

Документ подписан простой электронной подписью
 Информация о владельце:
 ФИО: Луковникова Елена Ивановна
 Должность: Проректор по учебной работе
 Дата подписания: 16.11.2021 14:46:13
 Уникальный программный ключ:
 890f5aae3463de1924cbcf76ac5d7ab89e9fe3d2

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
 ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
 ВЫСШЕГО ОБРАЗОВАНИЯ

САМАРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ

Проректор по учебной работе



Е.И. Луковникова
 Е.И. Луковникова
 21 мая 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
 Б1.О.20 Информационная безопасность

Закреплена за кафедрой **Базовая кафедра менеджмента и информационных технологий**

Учебный план б090303_21_ПИЭ.plx
 Направление: 09.03.03 Прикладная информатика

Квалификация **Бакалавр**

Форма обучения **очная**


Общая трудоемкость **4 ЗЕТ**

Виды контроля в семестрах:

Экзамен 6

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	6 (3.2)		Итого	
Неделя	16			
Вид занятий	УП	РП	УП	РП
Лекции	32	32	32	32
Лабораторные	32	32	32	32
В том числе инт.	16	16	16	16
Итого ауд.	64	64	64	64
Контактная работа	64	64	64	64
Сам. работа	44	44	44	44
Часы на контроль	36	36	36	36
Итого	144	144	144	144

Программу составил(и):
к.т.н., доц., Иванов М.Ю. 

Рабочая программа дисциплины

Информационная безопасность

разработана в соответствии с ФГОС:

Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 09.03.03 Прикладная информатика (приказ Минобрнауки России от 19.09.2017 г. № 922)

составлена на основании учебного плана:

Направление: 09.03.03 Прикладная информатика
утвержденного приказом ректора от 01.03.2021 протокол № 80.

Рабочая программа одобрена на заседании кафедры

Базовая кафедра менеджмента и информационных технологий

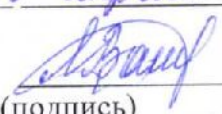
Протокол от 09 апреля 2021 г. № 12

Срок действия программы: 2021-2025 уч.г.

Зав. кафедрой Вахрушева М. Ю. 


Председатель МКФ

доцент, к.э.н., Акчурина И.Г. 19 апреля 2021 г. протокол № 7 

Ответственный за реализацию ОПОП  Вахрушева М.Ю.

(подпись)

(ФИО)

Директор библиотеки  Соткин Л.Р.

(подпись)

(ФИО)

№ регистрации 269
(методический отдел)

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

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

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП

Цикл (раздел) ООП:		Б1.О.20
2.1	Требования к предварительной подготовке обучающегося:	
2.1.1	Дисциплина «Информационная безопасность» базируется на знаниях, полученных при изучении учебных дисциплин «Информатика и программирование», «Информационные системы и технологии», «Компьютерный практикум».	
2.1.2	Информационные системы и технологии	
2.1.3	Информатика и программирование	
2.1.4	Компьютерный практикум	
2.2	Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:	
2.2.1	Системная архитектура информационных систем	
2.2.2	Разработка программных приложений	

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

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

Индикатор 1	Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
Индикатор 2	Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
Индикатор 3	Имеет навыки подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности

ОПК-4: Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью;

Индикатор 1	Знает основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы
Индикатор 2	Умеет применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы
Индикатор 3	Владеет навыками составления технической документации на различных этапах жизненного цикла информационной системы

В результате освоения дисциплины обучающийся должен

3.1	Знать:
3.1.1	Принципы, методы и средства решения стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности
3.1.2	Способы решения стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности
3.1.3	Основы подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе
3.1.4	Основные стандарты оформления технической документации с учетом требований информационной безопасности
3.1.5	Основные требования оформления технической документации с учетом требований информационной безопасности
3.1.6	Основные виды технической документации на различных стадиях жизненного цикла информационной системы с учетом требований информационной безопасности
3.2	Уметь:
3.2.1	Находить решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с учетом основных требований информационной безопасности
3.2.2	Решать стандартные задачи профессиональной деятельности с учетом основных требований информационной безопасности

