.ru/gosts/gost/54198/
11. ГОСТ Р ИСО/МЭК 15408-2-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности» http://www.internet-law.ru/gosts/gost/55439/
12. ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности» http://www.internet-law.ru/gosts/gost/55440/
13. ГОСТ Р ИСО/МЭК 18045-2013 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий» http://www.internet-law.ru/gosts/gost/55239/
14. Журнал «Информационная безопасность» http://www.itsec.ru/articles2/allpubliks
15. Журнал «Информация и безопасность» https://elibrary.ru/contents.asp?titleid=8748
16. Журнал «Вопросы кибербезопасности» http://cyberrus.com/

Основная литература

1. Прохорова О.В. Информационная безопасность и защита информации: Учебник / О.В. Прохорова. – Самара: Самарский госуд. арх.-строит. ун-т, 2014. – 113 с. http://biblioclub.ru/index.php?page=book_red&id=438331&sr=1
2. Ковалев, Д.В. Информационная безопасность : учебное пособие / Д.В. Ковалев, Е.А. Богданова ; Министерство образования и науки РФ, Южный федеральный университет. - Ростов-на-Дону : Издательство Южного федерального университета, 2016. - 74 с. http://biblioclub.ru/index.php?page=book&id=493175

Дополнительная литература

3. Иванов М.Ю. Информационная безопасность: Методические указания к выполнению лабораторных работ / М.Ю. Иванов. – Братск: Изд-во БрГУ, 2014. – 44 с.
4. Иванов М.Ю. Информационные технологии: методы криптографии: Учебное пособие / М.Ю. Иванов. – Братск: ГОУ ВПО «БрГУ», 2010. – 100 с.

5. Партыка Т.Л., Попов И.И. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. – М.: Форум; Инфра-М, 2014. – 432 с. – (Профессиональное образование).

6. Загинайлов Ю.Н. Теория информационной безопасности и методология защиты информации: Учебное пособие / Ю.Н. Загинайлов. – Москва-Берлин: DirectMedia**,** 2015. – 253 с. http://biblioclub.ru/index.php?page=book_red&id=276557&sr=1

7. Нестеров С.А. Основы информационной безопасности: Учебное пособие / С.А. Нестеров. – СПб: Изд-во Политехнического ун-та, 2014. – 322 с. http://biblioclub.ru/index.php?page=book_red&id=363040&sr=1

Контрольные вопросы для самопроверки:

1. Дайте определение и приведите характеристику шифров замены.
2. Перечислите наиболее известные шифры замены. Каковы их достоинства и недостатки?
3. В чем заключается стойкость шифра?
4. Опишите сущность шифра Цезаря.
5. Каким образом реализуются алгоритмические и математические основы шифрования заменой символов на практике?

Лабораторная работа №3

Тема:

Шифрование текстовой информации случайными сдвигами символов.

Цель работы:

Приобретение практических навыков криптографического преобразования (шифрования) текстовой информации случайными сдвигами символов.

Задание:

1. Осуществить криптографическое преобразование (шифрование) текстовой информации случайными сдвигами символов с использованием шифра Цезаря с помощью интегрированной среды разработки программного обеспечения Turbo Pascal.

Порядок выполнения:

Разработать алгоритм шифрования с учетом возможностей интегрированной среды разработки программного обеспечения Turbo Pascal, написать программу для ЭВМ для шифрования и дешифрования текстовой информации случайными сдвигами символов с учетом требований шифра Цезаря, протестировать работу программы для ЭВМ на предмет корректного шифрования и дешифрования текстовой информации.

Форма отчетности:

Письменный отчет, отражающий:

1. этапы пошаговой разработки программы для ЭВМ, всех использованных процедур, функций и т.п., а также скриншоты, иллюстрирующие основные моменты выполнения задания по шифрованию текстовой информации случайными сдвигами символов;
2. выводы, сформулированные в результате выполнения задания.

Задания для самостоятельной работы:

1. проанализировать рекомендуемые источники информации, основную и дополнительную литературу по изучаемому вопросу с целью углубления, систематизации и расширения полученных знаний.
2. письменно ответить на контрольные вопросы для самопроверки.

Рекомендации по выполнению задания и подготовке к лабораторной работе:

Проработка основной и дополнительной литературы, терминов, сведений, требующихся для запоминания и являющихся основополагающими в данной теме. Краткое конспектирование наиболее важных литературных источников. Анализ материалов по изучаемому вопросу, с использованием рекомендуемых ресурсов информационно-телекоммуникационной сети «Интернет». Подготовка к обсуждению особенностей практического использования изученных способов и инструментов криптографического преобразования (шифрования) текстовой информации случайными сдвигами символов в результате выполнения задания.

