МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«Национальный исследовательский ядерный университет «МИФИ»

Трехгорный технологический институт –

филиал федерального государственного автономного образовательного учреждения высшего образования
«Национальный исследовательский ядерный университет «МИФИ»

(ТТИ НИЯУ МИФИ)

УТВЕРЖДАЮ
Директор ТТИ НИЯУ МИФИ
_____Т.И. Улитина
«31» августа 2021 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«Информационная безопасность»

Направление подготовки: 09.03.01 Информатика и вычислительная техника

Профиль: Вычислительные машины, комплексы, системы и сети

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Трехгорный
2021

1. ЦЕЛИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Информация это нечто без чего мы не сможем продвигаться и развивать свои различные потребности. А важность информации в современном мире - признанный и неоспоримый факт.

Вот для чего и появилась необходимость в ее защите. Высокая уязвимость информационных технологий к различным злоумышленным действиям породила острую необходимость в средствах противодействия этому, что привело к возникновению и развитию области защиты информации (ЗИ) как неотъемлемой части информационной индустрии.

3.1 Цели дисциплины

Цель дисциплины «Информационная безопасность» заключается в ознакомлении с организационными, техническими, алгоритмическими и другими методами и средствами защиты компьютерной информации, с законодательством и стандартами в этой области, с современными криптосистемами, изучении методов идентификации пользователей, борьбы с вирусами, изучении способов применения методов защиты информации при проектировании вычислительных систем.

3.1 Задачи дисциплины

Основными задачами изучения дисциплины являются:

А) овладение теоретическими, практическими и методическими вопросами классификации угроз информационных ресурсов;

Б) ознакомление с современными проблемами информационной безопасности, основными концептуальными положениями системы защиты информации;

В) изучение основных направлений обеспечения информационной безопасности, меры законодательного, административного, процедурного и

программно-технического уровней при работе на вычислительной технике и в каналах связи;

Г) приобретение теоретических и практических навыков по использованию современных методов защиты информации в компьютерных системах;

Д) формирование практических навыков и способностей осуществления мероприятий по обеспечению информационной безопасности функционирования информационной системы при взаимодействии с информационными рынками по сетям или с использованием иных методов обмена данными.

Изучаемые вопросы рассматриваются в широком диапазоне современных проблем и затрагивают предметные области сферы защиты как документированной информации (на бумажных и технических носителях), циркулирующей в традиционном или электронном документообороте, находящейся в компьютерных системах, так и недокументированной информации, распространяемой персоналом в процессе управленческой (деловой) или производственной деятельности.

1.1. Цели дисциплины

Формирование у студентов основ знаний об информационной безопасности, роли и внедрении информации.

1.2. Задачи дисциплины

Обучение студентов приемам работы с современным программным обеспечением для практического освоения принципов и методов обеспечения информационной безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Дисциплина «Информационная безопасность» относится к циклу базовых дисциплин профессионального цикла, базируется на знаниях, получаемых студентами из курсов «Операционные системы», «Сети и телекоммуникации».

Знания, полученные в ходе изучения дисциплины необходимы при прохождении учебных и производственных практик, а также выполнении выпускной квалификационной работы.

3.КОМПЕТЕНЦИИ СТУДЕНТА, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ / ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ ОБРАЗОВАНИЯ И КОМПЕТЕНЦИИ СТУДЕНТА ПО ЗАВЕРШЕНИИ ОСВОЕНИЯ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1 Общекультурные и профессиональные компетенции

Изучение дисциплины «Информационная безопасность» направлено на формирование у студентов следующих компетенций:

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

3.1 Перечень результатов образования, формируемых дисциплиной, с указанием уровня их освоения

В результате освоения дисциплины обучающийся должен:

знать:

- основы саморазвития;
- основные методы и средства обеспечения информационной безопасности компьютерных систем;
- принципы классификации и примеры угроз безопасности компьютерным системам
- основные понятия в защите компьютерной информации, принципы классификации и примеры угроз безопасности;
- неисправности, влияющие на безопасность;

