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
«_29_» _____08_____ 2022 г.

Основы информационной безопасности Б1.О.11
рабочая программа дисциплины

Кафедра: Инфокоммуникационные технологии и системы связи
Направление подготовки: **10.03.01 Информационная безопасность**
Профиль: **Безопасность компьютерных систем.**
Формы обучения: **очная**

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	108/2сем		
Контактная работа, в том числе (по семестрам, курсам):		54/2сем		
Лекции		24/2сем		
Лабораторных работ		30/2сем		
Практических занятий				
Семинаров				
Самостоятельная работа		54/2сем		
Контроль				
Число контрольных работ (по курсам)				
Число КР (по семестрам, курсам)				
Число КП (по семестрам, курсам)				
Число зачетов с оценкой с разбивкой по семестрам (курсам)		1/2сем		
Число экзаменов с разбивкой по семестрам (курсам)				

Программу составил:
Профессор кафедры ИТСС, д.п.н., доцент Жуковский А.Г.

Рецензент:
Ведущий сотрудник ФГУП «РНИИРС, д.т.н., доцент Елисеев А.В.

Рабочая программа дисциплины
«Основы информационной безопасности»

разработана в соответствии с ФГОС ВО:
направления подготовки 10.03.01 «Информационная безопасность», утвержденным приказом Министерства образования и науки Российской Федерации от 17 ноября 2020г. N 1427.

Составлена на основании учебного плана
направления 10.03.01 «Информационная безопасность», профиля «Безопасность компьютерных систем», одобренного Учёным советом СКФ МТУСИ, протокол № 9 от 25.04.2022, и утвержденного директором СКФ МТУСИ 25.04.2022 г.

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

Протокол от «29» 08 2022 г. № 1

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 _____________________

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 преподавания дисциплины «Основы информационной безопасности» является формирование у обучаемых знаний в области основ информационной безопасности и навыков практического обеспечения защиты информации и безопасного использования программных и аппаратных средств в сетях и информационных системах.

2. Планируемые результаты обучения

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

Результатом освоения дисциплины являются сформированные у выпускника следующие компетенции:

Компетенции выпускника, формируемые в результате освоения дисциплины (в части, обеспечиваемой дисциплиной)
ОПК-1: Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства
Знать:
- понятия информации и информационной безопасности, место и роль информационной безопасности в системе национальной безопасности Российской Федерации; - направления обеспечения информационной безопасности; - классификацию методов криптографического преобразования информации; - структуру и принципы функционирования современных вычислительных систем; - основные способы защиты от потери информации и нарушений работоспособности сетей и систем.
Уметь:
- классифицировать и оценивать угрозы информационной безопасности; - проводить работы по сокрытию информации, проведению резервного копирования, восстановления информации; - использовать механизмы идентификации и аутентификации; - использовать антивирусные средства защиты; - восстанавливать потерянные компьютерные данные; - производить резервное копирование.
Владеть:
- основными понятиями, связанными с обеспечением информационно-психологической безопасности личности, общества и государства; информационного противоборства, информационной войны и формами их проявления в современном мире; - навыками работы по основам защиты информации с использованием программно-аппаратных комплексов.

3. Место дисциплины в структуре образовательной программы

Требования к предварительной подготовке обучающегося (предшествующие дисциплины, модули, темы):	
1	Дисциплина «Основы информационной безопасности» является логическим продолжением дисциплины Б1.О.03 «Информатика», знание которой в объеме требований образовательной программы является необходимым.
2	Успешное освоение дисциплины «Основы информационной безопасности» базируется также на знаниях, приобретенных из дисциплин: Б1.О.06 «Физика», Б1.О.07 «Иностранный язык», Б1.В.01 «Введение в профессию».

Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:	
1	Дисциплина является базовой для успешного освоения дисциплин: Б1.О.25 «Методы и средства криптографической защиты информации», Б1.О.26 «Безопасность операционных систем», Б1.О.29 «Основы управления информационной безопасностью», Б1.О.32 «Основы организационно-правового обеспечения информационной безопасности», Б1.О.33 «Программно-аппаратные средства защиты информации», Б1.О.37 «Комплексное обеспечение защиты информации»

4. Структура и содержание дисциплины

4.1 Очная форма обучения, 4 года (всего 108 часов, 54 аудиторных часов, 54 часов самостоятельной работы)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компетенции	УМИО
Курс 1, Семестр 2					
Модуль 1. Понятие информационной безопасности. Основные составляющие и направления обеспечения информационной безопасности. (26+28) часов					
1.1	Лекция 1. КОНЦЕПЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 1. Основные концептуальные положения системы защиты информации 2. Концептуальная модель информационной безопасности 3. Угрозы конфиденциальной информации 4. Действия, приводящие к неправомерному овладении конфиденциальной информацией	Л1.	4	ОПК-1	Л1.1 Л1.2 Л1.3
1.2	Лекция 2. НАПРАВЛЕНИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 1. Правовая защита 2. Организационная защита 3. Инженерно-техническая защита	Л2.	4	ОПК-1	Л1.1 Л1.2 Л1.3
1.3	Лекция 3. ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ 5.1.Общие положения 5.2.Защита информации от утечки по визуально оптическим каналам 5.3.Защита информации от утечки по акустическим каналам 5.4.Защита информации от утечки по электромагнитным каналам 5.5.Защита информации от утечки по материально - вещественным каналам	Л3.	4	ОПК-1	Л1.1 Л1.2 Л1.3
1.4	Лабораторная работа 1 Исследование характеристик и возможностей программ по защите и сокрытию файлов, папок	ЛР1	4	ОПК-1	Л3.1

1.5	Лабораторная работа 2 Исследование характеристик и возможностей программ по шифрованию, безвозвратному удалению, стеганографии	ЛР2	4	ОПК-1	Л3.1
1.6	Лабораторная работа 3 Основные 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	ЛР3	6	ОПК-1	Л3.1
1.7	Алгоритм симметричной системы шифрования данных – стандарт ГОСТ 28147-89. Алгоритм ассиметричной (двухключевой) системы шифрования данных RSA. Гостехкомиссия России. Руководящий документ Защита от несанкционированного доступа к информации. Термины и Определения. Доктрина информационной безопасности Российской Федерации. Указ президента российской федерации. Об утверждении перечня сведений конфиденциального характера. Положение о лицензировании деятельности по технической защите конфиденциальной информации. Постановление Правительства Российской Федерации от 30 апреля 2002 г. № 290. Инструкция по защите конфиденциальной информации при работе с зарубежными партнерами. Обеспечение сохранения коммерческой тайны предприятия. Каталог обобщенных мероприятий по защите конфиденциальной информации.	СРС	28	ОПК-1	Л1.1 Л1.2 Л1.3
Модуль 2 Основы защиты информации в инфокоммуникационных системах и сетях (28+26)					
2.1	Лекция 4. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ 1. Классификация методов криптографического преобразования информации 2. Шифрование. Основные понятия 3. Методы шифрования с симметричным ключом 4. Системы шифрования с открытым ключом 5. Стандарты шифрования 6. Перспективы использования криптозащиты информации в КС.	Л4	4	ОПК-1	Л1.1 Л1.2 Л1.3
2.2	Лекция 5. СТРУКТУРА И ПРИНЦИПЫ ФУНКЦИОНИРОВАНИЯ СОВРЕМЕННЫХ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ.	Л5	4	ОПК-1	Л1.1 Л1.2 Л1.3

