

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

УТВЕРЖДАЮ

Зам. директора по УР

Н.А. Андреева

«20» 04 2026 г.

Рабочая программа дисциплины

**Б1.О.32 Основы управления информационной
безопасностью**

Кафедра Информационная безопасность
Направление подготовки 10.03.01 «Информационная безопасность»
Профиль Безопасность компьютерных систем (по отрасли
или в сфере профессиональной деятельности)

Формы обучения очная

Распределение часов дисциплины по семестрам (для очной формы обучения (ОФО))

Вид учебной работы	ОФО	
	ЗЕ	часов/сем.
Общая трудоемкость дисциплины, в том числе (по семестрам, курсам):	4	144/5
Контактная работа, в том числе (по семестрам, курсам):		70/5
Лекции		34/5
Лабораторных работ		18/5
Практических занятий		18/5
Семинаров		
Самостоятельная работа		38/5
Контроль		36/5
Число контрольных работ (по курсам)		
Число КР (по семестрам, курсам)		
Число КП (по семестрам, курсам)		
Число зачетов с разбивкой по семестрам		
Число экзаменов с разбивкой по семестрам		1/5

Программу составил:
Доцент кафедры ИБ, к.пол.н. Жуковский Д.А.

Рабочая программа дисциплины
«Основы управления информационной безопасностью»

Разработана в соответствии с ФГОС ВО
направление подготовки **10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**,
утвержденное приказом Министерства науки и высшего образования Российской
Федерации от 17 ноября 2020 г. № 1427.

Составлена на основании учебного плана
направления **10.03.01 Информационная безопасность, профиля «Безопасность
компьютерных систем (по отрасли или в сфере профессиональной деятельности)»**,
одобренного Учёным советом СКФ МТУСИ, протокол № 8 от 31.03 2026 г.,
и утвержденного директором СКФ МТУСИ 31.03 2026 г.

Рассмотрена и одобрена на заседании кафедры
Информационная безопасность

Протокол от «28» 04 2026г. № 9

И.О.Зав. кафедрой  Жуковский А.Г.

1. Цели изучения дисциплины

Целью преподавания дисциплины «Основы управления информационной безопасностью» является изучение структуры, логической организации, системы управления службой защиты информации как основного звена системы защиты информации.

2. Планируемые результаты обучения

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

Результатом освоения дисциплины являются сформированные у обучающегося следующие компетенции:

ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства
Знать:
- основные понятия информатики и информационных, компьютерных и сетевых технологий, форматы применения информационных, компьютерных и сетевых технологий в современном обществе; - социальную значимость своей будущей профессии, основы профессиональной деятельности в области обеспечения информационной безопасности.
Уметь:
- осуществлять поиск, хранение и обработку информации из различных источников и баз данных, используя возможности вычислительной техники; - применять основы профессиональной деятельности в области обеспечения информационной безопасности.
Владеть:
- навыками анализа и представления обработанной информации в требуемом формате с использованием информационных, компьютерных и сетевых технологий; - навыками применения основ обеспечения информационной безопасности и защиты интересов личности, общества и государства, норм профессиональной этики.
ОПК-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты
Знать:
- угрозы информационной безопасности, меры защиты и противодействия; принципы разработки политики безопасности; - основные мероприятия по созданию и обеспечению функционирования комплексной системы защиты, требования и рекомендации по защите информации и требования по технической защите информации; - принципы управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации.
Уметь:
- строить концептуальные модели информационной безопасности объекта защиты; разрабатывать политики безопасности с учетом угроз безопасности информации и требований по защите информации; - использовать нормативно-правовую базу в решении задач обеспечения информационной безопасности и комплексной защиты информации на предприятии и в организации; - разрабатывать организационные и технические мероприятия управления доступом и информационными потоками в компьютерных системах с учетом особенностей конкретного предприятия.

Владеть:
- навыками выявления угроз информационной безопасности на объекте защиты; - навыками разработки, правильного оформления, презентации и внедрения разрабатываемых политик безопасности; - навыками работы с нормативно-правовыми и организационно-распорядительными документами в сфере информационной безопасности, вопросами технологии подбора сотрудников и работы с кадрами с точки зрения обеспечения информационной безопасности, основами организации внутриобъектового режима; - навыками проведения организационных и технических мероприятий по управлению доступом и информационными потоками в компьютерных системах.

3. Место дисциплины в структуре образовательной программы

Требования к предварительной подготовке обучающегося (предшествующие дисциплины, модули, темы):	
1	Б1.О.05 «Введение в информационные технологии»
2	Б1.О.27 «Основы информационной безопасности»
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:	
1	Б1.В.02 «Комплексное обеспечение защиты информации объекта информатизации»

4. Структура и содержание дисциплины

4.1 Очная форма обучения, 4 года (всего 144 часа, 70 часов контактной работы)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компетенции	УМИО
1	2	3	4	5	6
Курс 3, Семестр 5					
Модуль 1. Создание службы безопасности организации – 34 (16+10+8=34) часа					
1.1	ВВОДНАЯ. ОСНОВЫ БЕЗОПАСНОСТИ 1. Биологическая и психофизиологическая сущность поведения человека 2. Безопасность человека и организации как биосоциальной подсистемы современного общества 3. Социальные и социально-психологические факторы поведения человека в обеспечении безопасности 3. Психофункциональная надежность человека в обеспечении безопасности 4. Человеческий фактор в обеспечении безопасности	Лек..	4	ОПК-1	Л1.1 Л1.2 Л1.3
1.2	УГРОЗЫ, ОПАСНОСТИ, РИСКИ, КРИЗИСЫ И КОНФЛИКТЫ В ЖИЗНЕДЕЯТЕЛЬНОСТИ ЛИЧНОСТИ И ОРГАНИЗАЦИИ 1. Общие положения 2. Особенности обеспечения безопасности в	Лек.	4	ОПК-1	Л1.1 Л1.2 Л1.3

	организациях различных форм собственности и видов деятельности 3. Сущность и содержание системы комплексной безопасности 4. Обеспечение безопасности — ответственность и функция предпринимателей, руководителей менеджеров				
1.3	МЕНЕДЖМЕНТ В ОСНОВНЫХ ВИДАХ БЕЗОПАСНОСТИ 1. Менеджмент информационной безопасности 2. Менеджмент экономической безопасности 3. Производственный менеджмент и безопасность 4. Менеджмент экологической безопасности 5. Менеджмент коммерческой безопасности	Лек.	2	ОПК-1	Л1.1 Л1.2 Л1.3
1.4	МЕНЕДЖМЕНТ В ДЕЯТЕЛЬНОСТИ СЛУЖБЫ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ (СБО) 1. Служба безопасности как подсистема организации: структура, ответственность, полномочия и функции 2. Создание службы безопасности организации	Лек.	2	ОПК-1	Л1.1 Л1.2 Л1.3
1.5	СОЗДАНИЕ СЛУЖБЫ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ (продолжение лекции 4)	Лек.	2	ОПК-1	Л1.1 Л1.2 Л1.3
1.6	ПРАВОВОЙ СТАТУС СЛУЖБЫ БЕЗОПАСНОСТИ	Лек.	2	ОПК-1	Л1.1 Л1.2 Л1.3
1.7	МЕСТО И РОЛЬ СЛУЖБЫ ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМЕ ЗАЩИТЫ ИНФОРМАЦИИ Назначение службы защиты информации. Место службы защиты информации в системе безопасности предприятия. Служба защиты информации как составная часть системы защиты. Служба защиты информации как орган управления защитой информации. Служба защиты информации как координатор деятельности по обеспечению безопасности информации. Статус службы защиты информации в структуре предприятия.	ПЗ	4	ОПК-1	Л1.1 Л1.2 Л1.3 Л2.1 Л3.1
1.8	ЗАДАЧИ И ФУНКЦИИ СЛУЖБЫ ЗАЩИТЫ ИНФОРМАЦИИ Организационные задачи и функции службы защиты информации. Технологические задачи и функции службы защиты информации. Координационные задачи и функции службы защиты информации. Взаимосвязь и соотношение организационных, технологических и координационных задач и функций. Факторы, влияющие на определение задач и функций службы защиты информации.	ПЗ	4	ОПК-1	Л1.1 Л1.2 Л1.3 Л2.1 Л3.1
1.9	СТРУКТУРА И ШТАТЫ СЛУЖБЫ ЗАЩИТЫ ИНФОРМАЦИИ	ПЗ	2	ОПК-1	Л1.1 Л1.2