3.2.3	Составлять обзоры, аннотации, рефераты, научные доклады, публикации и библиографию по научно-исследовательской работе
3.2.4	Применять техническую документацию с учетом требований информационной безопасности
3.2.5	Применять стандарты оформления технической документации с учетом требований информационной безопасности
3.2.6	Применять стандарты для составления технической документации на различных стадиях жизненного цикла информационной системы с учетом требований информационной безопасности
3.3	Владеть:
3.3.1	Навыками применения информационно-коммуникационных технологий с учетом основных требований информационной безопасности
3.3.2	Методологией использования информационно-коммуникационных технологий с учетом основных требований информационной безопасности
3.3.3	Навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности
3.3.4	Навыками оформления технической документации на различных стадиях жизненного цикла информационной системы с учетом требований информационной безопасности
3.3.5	Навыками использования технической документации на различных стадиях жизненного цикла информационной системы с учетом требований информационной безопасности
3.3.6	Навыками составления технической документации на различных этапах жизненного цикла информационной системы с учетом требований информационной безопасности

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Вид занятия	Наименование разделов и тем	Семестр / Курс	Часов	Компетенции	Литература	Инте ракт.	Примечание
	Раздел	Раздел 1. Информационная безопасность и международные стандарты информационного обмена						
1.1	Лек	Понятие и основные положения информационной безопасности	6	2	ОПК-3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2	0	ОПК-3.1
1.2	Лек	Международные стандарты информационного обмена	6	2	ОПК-3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2	0	ОПК-3.1
1.3	Лек	Классификация угроз информационной безопасности	6	4	ОПК-3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2	4	Лекция-диспут, ОПК-3.1
1.4	Лек	Виды противников или «нарушителей» информационной безопасности	6	2	ОПК-3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2	0	ОПК-3.1
1.5	Ср	Подготовка к экзамену	6	5	ОПК-3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2	0	ОПК-3.1
	Раздел	Раздел 2. Способы возможных нарушений информационной безопасности						
2.1	Лек	Анализ способов возможных нарушений информационной безопасности	6	4	ОПК-3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2	4	Лекция-диспут, ОПК-3.1
2.2	Лек	Компьютерные вирусы	6	2	ОПК-3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2	0	ОПК-3.1

2.3	Ср	Подготовка к экзамену	6	4	ОПК-3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2	0	ОПК-3.1
	Раздел	Раздел 3. Основные положения теории информационной безопасности						
3.1	Лек	Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы	6	4	ОПК-3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2	0	ОПК-3.1
3.2	Лек	Модели безопасности и их применение	6	4	ОПК-3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2	0	ОПК-3.1
3.3	Ср	Подготовка к экзамену	6	4	ОПК-3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2	0	ОПК-3.1
	Раздел	Раздел 4. Основные технологии построения защищенных экономических информационных систем						
4.1	Лек	Концепция информационной безопасности	6	2	ОПК-3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2	0	ОПК-3.1
4.2	Лек	Методы криптографии	6	4	ОПК-3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1	0	ОПК-3.1
4.3	Лек	Защита и разработка защищенных экономических информационных систем	6	2	ОПК-3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1	0	ОПК-3.1
4.4	Лаб	Шифрование текстовой информации случайной перестановкой символов	6	4	ОПК-3 ОПК-4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2	4	Разбор конкретных ситуаций, ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3
4.5	Лаб	Шифрование текстовой информации заменой символов	6	6	ОПК-3 ОПК-4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2	0	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3
4.6	Лаб	Шифрование текстовой информации случайными сдвигами символов	6	4	ОПК-3 ОПК-4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2	4	Разбор конкретных ситуаций, ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3

4.7	Лаб	Шифрование текстовой информации сдвигами по паролю символов	6	6	ОПК-3 ОПК-4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2	0	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3
4.8	Лаб	Шифрование текстовой информации заменой части символов	6	6	ОПК-3 ОПК-4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2	0	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3
4.9	Лаб	Установка парольной защиты, учетных записей и разграничение прав доступа в клиентских приложениях	6	6	ОПК-3 ОПК-4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2	0	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3
4.10	Ср	Подготовка к лабораторным работам	6	13	ОПК-3 ОПК-4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1 Л3.2	0	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3
4.11	Ср	Подготовка к экзамену	6	18	ОПК-3 ОПК-4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2Л3.1	0	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3
4.12	Экзамен		6	36	ОПК-3 ОПК-4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2	0	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

