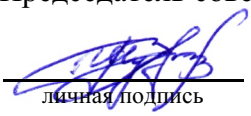
Автономная некоммерческая организация высшего образования "Московский информационно-технологический университет - Московский архитектурно-строительный институт"

Рассмотрено и одобрено на заседании учебно-методического совета

Протокол № 10/19 от 20.06.2019

Председатель совета



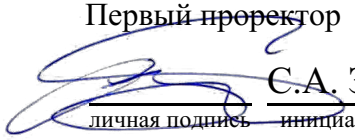
личная подпись

В.В. Шутенко

инициалы, фамилия

УТВЕРЖДАЮ

Первый проректор



личная подпись

С.А. Забелина

инициалы, фамилия

« 20 » июня 2019 г.

Кириллов Андрей Григорьевич

(уч. звание, степень, ФИО авторов программы)

Рабочая программа дисциплины (модуля)

Основы информационной безопасности в профессиональной деятельности

(наименование дисциплины (модуля))

Направление подготовки (специальность): 45.03.02 Лингвистика

(код, наименование без кавычек)

ОПОП: Теория и методика преподавания иностранных языков и культур

(наименование)

Форма освоения ОПОП: очная, очно-заочная

(очная, очно-заочная, заочная)

Общая трудоемкость: 2 (з.е.)

Всего учебных часов: 72 (ак. час.)

Формы промежуточной аттестации	СЕМЕСТР		
	очная	очно-заочная	заочная
Зачет	4	3	

Москва 2019 г.

Год начала подготовки студентов - 2019

1. Цель и задачи освоения дисциплины

Цель освоения дисциплины	Ознакомление студентов с тенденцией развития информационной безопасности, с моделями возможных угроз, терминологией и основными понятиями теории безопасности информации, а так же с нормативными документами РФ.
Задачи дисциплины	Приобретение студентами теоретических знаний и практических навыков защиты информации представленной в электронном виде, прежде всего средствами криптографии, типичными криптосистемами и другими методами, лежащими в ее основе. Получение студентами знаний по существующим угрозам безопасности информации, подбору и применению современных методов и способов защиты информации Формирование у студентов навыков защиты информации в локальных и глобальных компьютерных сетях.

2. Место дисциплины в структуре ОПОП

Дисциплины и практики, знания и умения по которым необходимы как "входные" при изучении данной дисциплины	Иностранный язык Информационные технологии в лингвистике
Дисциплины, практики, ГИА, для которых изучение данной дисциплины необходимо как предшествующее	Язык средств массовой информации

3. Требования к результатам освоения дисциплины

Компетенции обучающегося, формируемые в результате освоения дисциплины. Степень сформированности компетенций

Компетенции/ ЗУВ	Планируемые результаты обучения	Критерии оценивания	ФОС
ОПК11 владением навыками работы с компьютером как средством получения, обработки и управления информацией			
Знать	основные понятия сферы современных информационных технологий и их характеристики; классификацию и основные характеристики технических средств реализации ИТ; классификацию и основные характеристики программных средств реализации ИТ; возможности компьютера как средства получения, обработки и управления информацией	Студент должен знать: основные понятия сферы современных информационных технологий и их характеристики; классификацию и основные характеристики технических средств реализации ИТ; классификацию и основные характеристики программных средств реализации ИТ; возможности компьютера как средства получения, обработки и управления информацией	Тест

Уметь	грамотно оперировать основными понятиями сферы современных информационных технологий; применять техническое обеспечение информационных технологий в профессиональной деятельности; использовать программное обеспечение для решения профессиональных задач; выполнять основные операции по получению, обработке и управлению информации с использованием компьютера	Студент должен уметь: грамотно оперировать основными понятиями сферы современных информационных технологий; применять техническое обеспечение информационных технологий в профессиональной деятельности; использовать программное обеспечение для решения профессиональных задач; выполнять основные операции по получению, обработке и управлению информации с использованием компьютера	Выполнение реферата
Владеть	понятийным аппаратом сферы современных ИТ; навыками использования современных технических средств; технологией работы с современным программным обеспечением для решения профессиональных задач; приемами получения, обработки и управления информацией с помощью компьютера	Студент должен владеть: понятийным аппаратом сферы современных ИТ; навыками использования современных технических средств; технологией работы с современным программным обеспечением для решения профессиональных задач; приемами получения, обработки и управления информацией с помощью компьютера	Выполнение реферата
ОПК20 способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-лингвистических технологий и с учетом основных требований информационной безопасности			