	Общая структурная схема службы защиты информации. Подразделения службы защиты информации. Факторы, определяющие конкретную структуру службы защиты информации. Виды и типы организационных структур службы защиты информации. Централизованная и децентрализованная структуры службы защиты информации, условия, критерии, определяющие выбор структур. Должностной состав сотрудников службы защиты информации, его зависимость от характера выполняемых работ.				Л1.3 Л2.1 Л3.1
1.10	СТРУКТУРА И ШТАТЫ СЛУЖБЫ ЗАЩИТЫ ИНФОРМАЦИИ (продолжение) Задачи, функции, права и ответственность заместителя (помощника) руководителя предприятия по безопасности в области защиты информации. Задачи, функции, права и ответственность руководителя службы защиты информации, его заместителей, руководителей подразделений службы защиты. Функции сотрудников и уполномоченных службы защиты информации. Факторы, определяющие численность сотрудников службы защиты информации.	ЛР	2	ОПК-1	Л1.1 Л1.2 Л1.3 Л2.1 Л3.1
1.11	ОРГАНИЗАЦИОННЫЕ ОСНОВЫ И ПРИНЦИПЫ ДЕЯТЕЛЬНОСТИ СЛУЖБЫ ЗАЩИТЫ ИНФОРМАЦИИ Порядок создания службы защиты информации. Структура и содержание положения о службе защиты информации. Состав и содержание других нормативных документов, регламентирующих деятельность службы защиты информации.	ЛР	2	ОПК-1	Л1.1 Л1.2 Л1.3 Л2.1 Л3.1
1.12	ОРГАНИЗАЦИОННЫЕ ОСНОВЫ И ПРИНЦИПЫ ДЕЯТЕЛЬНОСТИ СЛУЖБЫ ЗАЩИТЫ ИНФОРМАЦИИ (продолжение) Основные принципы организации и деятельности службы защиты информации. Условия и факторы, влияющие на организацию работы службы защиты информации. Организация взаимодействия службы защиты информации и подразделений предприятия и соподчиненных внешних служб защиты информации.	ЛР	4	ОПК-1	Л1.1 Л1.2 Л1.3 Л2.1 Л3.1
1.10	Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27 июля 2006 №149-ФЗ. Федеральный закон "О связи" от 07.07.2003 №126-ФЗ. Федеральный закон "О безопасности" от 28.12.2010 №390-ФЗ Федеральный закон "Об электронной подписи" от 06.04.2011 №63-ФЗ.	СРС	19	ОПК-1	Л1.1 Л1.2 Л1.3

	Федеральный закон "О персональных данных" от 27.07.2006 №152-ФЗ. Закон РФ "О государственной тайне" от 21.07.1993 №5485-1. Федеральный закон "О коммерческой тайне" от 29.07.2004 №98-ФЗ. Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 №187-ФЗ. Федеральный закон "О федеральной службе безопасности" от 03.04.1995 №40-ФЗ				
Модуль 2. Управление службой безопасности организации. 3(18+8+10) 36 часов					
2.1	УПРАВЛЕНИЕ СЛУЖБОЙ БЕЗОПАСНОСТИ. 1. Функция организации охраны объектов и проведения режимных мероприятий 2. Функция организации оперативно-разведывательной деятельности специальных подразделений СБО	Лек.	4	ОПК-10	Л1.1 Л1.2 Л1.3
2.2	УПРАВЛЕНИЕ СЛУЖБОЙ БЕЗОПАСНОСТИ. (продолжение лекции 7)	Лек.	2	ОПК-10	Л1.1 Л1.2 Л1.3
2.3	ПРИНЦИПЫ И МЕТОДЫ РАБОТЫ МЕНЕДЖЕРА СЛУЖБЫ БЕЗОПАСНОСТИ 1. Примерный ежедневный план работы менеджера безопасности 2. Кодекс и методы оперативной работы менеджера безопасности предпринимательства 3. Правила применяемые менеджером, как специалистом по безопасности: 4. Источники информации и методы получения их менеджером СБ	Лек.	4	ОПК-10	Л1.1 Л1.2 Л1.3
2.4	ОСОБЕННОСТИ МЕНЕДЖМЕНТА И РОЛЕВОГО ПОВЕДЕНИЯ СПЕЦИАЛИСТОВ СБ В РАБОТЕ С КЛИЕНТАМИ, ПАРТНЕРАМИ, КОНКУРЕНТАМИ, ПРЕДСТАВИТЕЛЯМИ ОРГАНОВ ВЛАСТИ	Лек.	4	ОПК-10	Л1.1 Л1.2 Л1.3
2.5	МЕНЕДЖМЕНТ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ВНЕШНЕЭКОНОМИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ ПРЕДПРИЯТИЯ 1. Информационно-аналитическая деятельность СБО во внешнеэкономической сфере 2. Противодействие промышленной и технической разведке	Лек.	2	ОПК-10	Л1.1 Л1.2 Л1.3
2.6	РАБОТА МЕНЕДЖЕРА БЕЗОПАСНОСТИ В ОТДЕЛЬНЫХ ВИДАХ ДЕЯТЕЛЬНОСТИ СБО	Лек.	2	ОПК-10	Л1.1 Л1.2 Л1.3
2.4	ПОДБОР, РАССТАНОВКА И ОБУЧЕНИЕ СОТРУДНИКОВ СЛУЖБЫ ЗАЩИТЫ ИНФОРМАЦИИ Общие и специфические требования, предъявляемые к сотрудникам службы защиты информации. Особенности подбора кадров.	ПЗ	4	ОПК-10	ЛЗ.1

	Методы получения информации о кандидатурах на должности. Социально-психологические факторы, влияющие на расстановку кадров. Формы создания и способы поддержания необходимого микроклимата в коллективе. Формы повышения квалификации сотрудников. Подготовка кадрового резерва.				
2.5	ОРГАНИЗАЦИЯ ТРУДА СОТРУДНИКОВ Особенности содержания характера труда сотрудников службы защиты информации. Распределение обязанностей между сотрудниками службы защиты информации. Обеспечение персональной ответственности за сохранность носителей информации. Структура и содержание должностных инструкций сотрудников службы защиты информации.	ПЗ	2	ОПК-10	Л1.1 Л1.2 Л1.3 Л2.1 Л3.1
2.6	ОРГАНИЗАЦИЯ ТРУДА СОТРУДНИКОВ (продолжение) Организация рабочих мест сотрудников службы защиты информации (рациональное размещение, оснащение оборудованием, техническими средствами). Обеспечение необходимых условий труда. Охрана труда. Культура труда. Карты организации трудового процесса.	ПЗ	2	ОПК-10	Л1.1 Л1.2 Л1.3 Л2.1 Л3.1
2.7	ПРИНЦИПЫ И МЕТОДЫ УПРАВЛЕНИЯ СЛУЖБОЙ ЗАЩИТЫ ИНФОРМАЦИИ Принципы управления службой защиты информации. Понятие и сущность методов управления. Система методов управления. Административно-правовые методы управления. Экономические методы управления. Социально-психологические методы управления. Взаимосвязь методов управления. Необходимость комплексного и системного применения методов управления службой защиты информации.	ЛР	4	ОПК-10	Л1.1 Л1.2 Л1.3 Л2.1 Л3.1
2.8	ТЕХНОЛОГИЯ УПРАВЛЕНИЯ СЛУЖБОЙ ЗАЩИТЫ ИНФОРМАЦИИ Состав и содержание управленческих функций. Технология управления службой защиты информации. Значение управленческих решений. Цели планирования. Виды планирования, их назначение. Содержание и структура планов. Технология планирования.	ЛР	4	ОПК-10	Л1.1 Л1.2 Л1.3 Л2.1 Л3.1
2.9	ТЕХНОЛОГИЯ УПРАВЛЕНИЯ СЛУЖБОЙ ЗАЩИТЫ ИНФОРМАЦИИ (продолжение) Методы и формы контроля выполнения планов. Критерии эффективности работы службы защиты информации. Методы оценки качества работы службы защиты информации. Пути и способы повышения эффективности управления службой защиты информации.	ЛР	2	ОПК-10	Л1.1 Л1.2 Л1.3 Л2.1 Л3.1
2.10	Закон РФ "О частной детективной и охранной	СРС	19	ОПК-	Л1.1

	деятельности в Российской Федерации" от 11.03.1992 №2487-1 Федеральный закон "О лицензировании отдельных видов деятельности" от 04.05.2011 №99-ФЗ. Федеральный закон "Об экспортном контроле" от 18.07.1999 г. №183-ФЗ . Федеральный закон "О техническом регулировании" от 27.12.2002 №184-ФЗ. Трудовой кодекс Российской Федерации от 30.12.2001 №197-ФЗ. Гражданский кодекс Российской Федерации часть 4 (ГК РФ ч.4) 18.12.2006 №230-ФЗ. "Кодекс Российской Федерации об административных правонарушениях" от 30.12.2001 №195-ФЗ. "Уголовный кодекс Российской Федерации" от 13.06.1996 №63-ФЗ.			10	Л1.2 Л1.3
	Экзамен		36	ОПК-1; ОПК-10	Л1.1 Л1.2 Л1.3 Л2.1 Л3.1
Итого – 144 часа					

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Рекомендуемая литература				
5.1.1. Основная литература				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л1.1	А. К. Моденов	Основы экономической безопасности : учебное пособие	Санкт-Петербург : Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ, 2017. — 220 с.	Э1
Л1.2	А.Е. Мрачковский, Е.А. Кипервар, А.И. Чумаков.	Социальные аспекты экономической безопасности : учебное пособие	Омск : Омский государственный технический университет, 2021. — 138 с.	Э2
Л1.3	Овчинникова Е.А.	Овчинникова Е.А. Основы управления информационной безопасностью : учебное пособие	Новосибирск : Сибирский государственный университет телекоммуникаций и информатики, 2023. — 167 с.	Э3
5.1.2. Дополнительная литература				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.

