МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ
И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
Северо-Кавказский филиал
ордена Трудового Красного Знамени федерального государственного
бюджетного образовательного учреждения высшего образования
«Московский технический университет связи и информатики»

УТВЕРЖДАЮ
Зам. директора по УВР
_____ А.Г. Жуковский
«23» 05 2022 г.

Безопасность информационных процессов в компьютерных системах и сетях
Б1.В.ДВ.09.02
рабочая программа дисциплины

Кафедра: **Инфокоммуникационные технологии и системы связи**
Направление подготовки: **09.03.01 Информатика и вычислительная техника**
Профиль: **Вычислительные машины, комплексы, системы и сети**
Программное обеспечение и интеллектуальные системы
Формы обучения: **очная, заочная**

Распределение часов дисциплины по семестрам (для очной формы обучения), курсам (для заочной формы обучения)

Вид учебной работы	ОФ		ЗФ	
	ЗЕ	часов	ЗЕ	часов
Общая трудоемкость дисциплины, в том числе (по семестрам, курсам):	3	108/7	3	108/4
Контактная работа, в том числе (по семестрам, курсам):		48/7		14/4
Лекции		16/7		8/4
Лабораторных работ		16/7		
Практических занятий		16/7		6/4
Семинаров				
Самостоятельная работа		60/7		94/4
Контроль				
Число контрольных работ (по курсам)				
Число КР (по семестрам, курсам)				
Число КП (по семестрам, курсам)				
Число зачетов с разбивкой по семестрам (курсам)		1/7		1/4
Число экзаменов с разбивкой по семестрам (курсам)				

Программу составил:

Доцент кафедры ИТСС, к. т. н., Сосновский И.А.
……

Рецензент(ы):
Заведующий кафедрой ИВТ, д.т.н. профессор Соколов С.В.
……

Рабочая программа дисциплины «Безопасность информационных процессов в компьютерных системах и сетях»

Разработана в соответствии с ФГОС ВО:
направления подготовки 09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА, утверждённым приказом Министерства образования и науки Российской Федерации от 19 сентября 2017 г. N 929.

Составлена на основании учебных планов
направления 09.03.01 Информатика и вычислительная техника, профиля «Вычислительные машины, комплексы, системы и сети», одобренных Учёным советом СКФ МТУСИ, протокол №7 от 28.02.2022г., и утвержденного директором СКФ МТУСИ 28.02.2022 г.

Рассмотрена и одобрена на заседании кафедры
«Инфокоммуникационные технологии и системы связи»

Протокол от «25» 05 2022г. № 10

Зав. кафедрой _____Юхнов В.И.

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР
__ _______ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры «Инфокоммуникационные технологии и системы связи»

Протокол от __ __ 20__ г. № _

Зав. кафедрой ___________________ В.И. Юхнов

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР
__ _______ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры «Инфокоммуникационные технологии и системы связи»

Протокол от _ ________ 20__ г. № _

Зав. кафедрой _____________________

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР
__ _______ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры «Инфокоммуникационные технологии и системы связи»

Протокол от _ ________ 20__ г. № _

Зав. кафедрой _____________________

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР
__ _______ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры «Инфокоммуникационные технологии и системы связи»

Протокол от _ ________ 20__ г. № _

Зав. кафедрой _____________________

---

1. Цели изучения дисциплины

Целью изучения дисциплины является формирование у обучаемых знаний в области обеспечения защиты информации, комплексной защиты объектов информатизации и безопасности информационных процессов в компьютерных системах и сетях.

2. Планируемые результаты обучения

Изучение дисциплины направлено на формирование у выпускника способности решать профессиональные задачи в соответствии с **технологическим видом деятельности**.

Результатом освоения дисциплины являются сформированные у выпускника следующие компетенции:

Результатом освоения дисциплины являются сформированные у выпускника следующие компетенции:

Компетенции выпускника, формируемые в результате освоения дисциплины (в части, обеспечиваемой дисциплиной)
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;
Знать:
Основные требования, механизмы и уровни обеспечения информационной безопасности. Стандарты, нормативно-правовые основы безопасности информационных процессов в компьютерных системах и сетях. Методы решения задач профессиональной деятельности на основе информационной и библиографической культуры с применением инфокоммуникационных технологий и с учетом основных требований информационной безопасности в компьютерных системах и сетях.
Уметь:
Решать стандартные задачи профессиональной деятельности в соответствии требования информационной безопасности. Применять стандарты, нормативно-правовые основы безопасности информационных процессов при решении задач профессиональной деятельности. Организовывать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры автоматизированных систем, внешних воздействий, вероятных угроз и уровня развития технологии защиты информации.
Владеть:
Методами решения стандартных задач в области обеспечения безопасности информационных процессов в компьютерных системах и сетях. Способностью грамотно применять стандарты, нормативно-правовые основы безопасности информационных процессов в компьютерных системах и сетях при решении задач профессиональной деятельности. Способностью решать задачи обеспечения безопасности информационных процессов на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

3. Место дисциплины в структуре образовательной программы

Требования к предварительной подготовке обучающегося (предшествующие дисциплины, модули, темы):	
1	Б1.О.05 Информатика
2	Б1.О.09 Вычислительная техника
3	Б1.О.12 Архитектура информационных систем
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:	
1	Б2.О.02(П) Производственная (эксплуатационная) практика
2	Б2.О.03(Пд) Государственная итоговая аттестация

4. Структура и содержание дисциплины

4.1 Очная форма обучения, 4 года (всего 108 часов, 48 часов контактной работы)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компетенции	УМИО
Курс 4, Семестр 7					
Модуль 1. Основы обеспечения безопасности информационных процессов в компьютерных системах и сетях – 52 (28+24) часов					
1.1	Лекция 1. Основы информационной безопасности 1. Правовые основы информационной безопасности общества. Государственные информационные ресурсы. 2. Основные положения законодательных актов РФ в области информационной безопасности и защиты информации.	Лек	2	ОПК-3	Л1.1
1.2	Лекция 2. Безопасность информационных процессов в компьютерных системах и сетях. Основные непреднамеренные и преднамеренные угрозы. 1. Меры противодействия угрозам безопасности. Меры по обеспечению сохранности информации в компьютерных системах и сетях. 2. Основные задачи обеспечения безопасности информации в компьютерных системах и сетях. Защита локальных сетей и операционных систем. 3. Интеграция систем защиты. Internet в структуре информационно-аналитического обеспечения компьютерных систем и сетей. Рекомендации по защите информации в Internet.	Лек	2	ОПК-3	Л1.1
1.3	Лекция 3. Теория информационной безопасности и методология защиты информации в компьютерных системах и сетях. 1. Архитектура электронных систем обработки данных, формальные модели. 2. Модели безопасности; политика безопасности; критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем. 3. Стандарты по оценке защищенных систем; примеры практической реализации; построение парольных систем, особенности применения криптографических методов; способы реализации	Лек	2	ОПК-3	Л1.1

	криптографической подсистемы. 4. Особенности реализации систем с симметричными и несимметричными ключами, концепция защищенного ядра; методы верификации; защищенные домены				
1.4	Практическое занятие №1 Нормативно-правовая база защиты компьютерных сетей от несанкционированного доступа. Компьютерные преступления и особенности их расследования.	ПЗ1	4	ОПК-3	Л1.1
1.5	Практическое занятие №2. Основные виды формальных моделей безопасности. Применение иерархического метода для построения защищенной операционной системы; исследование корректности систем защиты; методология обследования и проектирования защиты; модель политики контроля целостности.	ПЗ2	4	ОПК-3	Л1.1
1.6	Шифрование – базовая технология безопасности. Основные понятия и определения. История появления шифров	СРС	8	ОПК-3	Л1.1
1.7	Вирусы как угроза информационной безопасности. Характерные черты компьютерных вирусов. Хронология развития компьютерных вирусов	СРС	8	ОПК-3	Л1.1
1.8	Схемы заражения файлов; схемы заражения загрузчиков; способы маркировки, используемые вирусами	СРС	8	ОПК-3	Л1.1
1.9	Лекция 4. Компьютерные вирусы как особый класс разрушающих программных воздействий. Защита от разрушающих программных воздействий. Понятие изолированной программной среды.	Лек	2	ОПК-3	Л1.2 Л2.1
1.10	Лабораторная работа №1. Модели взаимодействия прикладной программы и программной закладки. Методы перехвата и навязывания информации. Методы внедрения программных закладок.	ЛР1	2	ОПК-3	Л1.1
1.11	Лабораторная работа № 2 Защита от закладок и дизассемблирования. Способы встраивания защитных механизмов в программное обеспечение. Понятие разрушающего программного воздействия.	ЛР2	4	ОПК-3	Л1.1
1.12	Лекция 5. Программные методы защиты. Программно-аппаратные средства защиты ПЭВМ и сетей 1. Методы средства ограничения доступа к компонентам сети. 2. Методы и средства привязки программного обеспечения к аппаратному окружению к физическим носителям. 3. Методы и средства хранения ключевой информации, защита программ от изучения. 4. Защита от разрушающих программных воздействий, защита от изменений и контроль целостности.	Лек	2	ОПК-3	Л1.2 Л2.1
1.13	Практическое занятие №3. Основные этапы построения системы комплексной защиты вычислительных систем; анализ моделей нарушителя; угрозы информационно-программному обеспечению вычислительных систем и их классификация	ПЗ 3	4	ОПК-3	Л1.1