уметь:

- использовать самоконтроль и ответственность;
- конфигурировать встроенные средства безопасности в операционной системе; устанавливать и использовать одно из средств для шифрования информации и организации обмена данными с использованием электронной цифровой подписи; устанавливать и использовать один их межсетевых экранов;
- использовать средства защиты данных от разрушающих программных воздействий компьютерных вирусов
- проводить анализ и аудит информационных систем и систем безопасности;
- тщательно изучать компьютерные системы и неисправности;

владеть:

- умением правильно читать;
- навыками применения технических средств защиты информации;
- навыками применения методов и средств защиты информации;
- методами аудита безопасности информационных систем, методами системного анализа информационных систем;
- навыками исследования компьютерных систем и неисправностей, чтобы определить представляет ли неисправность угрозу.

3.3 Воспитательная работа

Направление/ цели	**Создание условий, обеспечивающих**	**Использование воспитательного потенциала учебных дисциплин**
Профессиональный модуль		
Профессиональное воспитание	- формирование чувства личной ответственности за научно-технологическое развитие России, за результаты исследований и их последствия **(В17)**	1.Использование воспитательного потенциала дисциплин профессионального модуля для формирования чувства личной ответственности за достижение лидерства России в ведущих научно-технических секторах и фундаментальных исследованиях, обеспечивающих ее экономическое развитие и внешнюю безопасность, посредством контекстного обучения, обсуждения социальной и практической значимости результатов научных исследований и технологических разработок. 2.Использование воспитательного потенциала дисциплин профессионального

		модуля для формирования социальной ответственности ученого за результаты исследований и их последствия, развития исследовательских качеств посредством выполнения учебно-исследовательских заданий, ориентированных на изучение и проверку научных фактов, критический анализ публикаций в профессиональной области, вовлечения в реальные междисциплинарные научно-исследовательские проекты.
	- формирование ответственности за профессиональный выбор, профессиональное развитие и профессиональные решения **(В18)**	Использование воспитательного потенциала дисциплин профессионального модуля для формирования у студентов ответственности за свое профессиональное развитие посредством выбора студентами индивидуальных образовательных траекторий, организации системы общения между всеми участниками образовательного процесса, в том числе с использованием новых информационных технологий.
	- формирование научного мировоззрения, культуры поиска нестандартных научно-технических/практических решений, критического отношения к исследованиям лженаучного толка **(В19)**	1.Использование воспитательного потенциала дисциплин/практик "Основы научных исследований", «"Учебная практика (научно-исследовательская работа (получение первичных навыков научно-исследовательской работы)" для: - формирования понимания основных принципов и способов научного познания мира, развития исследовательских качеств студентов посредством их вовлечения в исследовательские проекты по областям научных исследований. 2.Использование воспитательного потенциала дисциплин/практик "Введение в специальность", "Основы научных исследований", "Учебная практика (научно-исследовательская работа (получение первичных навыков научно-исследовательской работы)" для: - формирования способности отделять настоящие научные исследования от лженаучных посредством проведения со студентами занятий и регулярных бесед; - формирования критического мышления, умения рассматривать различные исследования с экспертной позиции посредством обсуждения со студентами современных исследований, исторических предпосылок появления тех или иных открытий и теорий.