Л2.1	К. А. Антипов, Е. М. Березина, А. А. Волочков [и др.] ; под редакцией З. П. Замаевой.	Социальная безопасность и защита человека в современном российском социуме : монография	Пермь : Пермский государственный национальный исследовательский университет, 2018. — 240 с.	Э4
5.1.3. Учебно-методическое обеспечение				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л3.1	Зырянова Т.Ю.	Зырянова Т.Ю. Управление информационной безопасностью : учебное пособие	Екатеринбург : Уральский государственный университет путей сообщения, 2023. — 96 с.	Э5
5.2. Электронные образовательные ресурсы				
Э1	https://www.iprbookshop.ru/80753.html			
Э2	https://www.iprbookshop.ru/124883.html			
Э3	https://www.iprbookshop.ru/138782.html			
Э4	https://www.iprbookshop.ru/117590.html			
Э5	https://www.iprbookshop.ru/149731.html			
5.3 Информационно-справочные системы и профессиональные базы данных				
5.3.1	Консультант Плюс – https://www.consultant.ru/			
5.3.2	Гарант – https://www.garant.ru/			
5.3.2	Консорциум Кодекс – https://docs.cntd.ru/			
5.3.3	Научная электронная библиотека – https://www.elibrary.ru/			
5.3.4	Профессиональная база данных: Федеральный портал «Российское образование»: [Электронный ресурс] – Режим доступа: http://www.edu.ru/ (открытый доступ)			
5.3.5	Профессиональная база данных: Федеральный центр информационно-образовательных ресурсов: [Электронный ресурс] – Режим доступа: http://fcior.edu.ru/ (открытый доступ)			
5.3.6	Национальный открытый университет «ИНТУИТ» - https://intuit.ru/			
5.3.7	Электронный ресурс http://www.securitylab.ru/			
5.4. Программное обеспечение				
СКФ МТУСИ обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства:				
П.1	MS Word, Power Point			
П.2	Kaspersky Endpoint Security			
П.3	Операционная система Linux			

6. Материально-техническое обеспечение дисциплины

6.1 МТО лекционных занятий	
1	Лекционная аудитория, оснащенная интерактивной доской, проектором, ПК (ноутбуком), экраном.
6.2 МТО лабораторных работ и практических занятий	
1	Учебные аудитории, оборудованные компьютерной техникой, с возможностью подключения к сети «Интернет», и обеспечением доступа в электронную информационно-образовательную среду СКФ МТУСИ
2	Лаборатория «Программно-аппаратные средства защиты информации», укомплектованная специализированной мебелью, оснащенную программно-аппаратными комплексами защиты информации, включающими в том числе средства криптографической защиты информации,
6.3 МТО рубежных контролей, зачетов, экзаменов	

1	Учебные аудитории, оборудованные компьютерной техникой с возможностью выхода в локальную сеть Филиала и Интернет.
6.4 МТО самостоятельной работы обучающихся	
1	Помещение для самостоятельной работы обучающихся оснащено компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду СКФ МТУСИ

7. Оценочные материалы	
Оценочные материалы и перечень видов оценочных средств текущего контроля и промежуточной аттестации представлены в Приложении 1 к рабочей программе дисциплины.	

8. Методические рекомендации для обучающихся по освоению дисциплины	
Методические рекомендации по освоению дисциплины представлены в Приложении 2 к рабочей программе дисциплины.	

9. Особенности реализации дисциплины (модуля) при обучении инвалидов и лиц с ограниченными возможностями здоровья

Рабочая программа дисциплины (модуля) при необходимости может быть адаптирована для обучения (в том числе с применением дистанционных образовательных технологий) лиц с ограниченными возможностями здоровья, инвалидов. Для этого требуется заявление обучающихся, являющихся лицами с ограниченными возможностями здоровья, инвалидами, или их законных представителей и рекомендации психолого-медико-педагогической комиссии. При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с нарушением слуха возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков.

Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания.

Доклад (реферат) также может быть представлен в письменной форме, при этом требования к содержанию остаются теми же, а требования к качеству изложения материала (понятность, качество речи, взаимодействие с аудиторией и т. д.) заменяются на соответствующие требования, предъявляемые к письменным работам (качество оформления текста и списка литературы, грамотность, наличие иллюстрационных материалов и т.д.).

Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т.д.). Допускается присутствие на занятиях ассистента (помощника), оказывающего обучающимся необходимую техническую помощь.

Текущий контроль успеваемости осуществляется в устной форме.

При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочитать задание, оформить ответ, общаться с преподавателем).

10. Дополнения и изменения в Рабочей программе

Лист актуализации рабочей программы дисциплины «Б1.О.32 Основы управления информационной безопасностью» для использования в 20__/20__ учебном году

Утверждаю

Зам. директора по УР _____
«__» _____ 20__ г.

Направление: 10.03.01 Информационная безопасность

Профиль: Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)

Форма обучения: очная

(Возможны следующие варианты):

а) Рабочая программа действует без изменений.

б) В рабочую программу вносятся следующие изменения:

- 1)
- 2)
- 3)

Разработчик (и): _____
(ФИО, ученая степень, ученое звание)

«__» _____ 20__ г.

Рабочая программа пересмотрена и одобрена на заседании кафедры ИБ

Протокол № _____ от «__» _____ 20__ г.

Заведующий кафедрой _____

Оценочные материалы для проведения текущего контроля и промежуточной аттестации по дисциплине

1. Оценочные материалы для проведения промежуточной аттестации по дисциплине

1.1 Шкала оценивания компетенций

Шкала оценивания компетенций		
Оценка	Уровень освоения компетенции	Критерии оценивания
«Отлично»	Высокий уровень	Обучающийся показывает всестороннее, систематическое и глубокое знание основного и дополнительного учебного материала, умеет свободно выполнять задания, предусмотренные программой; усвоил основную и знаком с дополнительной рекомендованной литературой; может объяснить взаимосвязь основных понятий дисциплины в их значении для последующей профессиональной деятельности; проявляет творческие способности в понимании, изложении и использовании учебного материала.
«Хорошо»	Повышенный уровень	Обучающийся показывает достаточный уровень знаний в пределах основного учебного материала, без существенных ошибок выполняет предусмотренные в программе задания; усвоил основную литературу, рекомендованную в программе; способен объяснить взаимосвязь основных понятий дисциплины при дополнительных вопросах преподавателя. Допускает не существенные погрешности в ответах, устраняет их без помощи преподавателя.
«Удовлетворительно»	Пороговый уровень	Обучающийся показывает знания основного учебного материала в минимальном объеме, необходимом для дальнейшей учебы; справляется с выполнением заданий, предусмотренных программой, допуская при этом большое количество не принципиальных ошибок; знаком с основной литературой, рекомендованной программой. Допускает существенные погрешности в ответах, но обладает необходимыми знаниями для их устранения под руководством

		преподавателя.
«Неудовлетворительно»	Минимальный уровень не достигнут	Обучающийся обнаруживает пробелы в знаниях основного учебного материала, допускает принципиальные ошибки в выполнении предусмотренных программой заданий, не знаком с рекомендованной литературой, не может исправить допущенные ошибки. Как правило, оценка «неудовлетворительно» ставится обучающимся, которые не могут продолжить обучение или приступить к профессиональной деятельности по окончании вуза без дополнительных занятий по соответствующей дисциплине.

1.2 Показатели, критерии и шкалы оценивания компетенций

Показатели компетенции	Критерии оценивания	Шкала оценивания
ОПК-1: Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства		
Знать:		
основные понятия информатики и информационных, компьютерных и сетевых технологий, форматы применения информационных, компьютерных и сетевых технологий в современном обществе;	Контрольная работа	Модуль 1 0÷5 «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3 «Хорошо» - 4 «Отлично» - 5
социальную значимость своей будущей профессии, основы профессиональной деятельности в области обеспечения информационной безопасности	Контрольная работа	Модуль 2 0÷5 «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3 «Хорошо» - 4 «Отлично» - 5
Уметь:		
осуществлять поиск, хранение и обработку информации из различных источников и баз данных, используя возможности вычислительной техники	Практические занятия 1-6	Модуль 1 0÷10 «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3-5 «Хорошо» - 6-8 «Отлично» - 9-10
применять основы профессиональной деятельности в области обеспечения информационной безопасности	Практические занятия 1-6	Модуль 2 0÷10 «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3-5 «Хорошо» - 6-8 «Отлично» - 9-10
Владеть:		

навыками анализа и представления обработанной информации в требуемом формате с использованием информационных, компьютерных и сетевых технологий	Лабораторная работа 1-6	Модуль 1 0÷10 «Неудовлетворительно» - 0-3 «Удовлетворительно» - 4-6 «Хорошо» - 7-8 «Отлично» - 9-10
навыками применения основ обеспечения информационной безопасности и защиты интересов личности, общества и государства, норм профессиональной этики	Лабораторная работа 1-6	Модуль 2 0÷10 «Неудовлетворительно» - 0-3 «Удовлетворительно» - 4-6 «Хорошо» - 7-8 «Отлично» - 9-10
ОПК-10: Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты		
Знать:		
угрозы информационной безопасности, меры защиты и противодействия; принципы разработки политики безопасности; основные мероприятия по созданию и обеспечению функционирования комплексной системы защиты, требования и рекомендации по защите информации и требования по технической защите информации;	Контрольная работа	Модуль 1 0÷5 «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3 «Хорошо» - 4 «Отлично» - 5
принципы управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации	Контрольная работа	Модуль 2 0÷5 «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3 «Хорошо» - 4 «Отлично» - 5
Уметь:		
строить концептуальные модели информационной безопасности объекта защиты; разрабатывать политики безопасности с учетом угроз безопасности информации и требований по защите информации;	Практические занятия 4-6	Модуль 1 0÷10 «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3-5 «Хорошо» - 6-8 «Отлично» - 9-10
использовать нормативно-правовую базу в решении задач обеспечения информационной безопасности и комплексной защиты информации на предприятии и в организации; разрабатывать организационные и технические мероприятия управления доступом и информационными потоками в компьютерных системах с учетом особенностей конкретного предприятия.	Практические занятия 4-6	Модуль 2 0÷10 «Неудовлетворительно» - 0-3 «Удовлетворительно» - 4-6 «Хорошо» - 7-8 «Отлично» - 9-10