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

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Контрольные вопросы и задания

Контрольные вопросы по разделам дисциплины

Раздел 1. Информационная безопасность и международные стандарты информационного обмена:

1. Понятие информационной безопасности
2. Основные составляющие информационной безопасности
3. Международные стандарты информационного обмена
4. Понятие угрозы и критерии классификации угроз
5. Виды возможных нарушений безопасности информационных систем
6. Типовые способы удаленных атак на информацию в сети
7. Методы сбора сведений для вторжения в компьютерную сеть
8. Модель нарушителя информационной безопасности

Раздел 2. Способы возможных нарушений информационной безопасности:

9. Несанкционированный доступ к информации. Способы НСД
10. Шпионские программные закладки

Раздел 3. Основные положения теории информационной безопасности:

11. Правовые основы защиты информации
12. Документы, регламентирующие деятельность по обеспечению защиты информации
13. Уровни информационной защиты
14. Модели информационной безопасности
15. Средства защиты информации от несанкционированного доступа

16. Классификация парольных средств защиты
- Раздел 4. Основные технологии построения защищенных экономических информационных систем:
17. Криптография. Основные понятия и определения, задачи криптографии
18. Классификация способов криптографического преобразования информации
19. Симметричные методы криптографии
20. Блочные шифры
21. Асимметричные методы криптографии
22. Формальные модели атак и угроз в криптографии
23. Понятие стойкости криптографического алгоритма
24. Классические методы криптоанализа
25. Использование методов криптографии в экономике (банковском деле, электронных платежных системах и т.п.)
26. Угрозы безопасности информации в платежных системах
27. Проблемы криптографической защиты платежных систем
28. Требования к криптографическим средствам защиты банковской информации
29. Новые направления обеспечения безопасности информации в банковском деле
30. Концепция защиты информации
31. Политика безопасности информации

6.2. Темы письменных работ

Не предусмотрено.

6.3. Фонд оценочных средств

Экзаменационные вопросы

Раздел 1. Информационная безопасность и международные стандарты информационного обмена:

1. Понятие информационной безопасности
2. Основные составляющие информационной безопасности
3. Международные стандарты информационного обмена
4. Понятие угрозы и критерии классификации угроз
5. Виды возможных нарушений безопасности информационных систем
6. Типовые способы удаленных атак на информацию в сети
7. Методы сбора сведений для вторжения в компьютерную сеть
8. Модель нарушителя информационной безопасности

Раздел 2. Способы возможных нарушений информационной безопасности:

9. Несанкционированный доступ к информации. Способы НСД
10. Шпионские программные закладки

Раздел 3. Основные положения теории информационной безопасности:

11. Правовые основы защиты информации
12. Документы, регламентирующие деятельность по обеспечению защиты информации
13. Уровни информационной защиты
14. Модели информационной безопасности
15. Средства защиты информации от несанкционированного доступа
16. Классификация парольных средств защиты

Раздел 4. Основные технологии построения защищенных экономических информационных систем:

17. Криптография. Основные понятия и определения, задачи криптографии
18. Классификация способов криптографического преобразования информации
19. Симметричные методы криптографии
20. Блочные шифры
21. Асимметричные методы криптографии
22. Формальные модели атак и угроз в криптографии
23. Понятие стойкости криптографического алгоритма
24. Классические методы криптоанализа
25. Использование методов криптографии в экономике (банковском деле, электронных платежных системах и т.п.)
26. Угрозы безопасности информации в платежных системах
27. Проблемы криптографической защиты платежных систем
28. Требования к криптографическим средствам защиты банковской информации
29. Новые направления обеспечения безопасности информации в банковском деле
30. Концепция защиты информации
31. Политика безопасности информации