Модуль 2 – Безопасность программного кода и сетевых служб – 56 (20+36) часов					
2.1	Лекция 6. Классификация удаленных угроз в вычислительных сетях. Типовые удаленные атаки и их характеристика. 1. Межсетевые экраны Режим функционирования межсетевых экранов и их основные компоненты. Основные схемы сетевой защиты на базе межсетевых экранов. Применение межсетевых экранов для организации виртуальных корпоративных сетей. 2. Маршрутизаторы. Шлюзы сетевого уровня. Усиленная аутентификация. 3. Методы защиты программ от излучения и разрушающих программных воздействий (программных закладок и вирусов).	Лек	2	ОПК-3	Л1.2 Л2.1
2.2	Этапы доступа к ресурсам вычислительной системы; использование простого пароля; использование динамически изменяющегося пароля; взаимная проверка подлинности и другие случаи опознания; способы разграничения доступа к компьютерным ресурсам; разграничение доступа по спискам.	ПЗ 4	4	ОПК-3	Л1.1
2.3	Анализ структуры и принципов функционирования вычислительных сетей с позиции обеспечения информационной безопасности	СРС	6	ОПК-3	Л1.1
2.4	Угрозы информационно-программному обеспечению, характерные только для распределённой вычислительной среды.	СРС	6	ОПК-3	Л1.1
2.5	Использование криптографических методов для защиты данных, циркулирующих в вычислительной сети.	СРС	6	ОПК-3	Л1.1
2.6	Лекция №7. Проблемы комплексного обеспечения информационной безопасности автоматизированных систем 1. Состав компонентов комплексной системы обеспечения информационной безопасности (КСИБ). 2. Функциональные и обеспечивающие подсистемы, технология, управление; методология формирования задач защиты: интеграция средств информационной безопасности в технологическую среду 3. Этапы проектирования КСИБ и требования к ним.	Лек	4	ОПК-3	Л1.4 Л3.1
2.7	Лабораторная работа № 3 Восстановление зараженных файлов. Профилактика проникновения «троянских программ». Настройка безопасности почтового клиента	ЛР 3	2	ОПК-3	Л1.4 Л3.1
2.8	Лабораторная работа № 4 Структура комплексной системы защиты информации от несанкционированного доступа (НСД); мониторинг и контроль окружающей среды; ведение специальной информационной базы данных КСИБ.	ЛР 4	4	ОПК-3	Л1.4 Л3.1
2.9	Лабораторная работа № 5. Настройка и использование межсетевого экрана. Создание VPN- подключения средствами Windows. Сетевые протоколы для секретной передачи данных.	ЛР 5	4	ОПК-3	Л1.4 Л3.1
2.10	Механизмы идентификации и аутентификации пользователей в компьютерных системах и сетях Защита	СРС	8	ОПК-3	Л1.4 Л3.1

	компьютерных систем от удаленных атак.				
2.11	Методы разграничения доступа. Виды разграничения доступа. Мандатное и дискретное управление доступом. Регистрация и аудит. Определение и содержание регистрации и аудита ИС. Межсетевое экранирование. Технология виртуальных частных сетей (VPN).	СРС	6	ОПК-3	Л1.4
2.12	Надёжность средств защиты компонент; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям.	СРС	4	ОПК-3	Л3.1
Итого – 108 часа					