Владеть:		
навыками выявления угроз информационной безопасности на объекте защиты; навыками разработки, правильного оформления, презентации и внедрения разрабатываемых политик безопасности; навыками работы с нормативно-правовыми и организационно-распорядительными документами в сфере информационной безопасности, вопросами технологии подбора сотрудников и работы с кадрами с точки зрения обеспечения информационной безопасности, основами организации внутриобъектового режима;	Лабораторная работа 4-6	Модуль 1 0÷10 «Неудовлетворительно» - 0-3 «Удовлетворительно» - 4-6 «Хорошо» - 7-8 «Отлично» - 9-10
навыками проведения организационных и технических мероприятий по управлению доступом и информационными потоками в компьютерных системах	Лабораторная работа 4-6	Модуль 2 0÷10 «Неудовлетворительно» - 0-3 «Удовлетворительно» - 4-6 «Хорошо» - 7-8 «Отлично» - 9-10
	Экзамен	0-100 «Неудовлетворительно» - 0-40 «Удовлетворительно» - 41-60 «Хорошо» - 61-80 «Отлично» - 81-100

1.3 Оценочные материалы: типовые контрольные задания, иные материалы

1.3.1 Оценочные материалы текущего контроля для очной формы обучения

Данная дисциплина формирует у обучающегося 2 компетенции, которые связаны, взаимодействуют между собой и объективно оценить каждую в отдельности при ответе обучающегося на контрольный вопрос или при выполнении практического или лабораторного задания достаточно сложно. Предлагается считать, что вклад 2-х компетенций в общую оценку при ответе на вопрос примерно одинаков.

Модуль 1 (50 баллов):

Модуль содержит 6 лекционных, 3 практических занятий и 3 лабораторных работ. Знание лекционного материала оценивается по контрольной работе, состоящей из двух вопросов, максимальное количество баллов за контрольную работу составляет 10. За практические занятия обучающийся получает максимум 40 баллов. Общее максимальное количество баллов за модуль 1 составляет 50.

Вопросы для контрольной работы (ОПК-1):

1. Биологическая и психофизиологическая сущность поведения человека.
2. Безопасность человека и организации как биосоциальной подсистемы современного общества.
3. Социальные и социально-психологические факторы поведения человека в обеспечении безопасности.
4. Психофункциональная надежность человека в обеспечении безопасности.
5. Человеческий фактор в обеспечении безопасности.
6. Особенности обеспечения безопасности в организациях различных форм собственности и видов деятельности.
7. Сущность и содержание системы комплексной безопасности.
8. Обеспечение безопасности — ответственность и функция предпринимателей, руководителей менеджеров.
9. Менеджмент информационной безопасности.
10. Менеджмент экономической безопасности.
11. Производственный менеджмент и безопасность.
12. Менеджмент экологической безопасности.
13. Менеджмент коммерческой безопасности.
14. Служба безопасности как подсистема организации: структура, ответственность, полномочия и функции
15. Создание службы безопасности организации.
16. Правовой статус службы безопасности.

Практическое занятие 1. МЕСТО И РОЛЬ СЛУЖБЫ ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМЕ ЗАЩИТЫ ИНФОРМАЦИИ (ОПК-1):

1. Назначение службы защиты информации.
2. Место службы защиты информации в системе безопасности предприятия.
3. Служба защиты информации как составная часть системы защиты.
4. Служба защиты информации как орган управления защитой информации.
5. Служба защиты информации как координатор деятельности по обеспечению безопасности информации.
6. Статус службы защиты информации в структуре предприятия.

Практическое занятие 2. ЗАДАЧИ И ФУНКЦИИ СЛУЖБЫ ЗАЩИТЫ ИНФОРМАЦИИ (ОПК-1):

1. Организационные задачи и функции службы защиты информации.
2. Технологические задачи и функции службы защиты информации.
3. Координационные задачи и функции службы защиты информации.
4. Взаимосвязь и соотношение организационных, технологических и координационных задач и функций.
5. Факторы, влияющие на определение задач и функций службы защиты информации.

Практическое занятие 3. СТРУКТУРА И ШТАТЫ СЛУЖБЫ ЗАЩИТЫ ИНФОРМАЦИИ (ОПК-1):

1. Общая структурная схема службы защиты информации.
2. Подразделения службы защиты информации.
3. Факторы, определяющие конкретную структуру службы защиты информации.
4. Виды и типы организационных структур службы защиты информации.
5. Централизованная и децентрализованная структуры службы защиты информации, условия, критерии, определяющие выбор структур.
6. Должностной состав сотрудников службы защиты информации, его зависимость от характера выполняемых работ.

Лабораторная работа 1. СТРУКТУРА И ШТАТЫ СЛУЖБЫ ЗАЩИТЫ ИНФОРМАЦИИ (Лабораторная работа) (ОПК-1):

1. Задачи, функции, права и ответственность заместителя (помощника) руководителя предприятия по безопасности в области защиты информации.
2. Задачи, функции, права и ответственность руководителя службы защиты информации, его заместителей, руководителей подразделений службы защиты.
3. Функции сотрудников и уполномоченных службы защиты информации.
4. Факторы, определяющие численность сотрудников службы защиты информации.

Лабораторная работа 2. ОРГАНИЗАЦИОННЫЕ ОСНОВЫ И ПРИНЦИПЫ ДЕЯТЕЛЬНОСТИ СЛУЖБЫ ЗАЩИТЫ ИНФОРМАЦИИ (ОПК-1):

1. Порядок создания службы защиты информации.
2. Структура и содержание положения о службе защиты информации.
3. Состав и содержание других нормативных документов, регламентирующих деятельность службы защиты информации.

Лабораторная работа 3. ОРГАНИЗАЦИОННЫЕ ОСНОВЫ И ПРИНЦИПЫ ДЕЯТЕЛЬНОСТИ СЛУЖБЫ ЗАЩИТЫ ИНФОРМАЦИИ (продолжение) (ОПК-1):

1. Основные принципы организации и деятельности службы защиты информации.
2. Условия и факторы, влияющие на организацию работы службы защиты информации.
3. Организация взаимодействия службы защиты информации и подразделений предприятия и соподчиненных внешних служб защиты информации.

Модуль 2: (50 баллов):

Модуль содержит 6 лекционных, 3 практических занятий и 3 лабораторных работ. Знание лекционного материала оценивается по контрольной работе, состоящей из двух вопросов, максимальное количество баллов за контрольную работу составляет 10. За практические занятия обучающийся получает максимум 40 баллов. Общее максимальное количество баллов за модуль 1 составляет 50.

Вопросы для контрольной работы (ОПК-10):

1. Функция организации охраны объектов и проведения режимных мероприятий.
2. Функция организации оперативно-разведывательной деятельности специальных подразделений СБО.
3. Примерный ежедневный план работы менеджера безопасности.
4. Кодекс и методы оперативной работы менеджера безопасности предпринимательства.
5. Правила применяемые менеджером, как специалистом по безопасности.
6. Источники информации и методы получения их менеджером СБ.
7. Особенности менеджмента и ролевого поведения специалистов СБ в работе с клиентами, партнерами, конкурентами, представителями органов власти.
8. Информационно-аналитическая деятельность СБО во внешнеэкономической сфере.
9. Противодействие промышленной и технической разведке.
10. Работа менеджера безопасности в отдельных видах деятельности СБО.

Практическое занятие 4. ПОДБОР, РАССТАНОВКА И ОБУЧЕНИЕ СОТРУДНИКОВ СЛУЖБЫ ЗАЩИТЫ ИНФОРМАЦИИ (ОПК-10):

1. Общие и специфические требования, предъявляемые к сотрудникам службы защиты информации.
2. Особенности подбора кадров.

3. Методы получения информации о кандидатурах на должности.
4. Социально-психологические факторы, влияющие на расстановку кадров.
5. Формы создания и способы поддержания необходимого микроклимата в коллективе.
6. Формы повышения квалификации сотрудников.
7. Подготовка кадрового резерва.

Практическое занятие 5. ОРГАНИЗАЦИЯ ТРУДА СОТРУДНИКОВ (ОПК-10):

1. Особенности содержания характера труда сотрудников службы защиты информации.
2. Распределение обязанностей между сотрудниками службы защиты информации.
3. Обеспечение персональной ответственности за сохранность носителей информации.
4. Структура и содержание должностных инструкций сотрудников службы защиты информации.

Практическое занятие 6. ОРГАНИЗАЦИЯ ТРУДА СОТРУДНИКОВ (продолжение) (ОПК-10):

1. Организация рабочих мест сотрудников службы защиты информации (рациональное размещение, оснащение оборудованием, техническими средствами).
2. Обеспечение необходимых условий труда.
3. Охрана труда.
4. Культура труда.
5. Карты организации трудового процесса.

Лабораторная работа 4. ПРИНЦИПЫ И МЕТОДЫ УПРАВЛЕНИЯ СЛУЖБОЙ ЗАЩИТЫ ИНФОРМАЦИИ (ОПК-10):

1. Принципы управления службой защиты информации.
2. Понятие и сущность методов управления.
3. Система методов управления.
4. Административно-правовые методы управления.
5. Экономические методы управления.
6. Социально-психологические методы управления.
7. Взаимосвязь методов управления.
8. Необходимость комплексного и системного применения методов управления службой защиты информации.