	- формирование навыков коммуникации, командной работы и лидерства **(В20)**; - формирование способности и стремления следовать в профессии нормам поведения, обеспечивающим нравственный характер трудовой деятельности и неслужебного поведения **(В21)**; - формирование творческого инженерного/профес-сионального мышления, навыков организации коллективной проектной деятельности **(В22)**	1.Использование воспитательного потенциала дисциплин профессионального модуля для развития навыков коммуникации, командной работы и лидерства, творческого инженерного мышления, стремления следовать в профессиональной деятельности нормам поведения, обеспечивающим нравственный характер трудовой деятельности и неслужебного поведения, ответственности за принятые решения через подготовку групповых курсовых работ и практических заданий, решение кейсов, прохождение практик и подготовку ВКР. 2.Использование воспитательного потенциала дисциплин профессионального модуля для: - формирования производственного коллективизма в ходе совместного решения как модельных, так и практических задач, а также путем подкрепление рационально-технологических навыков взаимодействия в проектной деятельности эмоциональным эффектом успешного взаимодействия, ощущением роста общей эффективности при распределении проектных задач в соответствии с сильными компетентностными и эмоциональными свойствами членов проектной группы.
	- формирование культуры информационной безопасности **(В23)**	Использование воспитательного потенциала дисциплин профессионального модуля для формирования базовых навыков информационной безопасности через изучение последствий халатного отношения к работе с информационными системами, базами данных (включая персональные данные), приемах и методах злоумышленников, потенциальном уроне пользователям.
	УГНС 09.00.00 «Информатика и вычислительная техника»: - формирование навыков цифровой гигиены **(В24)**; - формирование ответственности за обеспечение кибербезопасности **(В25)**; - формирование профессиональной	1. Использование воспитательного потенциала дисциплин "Информатика", "Программирование", "Объектно-ориентированное программирование" для формирования культуры написания и оформления программ, а также привития навыков командной работы за счет использования систем управления проектами и контроля версий. 2.Использование воспитательного потенциала профильных дисциплин для формирования навыков цифровой гигиены, а также системности и гибкости мышления, посредством изучения методологических и

	ответственности, этики и культуры инженера-разработчика информационно-управляющих систем различного назначения, удовлетворяющих современным требованиям к обеспечению безопасности и защиты информации **(В26)**	технологических основ обеспечения информационной безопасности и кибербезопасности при выполнении и защите результатов учебных заданий и лабораторных работ по криптографическим методам защиты информации в компьютерных системах и сетях. 3. Использование воспитательного потенциала дисциплин профессионального модуля и всех видов практик для формирования приверженности к профессиональным ценностям, ответственности, этике и культуре инженера-разработчика информационно-управляющих систем различного назначения посредством контекстного обучения, осознанного выбора тематики проектов, выполнения индивидуальных и совместных проектов при работе в команде, с последующей публичной презентацией результатов.

4. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 5 зачетных единиц.

№ п/п	Раздел учебной дисциплины	Недели	Виды учебной деятельности, включая самостоятельную работу студентов и трудоемкость (в часах)				Текущий контроль успеваемости (неделя, форма)	Аттестация раздела (неделя, форма)	Макс. балл за раздел *
			Лекции	Лаб. работы	Прак. работы	Самост. работа			
Семестр 7									
1	Раздел 1	1-4	3	7	3	4	Т1-2	КТ1-4	10
2	Раздел 2	5-8	3	7	3	4	Т2– 6	КТ2-8	15
3	Раздел 3	9-12	3	7	3	4	Т3– 10	КТ3-12	15
4	Раздел 4	13-18	5	7	5	4	Т4-14	КТ4-18	10
Итого			14	28	14	16			50
Экзамен			-						50
Итого за семестр									100
Семестр 8									
1	Раздел 1	1-4	5	4	4	4	Т1-2	КТ1-4	10
2	Раздел 2	5-8	5	5	5	4	Т2– 6	КТ2-8	15

3	Раздел 3	9-12	5	4	4	4	Т3– 10	КТ3-12	15
4	Раздел 4	13-18	5	5	5	4	Т4-14	КТ4-18	10
Итого			20	18	18	16			50
Экзамен			36						50
Итого за семестр									100

Т – Тест, КТ– Контрольная точка

4.1 Содержание лекций

Раздел 1 Концепция информационной безопасности

Тема 1.1 Актуальность информационной безопасности. Лицензирование и сертификация в области защиты информации.

Тема 1.2 Основные нормативные руководящие документы.

