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
«26» июня 2024 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«Защита информации»

Направление подготовки: 09.03.01 Информатика и вычислительная техника

Профиль: Вычислительные машины, комплексы, системы и сети

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Трехгорный
2024

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.

1.1. Цели дисциплины

Цель дисциплины «Защита информации» 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.

1.2. 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.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Дисциплина «Защита информации» относится к циклу базовых дисциплин профессионального цикла, базируется на знаниях, получаемых студентами из курсов «Операционные системы», «Сети и телекоммуникации». Дисциплина изучается в 7,8 семестрах.

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

3.1 Перечень компетенций

Изучение дисциплины «Защита информации» направлено на формирование у студентов следующих компетенций:

Изучение дисциплины «Защита информации» направлено на формирование у студентов следующих компетенций:

– Способен осваивать методики использования программных средств для решения практических задач (ОПК-9).

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

В результате освоения дисциплины обучающийся должен:

знать:

- 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:

- 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:

- 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,	1.Использование воспитательного потенциала дисциплин/практик "Основы научных исследований", «"Учебная практика (научно-исследовательская работа (получение первичных навыков научно-исследовательской работы)" для: - формирования понимания основных

	критического отношения к исследованиям лженаучного толка **(В19)**	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)**;	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,

	- формирование профессиональной ответственности, этики и культуры инженера-разработчика информационно-управляющих систем различного назначения, удовлетворяющих современным требованиям к обеспечению безопасности и защиты информации **(В26)**	посредством изучения методологических и 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 5									
1	Раздел 1	1-4	4	7	4	4	Т1 – 2	КТ-1	10
2	Раздел 2	5-8	4	7	4	4	Т2 – 6	КТ-2	15
3	Раздел 3	9-12	4	7	4	4	Т3 – 10	КТ-3	15
4	Раздел 4	13-18	2	7	2	4	Т4 – 14	КТ-4	10
Итого			14	28	14	16			50
Зачет									50
Итого за семестр									100
Семестр 6									
1	Раздел 5	1-4	5	4	4	4	Т5 – 2	КТ-1	10
2	Раздел 6	5-8	5	6	6	2	Т6 – 6	КТ-2	15
3	Раздел 7	9-12	5	4	4	6	Т7 – 10	КТ-3	15
4	Раздел 8	13-18	5	4	4	4	Т8 – 14	КТ-4	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 7,8. 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

1. Лицензирование и сертификация в области защиты информации.
2. Нормативные документы
3. Средства защиты от несанкционированного доступа и копирования.
4. Электронные ключи.
5. Матрица полномочий.
6. Системы регистрации.
7. Криптография.
8. Хеш-функции.
9. Поточные шифры и генераторы псевдослучайных чисел.
10. Криптография с открытым ключом.
11. Электронная цифровая подпись.
12. Совершенно секретные системы.
13. Помехоустойчивое кодирование.
14. Сжатие информации.
15. Антивирусные программы
16. Применение патентования и норм авторского права.
17. Охрана программ для ЭВМ и баз данных

4.3 Самостоятельная работа студентов

1. Проработка лекционного материала
2. Подготовка к лабораторным и практическим работам
3. Подготовка к рубежному контролю (по темам дисциплины, входящим в раздел).

4.4 Лабораторные работы студентов

1. Защита дисков от несанкционированного доступа и копирования
2. Создание ключевого носителя информации.
3. Выбор системы защиты.
4. Установление подлинности пользователя, файла, вычислительной системы
5. Выбор пароля.
6. Шифрование с закрытым ключом.
7. Блочные шифры с закрытым ключом.
8. Шифрование DES.
9. Преобразование данных по алгоритму ГОСТ 28147-89
10. Вредоносные программы
11. Антивирусная защита
12. Облачная антивирусная защита.
13. Защита персональных компьютеров.

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.