Знать	основные понятия прикладной лингвистики; направления использования ИКТ в лингвистике и возможности информационно лингвистических технологий для решения профессиональных задач; основные понятия сферы информационной безопасности и основные методы защиты информации.	Студент должен знать: основные понятия прикладной лингвистики; направления использования ИКТ в лингвистике и возможности информационно лингвистических технологий для решения профессиональных задач; основные понятия сферы информационной безопасности и основные методы защиты информации.	Тест
Уметь	грамотно использовать основные понятия прикладной лингвистики; решать профессиональные задачи с применением информационнолингвистических технологий; выполнять основные мероприятия по защите информации при решении профессиональных задач;	Студент должен уметь: грамотно использовать основные понятия прикладной лингвистики; решать профессиональные задачи с применением информационнолингвистических технологий; выполнять основные мероприятия по защите информации при решении профессиональных задач;	Выполнение реферата
Владеть	понятийным аппаратом прикладной лингвистики; информационной культурой осуществления профессиональной деятельности с применением информационно-лингвистических технологий; основными методами осуществления информационной безопасности.	Студент должен владеть: понятийным аппаратом прикладной лингвистики; информационной культурой осуществления профессиональной деятельности с применением информационно-лингвистических технологий; основными методами осуществления информационной безопасности.	Презентация

4. Структура и содержание дисциплины

Тематический план дисциплины

№	Название темы	Содержание	Литера-тура	Формируемые компетенции
1.	Основные понятия и общеметодологические принципы теории информационной безопасности.	Источники понятий в области информационной безопасности. Основные понятия информационной безопасности : документированная информация, безопасность информации, конфиденциальность , целостность , доступность информации , защита информации , система защиты информации. Общеметодологические принципы теории информационной безопасности.	8.1.1, 8.1.2, 8.2.1, 8.2.2, 8.2.3	ОПК11 Знать ОПК11 Уметь ОПК11 Владеть ОПК20 Знать ОПК20 Уметь ОПК20 Владеть
2.	Понятия и виды защищаемой информации.	Понятие и сущность защищаемой информации. Права и обязанности обладателя информации. Виды защищаемой информации:государственная тайна , служебная тайна , профессиональная тайна ,коммерческая тайна , персональные данные. Перечень сведений конфиденциального характера. Понятие интеллектуальной собственности и особенности ее защиты.	8.1.1, 8.1.2, 8.2.1, 8.2.2, 8.2.3	ОПК11 Знать ОПК11 Уметь ОПК11 Владеть ОПК20 Знать ОПК20 Уметь ОПК20 Владеть
3.	Понятие и виды угроз информационной безопасности.	Понятие угрозы информационной безопасности. Фактор , воздействующей на защищаемую информацию. Типы дестабилизирующих факторов. Классификация и виды угроз информацинной безопасности. Внутренние и внешние источники источники угроз информационной безопасности. Угрозы утечки информации угрозы безопасности информации.	8.1.1, 8.1.2, 8.2.1, 8.2.2, 8.2.3	ОПК11 Знать ОПК11 Уметь ОПК11 Владеть ОПК20 Знать ОПК20 Уметь ОПК20 Владеть
4.	Информационная безопасность и информационное противоборство.	Субъекты информационного противоборства, Цели информационного противоборства. Составные части и методы информационного противоборства. Информационное оружие, его классификация и возможности.	8.1.1, 8.1.2, 8.2.1, 8.2.2, 8.2.3	ОПК11 Знать ОПК11 Уметь ОПК11 Владеть ОПК20 Знать ОПК20 Уметь ОПК20 Владеть
5.	Обеспечение информационной безопасности объектов информационной сферы государства в условиях информационной войны.	Методы нарушения конфиденциальности , целостности и доступности информации. Причины , виды ,каналы утечки и искажения информации. Основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны. Компьютерная система как объект информационной войны.	8.1.1, 8.1.2, 8.2.1, 8.2.2, 8.2.3	ОПК11 Знать ОПК11 Уметь ОПК11 Владеть ОПК20 Знать ОПК20 Уметь ОПК20 Владеть

6.	Методы и средства обеспечения информационной безопасности компьютерных систем.	Компьютерная система как объект информационной безопасности. Общая характеристика способов и средств защиты информации. Правовая , техническая , криптографические методы обеспечения информационной безопасности. Программно-аппаратные средства обеспечения информационной безопасности.	8.1.1, 8.1.2, 8.2.1, 8.2.2, 8.2.3	ОПК11 Знать ОПК11 Уметь ОПК11 Владеть ОПК20 Знать ОПК20 Уметь ОПК20 Владеть
7.	Механизмы защиты информации в автоматизированных системах.	Содержащие сервисов безопасности программно-технического уровня. Идентификация и аутентификация , управление доступом и авторизация , протоколирование и аудит. Криптография для сервисов безопасности: шифрование и контроль целостности. Экранирование. Анализ защищенности. Обеспечение доступности. Туннелирование. Управление.	8.1.1, 8.1.2, 8.2.1, 8.2.2, 8.2.3	ОПК11 Знать ОПК11 Уметь ОПК11 Владеть ОПК20 Знать ОПК20 Уметь ОПК20 Владеть
8.	Формальные модели безопасности автоматизированных систем.	Назначение формальных моделей безопасности. Политика безопасности. Монитор безопасности обращений. Дискреционная и мандатная модели безопасности. Формальные модели управления доступом. Модель Харрисона-Руззо-Ульмана. Модель Белла-Ла Падулы. Формальные модели целостности. Модель Кларка-Вилсона. Модель Биба. Совместное использование моделей безопасности. Ролевое управление доступом.	8.1.1, 8.1.2, 8.2.1, 8.2.2, 8.2.3	ОПК11 Знать ОПК11 Уметь ОПК11 Владеть ОПК20 Знать ОПК20 Уметь ОПК20 Владеть
9.	Методы и критерии оценки защищенности компьютерных систем.	Модели. Стратегии и системы обеспечения информационной безопасности. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем. Критерии безопасности компьютерных систем «Оранжевая книга». Общие критерии безопасности информационных технологий. (ФСТЭК) России. Стандарты по управлению информационной безопасностью ISOЛЕС 27000. Руководящие документы Гостехкомиссии.	8.1.1, 8.1.2, 8.2.1, 8.2.2, 8.2.3	ОПК11 Знать ОПК11 Уметь ОПК11 Владеть ОПК20 Знать ОПК20 Уметь ОПК20 Владеть