Тема 1.3 Классификация средств защиты информации и программного обеспечения от несанкционированного доступа и копирования.

Раздел 2 Активные и пассивные методы защиты программного обеспечения

Тема 2.1 Средства и методы защиты дисков от несанкционированного доступа и копирования

Тема 2.2 Способы создания ключевых носителей информации. Привязка программных средств к конкретному компьютеру.

Тема 2.3 Критерии выбора системы защиты. Технические устройства защиты информации и программного обеспечения.

Тема 1.2 Принципы действия электронных ключей

Раздел 3 Организация систем защиты информации от несанкционированного доступа

Тема 3.1 Идентификация и установление подлинности. Установление подлинности пользователя, файла, вычислительной системы.

Тема 3.2 Выбор пароля.

Тема 3.4 Установление полномочий. Матрица установления полномочий.

Тема 3.3 Системы регистрации пользователей, событий, используемых ресурсов.

Раздел 4 Криптография

Тема 4.1 Основные понятия криптографии

Тема 4.2 Простейшие методы шифрования с закрытым ключом

Тема 4.3 Принципы построения блочных шифров с закрытым ключом

Тема 4.4 Алгоритмы шифрования DES и AES

Тема 4.5 Алгоритм криптографического преобразования данных ГОСТ 28147-89

Тема 4.6 Криптографические хеш-функции

Тема 4.7 Поточные шифры и генераторы псевдослучайных чисел

Тема 4.8 Введение к криптографию с открытым ключом

Тема 4.9 Основные положения теории чисел, используемые в криптографии с открытым ключом

Тема 4.10 Криптографические алгоритмы с открытым ключом и их использование

Тема 4.11 Электронная цифровая подпись

Тема 4.12 Совершенно секретные системы

Тема 4.13 Шифрование, помехоустойчивое кодирование

Тема 4.17 Сжатие информации

Раздел 5. Криптография с открытым ключом

Тема 5.1 Введение к криптографию с открытым ключом

Тема 5.2 Основные положения теории чисел, используемые в криптографии с открытым ключом

Тема 5.3 Криптографические алгоритмы с открытым ключом и их использование

Тема 5.4 Электронная цифровая подпись

Тема 5.5 Совершенно секретные системы

Тема 5.6 Шифрование, помехоустойчивое кодирование

Тема 5.7 Сжатие информации

Раздел 6. Компьютерные вирусы

Тема 6.1 Классификация вредоносных программ

Тема 6.2 Основы работы антивирусных программ

Тема 6.3 Облачная антивирусная защита

Тема 6.4 Защита персональных компьютеров и корпоративных систем от воздействия вредоносных программ и вирусов.

Раздел 7. Правовые основы защиты информации

Тема 6.1. Применение патентования и норм авторского права при защите программных продуктов.

Тема 6.2. Основные положения Закона об охране программ для ЭВМ и баз данных

4.2 Тематический план практических работ

Защита дисков от несанкционированного доступа и копирования

Создание ключевого носителя информации.

Выбор системы защиты.

Установление подлинности пользователя, файла, вычислительной системы

Выбор пароля.

Шифрование с закрытым ключом.

Блочные шифры с закрытым ключом.

Шифрование DES.

Преобразование данных по алгоритму ГОСТ 28147-89

Вредоносные программы

Антивирусная защита

Облачная антивирусная защита.

Защита персональных компьютеров.

4.3 Тематический план практических работ

Лицензирование и сертификация в области защиты информации.

Нормативные документы

Средства защиты от несанкционированного доступа и копирования.

Электронные ключи.

Матрица полномочий.

Системы регистрации.

Криптография.

Хеш-функции.

Поточные шифры и генераторы псевдослучайных чисел.

Криптография с открытым ключом.

Электронная цифровая подпись.

Совершенно секретные системы.

Помехоустойчивое кодирование.

Сжатие информации.

Антивирусные программы

Применение патентования и норм авторского права.