	Проблемы обеспечения безопасности обработки и хранения информации в вычислительных системах. Базовые этапы построения системы комплексной защиты вычислительных систем. Анализ моделей нарушителя; угрозы информационно-программному обеспечению.				
2.3	Лекция 6. ОСНОВНЫЕ СПОСОБЫ ЗАЩИТЫ ОТ ПОТЕРИ ИНФОРМАЦИИ И НАРУШЕНИЙ РАБОТОСПОСОБНОСТИ СЕТЕЙ И СИСТЕМ 1. Внесение функциональной и информационной избыточности. 2. Способы резервирования информации; правила обновления резервных данных. 3. Методы сжатия информации; архивация файловых данных; резервирование системных данных; подготовка к программной среде.	Л6	4	ОПК-1	Л1.1 Л1.2 Л1.3
2.4	Лабораторная работа 4 Исследование характеристик и возможностей антивирусного ПО	ЛР4	4	ОПК-1	Л3.1
2.5	Лабораторная работа 5 Исследование характеристик и возможностей программ по восстановлению потерянных данных	ЛР5	6	ОПК-1	Л3.1
2.6	Лабораторная работа 6 Исследование характеристик и возможностей программ по организации резервного копирования	ЛР6	6	ОПК-1	Л3.1
2.7	Анализ структуры и принципов функционирования вычислительных сетей с позиции обеспечения информационной безопасности Угрозы информационно-программному обеспечению, характерные только для распределённой вычислительной среды. Классификация компьютерных вирусов Методы и средства борьбы с вирусами Профилактика заражения вирусами компьютерных систем. Порядок действий пользователя при обнаружении заражения ЭВМ вирусами Анализ моделей нарушителя; угрозы информационно-программному обеспечению вычислительных систем и их классификация Основные способы защиты от потери информации и нарушений работоспособности сетей и систем; внесение функциональной и информационной избыточности; способы резервирования информации; правила обновления резервных данных	СРС	26	ОПК-1	Л1.1 Л1.2 Л1.3
	Зачет			ОПК-1	Л1.1 Л1.2 Л1.3
Итого – 108 часов					

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	Е. Б. Белов, В. Лось, Р. В. Мещеряков, Д. А. Шелупанов	Основы информационной безопасности	М.: Гор. линия-Телеком, 2011. - 558 с.: ил.; 60x88 1/16. - (Специальность; Учебное пособие для высших учебных заведений.	Э1
Л1.2	Бузов Г.А.	Защита информации ограниченного доступа от утечки по техническим каналам	М.:Гор. линия-Телеком, 2015. - 586 с.: 60x90 1/16 (Обложка) ISBN 978-5-9912-0424-8	Э2
Л1.3	Шаньгин В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование, 2019. — 702 с. — ISBN 978-5-4488-0070-2	Э3

5.1.2. Дополнительная литература

Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л2.1	Гатчин Ю.А., Климова Е.В.	Введение в комплексную защиту объектов информатизации	СПб.: Университет ИТМО, 2011. — 112 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/65808.html	Э4

5.1.3. Учебно-методическое обеспечение для самостоятельной работы обучающихся

Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л3.1	Жуковский А.Г., Жуковский Д.А., Швидченко С.А.	ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТЕЙ И СИСТЕМ. Учебное пособие. – Ростов-на-Дону: СКФ МТУСИ, 2020. – 52 с.	РнД: СКФ МТУСИ, 2020	Э6

5.2. Электронные образовательные ресурсы

Э1	http://znanium.com/catalog/product/405159
Э2	http://znanium.com/catalog/product/895240
Э3	https://www.iprbookshop.ru/87995.html
Э4	http://www.iprbookshop.ru/65808.html
Э5	http://www.skf-mtusi.ru/?page_id=659
Э6	http://www.skf-mtusi.ru/?page_id=659

5.3. Программное обеспечение

П.1	1. AVAST Free Antivirus 2. AVG AntiVirus Free 3. Dr.Web Antivirus 4. Антивирус Касперского 5. ESET NOD32 Антивирус	Антивирусное ПО. Свободное, условно свободное или триал-версии.

	6. AVZ Antivirus 7. Avira Free Antivirus 8. Norton AntiVirus 9. McAfee Antivirus 10. Emsisoft Anti-Malware 11. BullGuard Antivirus 12. Protector Plus Antivirus 13. Panda Antivirus 14. Ashampoo Anti-Virus 14. G Data AntiVirus 16. K7 AntiVirus 17. VIRUSfighter 18. Twister Antivirus	
П.2	1. Wise Folder Hider 2. Secure Folders 3. Anvide Lock Folder 4. Folder Lock 5. Easy File Locker 6. Folder Guard 7. DEKSI USB Security 8. Locker (защита папок и дисков) 9. Advanced Hider 10. Hide Folders XP 11. Hide Files	Программное обеспечение по защите и сокрытию файлов и папок. Свободное, условно свободное или триал-версии.
П.3	1. TrustPort Tools 2. Cryptic Disk 3. Locker (скрытие файлов) 4. Max File Encryption 5. Secure Disk 6. Masker 7.1 7. Fox Secret 8. HideInPicture 1.0 9. Шифровальщик 10. Advanced Encryption Package 11. Gpg4win 12. Cryptic Disk Professional 13. CyberSafe Files Encryption 14. Steganos Privacy Suite 15. Lavasoft Privacy Toolbox 16. pkiImage Free Edition	Программное обеспечение по шифрованию, безвозвратному удалению, стеганографии. Свободное, условно свободное или триал-версии.
П.4	1. Hetman Partition Recovery 2. Active File Recovery 3. R-Studio 7.6 4. Auslogics File Recovery 5. Active UNDELETE 6. Paragon Rescue Kit 7. Wise Data Recovery	Программное обеспечение по восстановлению данных. Свободное, условно свободное или триал-версии.