Лабораторная работа 5. ТЕХНОЛОГИЯ УПРАВЛЕНИЯ СЛУЖБОЙ ЗАЩИТЫ ИНФОРМАЦИИ (ОПК-10):

1. Состав и содержание управленческих функций.
2. Технология управления службой защиты информации.
3. Значение управленческих решений.
4. Цели планирования.
5. Виды планирования, их назначение.
6. Содержание и структура планов.
7. Технология планирования.

Лабораторная работа 6. ТЕХНОЛОГИЯ УПРАВЛЕНИЯ СЛУЖБОЙ ЗАЩИТЫ ИНФОРМАЦИИ (продолжение) (ОПК-10):

1. Методы и формы контроля выполнения планов.
2. Критерии эффективности работы службы защиты информации.

3. Методы оценки качества работы службы защиты информации.
4. Пути и способы повышения эффективности управления службой защиты информации.

1.3.2 Вопросы, выносимые на экзамен по дисциплине «Основы управления информационной безопасностью» (ОПК-1, ОПК-10) (промежуточная аттестация)

1. Биологическая и психофизиологическая сущность поведения человека
2. Безопасность человека и организации как биосоциальной подсистемы современного общества
3. Государственная безопасность во всех сферах жизнедеятельности общества
4. Социальные и социально-психологические факторы поведения человека в обеспечении безопасности
5. Психофункциональная надежность человека в обеспечении безопасности
6. Безопасность предприятия
7. Формы недобросовестной конкуренции
8. Уровни организации системы безопасности предприятия
9. Особенности обеспечения безопасности в организациях различных форм собственности и видов деятельности
10. Угрозы безопасности фирмы
11. Субъекты внутренней и внешней угрозы безопасности
12. Способы промышленного шпионажа
13. Сущность и содержание системы комплексной безопасности
14. Организация и функционирование системы безопасности должны осуществляться на основе следующих принципов
15. Цели и задачи системы комплексной безопасности
16. Меры по обеспечению безопасности предпринимательской деятельности
17. Факторы разработки системы комплексной безопасности
18. Критерии эффективности функционирования системы комплексной безопасности.
19. Аудит системы комплексной безопасности
20. Функции руководителя фирмы (руководителя СБО) по обеспечению безопасности
21. Задачи менеджмента по защите экономических интересов:
22. Концепция экономической безопасности предприятия. Цель и задачи обеспечения экономической безопасности предприятия
23. Последовательность формирования и введения в строй системы экономической безопасности (СЭБ)
24. Процесс управления рисками. Идентификация и способы контроля рисков,
25. Производственный менеджмент и безопасность
26. Несчастные случаи, связанные с производством
27. Действия при возникновении несчастного случая на производстве
28. Концепции экологической безопасности
29. Менеджмент коммерческой безопасности
30. Сущность и содержание организации как самоуправляемой системы,
31. Внутренняя и внешняя среда фирмы
32. Этапы создания самоуправляемой организации
33. Структура, численность и состав СБО
34. Совет безопасности предприятия и его задачи
35. Основные задачи СБ предприятия
36. Руководящие документы по деятельности СБ
37. Основные функции и задачи отделения режима и охраны
38. Основными функциями и задачи оперативного отделения

39. Основные функции отделения маркетинговой разведки
40. Основные функции информационно-аналитического отделения
41. Права и обязанности сотрудников СБ
42. Создание службы безопасности организации
43. Уровни развитости и возможностей СБО
44. Менеджмент-проект и его структура
45. Закон РФ «О частной детективной и охранной деятельности в Российской Федерации».
46. Внутренние нормативные акты, регулирующие деятельность всех подразделений и сотрудников службы безопасности.
47. Обеспечение деятельности службы безопасности материально-техническими ресурсами
48. Порядок создания и ликвидации службы безопасности.
49. Разделы типового Устава службы безопасности
50. Варианты организации СБ на предприятии.
51. Требования к охранникам и их обязанности
52. Режимные и общепрофилактические меры в охранной деятельности
53. Оперативная и оперативно-розыскная и оперативно-разведывательная деятельность
54. Основные направления оперативно-разведывательной деятельности в СБО
55. Принципы, цели, задачи и методы оперативно-разведывательной деятельности
56. Вопросы, интересующие разведку СБО в исследуемом «объекте»
57. Особенности проведения оперативно-разведывательных операций в средних и малых фирмах и организациях
58. Цели и направления управленческого и оперативного взаимодействия с правоохранительными и местными органами власти
59. Основания для возбуждения и прекращения уголовного дела
60. Примерный ежедневный план работы менеджера безопасности
61. Кодекс работы менеджера безопасности предпринимательства
62. Методы работы и правила применяемые менеджером, как специалистом по безопасности
63. Источники информации и методы получения их менеджером СБ при обеспечении безопасности
64. Образ потребителя, клиента и конкурента
65. Показатели производственной или экономической состоятельности клиентов и партнеров
66. Задачи и принцип действия информационно-аналитического подразделения
67. Источники получения и обработка информации службой безопасности
68. Действия СБ при чрезвычайных происшествиях, бедствиях и несчастных случаях и в экстремальных ситуациях
69. Планы действий в кризисных ситуациях состав антикризисного комитета.
70. Профилактика противоправных акций со стороны конкурентов и организованной преступности
71. Проведение конфиденциальных расследований
72. Цель и функции штабного подразделения СБ.
73. Состав и обязанности сотрудников штабного подразделения СБ.
74. Личная безопасность и ее аспекты.
75. Основные принципы, методы и способы обеспечения безопасности охраняемого лица
76. Деятельность телохранителей в обеспечении безопасности должностных лиц
77. Безопасность личности в особых обстоятельствах. Группы факторов экстремальности в деятельности телохранителя.

78. Виды особых обстоятельств и экстремальных ситуаций
79. Основные проблемы в деятельности служб безопасности и способы их решения
80. Проектирование системы обеспечения безопасности объекта. Построение профиля защиты
81. Функциональные обязанности Главного специалиста по защите информации
82. Совет безопасности фирмы. Задачи. Состав, Права и обязанности.
83. Перечень документации по пожарной безопасности.
84. Структура инструкции по организации охраны предприятия.
85. Функциональные обязанности должностных лиц суточного наряда
86. Обязанности старшего смены суточного наряда
87. Обязанности руководителя подразделения личной охраны
88. Обязанности оперативного дежурного на предприятии
89. Обязанности Руководителя службы охраны предприятия
90. Права и обязанности инспектора по работе с персоналом, допущенным к материалам с грифом «КТ».
91. Права и обязанности инспектора по режиму
92. Обязанности Администратора локальной сети.
93. Пути и способы повышения эффективности управления службой защиты информации
94. Обеспечение необходимых условий труда. Охрана труда.
95. Критерии эффективности работы службы защиты информации.

2. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Порядок и методика проведения текущего контроля и промежуточной аттестации.

Предусмотрены следующие виды контроля:

- текущий контроль по каждому модулю – в форме написания контрольной работы для оценки теоретических знаний;
- текущий контроль по каждому модулю – в форме отчетов по лабораторным работам и практическим занятиям для оценки практических навыков;
- промежуточная аттестация по дисциплине – в форме экзамена.

Текущий контроль успеваемости в форме защиты лабораторных и практических проводится в два этапа:

- 1-й этап: допуск к выполнению лабораторной работы – проводится в форме письменной «летучки» (5-10 мин) с целью контроля знаний обучающихся теоретической части лабораторной работы и готовности к выполнению практических исследований;
- 2-й этап выполняется по окончании каждой лабораторной работы (практического занятия) в форме индивидуального собеседования по выполненным исследованиям или расчетам. Проводится с целью контроля закрепления теоретической части материала и степени отработки обучающимся практических навыков исследования на аппаратуре.

Контрольные работы выполняются в виде короткого письменного ответа на один вопрос, изученный на предыдущей лекции в начале каждой последующей лекции. Ответ на вопрос дается в течение 5-10 минут. Таким образом, после лекционного курса каждого модуля формируется общая оценка за теоретические знания.

С целью повышения качества обучения за счет побуждения обучающихся к активной текущей учебной работе, четкого и оперативного контроля всего хода учебного процесса,

снижения роли случайных и субъективных факторов при оценивании учебной деятельности обучающихся в образовательном процессе реализована модульно-рейтинговая система.

Правила ее использования прописаны в «Положении об МРС».

Набранные обучающимися в рамках текущего контроля баллы могут быть переведены в оценку:

- «неудовлетворительно» - от 0 до 40 от максимального количества баллов;
- «удовлетворительно» - от 41 до 60 максимального количества баллов;
- «хорошо» - от 61 до 80 максимального количества баллов;
- «отлично» - от 81 до 100 максимального количества баллов.

Соотношения максимального количества баллов, полученных обучающимися по блокам модулей, показаны в Таблице 1.

Таблица 1 - Распределение баллов по модулям дисциплины «Основы управления информационной безопасностью»

Модуль	Всего баллов (Максимальное значение)	Теоретический блок (Контрольная работа)	Практический блок
Модуль 1	50	10	40
Модуль 2	50	10	40
Модуль - Экзамен	41-100		

Теоретический блок оценивается по результатам контрольной работы. Практический блок оценивается по результатам выполнения лабораторных работ и заданий на практических занятиях.