Охрана программ для ЭВМ и баз данных

4.4 Самостоятельная работа студентов

Проработка лекционного материала

Подготовка к лабораторным и практическим работам

Подготовка к рубежному контролю (по темам дисциплины, входящим в раздел).

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Выпускник вуза должен не просто обладать определенной суммой знаний, а уметь при помощи этих знаний решать конкретные задачи производства. Учитывая требования ОС НИЯУ МИФИ по направлению подготовки 09.03.01 «Информатика и вычислительная техника», реализация компетентностного подхода должна предусматривать широкое использование в учебном процессе активных и интерактивных форм проведения занятий в сочетании с

внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

Лекционные занятия проводятся в специализированной аудитории с применением мультимедийного проектора в виде учебной презентации. Учебные материалы предъявляются обучающимся для ознакомления и изучения, основные моменты лекционных занятий конспектируются. Отдельные темы предлагаются для самостоятельного изучения с обязательным составлением конспекта.

Практические занятия проводятся также с применением мультимедийного проектора с разбором типовых решений задач на прочность, жесткость и устойчивость с выдачей учебных материалов студентам.

.

Текущий контроль знаний студентов по отдельным разделам и в целом по дисциплине проводится в форме компьютерного или бумажного тестирования.

В таблице 6 представлены интерактивные образовательные технологии, используемые в аудиторных занятиях.

Таблица 6. Интерактивные образовательные технологии

Семестр	Вид занятия (Л, ПР, ЛР, ТК)	Используемые интерактивные образовательные технологии	Количество часов
3	Л	Мультимедийные технологии	12
	ПР	Мультимедийные технологии	2
	ЛР	Мультимедийные технологии	8
4	Л	Мультимедийные технологии	10
	ПР	Мультимедийные технологии	2
	ЛР	Мультимедийные технологии	8
Всего:			42

6. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯУСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ И УЧЕБНО-

МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Перечень оценочных средств, используемых для текущей аттестации

Код	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде
Т1	Тест №1	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося.	Тестовые задания по темам
Т2	Тест №2	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося.	Тестовые задания по темам
Т3	Тест №3	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося.	Тестовые задания по темам
Т4	Тест №4	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося.	Фонд тестовых заданий
КТ1	Контрольная точка №1	Средство проверки умений применять полученные знания для решения расчетно-графических задач определенного типа по теме или разделу	Комплект расчетно-графических заданий по вариантам
КТ2	Контрольная точка №2		
КТ3	Контрольная точка №2		
КТ4	Контрольная точка №2		

Расшифровка компетенций через планируемые результаты обучения

Связь между формируемыми компетенциями и планируемыми результатами обучения представлена в следующей таблице:

Код	Проектируемые результаты освоения дисциплины и индикаторы формирования компетенций			Средства и технологии оценки
	Знать (З)	Уметь (У)	Владеть (В)	
ОПК-7	З1, З2, З3, З4, З5	У1, У2, У3, У4, У5	В1, В2, В3, В4, В5	Семестры 7 и 8: Т1,Т2,Т4,Т5,КТ1,КТ2, КТ3,КТ4,Э
ОПК-9	З1, З2, З3, З4, З5	У1, У2, У3, У4, У5	В1, В2, В3, В4, В5	Семестры 7 и 8: Т1,Т2,Т4,Т5,КТ1,КТ2, КТ3,КТ4,Э