	8. Puran File Recovery	
	9. O&O DiskRecovery	
	10. Tenorshare Any Data Recovery	
	11. Power Data Recovery	
	12. GetDataBack	
	13. Recover My Files	
	14. R-Undelete	
	15. Handy Recovery	
	16. Ashampoo Undeleter	
П.5	1. Iperius Backup 2. FBackup 3. Backup4all 4. Uranium Backup Free 5. Simple Data Backup 6. Personal Backup 7. Back4Sure 8. SyncBackFree 9. Handy Backup 10. EASEUS Todo Backup 8.0 Free Edition 11. Exiland Backup Free 4.0 12. Nero BackItUp 13. Paragon Rescue Kit 14.0 Free 14. Action Backup 15. LimBackup 16. AVSbackup 17. ExtraBackup 18. Cobian Backup 19. Backup & Recovery 10 Build 9169 Free Edition 20. Information Backup System	Программное обеспечение по резервному копированию данных. Свободное, условно свободное или триал-версии.
П.6	MS Word – с лицензией	
П.7	Power Point – с лицензией	

6. Материально-техническое обеспечение дисциплины

6.1 МТО лекционных занятий	
1	Лекционная аудитория, оборудованная интерактивной доской, проектором
6.2 МТО лабораторных работ и практических занятий	
1	Компьютерная аудитория с выходом в интернет
2	Обнаружитель видеокамер «Оптик-2» или «Облик-2»
3	Имитатор сигналов сложного типа «Аврора-3»
4	Комплекс радиомониторинга и анализа сигналов «Кассандра» или «Пиранья»
5	ПАК поиска и измерения ПЭМИН «Навигатор-П» или «Пегас»
6	Комплекс для проведения акустических и виброакустических измерений «Спрут-11М»
7	Нелинейный локатор «NR-900EMS или «Лорнет Стар» или Orion 2.4HX
8	Анализатор проводных линий Talan
9	Подавитель диктофонов и микрофонов «Комар» или «Спикер»
10	Блокиратор мобильной связи «Кейс» или RS-6000
11	Генератор шума ЛГШ-501 или ЛГШ-503

12	Беспилотные летательные аппараты (дроны) – 2 шт.
6.3 МТО рубежных контролей, экзамена	
1	Компьютерная аудитория

7. Методические указания для обучающихся по освоению дисциплины

7.1 Указания по самостоятельной работе студента

Достижение целей эффективной подготовки студентов в вузах невозможно без их целеустремленной самостоятельной работы. При этом, безусловно, нельзя обойтись без живого общения и консультирования со стороны профессорско-преподавательского состава 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. Обязательным компонентом самостоятельной работы студентов является внеаудиторный практикум по иностранному языку.

Самостоятельная работа организуется преподавателями, обеспечивается и контролируется кафедрами. Она предусматривает, как правило, разработку рефератов, выполнение расчетно-графических, вычислительных работ, моделирования и других творческих заданий в соответствии с учебной программой (тематическим планом изучения дисциплины). Основная цель данного вида занятий состоит в обучении курсантов методам самостоятельной работы с учебным материалом.

Материал, подлежащий обработке на самостоятельных занятиях, намечается при разработке программы самостоятельной работы. Опыт, накопленный кафедрами в организации самостоятельных занятий, что материал выделяемый на такие занятия, должен удовлетворять следующим требованиям:

- быть изложенным в учебнике достаточно полно и с примерами;
- обеспечиваться достаточным количеством литературы, учебных пособий. учебно-методических материалов, образцов техники
- содержать материал. углубляющий знания, полученные на лекции;
- осваивать проблемные еще не полностью решенные вопросы.