10.	Защита автоматизированных систем от технических разведок.	Угрозы БИ в АС. Меры противодействия угрозам БИ в АС. Основные принципы построения систем ЗИ в АС.	8.1.1, 8.1.2, 8.2.1, 8.2.2, 8.2.3	ОПК11 Знать ОПК11 Уметь ОПК11 Владеть ОПК20 Знать ОПК20 Уметь ОПК20 Владеть

Распределение бюджета времени по видам занятий с учетом формы обучения

Форма обучения: очная, 4 семестр

№	Контактная работа	Аудиторные учебные занятия			Самостоятельная работа
		занятия лекционного типа	лабораторные работы	практические занятия	
1.	2	1	0	1	3
2.	2	1	0	1	3
3.	2	1	0	1	3
4.	2	1	0	1	3
5.	3	1	0	2	4
6.	3	1	0	2	4
7.	4	2	0	2	4
8.	4	2	0	2	4
9.	4	2	0	2	4
10.	4	2	0	2	4
	Промежуточная аттестация				
	2	0	0	0	4
	Консультации				
	0	0	0	0	0
Итого	32	14	0	16	40

Форма обучения: очно-заочная, 3 семестр

№	Контактная работа	Аудиторные учебные занятия			Самостоятельная работа
		занятия лекционного типа	лабораторные работы	практические занятия	
1.	2	1	0	1	3
2.	2	1	0	1	3
3.	2	1	0	1	3
4.	2	1	0	1	3
5.	3	1	0	2	4
6.	3	1	0	2	4
7.	3	2	0	1	4
8.	3	2	0	1	6
9.	2	1	0	1	6
10.	2	1	0	1	6
	Промежуточная аттестация				
	2	0	0	0	4

	Консультации				
	0	0	0	0	0
Итого	26	12	0	12	46

5. Методические указания для обучающихся по освоению дисциплины

В процессе освоения дисциплины обучающемуся необходимо посетить все виды занятий, предусмотренные рабочей программой дисциплины и выполнить контрольные задания, предлагаемые преподавателем для успешного освоения дисциплины. Также следует изучить рабочую программу дисциплины, в которой определены цели и задачи дисциплины, компетенции обучающегося, формируемые в результате освоения дисциплины и планируемые результаты обучения. Рассмотреть содержание тем дисциплины; взаимосвязь тем лекций и практических занятий; бюджет времени по видам занятий; оценочные средства для текущей и промежуточной аттестации; критерии итоговой оценки результатов освоения дисциплины. Ознакомиться с методическими материалами, программно-информационным и материально техническим обеспечением дисциплины.

Работа на лекции

Лекционные занятия включают изложение, обсуждение и разъяснение основных направлений и вопросов изучаемой дисциплины, знание которых необходимо в ходе реализации всех остальных видов занятий и в самостоятельной работе обучающегося. На лекциях обучающиеся получают самые необходимые знания по изучаемой проблеме. Непременным условием для глубокого и прочного усвоения учебного материала является умение обучающихся сосредоточенно слушать лекции, активно, творчески воспринимать излагаемые сведения. Внимательное слушание лекций предполагает интенсивную умственную деятельность обучающегося. Краткие записи лекций, конспектирование их помогает усвоить материал. Конспект является полезным тогда, когда записано самое существенное, основное. Запись лекций рекомендуется вести по возможности собственными формулировками. Желательно запись осуществлять на одной странице, а следующую оставлять для проработки учебного материала самостоятельно в домашних условиях. Конспект лучше подразделять на пункты, параграфы, соблюдая красную строку. Принципиальные места, определения, формулы следует сопровождать замечаниями. Работая над конспектом лекций, всегда следует использовать не только основную литературу, но и ту литературу, которую дополнительно рекомендовал лектор.

Практические занятия

Подготовку к практическому занятию следует начинать с ознакомления с лекционным материалом, с изучения плана практических занятий. Определившись с проблемой, следует обратиться к рекомендуемой литературе. Владение понятийным аппаратом изучаемого курса является необходимым, поэтому готовясь к практическим занятиям, обучающемуся следует активно пользоваться справочной литературой: энциклопедиями, словарями и др. В ходе проведения практических занятий, материал, излагаемый на лекциях, закрепляется, расширяется и дополняется при подготовке сообщений, рефератов, выполнении тестовых работ. Степень освоения каждой темы определяется преподавателем в ходе обсуждения ответов обучающийсяов.