Рекомендуемые источники:

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. Справочно-правовая система «КонсультантПлюс» www.consultant.ru
5. Научная электронная библиотека eLIBRARY.RU www.elibrary.ru/
6. Университетская информационная система РОССИЯ (УИС РОССИЯ) www.uisrussia.msu.ru
7. Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» http://www.consultant.ru/document/cons_doc_LAW_208191/
8. ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» http://www.internet-law.ru/gosts/gost/8419/
9. ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности» http://www.internet-law.ru/gosts/gost/54705/
10. ГОСТ Р ИСО/МЭК 15408-1-2012 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель» http://www.internet-law.ru/gosts/gost/54198/
11. ГОСТ Р ИСО/МЭК 15408-2-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности» http://www.internet-law.ru/gosts/gost/55439/
12. ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности» http://www.internet-law.ru/gosts/gost/55440/
13. ГОСТ Р ИСО/МЭК 18045-2013 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий» http://www.internet-law.ru/gosts/gost/55239/
14. Журнал «Информационная безопасность» http://www.itsec.ru/articles2/allpubliks
15. Журнал «Информация и безопасность» https://elibrary.ru/contents.asp?titleid=8748
16. Журнал «Вопросы кибербезопасности» http://cyberrus.com/

Основная литература

1. Прохорова О.В. Информационная безопасность и защита информации: Учебник / О.В. Прохорова. – Самара: Самарский госуд. арх.-строит. ун-т, 2014. – 113 с. http://biblioclub.ru/index.php?page=book_red&id=438331&sr=1

2. Ковалев, Д.В. Информационная безопасность : учебное пособие / Д.В. Ковалев, Е.А. Богданова ; Министерство образования и науки РФ, Южный федеральный университет. - Ростов-на-Дону : Издательство Южного федерального университета, 2016. - 74 с. http://biblioclub.ru/index.php?page=book&id=493175

Дополнительная литература

3. Иванов М.Ю. Информационная безопасность: Методические указания к выполнению лабораторных работ / М.Ю. Иванов. – Братск: Изд-во БрГУ, 2014. – 44 с.

4. Иванов М.Ю. Информационные технологии: методы криптографии: Учебное пособие / М.Ю. Иванов. – Братск: ГОУ ВПО «БрГУ», 2010. – 100 с.

5. Партыка Т.Л., Попов И.И. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. – М.: Форум; Инфра-М, 2014. – 432 с. – (Профессиональное образование).

6. Загинайлов Ю.Н. Теория информационной безопасности и методология защиты информации: Учебное пособие / Ю.Н. Загинайлов. – Москва-Берлин: DirectMedia, 2015. – 253 с. http://biblioclub.ru/index.php?page=book_red&id=276557&sr=1

7. Нестеров С.А. Основы информационной безопасности: Учебное пособие / С.А. Нестеров. – СПб: Изд-во Политехнического ун-та, 2014. – 322 с. http://biblioclub.ru/index.php?page=book_red&id=363040&sr=1

Контрольные вопросы для самопроверки:

1. Какие прикладные задачи решаются с помощью шифрования?
2. Что представляет собой гаммирование?
3. Перечислите базовые биективные математические функции, используемые в криптографии.
4. Предложите и обоснуйте способы повышения криптографической стойкости шифра Цезаря.

Лабораторная работа №4

Тема:

Шифрование текстовой информации сдвигами по паролю символов.

Цель работы:

Приобретение практических навыков криптографического преобразования (шифрования) текстовой информации сдвигами по паролю символов.

Задание:

1. Осуществить криптографическое преобразование (шифрование) текстовой информации сдвигами по паролю символов с использованием блочного шифра с помощью интегрированной среды разработки программного обеспечения Turbo Pascal.

Порядок выполнения:

Разработать алгоритм шифрования с учетом возможностей интегрированной среды разработки программного обеспечения Turbo Pascal, написать программу для ЭВМ для шифрования и дешифрования текстовой информации сдвигами по паролю символов, протестировать работу программы для ЭВМ на предмет корректного шифрования и дешифрования текстовой информации.

Форма отчетности:

Письменный отчет, отражающий:

1. этапы пошаговой разработки программы для ЭВМ, всех использованных процедур, функций и т.п., а также скриншоты, иллюстрирующие основные моменты выполнения задания по шифрованию текстовой информации сдвигами по паролю символов;
2. выводы, сформулированные в результате разбора конкретных ситуаций.

Задания для самостоятельной работы:

1. проанализировать рекомендуемые источники информации, основную и дополнительную литературу по изучаемому вопросу с целью углубления, систематизации и расширения полученных знаний.

2. письменно ответить на контрольные вопросы для самопроверки.

Рекомендации по выполнению задания и подготовке к лабораторной работе:

Проработка основной и дополнительной литературы, терминов, сведений, требующихся для запоминания и являющихся основополагающими в данной теме. Краткое конспектирование наиболее важных литературных источников. Анализ материалов по изучаемому вопросу, с использованием рекомендуемых ресурсов информационно-телекоммуникационной сети «Интернет». Подготовка к обсуждению особенностей практического использования изученных способов и инструментов криптографического преобразования (шифрования) текстовой информации сдвигами по паролю символов в результате разбора конкретных ситуаций.