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

	ПР	Мультимедийные технологии
	ЛР	Мультимедийные технологии

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
Т5	Тест №5	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося.	Фонд тестовых заданий

Т6	Тест №6	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося.	Фонд тестовых заданий
Т7	Тест №7	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося.	Фонд тестовых заданий
З	Зачет	Средство проверки, полученных знаний по дисциплине	Комплект вопросов по пройденным темам
Э	Экзамен	Средство проверки, полученных знаний по дисциплине	Комплект вопросов по пройденным темам

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-9	З1, З2, З3, З4, З5	У1, У2, У3, У4, У5	В1, В2, В3, В4, В5	,Т1, Т2, Т3, Т4, Т5, Т6, Т7, Т8, КТ1-8,Э

Шкала оценки образовательных достижений

Код	**Вид оценочного средства**	**Критерии**	**Балл**	**Макс. балл– мин. балл**
Т	Тестовое задание	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	
		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.

Контроль остаточных знаний

1. **Какова стратегия при защите от всех известных угроз?**

1) Наступательная;
2) Оборонительная;
3) Упреждающая.

2. **В чем сходства теории нечетких множеств и нестрогой математики?**

1) Оценивание меры принадлежности элемента множеству происходит количественно;
2) Решение соответствующей задачи происходит с помощью строгого алгоритма;
3) В основе обоих методологий лежит представление о размытости границ принадлежности элементов определенному множеству;
4) Нечеткость рассуждений последовательно проводится вплоть до алгоритма решения соответствующей задачи.

3. **Сбой – это …**

1) Нарушение работоспособности какого-либо элемента системы, приводящее к невозможности выполнения им основных своих функций;

2) Временное нарушение работоспособности какого-либо элемента системы, следствием чего может быть неправильное выполнение им в этот момент своей функции;

3) Неправильное выполнение элементом одной или нескольких функций, происходящее вследствие специфического его состояния;

4) негативное воздействие на систему в целом или отдельные ее элементы, оказываемое какими-либо явлениями, происходящими внутри системы или во внешней среде.

4. **Определите эмпирическую формулу расчета потерь от i-ой угрозы**

1) $Ri = 12^{(Si+Vi-4)}$;
2) $Ri = 10^{(Si+Vi-4)}$;
3) $Ri = 8^{(Si+Vi-4)}$;
4) $Ri = 4^{(Si+Vi-4)}$.

5. **Определите формальные средства защиты информации из предложенных**

1) Физические;
2) Организационные
3) Аппаратные;
4) Программные;
5) Законодательные.

6. **Слово «ЯВЛЯЕТСЯ» зашифрованное по методу таблицы Вижинера с монофонической подстановкой с ключем «САЛЬЕРИ» будет закодировано как**

1) РВЦЩКВЩР;
2) САЛЬРИЕР;
3) РИРАЛЬЕС;
4) ЛЬАРСИЕР.

7. **Специальный компонент, предназначенный для объединения всех подсистем СЗИ в единую целостную систему организации, обеспечения и контроля ее функционирования называется?**

1) Центральный процессор;
2) Ядро;
3) Центральная БД;
4) Супервизор (root).

8. **К какому классу антивирусных программ относятся программы просмотра оперативной памяти, состав и характеристики находящихся там модулей?**

1) А;

2) Б;
3) В;
4) Г.

9. **Расположить в порядке возрастания уровни эталонной модели ISO/OSI**

1) Представительный;
2) Транспортный;
3) Сетевой;
4) Канальный (или передачи данных);
5) Сеансовый;
6) Физический;
7) Прикладной.

10. **Конфиденциальность информационного ресурса – это?**

1) Уровень секретности сведений, которые обрабатываются и передаются ресурсом;
2) Степень влияния информационного ресурса на эффективность функционирования производственных процессов.

11. **При статистическом моделировании …**

1) Структура системы и процессы ее функционирования представляются в виде некоторых выражений, отображающих зависимость определяемых характеристик от параметров системы и параметров внешней среды.
2) Структура моделируемой системы адекватно отображается в модели, а процессы ее функционирования проигрываются (имитируются) на построенной модели.

12. **Показатель полноты информации – это?**

1) Значимость с точки зрения тех задач, для решения которых используется оцениваемая информация;
2) Показатель, характеризующий меру достаточности информации для решения соответствующих задач;
3) Степень ее соответствия действительному состоянию тех реалий, которые отображает оцениваемая информация;
4) Показатель, который характеризует соответствие ее потребностям решаемой задачи;
5) Показатель, который характеризует удобство восприятия и использования информации в процессе решения задач.