Самостоятельная работа

Обучающийся в процессе обучения должен не только освоить учебную программу, но и приобрести навыки самостоятельной работы. Самостоятельная работа обучающийсяов играет важную роль в воспитании сознательного отношения самих обучающийсяов к овладению теоретическими и практическими знаниями, привитии им привычки к направленному интеллектуальному труду. Самостоятельная работа проводится с целью углубления знаний по дисциплине. Материал, законспектированный на лекциях, необходимо регулярно дополнять сведениями из литературных источников, представленных в рабочей программе. Изучение литературы следует начинать с освоения соответствующих разделов дисциплины в учебниках, затем ознакомиться с монографиями или статьями по той тематике, которую изучает обучающийся, и после этого – с брошюрами и статьями, содержащими материал, дающий углубленное представление о тех или иных аспектах рассматриваемой проблемы. Для расширения знаний по дисциплине обучающемуся необходимо использовать Интернет-ресурсы и специализированные базы данных: проводить поиск в различных системах и использовать материалы сайтов, рекомендованных преподавателем на лекционных занятиях.

Подготовка к сессии

Основными ориентирами при подготовке к промежуточной аттестации по дисциплине являются конспект лекций и перечень рекомендуемой литературы. При подготовке к сессии обучающемуся следует так организовать учебную работу, чтобы перед первым днем начала сессии были сданы и защищены все практические работы. Основное в подготовке к сессии – это повторение всего материала курса, по которому необходимо пройти аттестацию. При подготовке к сессии следует весь объем работы распределять равномерно по дням, отведенным для подготовки, контролировать каждый день выполнения работы.

6. Фонды оценочных средств для текущего контроля успеваемости, промежуточной аттестации и самоконтроля по итогам освоения дисциплины

Технология оценивания компетенций фондами оценочных средств:

- формирование критериев оценивания компетенций;
- ознакомление обучающихся в ЭИОС с критериями оценивания конкретных типов оценочных средств;
- оценивание компетенций студентов с помощью оценочных средств программы практики - защита отчета по практике в форме собеседования;
- публикация результатов освоения ОПОП в личном кабинете в ЭИОС обучающегося;

Тест для формирования «Знать» компетенции ОПК11

Вопрос №1.

Кто является основным ответственным за определение уровня классификации информации?

Варианты ответов:

1. Руководитель среднего звена
2. Высшее руководство
3. Владелец
4. Пользователь

Вопрос №2.

Что самое главное должно продумать руководство при классификации данных :

Варианты ответов:

1. Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным
2. Необходимый уровень доступности, целостности и конфиденциальности
3. Оценить уровень риска и отменить контрмеры
4. Управление доступом, которое должно защищать данные

Вопрос №3.

Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены :

Варианты ответов:

1. Владельцы данных
2. Пользователи
3. Администраторы
4. Руководство

Вопрос №4.

Что такое процедура :

Варианты ответов:

1. Правила использования программного и аппаратного обеспечения в компании
2. Пошаговая инструкция по выполнению задачи
3. Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах
4. Обязательные действия

Вопрос №5.

Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков :

Варианты ответов:

1. Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски
2. Когда риски не могут быть приняты во внимание по политическим соображениям
3. Когда необходимые защитные меры слишком сложны
4. Когда стоимость контрмер превышает ценность актива и потенциальные потери

Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	от 0% до 30% правильных ответов из общего числа тестовых заданий
Удовлетворительно	от 31% до 50% правильных ответов из общего числа тестовых заданий
Хорошо	от 51% до 80% правильных ответов из общего числа тестовых заданий
Отлично	от 81% до 100% правильных ответов из общего числа тестовых заданий

Выполнение реферата для формирования «Уметь» компетенции ОПК11

1. Информация - фактор существования и развития общества. Основные формы проявления информации, её свойства как объекта безопасности.
2. Понятие безопасности и её составляющие. Безопасность информации.
3. Обеспечение информационной безопасности: содержание и структура понятия.
4. Национальные интересы в информационной сфере.
5. Источники и содержание угроз в информационной сфере.
6. Соотношение понятий «информационная безопасность» и «национальная безопасность»
7. Понятие национальной безопасности. Интересы и угрозы в области национальной безопасности.

Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	Обучающийся не раскрыл материал по теме задания или материал раскрыт поверхностно, излагаемый материал не систематизирован, выводы недостаточно аргументированы, обучающийся не высказывал своего мнения, не проявил способность к анализу, имеются смысловые и речевые ошибки в реферате
Удовлетворительно	Обучающийся демонстрирует логичность и доказательность изложения материала по теме задания, но допускает отдельные неточности при использовании ключевых понятий. Обучающийся не продемонстрировал способность к научному анализу, не высказывал в работе своего мнения, допустил ошибки в логическом обосновании своего ответа
Хорошо	Реферат написан грамотным научным языком, имеет чёткую структуру и логику изложения, точка зрения обучающегося обоснована, в работе присутствуют ссылки на научные источники, мнения известных учёных в данной области
Отлично	Реферат написан грамотным научным языком, имеет чёткую структуру и логику изложения, точка зрения обучающегося обоснована, при разработке реферата использовано не менее 5-8 научных источников. В работе выдвигаются новые идеи и трактовки, демонстрируется способность обучающегося анализировать материал, выражается его мнение по проблеме

Выполнение реферата для формирования «Владеть» компетенции ОПК11

1. Влияние процессов информатизации общества на составляющие национальной безопасности и их содержание.
2. Система обеспечения информационной безопасности. Обеспечение информационной безопасности Российской Федерации.
3. Понятие информационной войны. Проблемы информационной войны.
4. Информационное оружие и его классификация.
5. Цели информационной войны, её составные части и средства её ведения. Объекты воздействия в информационной войне.
6. Уровни ведения информационной войны. Информационные операции. Психологические операции. Оперативная маскировка. Радиоэлектронная борьба. Воздействие на сети.
7. Основные положения государственной информационной политики Российской Федерации. Первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности.
8. Виды защищаемой информации в сфере государственного и муниципального управления.
9. Обеспечение информационной безопасности организации.

Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	Обучающийся не раскрыл материал по теме задания или материал раскрыт поверхностно, излагаемый материал не систематизирован, выводы недостаточно аргументированы, обучающийся не высказывал своего мнения, не проявил способность к анализу, имеются смысловые и речевые ошибки в реферате
Удовлетворительно	Обучающийся демонстрирует логичность и доказательность изложения материала по теме задания, но допускает отдельные неточности при использовании ключевых понятий. Обучающийся не продемонстрировал способность к научному анализу, не высказывал в работе своего мнения, допустил ошибки в логическом обосновании своего ответа
Хорошо	Реферат написан грамотным научным языком, имеет чёткую структуру и логику изложения, точка зрения обучающегося обоснована, в работе присутствуют ссылки на научные источники, мнения известных учёных в данной области
Отлично	Реферат написан грамотным научным языком, имеет чёткую структуру и логику изложения, точка зрения обучающегося обоснована, при разработке реферата использовано не менее 5-8 научных источников. В работе выдвигаются новые идеи и трактовки, демонстрируется способность обучающегося анализировать материал, выражается его мнение по проблеме

Тест для формирования «Знать» компетенции ОПК20

Вопрос №1.
Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:

Варианты ответов:

1. Внедрение управления механизмами безопасности
2. Классификацию данных после внедрения механизмов безопасности
3. Уровень доверия, обеспечиваемый механизмом безопасности
4. Соотношение затрат / выгод

Вопрос №2.
Если используются автоматизированные инструменты для анализа рисков, почему все равно требуется

так много времени для проведения анализа:

Варианты ответов:

1. Много информации нужно собрать и ввести в программу
2. Руководство должно одобрить создание группы
3. Анализ рисков не может быть автоматизирован, что связано с самой природой оценки
4. Множество людей должно одобрить данные

Вопрос №3.
Что является наилучшим описанием количественного анализа рисков:

Варианты ответов:

1. Анализ, основанный на сценариях, предназначенный для выявления различных угроз безопасности
2. Метод, используемый для точной оценки потенциальных потерь, вероятности потерь и рисков
3. Метод, сопоставляющий денежное значение с каждым компонентом оценки рисков
4. Метод, основанный на суждениях и интуиции

Вопрос №4.
Как рассчитать остаточный риск:

Варианты ответов:

1. Угрозы х Риски х Ценность актива
2. (Угрозы х Ценность актива х Уязвимости) х Риски
3. SLE х Частоту = ALE
4. (Угрозы х Уязвимости х Ценность актива) х Недостаток контроля

Вопрос №5.
Что такое CobiT и как он относится к разработке систем информационной безопасности и программ безопасности:

Варианты ответов:

1. Список стандартов, процедур и политик для разработки программы безопасности
2. Текущая версия ISO 17799
3. Структура, которая была разработана для снижения внутреннего мошенничества в компаниях
4. Открытый стандарт, определяющий цели контроля

Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	от 0% до 30% правильных ответов из общего числа тестовых заданий
Удовлетворительно	от 31% до 50% правильных ответов из общего числа тестовых заданий
Хорошо	от 51% до 80% правильных ответов из общего числа тестовых заданий
Отлично	от 81% до 100% правильных ответов из общего числа тестовых заданий

Выполнение реферата для формирования «Уметь» компетенции ОПК20

1. Управление и защита информации в информационно-телекоммуникационных сетях.
2. Характеристика эффективных стандартов по безопасности. Требования к полноте эффективных стандартов по безопасности.
3. Риск работы на персональном компьютере. Планирование безопасной работы на персональном компьютере.
4. Стандарты предприятия по использованию персональных компьютеров. Практические меры

безопасности для персональных компьютеров.

Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	Обучающийся не раскрыл материал по теме задания или материал раскрыт поверхностно, излагаемый материал не систематизирован, выводы недостаточно аргументированы, обучающийся не высказывал своего мнения, не проявил способность к анализу, имеются смысловые и речевые ошибки в реферате
Удовлетворительно	Обучающийся демонстрирует логичность и доказательность изложения материала по теме задания, но допускает отдельные неточности при использовании ключевых понятий. Обучающийся не продемонстрировал способность к научному анализу, не высказывал в работе своего мнения, допустил ошибки в логическом обосновании своего ответа
Хорошо	Реферат написан грамотным научным языком, имеет чёткую структуру и логику изложения, точка зрения обучающегося обоснована, в работе присутствуют ссылки на научные источники, мнения известных учёных в данной области
Отлично	Реферат написан грамотным научным языком, имеет чёткую структуру и логику изложения, точка зрения обучающегося обоснована, при разработке реферата использовано не менее 5-8 научных источников. В работе выдвигаются новые идеи и трактовки, демонстрируется способность обучающегося анализировать материал, выражается его мнение по проблеме

Презентация для формирования «Владеть» компетенции ОПК20

Информационная безопасность – состояние защищенности

Меры по обеспечению информационной безопасности

Правовые основы информационной безопасности

Правовые основы информационной безопасности Федеральный закон 149-ФЗ Об информации

Правовые основы информационной безопасности Федеральный закон 152-ФЗ «О персональных данных»

Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	В презентации не раскрыто содержание представляемой темы; имеются фактические (содержательные), орфографические и стилистические ошибки. Не представлен перечень источников. Цветовые, шрифтовые решения, расположение текстов и схем не соответствуют требованиям реализации принципа наглядности в обучении
Удовлетворительно	Презентация включает менее 8 слайдов основной части. В презентации не полностью раскрыто содержание представляемой темы, нечетко определена структура презентации, имеются содержательные, орфографические и стилистические ошибки (более трех), представлен перечень источников. Цветовые, шрифтовые решения, расположение текстов и схем соответствуют требованиям реализации принципа наглядности в обучении

Хорошо	Презентация включает менее 12 слайдов основной части. В презентации не полностью раскрыто содержание представляемой темы, четко определена структура презентации, имеются незначительные содержательные, орфографические и стилистические ошибки (не более трех), представлен перечень источников. Цветовые, шрифтовые решения, расположение текстов и схем в полной мере соответствуют требованиям реализации принципа наглядности в обучении
Отлично	Презентация включает не менее 12 слайдов основной части. В презентации полностью и глубоко раскрыто содержание представляемой темы, четко определена структура презентации, отсутствуют фактические (содержательные), орфографические и стилистические ошибки, представлен перечень источников. Цветовые, шрифтовые решения, расположение текстов и схем соответствуют требованиям реализации принципа наглядности в обучении

Вопросы для проведения промежуточной аттестации по итогам освоения дисциплины

Тема 1. Основные понятия и общеметодологические принципы теории информационной безопасности.

1. Контроль качества информации.
2. Управление информационными ресурсами.
3. Классификационная политика в области информации.
4. Организация и ответственность в области управления информацией.

Тема 2. Понятия и виды защищаемой информации.

5. особенности правовой информации.
6. критерии классификации правовой информации.
7. доступность информации.
8. конфиденциальность информации.

Тема 3. Понятие и виды угроз информационной безопасности.

9. ошибки пользователей и сисадминов
10. сбои в работе компьютерного оборудования
11. нарушение сотрудниками компании регламентов по работе с информацией

Тема 4. Информационная безопасность и информационное противоборство.

12. Субъекты информационного противоборства,
13. Цели информационного противоборства.
14. Составные части и методы информационного противоборства.
15. Информационное оружие, его классификация и возможности.

Тема 5. Обеспечение информационной безопасности объектов информационной сферы государства в условиях информационной войны.

16. Методы нарушения конфиденциальности , целостности и доступности информации.
17. Причины , виды ,каналы утечки и искажения информации.
18. Основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны.
19. Компьютерная система как объект информационной войны.

Тема 6. Методы и средства обеспечения информационной безопасности компьютерных систем.

20. Компьютерная система как объект информационной безопасности.
21. Общая характеристика способов и средств защиты информации.
22. Правовая , техническая , криптографические методы обеспечения информационной безопасности.
23. Программно-аппаратные средства обеспечения информационной безопасности.

Тема 7. Механизмы защиты информации в автоматизированных системах.

24. Содержащие сервисов безопасности программно-технического уровня.

25. Идентификация и аутентификация , управление доступом и авторизация , протоколирование и аудит.
26. Криптография для сервисов безопасности: шифрование и контроль целостности.
27. Экранирование.
28. Анализ защищенности.
29. Обеспечение доступности.
30. Туннелирование.
31. Управление.

Тема 8. Формальные модели безопасности автоматизированных систем.