На экзамене производится оценка тех компетенций, которые должны быть в той или иной форме освоены в процессе изучения. Рекомендуются формировать вопросы в билетах таким образом, чтобы преподаватель смог оценить все компетенции данной дисциплины.

3. Промежуточная аттестация

Промежуточная аттестация проводится в форме экзамена. Экзамен проводится по расписанию промежуточной аттестации в устном виде по экзаменационным билетам. Результаты аттестации заносятся в ведомость и зачетную книжку обучающегося.

Образец экзаменационного билета

	МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»	Утверждаю И.о.зав. кафедрой «ИБ» _____ А.Г. Жуковский «___» _____ 20__ г.
	Направление подготовки: 11.03.01 Информационная безопасность Курсы: 3 Дисциплина: Основы управления информационной безопасности	
Билет №1 1. Субъекты внутренней и внешней угрозы безопасности. 2. Структура, численность и состав СБО. Доцент кафедры «ИБ» к.пол.н. _____ Жуковский Д.А. «___» _____ 20__ г.		

Один комплект отпечатанных экзаменационных билетов, подписанных преподавателем кафедры и утвержденных заведующим кафедрой хранится у заведующего кафедрой, другой комплект – у преподавателя, ведущего дисциплину

4 Тестовые задания по дисциплине «Основы управления информационной безопасности»

Тестовые задания позволяют оценить уровень сформированности 2-х компетенций ОПК-1 и ОПК-10.

Задания распределены по блокам в соответствии с уровнем сложности. Каждый блок содержит номер задания, и текст задания.

Базовый уровень содержит примерно 50 % заданий.

Он формируется из заданий с выбором одного или нескольких верных ответов из предложенных или воспроизведения фактического материала (терминология, факты, классификация, параметры и др.);

Повышенный уровень в среднем составляет 35 % заданий.

В нем используются задания на сопоставление, сравнение, установление последовательности;

Высокий уровень в среднем составляют – 15 % заданий.

В задании используются: решения нетиповых задач, алгоритмы, доказательства, задания с развернутым ответом – определения, перечисление, изображение схемы, структуры и др.

Количество заданий по каждой компетенции равно 20. Всего 40 заданий.

Один комплект тестовых вопросов с указанием правильных ответов хранится у заведующего кафедрой, другой комплект – у преподавателя, ведущего дисциплину.

ОПК-1

Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства

БЛОК А (базовый уровень) – Задание с выбором одного или нескольких верных ответов из предложенных

Инструкция по тестам Блока А: Прочитайте текст и выберите один или несколько правильных ответов

№ задания	Тексты заданий
1	Организационная структура службы информационной безопасности определяется: 1) требованиями законодательства 2) требованиями государственных и международных стандартов 3) потребностями в защите информационных ресурсах и возможностями в соответствии с оценками руководителей предприятия
2	Передача функций по обеспечению информационной безопасности на аутсорсинг обуславливается: 1) требованиями законодательства 2) экономической целесообразностью 3) имиджевыми соображениями
3	4. "Информационная безопасность" - это: 1) множество факторов, влияющих на состояние информационных ресурсов 2) уровень защищенности информационных ресурсов 3) совокупность методов управления информационными рисками
4	Государственные органы разрабатывают и совершенствуют законодательное регулирование в сфере информационной безопасности с целью: 1) поддержки отечественных производителей средств защиты информации 2) обеспечения защиты государственных информационных ресурсов 3) увеличения объема информации, циркулирующей в информационных сетях 4) защиты интересов правообладателей
5	Аудит информационной безопасности подразделяется на: 1) текущий и итоговый

№ задания	Тексты заданий
	2) внешний и внутренний 3) объективный и субъективный
6	Лицензированием деятельности по разработке средств защиты информации в РФ занимается: 1) ФСО 2) СВР 3) ФСТЭК 4) МВД
7	Долгосрочное развитие политики информационной безопасности предприятия предполагает: 1) статичность 2) пропорциональность 3) цикличность
8	Основным противодействием методам "социальной инженерии" является: 1) повышение надежности криптографических алгоритмов 2) информационная работа с персоналом предприятия 3) страхование информационных ресурсов
9	Для поддержки разработки политик безопасности используются: 1) автоматизированные сканеры уязвимостей 2) электронные справочные системы 3) средства управления паролями
10	Целью экономического анализа вложений в средства защиты информации является: 1) отказ от ручного труда при обработке информации в пользу средств автоматизации 2) принятие обоснованных решений о необходимости реализации мер по защите информации 3) контроль эффективности средств защиты информации

БЛОК Б (повышенный уровень) – Задание закрытого типа на установление соответствия

Инструкция: Прочитайте текст и установите соответствие

№ задания	Тексты заданий
11	В определении задач менеджмента в сфере информационной безопасности фигурируют такие понятия как: 1) Комплексность 2) Непрерывность 3) Методические задачи Какие понятия им соответствуют? А. Взаимоувязанное выявление всех значимых информационных объектов, а также существующих и потенциально возможных угроз. На основе этого анализа необходимо обеспечить комплексное внедрение и применение средств защиты информации. Б. Разработка, совершенствование и поддержание в актуальном состоянии методических основ управления информационной безопасностью. К ним относятся вопросы управления рисками, экономическое моделирование и т. п. В. Выделение необходимых ресурсов и организация выполнения функций по защите информации в течение всего времени функционирования информационных систем и выполнения бизнес-функций.
12	Цели аудита информационной безопасности могут включать в себя: 1) Оценка рисков; 2) Соответствие стандартам; 3) Выявление уязвимостей. Какие понятия им соответствуют? А. Оценка эффективности защитных средств и поиск слабых мест в системе безопасности. Б. Проверка соблюдения внутренних политик и внешних нормативных требований. В. Идентификация и анализ потенциальных угроз для информационных ресурсов.
13	Риски в сфере информационной безопасности включают в себя: 1) Нарушение конфиденциальности 2) Необратимую утрату информации 3) Недоступность информационных ресурсов Какие примеры им соответствуют? А. Незаконное разглашение, использование или несанкционированный доступ к конфиденциальным сведениям без согласия их владельца;

№ задания	Тексты заданий
	Б. Происходит в некоторых случаях, например, когда перезаписаны биты, произошло механическое повреждение диска или уничтожена намагниченность; В. Невозможность доступа к данным по запросу в предусмотренное расписанием работы системы время.
14	К задачам обучения и информационной работы с персоналом предприятия относится: 1) Недопущение утечек информации с использованием уязвимостей в сетях и программном обеспечении; 2) Ознакомление с требованиями законодательства и локальных регламентов; 3) Противодействие методам "социальной инженерии". Реализуется с помощью: А. Разработка и внедрение чётких политик безопасности. Политика паролей. Правила использования электронной почты. Правила использования социальных сетей. Процедуры проверки личности и авторизации доступа. Регулярные аудиты безопасности. Б. Составить лист ознакомления. Завести журнал ознакомления. Включить пункты об ознакомлении с локальными нормативными актами в трудовой договор. Сотрудник подписывает сам договор и ставит подпись в отдельной графе об ознакомлении с локальными актами. Оставить в самом локальном нормативном акте место для подписи сотрудника. В. Разработка политики безопасности. Внедрение процедур реагирования на инциденты. Регулярный аудит безопасности. Управление доступом.

БЛОК Б (повышенный уровень) – Задание закрытого типа на установление последовательности

Инструкция: Прочитайте текст и установите правильную последовательность

№ задания	Тексты заданий
15	Расставьте в правильной последовательности этапы допуска к сведениям, составляющим государственную тайну, предполагает: 1) проведение проверочных мероприятий в отношении лица, получающего допуск 2) ознакомление лица, получающего допуск, с соответствующими нормами законодательства 3) получение согласия на временное ограничение прав от лица, получающего допуск
16	Экономическая целесообразность аутсорсинга функций безопасности (например, информационной безопасности) обусловлена оптимизацией затрат и концентрацией на основной деятельности. Распределите в возрастающей последовательности эффективность мероприятий при возможной передачи задач сторонним специализированным поставщикам услуг позволяет компаниям 1) Сократить затраты на содержание собственного центра мониторинга (Security Operations Center, SOC) и штатных специалистов; 2) Обеспечить круглосуточный мониторинг и оперативное реагирование на инциденты; 3) Получить доступ к передовым технологиям и опыту профессионалов без значительных инвестиций.
17	Распределите в последовательности этапы стадии создания системы защиты информации: 1) Внедрение системы защиты информации. 2) Разработка системы защиты информации. 3) Формирование требований к системе защиты информации. 4) Подтверждение соответствия системы защиты информации.

БЛОК В (высокий уровень) – Задание открытого типа с развернутым ответом

Инструкция: Прочитайте текст и запишите обоснованный ответ

№ задания	Тексты заданий
18	Комплексный показатель, который характеризует выполнение требований, нейтрализующих угрозы безопасности информационных систем персональных данных называется _____ защищённости персональных данных.
19	За счёт мониторинга событий безопасности, их регистрации и последующего анализа. производится _____ в области информационной безопасности
20	На персонал, отвечающий за обнаружение вторжений, оказывает влияние такой негативный психологический фактор как _____ пользователей о предполагаемом заражении вирусами.