4.2 Заочная форма обучения 5 лет (всего 108 часа, аудиторных 14 часов)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компетенции	УМИО
Курс 4, Семестр 7					
Модуль 1. Основы обеспечения безопасности информационных процессов в компьютерных системах и сетях – 52 (6+46) часов					
1.14	Лекция 1. Основы информационной безопасности 3. Правовые основы информационной безопасности общества. Государственные информационные ресурсы. 4. Основные положения законодательных актов РФ в области информационной безопасности и защиты информации.	СРС	2	ОПК-3	Л1.1
1.15	Лекция 2. Безопасность информационных процессов в компьютерных системах и сетях. Основные непреднамеренные и преднамеренные угрозы. 4. Меры противодействия угрозам безопасности. Меры по обеспечению сохранности информации в компьютерных системах и сетях. 5. Основные задачи обеспечения безопасности информации в компьютерных системах и сетях. Защита локальных сетей и операционных систем. 6. Интеграция систем защиты. Internet в структуре информационно-аналитического обеспечения компьютерных систем и сетей. Рекомендации по защите информации в Internet.	СРС	2	ОПК-3	Л1.1
1.16	Лекция 3. Теория информационной безопасности и методология защиты информации в компьютерных системах и сетях. 5. Архитектура электронных систем обработки данных, формальные модели. 6. Модели безопасности; политика безопасности; критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем. 7. Стандарты по оценке защищенных систем; примеры практической реализации; построение парольных систем, особенности применения криптографических методов; способы реализации криптографической подсистемы.	Лек	2	ОПК-3	Л1.1

	8. Особенности реализации систем с симметричными и несимметричными ключами, концепция защищенного ядра; методы верификации; защищенные домены				
1.17	Практическое занятие №1 Нормативно-правовая база защиты компьютерных сетей от несанкционированного доступа. Компьютерные преступления и особенности их расследования.	СРС	4	ОПК-3	Л1.1
1.18	Практическое занятие №2. Основные виды формальных моделей безопасности. Применение иерархического метода для построения защищенной операционной системы; исследование корректности систем защиты; методология обследования и проектирования защиты; модель политики контроля целостности.	ПЗ2	2	ОПК-3	Л1.1
1.19	Шифрование – базовая технология безопасности. Основные понятия и определения. История появления шифров	СРС	10	ОПК-3	Л1.1
1.20	Вирусы как угроза информационной безопасности. Характерные черты компьютерных вирусов. Хронология развития компьютерных вирусов	СРС	8	ОПК-3	Л1.1
1.21	Схемы заражения файлов; схемы заражения загрузчиков; способы маркировки, используемые вирусами	СРС	8	ОПК-3	Л1.1
1.22	Лекция 4. Компьютерные вирусы как особый класс разрушающих программных воздействий. Защита от разрушающих программных воздействий. Понятие изолированной программной среды.	Лек	2	ОПК-3	Л1.2 Л2.1
1.23	Лабораторная работа №1. Модели взаимодействия прикладной программы и программной закладки. Методы перехвата и навязывания информации. Методы внедрения программных закладок.	СРС	2	ОПК-3	Л1.1
1.24	Лабораторная работа № 2 Защита от закладок и дизассемблирования. Способы встраивания защитных механизмов в программное обеспечение. Понятие разрушающего программного воздействия.	СРС	4	ОПК-3	Л1.1
1.25	Лекция 5. Программные методы защиты. Программно-аппаратные средства защиты ПЭВМ и сетей 5. Методы средства ограничения доступа к компонентам сети. 6. Методы и средства привязки программного обеспечения к аппаратному окружению к физическим носителям. 7. Методы и средства хранения ключевой информации, защита программ от изучения. 8. Защита от разрушающих программных воздействий, защита от изменений и контроль целостности.	СРС	2	ОПК-3	Л1.2 Л2.1
1.26	Практическое занятие №3. Основные этапы построения системы комплексной защиты вычислительных систем; анализ моделей нарушителя; угрозы информационно-программному обеспечению вычислительных систем и их классификация	ПЗ3	4	ОПК-3	Л1.1