32. Назначение формальных моделей безопасности.
33. Политика безопасности.
34. Монитор безопасности обращений.
35. Дискреционная и мандатная модели безопасности.
36. Формальные модели управления доступом.
37. Модель Харрисона-Руззо-Ульмана.
38. Модель Белла-Ла Падулы.
39. Формальные модели целостности.
40. Модель Кларка-Вилсона.
41. Модель Биба.
42. Совместное использование моделей безопасности. Ролевое управление доступом.

Тема 9. Методы и критерии оценки защищенности компьютерных систем.

43. Модели.
44. Стратегии и системы обеспечения информационной безопасности.
45. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем.
46. Критерии безопасности компьютерных систем «Оранжевая книга».
47. Общие критерии безопасности информационных технологий.
48. (ФСТЭК) России.
49. Стандарты по управлению информационной безопасностью ISOЛЕС 27000.
50. Руководящие документы Гостехкомиссии.

Тема 10. Защита автоматизированных систем от технических разведок.

51. Классификация в возможности технических разведок, Компьютерная разведка.
52. Технические каналы утечки информации при эксплуатации автоматизированных систем. Электромагнитное воздействие и эффекты его воздействия.
53. Защита автоматизированных систем и средств вычислительной техники от внезапного электромагнитного импульса

Уровни и критерии итоговой оценки результатов освоения дисциплины

	Критерии оценивания	Итоговая оценка
Уровень1. Недостаточный	Незнание значительной части программного материала, неумение даже с помощью преподавателя сформулировать правильные ответы на задаваемые вопросы, невыполнение практических заданий	Неудовлетворительно/Незачтено
Уровень 2. Базовый	Знание только основного материала, допустимы неточности в ответе на вопросы, нарушение логической последовательности в изложении программного материала, затруднения при решении практических задач	Удовлетворительно/зачтено

Уровень 3. Повышенный	Твердые знания программного материала, допустимые несущественные неточности при ответе на вопросы, нарушение логической последовательности в изложении программного материала, затруднения при решении практических задач	Хорошо/зачтено
Уровень 4. Продвинутый	Глубокое освоение программного материала, логически стройное его изложение, умение связать теорию с возможностью ее применения на практике, свободное решение задач и обоснование принятого решения	Отлично/зачтено

7. Ресурсное обеспечение дисциплины

Лицензионное программно-информационное обеспечение	1. Microsoft Windows 2. Microsoft Office 3. Google Chrome 4. Kaspersky Endpoint Security 5. AnyLogic 6. ArgoUML 7. ARIS EXPRESS 8. Erwin 9. Inkscape 10. iTALC 11. Maxima 12. Microsoft SQL Server Management Studio 13. Microsoft Visio 14. Microsoft Visual Studio 15. MPLAB 16. Notepad++ 17. Oracle VM VirtualBox 18. Paint .NET 19. SciLab 20. WinAsm 21. Консультант+ 22. GNS 3 23. Спутник 24. «Антиплагиат.ВУЗ»
Современные профессиональные базы данных	1. Консультант+ 2. http://www.garant.ru (ресурсы открытого доступа)
Информационные справочные системы	1. https://elibrary.ru - Научная электронная библиотека eLIBRARY.RU (ресурсы открытого доступа) 2. https://www.rsl.ru - Российская Государственная Библиотека (ресурсы открытого доступа) 3. https://link.springer.com - Международная реферативная база данных научных изданий Springerlink (ресурсы открытого доступа) 4. https://zbmath.org - Международная реферативная база данных научных изданий zbMATH (ресурсы открытого доступа)

Интернет-ресурсы	1. http://window.edu.ru - Информационная система "Единое окно доступа к образовательным ресурсам" 2. https://openedu.ru - «Национальная платформа открытого образования» (ресурсы открытого доступа)
Материально-техническое обеспечение	Учебные аудитории для проведения: занятий лекционного типа, обеспеченные наборами демонстрационного оборудования и учебно-наглядных пособий, обеспечивающих тематические иллюстрации, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, помещения для самостоятельной работы, оснащенные компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду организации, помещения для хранения и профилактического обслуживания учебного оборудования. Лаборатории и кабинеты: 1. Лаборатория информатики Компьютерный класс, включая оборудование: Комплекты учебной мебели, демонстрационное оборудование – проектор и компьютер, учебно-наглядные пособия, обеспечивающие тематические иллюстрации, доска, персональные компьютеры.