Система оценивания выполнения тестовых заданий по компетенции ОПК-1

Номер задания	Указания по оцениванию	Результат оценивания (баллы, полученные за выполнение задания/характеристика правильности ответа)
Задания 1-10	Задания с выбором одного или нескольких верных ответов из предложенных считается верным, если правильно указана цифра или цифры, означающие верные ответы.	Совпадение с верным ответом оценивается 1 баллом; неверный ответ или его отсутствие - 0 баллов.
Задания 11-14	Задания закрытого типа на установление соответствия считается верным, если правильно установлены все соответствия (позиции из одного столбца верно сопоставлены с позициями другого)	Полное совпадение с верным ответом оценивается 1 баллом; неверный ответ или его отсутствие - 0 баллов.
Задания 15-17	Задания закрытого типа на установление последовательности считается верным, если правильно указана вся последовательность цифр	Полное совпадение с верным ответом оценивается 1 баллом; если допущены ошибки или ответ отсутствует- 0 баллов.
Задания 18-20	Задание открытого типа с развернутым ответом считается верным, если ответ совпадает с эталонным по содержанию и полноте.	Полный правильный ответ на задание оценивается 1 баллом. Если в ответе используются перечисления, то различный порядок следования правильных ответов в перечислении не считается ошибкой. Если допущена ошибка, ответ не полный, неправильный или отсутствует - 0 баллов.

ОПК-10

Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты

БЛОК А (базовый уровень) – Задание с выбором одного или нескольких верных ответов из предложенных

Инструкция по тестам Блока А: Прочитайте текст и выберите один или несколько правильных ответов

№ задания	Тексты заданий
1	Контроль за соблюдением правил защиты персональных данных осуществляется: 1) ФСТЭК; 2) Роскомнадзором; 3) МВД.
2	Политика опубликования материалов в открытых источниках нацелена на: 1) предотвращение утечек конфиденциальной информации; 2) недопущение нарушений авторских прав на объекты интеллектуальной собственности; 3) повышение уровня доступности информации.
3	Функции Роскомнадзора в сфере информационной безопасности включают в себя: 1) защиту информационных ресурсов органов государственного управления; 2) надзор за соблюдением частными компаниями правил защиты сведений, составляющих государственную тайну; 3) контроль за соблюдением правил защиты персональных данных.
4	Отбор персонала при назначении на должности, связанные с обработкой конфиденциальной информации, включает в себя: 1) психологическую оценку; 2) проверку знания внутренних регламентов работы с информацией; 3) оценку навыков использования средств обнаружения вторжений.
5	Перечень сведений, относимых к государственной тайне утверждается: 1) Правительством РФ; 2) Президентом РФ; 3) ФСБ; 4) ФСТЭК.
6	Биометрические средства идентификации основаны на распознавании: 1) персональных кодов доступа; 2) персональных идентификационных карт и жетонов; 3) индивидуальных физических особенностей.
7	К целям аудита информационной безопасности относятся: 1) проверка достижения поставленных целей в сфере информационной безопасности; 2) выявление фактов нарушения информационной безопасности; 3) привлечение к ответственности лиц, виновных в краже и утрате конфиденциальных данных.
8	ФСТЭК осуществляет: 1) лицензирование деятельности по разработке средств защиты информации; 2) контроль за соблюдением требований к защите персональных данных; 3) текущий надзор за соблюдением правил обращения со сведениями, составляющими государственную тайну.
9	Разрушение информации является: 1) сценарием нарушения информационной безопасности; 2) риском для информационных ресурсов; 3) угрозой информационной безопасности.
10	Приемы социотехники основаны на: 1) особенностях человеческой психологии; 2) недостатках организационных структур; 3) недостатках программных и аппаратных средств защиты информации.

БЛОК Б (повышенный уровень) – Задание закрытого типа на установление соответствия

Инструкция: Прочитайте текст и установите соответствие

№ задания	Тексты заданий
11	Обнаружение вторжений осуществляется на основе: 1) косвенных признаков; 2) сигнатур; 3) сообщений пользователей. Установите соответствие видов их описанию А. Действия, которые не связаны с физическим доступом к элементам информационной системы, но указывают на потенциальную опасность утечки информации, неправомерного вмешательства в функционирование системы или нарушения работоспособности системы. Такие признаки позволяют прогнозировать угрозы и определять объекты, на которые они будут направлены; Б. определённые последовательности символов, которые используются для обнаружения вредоносных запросов; В. Рассматриваются сведения о составе и архитектуре, о группах пользователей и уровне их полномочий и типов доступа, внешних и внутренних интерфейсах.
12	Управление информационной безопасностью (ИБ) осуществляется с помощью различных инструментов и мер, среди которых: 1) Оценка рисков; 2) Разработка и внедрение политик безопасности; 3) Обучение и воспитание культуры безопасности; 4) Процессные и технологические решения для защиты информации. Установите соответствие инструментов и мер их описанию: А. К ним относятся системы защиты, антивирусные программы, средства шифрования и другие инструменты безопасности; Б. Важно не только обучать сотрудников основам ИБ, но и формировать в них культуру безопасности; В. Политики охватывают все аспекты ИБ — от методов защиты данных и контроля доступа до правил использования корпоративных устройств и удалённой работы; Г. Включает в себя идентификацию активов, анализ возможных угроз и уязвимостей, а также определение вероятности и потенциального ущерба от инцидентов.
13	Функционирование службы безопасности основывается на части следующих принципах: 1) Законность; 2) Самостоятельность и ответственность; 3) Экономическая целесообразность и прибыльность.. Установите соответствие принципов их содержанию. А. Меры безопасности разрабатываются на основе норм права с применением всех дозволенных методов обнаружения и пресечения правонарушений; Б. Мероприятия по обеспечению безопасности не должны приводить к ухудшению экономических показателей деятельности предприятия; В. Служба безопасности располагает всеми необходимыми для своей деятельности видами ресурсов, при использовании которых обеспечивается строгое соответствие производимых затрат и достигаемых результатов.
14	Обучение персонала, ответственного за обработку информации, включает в себя некоторые аспекты, которым обучают сотрудников: 1) Организационно-распорядительная документация компании; 2) Правила обработки, изменения и уничтожения персональных данных; 3) Правила своевременного оповещения. Установите соответствие категорий их содержанию. А. Ознакомление сотрудников организации с документами, которые фиксируют распоряжения руководства и помогают организовать деятельность сотрудников; Б. Создание и реализация регламента мониторинга и оповещения об инцидентах; В. Ознакомления персонала с Федеральным законом от 27.07.2006 N 152-ФЗ (ред. от 28.02.2025).

БЛОК Б (повышенный уровень) – Задание закрытого типа на установление последовательности

Инструкция: Прочитайте текст и установите правильную последовательность

№ задания	Тексты заданий
15	Расставьте в последовательном порядке этапы построения системы информационной безопасности: 1. Разработка технического задания на создание системы защиты; 2. Определение требований к системе защиты; 3. Обследование ИС (аудит).
16	Расставьте в последовательном порядке этапы процесса определения угроз безопасности информации: 1. Идентификация угроз; 2. Оценка вероятности (возможности) реализации угроз безопасности информации и степени возможного ущерба; 3. Мониторинг и переоценка угроз безопасности информации; 4. Определение области применения модели угроз (обследование).
17	Расставьте в последовательном порядке нормативно-правовое обеспечение информационной безопасности: 1. Политика ИБ; 2. Частные политики информационной безопасности; 3. Инструкции информационной безопасности; 4. Регламенты информационной безопасности.

БЛОК В (высокий уровень) – Задание открытого типа с развернутым ответом

Инструкция: Прочитайте текст и запишите обоснованный ответ

№ задания	Тексты заданий
18	Начальник службы безопасности обычно является одним из заместителей _____
19	Циклический процесс, который включает в себя: сбор и анализ данных о состоянии информационной безопасности в организации, оценку информационных рисков, планирование мер по обработке рисков, оперативную работу по осуществлению защитных мероприятий, мониторинг функционирования механизмов контроля представляет собой _____ информационной безопасностью
20	_____ информационной безопасности может проводиться, как внутренними специалистами организации, так и внешними независимыми аудиторами

Система оценивания выполнения тестовых заданий по компетенции ОПК-10

Номер задания	Указания по оцениванию	Результат оценивания (баллы, полученные за выполнение задания/характеристика правильности ответа)
Задания 1-10	Задания с выбором одного или нескольких верных ответов из предложенных считается верным, если правильно указана цифра или цифры, означающие верные ответы.	Совпадение с верным ответом оценивается 1 баллом; неверный ответ или его отсутствие - 0 баллов.
Задания 11-14	Задания закрытого типа на установление соответствия считается верным, если правильно установлены все соответствия (позиции из одного столбца верно сопоставлены с позициями другого)	Полное совпадение с верным ответом оценивается 1 баллом; неверный ответ или его отсутствие - 0 баллов.
Задания 15-17	Задания закрытого типа на установление последовательности считается верным, если правильно указана вся последовательность цифр	Полное совпадение с верным ответом оценивается 1 баллом; если допущены ошибки или ответ отсутствует- 0 баллов.
Задания 18-20	Задание открытого типа с развернутым ответом считается верным, если ответ совпадает с эталонным по содержанию и полноте.	Полный правильный ответ на задание оценивается 1 баллом. Если в ответе используются перечисления, то различный порядок следования правильных ответов в перечислении не считается ошибкой. Если допущена ошибка, ответ не полный, неправильный или отсутствует - 0 баллов.