Модуль 2 – Безопасность программного кода и сетевых служб – 56 (8+48) часов					
2.13	Лекция 6. Классификация удаленных угроз в вычислительных сетях. Типовые удаленные атаки и их характеристика. 4. Межсетевые экраны Режим функционирования межсетевых экранов и их основные компоненты. Основные схемы сетевой защиты на базе межсетевых экранов. Применение межсетевых экранов для организации виртуальных корпоративных сетей. 5. Маршрутизаторы. Шлюзы сетевого уровня. Усиленная аутентификация. 6. Методы защиты программ от излучения и разрушающих программных воздействий (программных закладок и вирусов).	СРС	2	ОПК-3	Л1.2 Л2.1
2.14	Этапы доступа к ресурсам вычислительной системы; использование простого пароля; использование динамически изменяющегося пароля; взаимная проверка подлинности и другие случаи опознания; способы разграничения доступа к компьютерным ресурсам; разграничение доступа по спискам.	СРС	4	ОПК-3	Л1.1
2.15	Анализ структуры и принципов функционирования вычислительных сетей с позиции обеспечения информационной безопасности	СРС	6	ОПК-3	Л1.1
2.16	Угрозы информационно-программному обеспечению, характерные только для распределённой вычислительной среды.	СРС	6	ОПК-3	Л1.1
2.17	Использование криптографических методов для защиты данных, циркулирующих в вычислительной сети.	СРС	6	ОПК-3	Л1.1
2.18	Лекция №7. Проблемы комплексного обеспечения информационной безопасности автоматизированных систем 4. Состав компонентов комплексной системы обеспечения информационной безопасности (КСИБ). 5. Функциональные и обеспечивающие подсистемы, технология, управление; методология формирования задач защиты: интеграция средств информационной безопасности в технологическую среду 6. Этапы проектирования КСИБ и требования к ним.	Лек	4	ОПК-3	Л1.4 Л3.1
2.19	Лабораторная работа № 3 Восстановление зараженных файлов. Профилактика проникновения «троянских программ». Настройка безопасности почтового клиента	СРС	2	ОПК-3	Л1.4 Л3.1
2.20	Лабораторная работа № 4 Структура комплексной системы защиты информации от несанкционированного доступа (НСД); мониторинг и контроль окружающей среды; ведение специальной информационной базы данных КСИБ.	СРС	4	ОПК-3	Л1.4 Л3.1
2.21	Лабораторная работа № 5. Настройка и использование межсетевого экрана. Создание VPN- подключения средствами Windows. Сетевые протоколы для секретной передачи данных.	СРС	4	ОПК-3	Л1.4 Л3.1
2.22	Механизмы идентификации и аутентификации пользователей в компьютерных системах и сетях Защита	СРС	8	ОПК-3	Л1.4 Л3.1

	компьютерных систем от удаленных атак.				
2.23	Методы разграничения доступа. Виды разграничения доступа. Мандатное и дискретное управление доступом. Регистрация и аудит. Определение и содержание регистрации и аудита ИС. Межсетевое экранирование. Технология виртуальных частных сетей (VPN).	СРС	6	ОПК-3	Л1.4
2.24	Надёжность средств защиты компонент; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям.	СРС	4	ОПК-3	Л3.1
Итого – 108 часа					

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Рекомендуемая литература				
5.1.1. Основная литература				
Код	**Авторы, составители**	**Заглавие**	**Издательство, год**	**Кол.**
Л1.1	Рябко Б.Я., Фионов А.Н.	Криптографические методы защиты информации: Учебное пособие для вузов.	М.: Горячая линия - Теле-ком, 2014. – 229 с	Э1
Л1.2	Каторин Ю.Ф., Разумовский А.В., Спивак А.И.	Защита информации техническими средствами. Учебное пособие.	Санкт-Петербург: НИУ ИТ-МО, 2012 – 416 с.	Э2
Л1.3	Креопалов В.В.	Технические средства и методы защиты информации [Электронный ресурс]: учебное пособие.- 278 с. - Режим доступа.	М.: Евразийский открытый институт, 2011.	Э3
Л1.4	Алешников С.И.	Математические методы защиты информации. Часть 4. Вычислительный практикум по эллиптическим кривым и криптографии на эллиптических кривых.	Калининград: Балтийский федеральный университет им. Иммануила Канта, 2007.	Э4
5.1.2. Дополнительная литература				
Код	**Авторы, составители**	**Заглавие**	**Издательство, год**	**Кол.**
Л2.1	Аверченков В.И.	Методы и средства инженерно-технической защиты информации [Электронный ресурс]: учебное пособие.—Режим доступа.	Брянск: Брянский государственный технический университет, 2012.– 187 с	Э5
Л2.2	Соколов С.В., Шевчук П.С., Панкратов В.А.	Перспективные устройства обработки и защиты информации для помехозащитных АСУ.	М.: Радио и связь. 2002.	Э6
5.1.3. Учебно-методическое обеспечение для самостоятельной работы обучающихся				
Код	**Авторы, составители**	**Заглавие**	**Издательство, год**	**Кол.**
Л3.1	Шевчук П.С.	Методические указания по проведению практических занятий по дисциплине «Методы и средства защиты компьютерной	РнД: СКФ МТУСИ, 2016	Э7