Рекомендуемые источники:

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. Справочно-правовая система «КонсультантПлюс» www.consultant.ru
5. Научная электронная библиотека eLIBRARY.RU www.elibrary.ru/
6. Университетская информационная система РОССИЯ (УИС РОССИЯ) www.uisrussia.msu.ru
7. Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» http://www.consultant.ru/document/cons_doc_LAW_208191/
8. ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» http://www.internet-law.ru/gosts/gost/8419/
9. ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности» http://www.internet-law.ru/gosts/gost/54705/
10. ГОСТ Р ИСО/МЭК 15408-1-2012 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель» http://www.internet-law.ru/gosts/gost/54198/
11. ГОСТ Р ИСО/МЭК 15408-2-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности» http://www.internet-law.ru/gosts/gost/55439/
12. ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности» http://www.internet-law.ru/gosts/gost/55440/
13. ГОСТ Р ИСО/МЭК 18045-2013 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий» http://www.internet-law.ru/gosts/gost/55239/
14. Журнал «Информационная безопасность» http://www.itsec.ru/articles2/allpubliks
15. Журнал «Информация и безопасность» https://elibrary.ru/contents.asp?titleid=8748
16. Журнал «Вопросы кибербезопасности» http://cyberrus.com/

Основная литература

1. Прохорова О.В. Информационная безопасность и защита информации: Учебник / О.В. Прохорова. – Самара: Самарский госуд. арх.-строит. ун-т, 2014. – 113 с. http://biblioclub.ru/index.php?page=book_red&id=438331&sr=1
2. Ковалев, Д.В. Информационная безопасность : учебное пособие / Д.В. Ковалев, Е.А. Богданова ; Министерство образования и науки РФ, Южный федеральный университет. -

Ростов-на-Дону : Издательство Южного федерального университета, 2016. - 74 с. http://biblioclub.ru/index.php?page=book&id=493175

Дополнительная литература

3. Иванов М.Ю. Информационная безопасность: Методические указания к выполнению лабораторных работ / М.Ю. Иванов. – Братск: Изд-во БрГУ, 2014. – 44 с.

4. Иванов М.Ю. Информационные технологии: методы криптографии: Учебное пособие / М.Ю. Иванов. – Братск: ГОУ ВПО «БрГУ», 2010. – 100 с.

5. Партыка Т.Л., Попов И.И. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. – М.: Форум; Инфра-М, 2014. – 432 с. – (Профессиональное образование).

6. Загинайлов Ю.Н. Теория информационной безопасности и методология защиты информации: Учебное пособие / Ю.Н. Загинайлов. – Москва-Берлин: DirectMedia**,** 2015. – 253 с. http://biblioclub.ru/index.php?page=book_red&id=276557&sr=1

7. Нестеров С.А. Основы информационной безопасности: Учебное пособие / С.А. Нестеров. – СПб: Изд-во Политехнического ун-та, 2014. – 322 с. http://biblioclub.ru/index.php?page=book_red&id=363040&sr=1

Контрольные вопросы для самопроверки:

1. В чем заключается сущность блочного шифрования?
2. Чем принципиально отличается алгоритм блочного шифрования с использованием пароля?
3. Дайте определение понятию «пароль».
4. Какие недостатки присущи стандартным датчикам случайных чисел?

Лабораторная работа №5

Тема:

Шифрование текстовой информации заменой части символов.

Цель работы:

Приобретение практических навыков криптографического преобразования (шифрования) текстовой информации заменой части символов.

Задание:

1. Осуществить криптографическое преобразование (шифрование) текстовой информации заменой части символов с использованием блочного шифра с помощью интегрированной среды разработки программного обеспечения Turbo Pascal.

Порядок выполнения:

Разработать алгоритм шифрования с учетом возможностей интегрированной среды разработки программного обеспечения Turbo Pascal, написать программу для ЭВМ для шифрования и дешифрования текстовой информации заменой части символов, протестировать работу программы для ЭВМ на предмет корректного шифрования и дешифрования текстовой информации.

Форма отчетности:

Письменный отчет, отражающий:

1. этапы пошаговой разработки программы для ЭВМ, всех использованных процедур, функций и т.п., а также скриншоты, иллюстрирующие основные моменты выполнения задания по шифрованию текстовой информации заменой части символов;
2. выводы, сформулированные в результате разбора конкретных ситуаций.

Задания для самостоятельной работы:

1. проанализировать рекомендуемые источники информации, основную и

дополнительную литературу по изучаемому вопросу с целью углубления, систематизации и расширения полученных знаний.

2. письменно ответить на контрольные вопросы для самопроверки.

Рекомендации по выполнению задания и подготовке к лабораторной работе:

Проработка основной и дополнительной литературы, терминов, сведений, требующихся для запоминания и являющихся основополагающими в данной теме. Краткое конспектирование наиболее важных литературных источников. Анализ материалов по изучаемому вопросу, с использованием рекомендуемых ресурсов информационно-телекоммуникационной сети «Интернет». Подготовка к обсуждению особенностей практического использования изученных способов и инструментов криптографического преобразования (шифрования) текстовой информации заменой части символов в результате разбора конкретных ситуаций.