Проведению самостоятельной работы (как и любого другого вида занятий) должна предшествовать подготовка как преподавателя, так и обучаемых.

Постановку задачи обучаемым на проведение самостоятельного занятия преподаватель осуществляет на одном из занятия, предшествующему данному. Он разъясняет смысл занятия и указывает, что к нему студенты должны приготовить. Задание на самостоятельную работу должно быть выдано заблаговременно с тем, чтобы слушатели имели время на информационный поиск в библиотеке необходимых пособий.

Методику самостоятельной работы все обучаемые выбирают индивидуально, но методика достижения конечной цели может определяться преподавателем и включать: последовательность изучения и усвоения учебно-методического материала, пособий, руководств, наставлений, техники и т.д.; определение главного в изучаемом материале, материале, который необходимо законспектировать; просмотр учебных кинофильмов и их обсуждение; работу студентов по индивидуальным заданиям; опрос обучаемых в течении 7-10 минут с целью проверки усвоения главного из прочитанного материала.

При возникновении затруднений у обучаемых в разрешении вопросов задания преподавателю необходимо предусмотреть, чтобы каждый обучаемый мог получить оперативную консультацию по любому вопросу, если же при самостоятельной работе возникают затруднения по одному и тому же материалу (вопросу) у многих обучаемых, то желательно провести групповую консультацию.

Для контроля усвоения учебного материала целесообразно проводить в групповое собеседование или обсуждение изучаемого материала, проведение контрольных работ и т.п. Контрольные мероприятия при должной их организации позволяют не только оценивать знания материала, но и углубить и закрепить его у обучаемых.

Приветствуется использование компьютеров, которое:

- расширяет информационную баз) учебных занятий;
- повышает активность обучаемых, из пассивного получателя информации они превращаются в её добытчиков:
- способствует развитию способностей к анализу и обобщению, улучшает связанность, широту и глубину мышления;
- облегчает усвоение абстрактного материала, позволяет многое из него представить в виде конкретных образов;
- приучает к точности, аккуратности, последовательности действий способствует развитию самостоятельности.

Компьютерные технологии и программные продукты для выполнения самостоятельной работы по освоению учебного материала необходимо использовать в соответствии с указаниями методических разработок раздела 5 настоящей Рабочей программы.

Для более углубленного изучения материала по дисциплине целесообразно использовать учебные курсы сайта http://www.intuit.ru/ .

Таблица 7.1 – 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: 28	Неделя
Модуль 1 – 24 часа			
1	Алгоритм симметричной системы шифрования данных – стандарт ГОСТ 28147-89	3	1
2	Алгоритм ассиметричной (двухключевой) системы шифрования данных RSA;	3	2
3	Гостехкомиссия России. Руководящий документ Защита от несанкционированного доступа к информации. Термины и Определения;	4	3
4	Доктрина информационной безопасности Российской Федерации;	3	4
5	Указ президента российской федерации. Об утверждении перечня сведений конфиденциального характера;	3	5
6	Положение о лицензировании деятельности по технической защите конфиденциальной информации. Постановление Правительства Российской Федерации от 30 апреля 2002 г. № 290.	4	6
7	Инструкция по защите конфиденциальной информации при работе с зарубежными партнерами.	4	7
8	Обеспечение сохранения коммерческой тайны предприятия. Каталог обобщенных мероприятий по защите конфиденциальной информации.	4	8
Модуль 2 – 26 часов			
9	Анализ структуры и принципов функционирования вычислительных сетей с позиции обеспечения информационной безопасности.	3	9
10	Угрозы информационно-программному обеспечению, характерные только для распределённой вычислительной среды.	3	10

11	Классификация компьютерных вирусов	3	11
12	Методы и средства борьбы с вирусами	3	12
13	Профилактика заражения вирусами компьютерных систем.	3	13
14	Порядок действий пользователя при обнаружении заражения ЭВМ вирусами	3	14
15	Анализ моделей нарушителя; угрозы информационно-программному обеспечению вычислительных систем и их классификация.	4	15
16	Основные способы защиты от потери информации и нарушений работоспособности сетей и систем; внесение функциональной и информационной избыточности; способы резервирования информации; правила обновления резервных данных.	4	16

Дополнения и изменения в рабочей программе