13. **Шифрование – это …**

1) Такой вид криптографического закрытия, при котором преобразованию подвергается каждый символ защищаемого сообщения;
2) Такой вид криптографического закрытия, когда некоторые элементы защищаемых данных заменяются заранее выбранными кодами;

3) Рассечение массива защищаемых данных на такие элементы, каждый из которых в отдельности не позволяет раскрыть содержание защищаемой информации;

4) Замена часто встречающихся одинаковых данных или последовательностей одинаковых символов некоторыми заранее выбранными символами.

14. **К какому классу программных средств антивирусной защиты относятся программы – оптимизаторы дискового пространства**

1) А;
2) Б;
3) В;
4) Г.

15. **Под кодированием понимается:**

1) такой вид криптографического закрытия, когда некоторые элементы защищаемых данных (это не обязательно отдельные символы) заменяются заранее выбранными кодами (цифровыми, буквенными, буквенно-цифровыми сочетаниями и т.п.);

2) такой вид криптографического закрытия, при котором преобразованию подвергается каждый символ защищаемого сообщения.

16. **Электронные вирусы – это:**

1) вредоносные программы, которые не только осуществляют несанкционированные действия, но обладают способностью к саморазмножению, в силу чего представляют особую опасность для вычислительных сетей. Однако, для размножения им необходим носитель (файл, диск), что естественно создает для злоумышленников определенные трудности в осуществлении их несанкционированных действий;

2) вредоносные программы, которые злоумышленно вводятся в состав программного обеспечения и в процессе обработки информации осуществляют несанкционированные процедуры, чаще всего – процедуры незаконного захвата защищаемой информации, например, записывая ее в определенные места ЗУ или выдавая злоумышленникам;

3) вредоносные программы, не требующие для своего размножения специального носителя. Они обычно используют дополнительный вход в операционную систему, который создается для удобства ее отладки и, которые, нередко забывают убрать по окончании отладки.

17. **Интервьюирование при привлечении экспертов к решению задач заключается в:**

1) эксперт устно или письменно высказывается по поставленному вопросу;

2) каждый эксперт устно или письменно отвечает (в диалоговом режиме) на серию вопросов, которые ставит организатор экспертизы;

3) каждый эксперт отвечает письменно на вопросы, содержащиеся в заблаговременно составляемых одной или нескольких анкетах.

18. **Высотой нечеткого множества вида** $\mathbf{A} = \sum_{i=1}^{n} \frac{\mu A(ui)}{ui} = \sum_{i=1}^{n} \frac{\mu i}{ui}$ **называется:**

1) значение Sup $\mu A(u)$, то есть верхняя граница $\mu A(u)$.

2) множество всех элементов универсального множества U, имеющих ненулевую меру (степень) принадлежности множеству A

19. **Коэффициент значимости эксперта необходим для:**

1) он ничего не определяет;

2) определения компетентности эксперта;

3) получение такой выборки оценок экспертов, на которой статистически устойчиво проявилось бы их общее мнение по решаемой проблеме.

20. **Какая функция является лишней в определении шагов по смене состояний системы во времени, в структуре модели:**

1) слежение за тем, чтобы моделирование осуществлялось в соответствии с заданным (или определяемым по заданным условиям) числом шагов;

2) определение на каждом шаге тех сигналов и той информации, которые должны поступить на вход каждого элемента моделируемой системы;

3) определение на каждом шаге для каждого элемента моделируемой системы его реакции на входные сигналы и поступающую информацию в соответствии с правилами его функционирования;

4) формирование заранее определенных форм отчетов о выполненных работах с занесением в общий протокол работы моделируемой системы.

Таблица правильных ответов:

№ вопроса	№ ответа
1.	1
2.	3
3.	2
4.	2
5.	1, 3, 4

6.	1
7.	2
8.	4
9.	6,4,3,2,5,1,7
10.	1
11.	2
12.	2
13.	1
14.	4
15.	1
16.	1
17.	2
18.	1
19.	2
20.	4

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 с.— 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 с.— Режим доступа: http://www.iprbookshop.ru/15847.— ЭБС «IPRbooks», по паролю

7.3 Периодические издания

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