Рекомендуемые источники:

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. Справочно-правовая система «КонсультантПлюс» www.consultant.ru

5. Научная электронная библиотека eLIBRARY.RU www.elibrary.ru/

6. Университетская информационная система РОССИЯ (УИС РОССИЯ) www.uisrussia.msu.ru

7. Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» http://www.consultant.ru/document/cons_doc_LAW_208191/

8. ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» http://www.internet-law.ru/gosts/gost/8419/

9. ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности» http://www.internet-law.ru/gosts/gost/54705/

10. ГОСТ Р ИСО/МЭК 15408-1-2012 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель» http://www.internet-law.ru/gosts/gost/54198/

11. ГОСТ Р ИСО/МЭК 15408-2-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности» http://www.internet-law.ru/gosts/gost/55439/

12. ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности» http://www.internet-law.ru/gosts/gost/55440/

13. ГОСТ Р ИСО/МЭК 18045-2013 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий» http://www.internet-law.ru/gosts/gost/55239/

14. Журнал «Информационная безопасность» http://www.itsec.ru/articles2/allpubliks

15. Журнал «Информация и безопасность» https://elibrary.ru/contents.asp?titleid=8748

16. Журнал «Вопросы кибербезопасности» http://cyberrus.com/

Основная литература

1. Прохорова О.В. Информационная безопасность и защита информации: Учебник / О.В. Прохорова. – Самара: Самарский госуд. арх.-строит. ун-т, 2014. – 113 с. http://biblioclub.ru/index.php?page=book_red&id=438331&sr=1

2. Ковалев, Д.В. Информационная безопасность : учебное пособие / Д.В. Ковалев, Е.А. Богданова ; Министерство образования и науки РФ, Южный федеральный университет. - Ростов-на-Дону : Издательство Южного федерального университета, 2016. - 74 с. http://biblioclub.ru/index.php?page=book&id=493175

Дополнительная литература

3. Иванов М.Ю. Информационная безопасность: Методические указания к выполнению лабораторных работ / М.Ю. Иванов. – Братск: Изд-во БрГУ, 2014. – 44 с.

4. Иванов М.Ю. Информационные технологии: методы криптографии: Учебное пособие / М.Ю. Иванов. – Братск: ГОУ ВПО «БрГУ», 2010. – 100 с.

5. Партыка Т.Л., Попов И.И. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. – М.: Форум; Инфра-М, 2014. – 432 с. – (Профессиональное образование).

6. Загинайлов Ю.Н. Теория информационной безопасности и методология защиты информации: Учебное пособие / Ю.Н. Загинайлов. – Москва-Берлин: DirectMedia**,** 2015. – 253 с. http://biblioclub.ru/index.php?page=book_red&id=276557&sr=1

7. Нестеров С.А. Основы информационной безопасности: Учебное пособие / С.А. Нестеров. – СПб: Изд-во Политехнического ун-та, 2014. – 322 с. http://biblioclub.ru/index.php?page=book_red&id=363040&sr=1

Контрольные вопросы для самопроверки:

1. Какие недостатки присущи криптографическим преобразованиям текста на основе перестановок и циклических замен?
2. Каким образом осуществляется шифрование текстовой информации заменой части символов?
3. Какие процедуры дополнительно необходимы (по сравнению с традиционным шифром Цезаря) для реализации алгоритма шифрования текстовой информации заменой части символов?

Лабораторная работа №6

Тема:

Установка парольной защиты, учетных записей и разграничение прав доступа в клиентских приложениях.

Цель работы:

Приобретение практических навыков установки парольной защиты, учетных записей и разграничения прав доступа в клиентских приложениях.

Задание:

1. Осуществить установку парольной защиты, учетных записей и разграничение прав доступа в клиентских приложениях, созданных с помощью СУБД MS Access.

Порядок выполнения:

Установить парольную защиту с учётом современных требований, предъявляемых к паролям, учетные записи пользователей и разграничение прав доступа в клиентском приложении, созданном с помощью СУБД MS Access (клиентское приложение создается при изучении дисциплины «Информационные системы и технологии»), протестировать работу парольной защиты и разграничения прав доступа.

Форма отчетности:

Письменный отчет, отражающий:

1. этапы пошаговой установки парольной защиты, учётных записей и разграничения прав доступа в клиентских приложениях, описание всех использованных команд и опций

СУБД MS Access, а также скриншоты, иллюстрирующие основные моменты выполнения задания;

2. выводы, сформулированные в результате выполнения задания.

Задания для самостоятельной работы:

1. проанализировать рекомендуемые источники информации, основную и дополнительную литературу по изучаемому вопросу с целью углубления, систематизации и расширения полученных знаний.

2. письменно ответить на контрольные вопросы для самопроверки.

Рекомендации по выполнению задания и подготовке к лабораторной работе:

Проработка основной и дополнительной литературы, терминов, сведений, требующихся для запоминания и являющихся основополагающими в данной теме. Краткое конспектирование наиболее важных литературных источников. Анализ материалов по изучаемому вопросу, с использованием рекомендуемых ресурсов информационно-телекоммуникационной сети «Интернет». Подготовка к обсуждению особенностей практического использования изученных способов и инструментов парольной защиты, учетных записей и разграничения прав доступа в клиентских приложениях, созданных с помощью СУБД MS Access в результате выполнения задания.