Этапы формирования компетенций

Раздел	Темы занятий	Коды компетенций	Знания, умения и навыки	Виды аттестации		
				Текущий контроль – неделя	Аттестация раздела – неделя	Промежуточная аттестация
7 семестр						
Раздел 1	Концепция информационной безопасности	ОПК-7 ОПК-9	З1, З2, З3, З4, З5, У1, У2, У3, У4, У5, В1, В2, В3, В4, В5	Т1-2	КТ1-4	Зачёт
Раздел 2	Активные и пассивные методы защиты программного обеспечения	ОПК-7 ОПК-9	З1, З2, З3, З4, З5, У1, У2, У3, У4, У5, В1, В2, В3, В4, В5	Т2-4	КТ2-8	
Раздел 3	Организация систем защиты информации от несанкционированного доступа	ОПК-7 ОПК-9	З1, З2, З3, З4, З5, У1, У2, У3, У4, У5, В1, В2, В3, В4, В5	Т3-10	КТ3-12	
Раздел 4	Криптография	ОПК-7 ОПК-9	З1, З2, З3, З4, З5, У1, У2, У3, У4, У5, В1, В2, В3, В4, В5	Т4-14	КТ4-18	
8 семестр						

Раздел 1	Криптография с открытым ключом	ОПК-7 ОПК-9	З1, З2, З3, З4, З5, У1, У2, У3, У4, У5, В1, В2, В3, В4, В5	Т1-2	КТ1-4	Экзамен
Раздел 2	Компьютерные вирусы	ОПК-7 ОПК-9	З1, З2, З3, З4, З5, У1, У2, У3, У4, У5, В1, В2, В3, В4, В5	Т2-4	КТ2-8	
Раздел 3	Правовые основы защиты информации	ОПК-7 ОПК-9	З1, З2, З3, З4, З5, У1, У2, У3, У4, У5, В1, В2, В3, В4, В5	Т3-10	КТ3-12	
Раздел 4	(Отсуствует)	ОПК-7 ОПК-9	З1, З2, З3, З4, З5, У1, У2, У3, У4, У5, В1, В2, В3, В4, В5	Т4-14	КТ4-18	

Шкала оценки образовательных достижений

Код	Вид оценочного средства	Критерии	Балл	Макс. балл– мин. балл
Т1 Т2 Т3 Т4	Тестовое задание 1,2,3,4	выставляется студенту, если 90-100% тестовых вопросов выполнено правильно	10	**10 – 7**
		выставляется студенту, если 80-89% тестовых задач выполнено правильно	8,5	
		выставляется студенту, если 60-79% тестовых задач выполнено правильно	7	
		при ответе студента менее, чем на 60% вопросов тестовое задание не зачитывается и у студента образуется долг, который должен быть закрыт в течение семестра или на зачетной неделе	<7	
КТ1 КТ2 КТ3 КТ4	Контрольная точка 1,2,3,4	выставляется студенту, если 90-100% тестовых вопросов выполнено правильно	5	**5 – 3**
		выставляется студенту, если 80-89% тестовых задач выполнено правильно	4	
		выставляется студенту, если 60-79% тестовых задач выполнено правильно	3	
		при ответе студента менее, чем на 60% вопросов тестовое задание не зачитывается и у студента образуется долг, который должен быть закрыт в течение семестра или на зачетной неделе	<3	

РГР1 РГР2 РГР3	Расчетно-графическая работа 1,2,3	выставляется студенту, если все сделано правильно	5	**5 – 3**
		выставляется студенту, если решение содержит ошибки	4	
		выставляется студенту, если решения содержат ошибки и было сдано не в срок	3	
		выставляется студенту, во всех остальных случаях	<3	
УО1 УО2 УО3 УО4	Устный опрос 1,2,3,4	выставляется студенту, если все ответы верные	5	**5 – 3**
		выставляется студенту, если ответы не точные	4	
		выставляется студенту, если ответил не на все вопросы	3	
		выставляется студенту, во всех остальных случаях	<3	
ПО	Письменный опрос	выставляется студенту, если все ответы верные	5	**5 – 3**
		выставляется студенту, если ответы не точные	4	
		выставляется студенту, если ответил не на все вопросы	3	
		выставляется студенту, во всех остальных случаях	<3	
Э	Экзамен	выставляется студенту при правильно написанном билете и при ответе на все дополнительные вопросы по курсу с незначительными неточностями, которые студент должен устранить в процессе беседы с преподавателем, в рамках которой он демонстрирует углубленное понимание предмета и владение ключевыми знаниями, умениями и навыками, предусмотренными данной дисциплиной	40-50	**50 – 30**
		выставляется студенту при правильно написанном билете и при ответе на часть дополнительных вопросов по курсу с демонстраций базовых знаний, умений и навыков, предусмотренных данной дисциплиной	35-39	
		выставляется студенту при написанных ответах на вопросы билета (допускается содержание некоторых неточностей) и демонстрации базовых знаний, умений и навыков по данной дисциплине	30-34	
		если студент не написал ответ хотя бы на один из вопросов билета и не может ответить на дополнительные компетентностно–ориентированные вопросы	<30	