6.4. Перечень видов оценочных средств

Экзаменационные вопросы

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

7.1. Рекомендуемая литература

7.1.1. Основная литература

	Авторы,	Заглавие	Издательство,	Кол-во	Эл. адрес
--	---------	----------	---------------	--------	-----------

	Авторы,	Заглавие	Издательство,	Кол-во	Эл. адрес
ЛП. 1	Моргунов А. В.	Информационная безопасность: учебно-методическое пособие	Новосибирск: Новосибирский государственный технический университет, 2019	1	http://biblioclub.ru/index.php?page=book&id=576726
ЛП. 2	Ишейнов В. Я.	Информационная безопасность и защита информации: теория и практика: учебное пособие	Москва Берлин: Директ-Медиа, 2020	1	http://biblioclub.ru/index.php?page=book&id=571485
ЛП. 3	Кубашева Е. С., Малашкевич И. А., Чекулаева Е. Н.	Информатика и вычислительная техника. Информационная безопасность автоматизированных систем: учебно-методическое пособие	Йошкар-Ола: Поволжский государственный технологический университет, 2019	1	http://biblioclub.ru/index.php?page=book&id=562246
ЛП. 4	Ковалев Д. В., Богданова Е. А.	Информационная безопасность: учебное пособие	Ростов-на-Дону: Южный федеральный университет, 2016	1	http://biblioclub.ru/index.php?page=book&id=493175
ЛП. 5	Прохорова О. В.	Информационная безопасность и защита информации: учебник	Самара: Самарский государственный архитектурно-строительный университет, 2014	1	http://biblioclub.ru/index.php?page=book&id=438331

7.1.2. Дополнительная литература

	Авторы,	Заглавие	Издательство,	Кол-во	Эл. адрес
ЛП. 1	Трушин В. А., Котов Ю. А., Левин Л. С., Донской К. А.	Введение в информационную безопасность и защиту информации: учебное пособие	Новосибирск: Новосибирский государственный технический университет, 2017	1	http://biblioclub.ru/index.php?page=book&id=575113
ЛП. 2	Гулятьева Т. А.	Основы информационной безопасности: учебное пособие	Новосибирск: Новосибирский государственный технический университет, 2018	1	http://biblioclub.ru/index.php?page=book&id=574729

7.1.3. Методические разработки

	Авторы,	Заглавие	Издательство,	Кол-во	Эл. адрес
ЛЗ. 1	Иванов М.Ю.	Информационные технологии: методы криптографии: учебное пособие	Братск: БрГУ, 2010	30	
ЛЗ. 2	Иванов М.Ю.	Информационная безопасность: методические указания к выполнению лабораторных работ	Братск: БрГУ, 2014	20	

7.3.1 Перечень программного обеспечения

7.3.1.1	Microsoft Windows Professional 7 Russian Upgrade Academic OPEN No Level
7.3.1.2	Microsoft Office 2007 Russian Academic OPEN No Level
7.3.1.3	PascalABC
7.3.1.4	Turbo Pascal

7.3.2 Перечень информационных справочных систем

7.3.2.1	ИСС "Кодекс". Информационно-справочная система
7.3.2.2	Справочно-правовая система «Консультант Плюс»
7.3.2.3	Издательство "Лань" электронно-библиотечная система
7.3.2.4	«Университетская библиотека online»

7.3.2.5	Электронный каталог библиотеки БрГУ
7.3.2.6	Электронная библиотека БрГУ
7.3.2.7	Информационная система "Единое окно доступа к образовательным ресурсам"
7.3.2.8	Научная электронная библиотека eLIBRARY.RU
7.3.2.9	Университетская информационная система РОССИЯ (УИС РОССИЯ)
7.3.2.10	
7.3.2.11	Национальная электронная библиотека НЭБ

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

3217	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, учебная мебель.
3234	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.), учебная мебель.
3236	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.), учебная мебель.

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

Дисциплина «Информационная безопасность» направлена на овладение основами теоретических и практических знаний в области выявления угроз информационной безопасности, 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.

Помимо освоения основных разделов дисциплины необходимо овладеть навыками и умениями применения изученных методов для управления информационной безопасностью, 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 информационной безопасности.

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.