Рекомендуемые источники:

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. Справочно-правовая система «КонсультантПлюс» www.consultant.ru

5. Научная электронная библиотека eLIBRARY.RU www.elibrary.ru/

6. Университетская информационная система РОССИЯ (УИС РОССИЯ) www.uisrussia.msu.ru

7. Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» http://www.consultant.ru/document/cons_doc_LAW_208191/

8. ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» http://www.internet-law.ru/gosts/gost/8419/

9. ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности» http://www.internet-law.ru/gosts/gost/54705/

10. ГОСТ Р ИСО/МЭК 15408-1-2012 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель» http://www.internet-law.ru/gosts/gost/54198/

11. ГОСТ Р ИСО/МЭК 15408-2-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности» http://www.internet-law.ru/gosts/gost/55439/

12. ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности» http://www.internet-law.ru/gosts/gost/55440/

13. ГОСТ Р ИСО/МЭК 18045-2013 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий» http://www.internet-law.ru/gosts/gost/55239/

14. Журнал «Информационная безопасность» http://www.itsec.ru/articles2/allpubliks

15. Журнал «Информация и безопасность» https://elibrary.ru/contents.asp?titleid=8748

16. Журнал «Вопросы кибербезопасности» http://cyberrus.com/

Основная литература

1. Прохорова О.В. Информационная безопасность и защита информации: Учебник / О.В. Прохорова. – Самара: Самарский госуд. арх.-строит. ун-т, 2014. – 113 с. http://biblioclub.ru/index.php?page=book_red&id=438331&sr=1

2. Ковалев, Д.В. Информационная безопасность : учебное пособие / Д.В. Ковалев, Е.А. Богданова ; Министерство образования и науки РФ, Южный федеральный университет. - Ростов-на-Дону : Издательство Южного федерального университета, 2016. - 74 с. http://biblioclub.ru/index.php?page=book&id=493175

Дополнительная литература

3. Иванов М.Ю. Информационная безопасность: Методические указания к выполнению лабораторных работ / М.Ю. Иванов. – Братск: Изд-во БрГУ, 2014. – 44 с.

4. Иванов М.Ю. Информационные технологии: методы криптографии: Учебное пособие / М.Ю. Иванов. – Братск: ГОУ ВПО «БрГУ», 2010. – 100 с.

5. Партыка Т.Л., Попов И.И. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. – М.: Форум; Инфра-М, 2014. – 432 с. – (Профессиональное образование).

6. Загинайлов Ю.Н. Теория информационной безопасности и методология защиты информации: Учебное пособие / Ю.Н. Загинайлов. – Москва-Берлин: DirectMedia**,** 2015. – 253 с. http://biblioclub.ru/index.php?page=book_red&id=276557&sr=1

7. Нестеров С.А. Основы информационной безопасности: Учебное пособие / С.А. Нестеров. – СПб: Изд-во Политехнического ун-та, 2014. – 322 с. http://biblioclub.ru/index.php?page=book_red&id=363040&sr=1

Контрольные вопросы для самопроверки:

1. Назовите самое распространённое в настоящее время в автоматизированных информационных системах средство защиты. Почему, на ваш взгляд, оно является таковым?
2. Перечислите наиболее известные группы паролей и дайте им характеристику?
3. Опишите функции систем разграничения прав доступа.
4. Перечислите уровни защиты клиентских приложений и связанных с ними баз данных.
5. Перечислите встроенные учётные записи СУБД MS Access и дайте им краткую характеристику.
6. Опишите существующие типы разрешений на доступ к базе данных в СУБД MS Access.

9.2 Методические указания по выполнению контрольной работы

Контрольная работа должна представлять собой реферат на тему, связанную с информационной и компьютерной безопасностью, применением современных организационных правовых и технических средств защиты информации на объектах, в компьютерных системах и сетях.

Структурно контрольная работа выполняется в виде реферата, содержащего: введение (цель, задачи, ожидаемые результаты), основную часть (анализ состояния проблемы, задачи предметной области) и заключение (оценка состояния проблемы, выводы), перечень использованной литературы.

Основная (аналитическая) часть состоит из двух-четырех вопросов, и рассматривается как единое целое, в котором автор раскрывает содержание вопросов темы, показывая умение самостоятельного изложения изученных вопросов на основе анализа опубликованной литературы. Каждый вопрос должен иметь заголовок, отражающий содержание и не повторяющий название работы, заканчивающийся кратким выводом.

Логическим завершением всей работы является заключение, где автор показывает значение рассматриваемых теоретических положений и формулирует выводы, характеризует

практическую значимость освоенной темы для изучения предмета в целом и предлагает свои рекомендации о возможности внедрения полученных результатов исследования в практику, что является отражением качества выполнения поставленной автором задачи.

В список литературы включаются: научная литература, материалы периодической печати и другие источники, изученные автором в процессе подготовки работы. Список литературы составляется в алфавитном порядке с учетом правил оформления библиографии.

Объем работы – 12-15 листов формата А4 в компьютерном исполнении. Контрольная работа выполняется в соответствии с общими требованиями, предъявляемыми к оформлению контрольных работ.

К рассмотрению в контрольной работе представлены следующие темы:

1. Основы информационной безопасности и защиты информации
2. Теоретические и концептуальные основы защиты информации.
3. Принципы защиты информации.
4. Цели и значение защиты информации.
5. Задачи защиты информации и функции по их реализации.
6. Виды, методы и средства защиты информации.
7. Кадровое и ресурсное обеспечение защиты информации.
8. Нормативно-правовая база информационной безопасности
9. Виды и особенности угроз информационной безопасности
10. Каналы утечки информации
11. Организационные основы защиты информации организации
12. Инженерно-технические и программные методы защиты информации в организации
13. Оценка эффективности мероприятий по защите информации в организации
14. Шифрование информации в России: исторический аспект
15. Ответственность за разглашение конфиденциальной информации и государственной тайны
16. Угрозы информационной безопасности организации: виды, способы предупреждения
17. Организация защиты информации в системе менеджмента качества (стандарты ИСО серии 9000)
18. Информационная безопасность в условиях функционирования в России глобальных сетей.