8. Учебно-методические материалы

№	Автор	Название	Издательство	Год издания	Вид издания	Кол-во в библио-теке	Адрес электронного ресурса	Вид доступа
1	2	3	4	5	6	7	8	9
8.1 Основная литература								
8.1.1	Галатенко В.А.	Основы информационной безопасности	Интернет-Университет Информационных Технологий (ИНТУИТ)	2016	учебное пособие	-	http://www.iprbookshop.ru/52209.html	по логину и паролю
8.1.2	Фаронов А.Е.	Основы информационной безопасности при работе на компьютере	Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа	2020	учебное пособие	-	http://www.iprbookshop.ru/89453.html	по логину и паролю
8.2 Дополнительная литература								
8.2.1	Рогозин В.Ю. Галушкин И.Б. Новиков В.К. Вепрев С.Б.	Основы информационной безопасности	ЮНИТИ-ДАНА	2017	учебник	-	http://www.iprbookshop.ru/72444.html	по логину и паролю
8.2.2	Сычев Ю.Н.	Основы информационной безопасности	Евразийский открытый институт	2010	учебное пособие	-	http://www.iprbookshop.ru/10746.html	по логину и паролю
8.2.3	Голиков А.М.	Основы информационной безопасности	Томский государственный университет систем управления и радиоэлектроники	2007	учебное пособие	-	http://www.iprbookshop.ru/13957.html	по логину и паролю

9. Особенности организации образовательной деятельности для лиц с ограниченными возможностями здоровья

В МИТУ - МАСИ созданы специальные условия для получения высшего образования по образовательным программам обучающимися с ограниченными возможностями здоровья (ОВЗ).

Для перемещения инвалидов и лиц с ограниченными возможностями здоровья в МИТУ - МАСИ созданы специальные условия для беспрепятственного доступа в учебные помещения и другие

помещения, а также их пребывания в указанных помещениях с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

При получении образования обучающимся с ограниченными возможностями здоровья при необходимости предоставляются бесплатно специальные учебники и учебные пособия, иная учебная литература. Также имеется возможность предоставления услуг ассистента, оказывающего обучающимся с ограниченными возможностями здоровья необходимую техническую помощь, в том числе услуг сурдопереводчиков и тифлосурдопереводчиков.

Получение доступного и качественного высшего образования лицами с ограниченными возможностями здоровья обеспечено путем создания в университете комплекса необходимых условий обучения для данной категории обучающихся. Информация о специальных условиях, созданных для обучающихся с ограниченными возможностями здоровья, размещена на сайте университета (https://mitu-masi.ru/sveden/objects/).

Для обучения инвалидов и лиц с ОВЗ, имеющих нарушения опорно-двигательного аппарата обеспечиваются и совершенствуются материально-технические условия беспрепятственного доступа в учебные помещения, столовую, туалетные, другие помещения, условия их пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных проемов и др.).

Для адаптации к восприятию обучающимися инвалидами и лицами с ОВЗ с нарушенным слухом справочного, учебного материала, предусмотренного образовательной программой по выбранным направлениям подготовки, обеспечиваются следующие условия:

- звуковая справочная информация о расписании учебных занятий дублируется визуальной информацией на сайте, на доске объявлений;
- для лучшей ориентации в аудитории, применяются сигналы, оповещающие о начале и конце занятия (слово «звонок» пишется на доске);
- внимание слабослышащего обучающегося привлекается педагогом жестом (на плечо кладется рука, осуществляется нерезкое похлопывание);
- разговаривая с обучающимся, педагог смотрит на него, говорит ясно, короткими предложениями, обеспечивая возможность чтения по губам.

Компенсация затруднений речевого и интеллектуального развития слабослышащих инвалидов и лиц с ОВЗ проводится за счет:

- использования схем, диаграмм, рисунков, компьютерных презентаций с гиперссылками, комментирующими отдельные компоненты изображения;
- регулярного применения упражнений на графическое выделение существенных признаков предметов и явлений;
- обеспечения возможности для обучающегося получить адресную консультацию по электронной почте по мере необходимости.

Для адаптации к восприятию инвалидами и лицами с ОВЗ с нарушениями зрения справочного, учебного, просветительского материала, предусмотренного образовательной программой МИТУ - МАСИ по выбранной специальности, обеспечиваются следующие условия:

- ведется адаптация официального сайта в сети Интернет с учетом особых потребностей инвалидов по зрению, обеспечивается наличие крупношрифтовой справочной информации о расписании учебных занятий;
- в начале учебного года обучающихся несколько раз проводят по зданию МИТУ - МАСИ для запоминания месторасположения кабинетов, помещений, которыми они будут пользоваться;
- педагог, его собеседники, присутствующие представляются обучающимся, каждый раз называется тот, к кому педагог обращается;
- действия, жесты, перемещения педагога коротко и ясно комментируются;
- печатная информация предоставляется крупным шрифтом (от 18 пунктов), тотально озвучивается;
- обеспечивается необходимый уровень освещенности помещений;
- предоставляется возможность использовать компьютеры во время занятий и право записи объяснения на диктофон (по желанию обучающегося).

Форма проведения текущей и промежуточной аттестации для обучающихся с ОВЗ определяется

преподавателем в соответствии с учебным планом. При необходимости обучающемуся с ОВЗ с учетом его индивидуальных психофизических особенностей дается возможность пройти промежуточную аттестацию устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п., либо предоставляется дополнительное время для подготовки ответа.

Обучающиеся с ОВЗ могут обучаться по индивидуальному учебному плану в установленные сроки с учетом особенностей и образовательных потребностей конкретного обучающегося. Индивидуальный график обучения предусматривает различные варианты проведения занятий в университете как в академической группе, так и индивидуально.