		информации» Сосновский И.А.. – Ростов-на -Дону: Изд-во СКФ МТУСИ, 2019.		
Л3.2	Шевчук П.С.	Методические указания по проведению лабораторных работ по дисциплине «Методы и средства защиты компьютерной информации» Сосновский И.А.. – Ростов-на -Дону: Изд-во СКФ МТУСИ, 2019.	РнД: СКФ МТУСИ, 2016	Э8

6.2. Электронные образовательные ресурсы	
Э1	http://znanium.com/catalog.php?bookinfo=370317
Э2	http://znanium.com/bookread2.php?book
Э3	http://znanium.com/bookread2.php?book
Э4	http://znanium.com/bookread2.php?book
Э5	http://znanium.com/bookread2.php?book
Э6	http://znanium.com/bookread2.php?book
Э7	http://www.skf-mtusi.ru/
Э8	http://www.skf-mtusi.ru/
6.3. Программное обеспечение	
П.1	Python for Linux
П.2	Scilab for Linux
П.3	Word processor Microsoft Word or LibreOffice Writer.

6. Материально-техническое обеспечение дисциплины

8.1 МТО лекционных занятий	
1	Лекционная аудитория, оборудованная интерактивной доской, проектором
8.2 МТО лабораторных работ и практических занятий	
1	Компьютерная аудитория
8.3 МТО рубежных контролей, защиты КР, экзамена	
1	Компьютерная аудитория

9. Методические рекомендации для обучающихся по самостоятельной работе

9.1 Указания по самостоятельной работе студента

Самостоятельная работа студентов является составной частью учебной работы и имеет целью закрепление и углубление полученных знаний и навыков, поиск и приобретение новых знаний, в том числе с использованием автоматизированных обучающих курсов (систем), а также выполнение учебных заданий, подготовку к предстоящим занятиям, зачетам и экзаменам.

Постановку задачи обучаемым на проведение самостоятельной работы преподаватель осуществляет на одном из занятии, предшествующему данному.

Методику самостоятельной работы все обучаемые выбирают индивидуально.

Студентам очной формы обучения при освоении вопросов для самостоятельного изучения, представленных в подразделе 4.1, рекомендуется соблюдать последовательность их изучения, представленную в таблице 3.

Таблица 3 – Учебный материал, выносимый на самостоятельное изучение студентам очной формы обучения

№	Темы, разделы, вынесенные на самостоятельную подготовку, вопросы для подготовки к практическим и лабораторным занятиям; курсовые работы, содержание контрольных работ; рекомендации по использованию литературы, ЭВМ и др.	Часов всего: 54	Неделя
Модуль 1			
1	Шифрование – базовая технология безопасности. Основные понятия и определения. История появления шифров	8	1-2
2	Вирусы как угроза информационной безопасности. Характерные черты компьютерных вирусов. Хронология развития компьютерных вирусов	8	3-4
3	Схемы заражения файлов; схемы заражения загрузчиков; способы маркировки, используемые вирусами	8	5-7
Модуль 2			
4	Анализ структуры и принципов функционирования вычислительных сетей с позиции обеспечения информационной безопасности	6	8-9
5	Угрозы информационно-программному обеспечению, характерные только для распределённой вычислительной среды.	6	10-11
6	Использование криптографических методов для защиты данных, циркулирующих в вычислительной сети.	6	12-13
7	Механизмы идентификации и аутентификации пользователей в компьютерных системах и сетях Защита компьютерных систем от удаленных атак.	8	14-15
8	Методы разграничения доступа. Виды разграничения доступа. Мандатное и дискретное управление доступом. Регистрация и аудит. Определение и содержание регистрации и аудита ИС. Межсетевое экранирование. Технология виртуальных частных сетей (VPN).	6	16
9	Надёжность средств защиты компонент; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям.	4	17

Студенты заочной формы обучения могут осваивать вопросы для самостоятельного изучения, представленные в подразделе 4.2 в произвольной последовательности, в удобное для них время. Однако к началу сессии они должны ориентироваться в материале, вынесенном на самостоятельное изучение.

Дополнения и изменения в Рабочей программе