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

— Microsoft Windows Professional Russian;
— Microsoft Office Russian;
— Антивирусное программное обеспечение Kaspersky Security;
— Справочно-правовая система «Консультант Плюс»;
— PascalABC

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

Вид занятия	*Наименование аудитории*	*Перечень основного оборудования*	*№ Лк или ЛР*
1	**2**	**3**	**4**
Лк	Лекционная аудитория (мультимедийный класс)	Интерактивная доска SMART Board 680i2/Unifl, Интерактивный планшет Wacom PL-720, Колонки Microlab Solo-7C, Ноутбук Samsung R610<NP-R610-FS08>, Телевизор плазменный Samsung 63 PS-63A756T1M	Лк № 1-4
ЛР	Дисплейный класс	Системный блок AMD A10-7800 Radeon R7 (12 шт.), Системный блок для слабовидящих пользователей AMD A10-7850K (1 шт.), Монитор Philips233 V5QHABP (13 шт.)	ЛР № 1-6
СР	Читальный зал №1	Оборудование 10 ПК i5-2500/H67/4Gb(монитор TFT19 Samsung); принтер HP LaserJet P2055D	-

Приложение 1

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

1. Описание фонда оценочных средств (паспорт)

№ компе-тенции	Элемент компетенции	Раздел	Тема	ФОС
ОК-4 ПК-12 ПК-15 ПК-18	Способность использовать основы правовых знаний в различных сферах деятельности Способность проводить тестирование компонентов программного обеспечения информационных систем Способность осуществлять тестирование компонентов информационных систем по заданным сценариям Способность принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью (далее – ИБ)	**1.** Международные стандарты информационного обмена и угрозы ИБ	**1.1** Международные стандарты информационного обмена **1.2** Понятие и классификация угроз ИБ **1.3** Виды противников или «нарушителей» ИБ	Вопросы к экзамену № 1.1-1.3
		2. Три вида возможных нарушений безопасности информационной системы	**2.1** Анализ способов нарушений ИБ **2.2** Виды компьютерных вирусов	Вопросы к экзамену № 2.1-2.2
		3. Основные положения теории ИБ	**3.1** Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы **3.2** Модели безопасности и их применение	Вопросы к экзамену № 3.1-3.2
		4. Основные технологии построения защищенных экономических информационных систем	**4.1** Место ИБ экономических систем в национальной безопасности страны **4.2** Концепция ИБ **4.3** Методы криптографии **4.4** Защита и использование защищенных информационных систем	Вопросы к экзамену № 4.1-4.4

2. Экзаменационные вопросы

№ п/п	Компетенции		ЭКЗАМЕНАЦИОННЫЕ ВОПРОСЫ	№ и наименование раздела
	Код	Определение		
1	2	3	4	5
1.	ОК-4	Способность использовать основы правовых знаний в различных сферах деятельности	**1**. Международные стандарты информационного обмена **2**. Понятие и классификация угроз ИБ **3**. Виды противников или «нарушителей» ИБ	**1.** Международные стандарты информационного обмена и угрозы ИБ
2.	ПК-12	Способность проводить тестирование компонентов программного обеспечения информационных систем	**1**. Анализ способов нарушений ИБ **2**. Виды компьютерных вирусов	**2**. Три вида возможных нарушений безопасности информационной системы
			1. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы **2**. Модели безопасности и их применение	**3**. Основные положения теории ИБ
3.	ПК-15	Способность осуществлять тестирование компонентов информационных систем по заданным сценариям	**1**. Место ИБ экономических систем в национальной безопасности страны **2**. Концепция ИБ **3**. Методы криптографии **4**. Защита и использование защищенных информационных систем	**4**. Основные технологии построения защищенных экономических информационных систем
4.	ПК-18	Способность принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью (далее – ИБ)		