Методические рекомендации по освоению дисциплины

1. Методические рекомендации преподавателю

Перед началом изучения дисциплины преподаватель должен ознакомить обучающихся с рабочей программой и оценочными материалами по дисциплине, с видами учебной и самостоятельной работы, перечнем литературы и интернет-ресурсов, с формами текущей и промежуточной аттестации, с критериями оценки качества знаний для итоговой оценки по дисциплине.

При проведении лекций, преподаватель:

- 1) формулирует тему и цель занятия, объявляет учебные вопросы;
- 2) излагает основные теоретические положения;
- 3) с помощью технических средств обучения и/или под запись дает определения основных понятий, расчетных формул;
- 4) проводит примеры из отечественного и зарубежного опыта, дает текущие статистические данные для наглядного и образного представления изучаемого материала;
- 5) в конце занятия выдает вопросы для самостоятельного изучения.

На занятиях лабораторного цикла следует обратить внимание на соответствие выбираемых обучающимся средств выполнения решаемым в работе задачам.

Каждая лабораторная работа должна быть оформлена и защищена в соответствии с требованиями. Защита производится после оформления отчета по работе.

Во время выполнения заданий в учебной аудитории обучающийся может консультироваться с преподавателем, определять наиболее эффективные методы решения поставленных задач. Если какая-то часть задания остается не выполненной, обучающийся может продолжить её выполнение во время внеаудиторной самостоятельной работы.

Для оценки полученных знаний и освоения учебного материала по каждому разделу и в целом по дисциплине преподаватель использует формы текущего контроля и промежуточной аттестации знаний обучающихся.

2. Методические рекомендации обучающимся

Приступая к изучению новой учебной дисциплины, обучающиеся должны ознакомиться с рабочей программой, оценочными материалами, учебной, научной и методической литературой, имеющейся в ЭИОС СКФ МТУСИ,

Глубина усвоения дисциплины зависит от активной и систематической работы обучающегося на лекциях и практических занятиях, а также в ходе самостоятельной работы, по изучению рекомендованной литературы.

2.1 Методические указания для обучающихся по лекционным занятиям

Важно сосредоточить внимание на содержании лекции. Это поможет лучше воспринимать учебный материал и уяснить взаимосвязь проблем по всей дисциплине.

Основное содержание лекции целесообразнее записывать в тетради в виде ключевых фраз, понятий, тезисов, обобщений, схем, опорных выводов. Необходимо обращать внимание на термины, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации. Желательно оставлять в конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющей материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

С целью уяснения теоретических положений, разрешения спорных ситуаций необходимо задавать преподавателю уточняющие вопросы. Для закрепления содержания лекции в памяти, необходимо во время самостоятельной работы внимательно прочесть свой конспект и дополнить его записями из учебников и рекомендованной литературы.

Конспектирование читаемых лекций и их последующая доработка способствует более глубокому усвоению знаний, и поэтому являются важной формой учебной деятельности обучающихся.

2.2 Методические указания для обучающихся по подготовке к лабораторным работам

Лабораторные занятия по любой учебной дисциплине проводятся в соответствии с рабочей программой этой учебной дисциплины в установленные расписанием часы.

Инструктаж по технике безопасности, правилам пожарной безопасности и правилам внутреннего распорядка в лаборатории проводится преподавателем на первом лабораторном занятии. На этом же занятии обучающимся сообщаются:

- программа всего предстоящего лабораторного цикла;
- условия взаимодействия обучающихся с преподавателем в процессе выполнения лабораторных работ;
- условия контроля самостоятельной работы обучающихся, включая правила оформления отчетов по лабораторным работам и их последующей защиты;
- другая необходимая информация.

Организация лабораторных работ включает:

- самостоятельную внеаудиторную подготовку обучающегося к выполнению каждой отдельной лабораторной работы в соответствии с ее программой в рамках часов, выделенных на самостоятельную проработку материала в программе дисциплины;
- входной контроль преподавателем степени подготовленности каждого обучающегося к выполнению лабораторных работ;
- выполнение программы лабораторных работ в полном объеме;
- оформление отчета и его защиту каждым обучающимся в установленные сроки;
- формирование преподавателем рейтингов каждого из обучающихся по результатам выполнения и защиты им отдельных лабораторных работ и их циклов (используется Модульно-рейтинговая система).

Оценка качества выполнения лабораторных работ каждым обучающимся производится преподавателем отдельно за подготовку к работе, ее выполнение и защиту.

2.3 Методические указания для обучающихся по подготовке к практическим занятиям

Целью практических занятий является закрепление теоретических знаний, полученных при изучении дисциплины.

При подготовке к практическому занятию целесообразно выполнить следующие рекомендации:

- изучить основную литературу; ознакомиться с дополнительной литературой, новыми публикациями в периодических изданиях: журналах, газетах и т.д.;
- при необходимости доработать конспект лекций. При этом учесть рекомендации преподавателя и требования учебной программы.

При выполнении практических занятий основным методом обучения является самостоятельная работа обучающегося под управлением преподавателя. На них пополняются теоретические знания обучающихся, их умение творчески мыслить, анализировать, обобщать изученный материал, проверяется отношение обучающихся к будущей профессиональной деятельности.

Оценка выполненной работы осуществляется преподавателем комплексно: по результатам выполнения заданий, устному сообщению и оформлению работы.

После подведения итогов занятия обучающийся обязан устранить недостатки, отмеченные преподавателем при оценке его работы.

Методические указания по выполнению лабораторных и практических работ по дисциплине «*Основы управления информационной безопасностью*» для обучающихся очной формы обучения, размещенные на сайте СКФ МТУСИ в разделе «Методические материалы»:

3. Методические рекомендации для обучающихся по самостоятельной работе

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

Самостоятельная работа во внеаудиторное время включает в себя:

- повторение лекционного материала;
- подготовки к лабораторным работам (практическим занятиям);
- изучения учебной и научной литературы;
- решения задач, выданных на практических занятиях;
- подготовки к тестированию;
- выделение наиболее сложных и проблемных вопросов по изучаемой теме, получение разъяснений и рекомендаций по данным вопросам с преподавателями кафедры на их еженедельных консультациях.
- проведение самоконтроля путем ответов на вопросы текущего контроля знаний, решения представленных в учебно-методических материалах кафедры задач, тестов, написания рефератов по отдельным вопросам изучаемой дисциплины.

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

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

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

Перед выполнением внеаудиторной самостоятельной работы преподаватель проводит инструктаж (консультацию) с определением цели задания, его содержания, сроков выполнения, основных требований к результатам работы, критериев оценки, форм контроля и перечня источников и литературы.

Обычно постановку задачи обучающимся на проведение самостоятельной работы преподаватель осуществляет на одном из занятии, предшествующему данному.

Методику самостоятельной работы все обучаемые выбирают индивидуально, но методика достижения конечной цели может определяться преподавателем и включать: последовательность изучения и усвоения учебно-методического материала, пособий, руководств, наставлений, техники и т.д.; определение главного в изучаемом материале, материале, который необходимо законспектировать; просмотр учебных кинофильмов и их

обсуждение; работу обучающихся по индивидуальным заданиям; опрос обучаемых в течении 7-10 минут с целью проверки усвоения главного из прочитанного материала.

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

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

Приветствуется использование компьютеров, которое:

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

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

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

№	Темы, разделы, вынесенные на самостоятельную подготовку, вопросы для подготовки к практическим и лабораторным занятиям; курсовые работы, содержание контрольных работ; рекомендации по использованию литературы, ЭВМ и др.	Часов всего: 38	Неделя
Модуль 1 – 36 часов			
1	Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27 июля 2006 №149-ФЗ.	4	1
2	Федеральный закон "О связи" от 07.07.2003 №126-ФЗ.	4	2
3	Федеральный закон "О безопасности" от 28.12.2010 №390-ФЗ	4	3
4	Федеральный закон "Об электронной подписи" от 06.04.2011 №63-ФЗ.	2	4
5	Федеральный закон "О персональных данных" от 27.07.2006 №152-ФЗ.	2	5
6	Закон РФ "О государственной тайне" от 21.07.1993 №5485-1.	2	6
7	Федеральный закон "О коммерческой тайне" от 29.07.2004 №98-ФЗ.	2	7
8	Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 №187-ФЗ. Федеральный закон "О федеральной службе безопасности" от 03.04.1995 №40-ФЗ	2	8
Модуль 2 – 36 часов			
9	Закон РФ "О частной детективной и охранной деятельности в Российской Федерации" от 11.03.1992 №2487-1	2	9
10	Федеральный закон "О лицензировании отдельных видов деятельности" от 04.05.2011 №99-ФЗ.	2	10
11	Федеральный закон "Об экспортном контроле" от 18.07.1999 г. №183-ФЗ .	2	11
12	Федеральный закон "О техническом регулировании" от 27.12.2002 №184-ФЗ.	2	12
13	Трудовой кодекс Российской Федерации от 30.12.2001 №197-ФЗ.	2	13
14	Гражданский кодекс Российской Федерации часть 4 (ГК РФ ч.4) 18.12.2006 №230-ФЗ.	2	14

15	"Кодекс Российской Федерации об административных правонарушениях" от 30.12.2001 №195-ФЗ.	2	15
16	"Уголовный кодекс Российской Федерации" от 13.06.1996 №63-ФЗ.	2	16

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

Самостоятельная работа обучающихся над усвоением материала по дисциплине может выполняться в помещении для самостоятельной работы СКФ МТУСИ, посредством использования электронной библиотеки и ЭИОС.