Итоговая оценка представляет собой сумму баллов, заработанных студентом при выполнении заданий в рамках текущего и промежуточного контроля и выставляется в соответствии с Положением о кредитно-модульной системе в соответствии со следующей шкалой:

Оценка по 5-балльнойшкале	Сумма баллов за разделы	Оценка ECTS
5 – *«отлично»*	90-100	A
4 – «*хорошо*»	85-89	B
	75-84	C
	70-74	D
3 – «*удовлетворительно*»	65-69	
	60-64	E
2 – «*неудовлетворительно*»	Ниже 60	F

Расшифровка уровня знаний, соответствующего полученным баллам, дается в таблице указанной ниже

Оценка по 5-балльной шкале – оценка по ECTS	**Сумма баллов за разделы**	**Требования к знаниям на экзамене**
«отлично» – *A*	90 ÷ 100	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, использует в ответе материал монографической литературы.
«хорошо» – *D, C, B*	70 ÷ 89	Оценка «хорошо» выставляется студенту, если он твёрдо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.
«удовлетворительно» – *E, D*	60 ÷ 69	Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала.
«неудовлетворительно» – *F*	менее 60	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.

7 УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

7.1 Основная литература

1. Мельников, В.П. Информационная безопасность и защита информации [Текст] : учеб. пособие / В. П. Мельников, С. А. Клейменов, А. М. Петраков; под ред. С. А. Клейменова. - 5-е изд., стер. - Москва: Академия, 2011. - 332 с. : ил., табл.; 22 см. - (Высшее профессиональное образование. Информатика и вычислительная техника). - Библиогр.: с. 327-328. - ISBN 978-5-7695-7738-3 (в пер.)
2. Проскурин, В.Г.Защита программ и данных [Текст]: учебное пособие для вузов / В. Г. Проскурин. - Москва: Академия, 2011. - 198, [1] с. : ил. ; 22 см. - (Серия Бакалавриат). - Библиогр.: с. 195-196. - ISBN 978-5-7695-7933-2 (в пер.)
3. Федин Ф.О. Информационная безопасность [Электронный ресурс]: учебное пособие/ Федин Ф.О., Офицеров В.П., Федин Ф.Ф.— Электрон. текстовые данные.— М.: Московский городской педагогический университет, 2011.— 260 с.— Режим доступа: http://www.iprbookshop.ru/26486.— ЭБС «IPRbooks», по паролю
4. Спицын В.Г. Информационная безопасность вычислительной техники [Электронный ресурс]: учебное пособие/ Спицын В.Г.— Электрон. текстовые данные.— Томск: Эль Контент, Томский государственный университет систем управления и радиоэлектроники, 2011.— 148 с.— Режим доступа: http://www.iprbookshop.ru/13936.— ЭБС «IPRbooks», по паролю
5. Башлы П.Н. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие/ Башлы П.Н., Бабаш А.В., Баранова Е.К.— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2012.— 311 с.— Режим доступа: http://www.iprbookshop.ru/10677.— ЭБС «IPRbooks», по паролю

6. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс]/ Шаньгин В.Ф.— Электрон. текстовые данные.— М.: ДМК Пресс, 2014.— 702 с.— Режим доступа: http://www.iprbookshop.ru/29257.— ЭБС «IPRbooks», по паролю
7. Малюк А.А. Введение в информационную безопасность [Электронный ресурс]: учебное пособие/ Малюк А.А., Горбатов В.С., Королев В.И.— Электрон. текстовые данные.— М.: Горячая линия - Телеком, 2011.— 288 с.— Режим доступа: http://www.iprbookshop.ru/11979.— ЭБС «IPRbooks», по паролю
8. Малюк А.А. Теория защиты информации [Электронный ресурс]: монография/ Малюк А.А.— Электрон. текстовые данные.— М.: Горячая линия - Телеком, 2012.— 184 с.— Режим доступа: http://www.iprbookshop.ru/12048.— ЭБС «IPRbooks», по паролю
9. Скрипник Д.А. Общие вопросы технической защиты информации [Электронный ресурс]/ Скрипник Д.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2012.— 264 с.— Режим доступа: http://www.iprbookshop.ru/16710.— ЭБС «IPRbooks», по паролю.

7.2 Дополнительная литература

1. Информационная безопасность и защита информации [Текст] : [учеб. пособие для вузов] / Ю. Ю. Громов [и др.]. - Старый Оскол: ТНТ, 2010. - 384 с.: рис., табл. - Библиогр.: с. 382-383. - ISBN 978-5-94178-216-1
2. Гашков, С.Б. Криптографические методы защиты информации [Текст] : учеб. пособие для студ. вузов, обуч. по напр. "Прикладная математика и информатика" и "Информ. технологии" / С. Б. Гашков, Э. А. Применко, М. А. Черепнев. - Москва: Академия, 2010. - 297, [1] с.; 22 см. - (Высшее профессиональное образование. Информационная безопасность). - Предм. указ.: с. 285-286. - Библиогр.: с. 287-294 (157 назв.). - ISBN 978-5-7695-4962-5

3. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс]/ Шаньгин В.Ф.— Электрон. текстовые данные.— М.: ДМК Пресс, 2010.— 544 c.— Режим доступа: http://www.iprbookshop.ru/7943.— ЭБС «IPRbooks», по паролю

4. Фороузан Бехроуз А. Криптография и безопасность сетей [Электронный ресурс]: учебное пособие/ Фороузан Бехроуз А.— Электрон. текстовые данные.— М.: БИНОМ. Лаборатория знаний, Интернет-Университет Информационных Технологий (ИНТУИТ), 2010.— 784 c.— Режим доступа: http://www.iprbookshop.ru/15847.— ЭБС «IPRbooks», по паролю

7.3 Периодические издания

1 1 Информационные технологии

2 Информационные технологии в проектировании и производстве

7.4 Интернет-ресурсы

№	Наименование ресурса	Интернет-ссылка на ресурс
1	Электронная библиотечная система ЮРАЙТ	https://urait.ru/
2	Электронная библиотечная система «Лань» ООО "Издательство Лань"	e.lanbook.com
3	Электронная библиотечная система IPR BOOKS	https://www.iprbookshop.ru/
4	Электронная библиотечная система eLIBRARY ООО "РУНЭБ"	http://elibrary.ru
5	Научные полнотекстовые ресурсы издательства Springer (архив) Springer Customer Service Center GmbH, обеспечение доступа ФГБУ "ГПНТБ России"	http://link.springer.com/
6	Единое окно доступа к образовательным ресурсам	http://window.edu.ru/

8 МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для проведения учебных занятий лекционного и семинарского типа, групповые и индивидуальных консультаций, текущего контроля, промежуточной аттестации используются учебные аудитории, оснащенные оборудованием и техническими средствами обучения.

Учебные аудитории для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду вуза.

ТТИ НИЯУ МИФИ обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения.

Сведения о наличии оборудованных учебных кабинетов, объектов для проведения практических занятий представлены на официальном сайте ТТИ НИЯУ МИФИ: http://tti-mephi.ru/sveden/objects