3. Описание показателей и критериев оценивания компетенций

Показатели	Оценка	Критерии
Знать (ОК-4) - основы правовых знаний (ПК-12) - основы настройки параметров информационных систем в области ИБ и тестирования результатов настройки (ПК-15) - основы тестирования компонентов информационных систем в области ИБ по заданным сценариям (ПК-18) - методы координации работ по созданию, адаптации и сопровождению информационных систем в области ИБ **Уметь** (ОК-4) - использовать основы правовых знаний в различных сферах деятельности (ПК-12) - вести техническую документацию в области ИБ (ПК-15) - принимать участие в экспертном тестировании информационных систем в области ИБ на этапе опытной эксплуатации (ПК-18) - управлять техническим сопровождением информационной системы в процессе ее эксплуатации с целью обеспечения ИБ **Владеть** (ОК-4) - навыками использования основ правовых знаний в различных сферах деятельности (ПК-12) - навыками технического сопровождения информационных систем в области ИБ в процессе их эксплуатации (ПК-15) - информационным	**отлично**	Оценка «отлично» выставляется обучающемуся, который глубоко усвоил материал дисциплины, исчерпывающе полно, четко и логически последовательно его излагает, демонстрирует абсолютные способности самостоятельно находить решения вопросов в области информационной безопасности (далее – ИБ)
	хорошо	Оценка «хорошо» выставляется обучающемуся, который твердо знает материал дисциплины, грамотно и по сути излагает его, не допуская существенных неточностей в ответе, способен в большинстве случаев самостоятельно находить решения вопросов в области ИБ
	удовлетворительно	Оценка «удовлетворительно» выставляется обучающемуся, который имеет знания только по основному материалу дисциплины, но не усвоил его деталей, допускает неточности в ответе, но сохраняет способность находить частичные решения вопросов в области ИБ
	неудовлетворительно	Оценка «неудовлетворительно» выставляется обучающемуся, который не знает значительной части программного материала, допускает существенные ошибки в его изложении. Оценка «неудовлетворительно» ставится тем обучающимся, которые не освоили необходимых компетенций

обеспечением прикладных процессов в области ИБ (ПК-18) - навыками управления ИБ информационных систем		

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

Дисциплина «Информационная безопасность» направлена на овладение основами теоретических и практических знаний в области выявления угроз ИБ, организационно-технических мероприятий по защите информации в информационных системах, обеспечения сохранности, целостности и безопасности информационных ресурсов.

Изучение дисциплины «Информационная безопасность» предусматривает:

- лекции;
- лабораторные работы;
- самостоятельную работу обучающихся;
- экзамен.

В ходе освоения раздела 1 «Международные стандарты информационного обмена и угрозы ИБ» обучающиеся должны изучить международные стандарты информационного обмена, рассмотреть понятие и классификацию угроз ИБ, а также виды противников или «нарушителей» ИБ.

В ходе освоения раздела 2 «Три вида возможных нарушений безопасности информационной системы» обучающиеся должны получить представление об анализе способов нарушений ИБ и видах компьютерных вирусов.

В ходе освоения раздела 3 «Основные положения теории ИБ» обучающиеся должны рассмотреть основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы, а также модели безопасности и их применение.

В ходе освоения раздела 4 «Основные технологии построения защищенных экономических информационных систем» обучающиеся должны усвоить место ИБ экономических систем в национальной безопасности страны, концепцию ИБ, изучить методы криптографии, защиты и использования защищенных информационных систем.

Также необходимо овладеть навыками и умениями применения изученных методов для управления ИБ, применения и реализации тех или иных методов в конкретных ситуациях.

В процессе изучения дисциплины на первом этапе рекомендуется обратить внимание на понятийно-категориальный аппарат дисциплины. Овладение ключевыми понятиями является важным этапом в освоении содержания современных методов обеспечения ИБ.

При подготовке к сдаче экзамена рекомендуется особое внимание уделить вопросам, связанным с современными методами криптографического преобразования информации.

В процессе выполнения лабораторных работ происходит закрепление знаний, формирование умений и навыков шифрования и дешифрования текстовой информации с использованием возможностей распространенных языков программирования и блочных шифров, кроме того, рассматриваются вопросы установки парольной защиты, учетных записей и разграничения прав доступа в клиентских приложениях информационных систем.

Самостоятельную работу по изучению дисциплины необходимо начинать с проработки конспекта лекций, обобщения, систематизации, углубления и конкретизации полученных теоретических знаний с использованием основной и дополнительной литературы, а также рекомендуемых ресурсов информационно-телекоммуникационной сети «Интернет».

В процессе консультации с преподавателем необходимо уточнять вопросы, термины, материал, вызвавший трудности при самостоятельной работе.

Работа с литературой является важнейшим элементом в получении знаний по дисциплине. Прежде всего, необходимо воспользоваться списком рекомендуемой по данной

дисциплине литературой. Дополнительные сведения по изучаемым темам можно найти в периодической печати и информационно-телекоммуникационной сети «Интернет».

Предусмотрено проведение аудиторных занятий (в виде лекций и лабораторных работ) в сочетании с внеаудиторной работой.

Приложение 2

АННОТАЦИЯ
рабочей программы дисциплины
Информационная безопасность

1. Цель и задачи дисциплины

Цель изучения дисциплины – овладение основами теоретических и практических знаний в области методов и способов обеспечения сохранности, целостности и безопасности информационных ресурсов.

Задачами изучения дисциплины является формирование у обучающихся систематизированных знаний в области криптографии и шифрования.

2. Структура дисциплины

2.1 Распределение трудоемкости по отдельным видам учебных занятий, включая самостоятельную работу: лекции – 36 часов; лабораторные работы – 18 часов; самостоятельная работа – 54 часа.

Общая трудоемкость дисциплины составляет 144 часа, 4 зачетных единицы.

2.2 Основные разделы дисциплины:

1 – Международные стандарты информационного обмена и угрозы информационной безопасности;

2 – Три вида возможных нарушений безопасности информационной системы;

3 – Основные положения теории информационной безопасности;

4 – Основные технологии построения защищенных экономических информационных систем.

3. Планируемые результаты обучения (перечень компетенций)

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- ОК-4 Способность использовать основы правовых знаний в различных сферах деятельности;
- ПК-12 Способность проводить тестирование компонентов программного обеспечения информационных систем;
- ПК-15 Способность осуществлять тестирование компонентов информационных систем по заданным сценариям;
- ПК-18 Способность принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью.

4. Вид промежуточной аттестации: экзамен.

Приложение 3

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.)*

Приложение 4

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ ПО ДИСЦИПЛИНЕ

1. Описание фонда оценочных средств (паспорт)

№ компе-тенции	Элемент компетенции	Раздел	Тема	ФОС
ОК-4	Способность использовать основы правовых знаний в различных сферах деятельности	**1.** Международные стандарты информационного обмена и угрозы ИБ	**1.1** Международные стандарты информационного обмена **1.2** Понятие и классификация угроз ИБ **1.3** Виды противников или «нарушителей» ИБ	Контрольные вопросы
ПК-12	Способность проводить тестирование компонентов программного обеспечения информационных систем	**2.** Три вида возможных нарушений безопасности информационной системы	**2.1** Анализ способов нарушений ИБ **2.2** Виды компьютерных вирусов	Контрольные вопросы
ПК-15	Способность осуществлять тестирование компонентов информационных систем по заданным сценариям	**3.** Основные положения теории ИБ	**3.1** Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы **3.2** Модели безопасности и их применение	Контрольные вопросы
ПК-18	Способность принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью (далее – ИБ)	**4.** Основные технологии построения защищенных экономических информационных систем	**4.1** Место ИБ экономических систем в национальной безопасности страны **4.2** Концепция ИБ **4.3** Методы криптографии **4.4** Защита и использование защищенных информационных систем	Контрольные вопросы, отчеты о выполнении ЛР

3. Описание показателей и критериев оценивания компетенций

Показатели	Оценка	Критерии
Знать (ОК-4) - основы правовых знаний (ПК-12) - основы настройки параметров информационных систем в области ИБ и тестирования результатов настройки (ПК-15) - основы тестирования компонентов информационных систем в области ИБ по заданным сценариям (ПК-18) - методы координации работ по созданию, адаптации и сопровождению информационных систем в области ИБ **Уметь** (ОК-4) - использовать основы правовых знаний в различных сферах деятельности (ПК-12) - вести техническую документацию в области ИБ (ПК-15) - принимать участие в экспертном тестировании информационных систем в области ИБ на этапе опытной эксплуатации (ПК-18) - управлять техническим сопровождением информационной системы в процессе ее эксплуатации с целью обеспечения ИБ **Владеть** (ОК-4) - навыками использования основ правовых знаний в различных сферах деятельности (ПК-12) - навыками технического сопровождения информационных систем в области ИБ в процессе их эксплуатации (ПК-15) - информационным обеспечением	**отлично**	Оценка «отлично» выставляется обучающемуся, который глубоко усвоил материал дисциплины, исчерпывающе полно, четко и логически последовательно его излагает, демонстрирует абсолютные способности самостоятельно находить решения вопросов в области информационной безопасности (далее – ИБ)
	хорошо	Оценка «хорошо» выставляется обучающемуся, который твердо знает материал дисциплины, грамотно и по сути излагает его, не допуская существенных неточностей в ответе, способен в большинстве случаев самостоятельно находить решения вопросов в области ИБ
	удовлетворительно	Оценка «удовлетворительно» выставляется обучающемуся, который имеет знания только по основному материалу дисциплины, но не усвоил его деталей, допускает неточности в ответе, но сохраняет способность находить частичные решения вопросов в области ИБ
	неудовлетворительно	Оценка «неудовлетворительно» выставляется обучающемуся, который не знает значительной части программного материала, допускает существенные ошибки в его изложении. Оценка «неудовлетворительно» ставится тем обучающимся, которые не освоили необходимых компетенций

прикладных процессов в области ИБ (ПК-18) - навыками управления ИБ информационных систем		

Программа составлена в соответствии с федеральным государственным образовательным стандартом высшего образования по направлению подготовки 09.03.03 Прикладная информатика от 12.03.2015 г. № 207

для набора 2014 года: и учебным планом ФГБОУ ВО «БрГУ» для заочной формы обучения от «03» июля 2018 г. № 413

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

для набора 2016 года: и учебным планом ФГБОУ ВО «БрГУ» для очной формы обучения от «05» мая 2016 г. № 342

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:
Иванов М.Ю., доцент базовой кафедры МиИТ, к.т.н., доцент _____

Розанова А.А., ст. препод. базовой кафедры МиИТ _____

Рабочая программа рассмотрена и утверждена на заседании базовой кафедры МиИТ

от «19» декабря 2018 г., протокол № 8

И.о. заведующего базовой кафедрой МиИТ _____ Луковникова Е.И.

СОГЛАСОВАНО:

И.о. заведующего базовой кафедрой МиИТ _____ Луковникова Е.И.

Директор библиотеки _____ Сотник Т.Ф.

Рабочая программа одобрена методической комиссией факультета Экономики и управления

от «28» декабря 2018 г., протокол № 4

Председатель методической комиссии факультета _____ Трапезникова Е.В.

СОГЛАСОВАНО:

Начальник
учебно-методического управления _____ Нежевец Г.П.

Регистрационный №_____