

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

«08» 04 2026 г.

Рабочая программа практики

Б2.В.03(Пд) Производственная (преддипломная) практика

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/семестр
Общая трудоемкость дисциплины, в том числе (по семестрам, курсам):	6	216/8
Контактная работа, в том числе (по семестрам, курсам):		
Лекции		
Лабораторных работ		
Практических занятий		
Семинаров		
Иная контактная работа		2/8
Самостоятельная работа		214/8
Контроль		
Число контрольных работ (по курсам)		
Число КР (по семестрам, курсам)		
Число КП (по семестрам, курсам)		
Число зачетов с оценкой с разбивкой по семестрам (курсам)		1/8
Число экзаменов с разбивкой по семестрам (курсам)		

Программу составил:
К.т.н., доцент Маршаков Д.В.

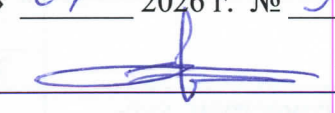
Рабочая программа дисциплины
«Производственная (преддипломная) практика»

Разработана в соответствии с ФГОС ВО:
направления подготовки 10.03.01 «Информационная безопасность», утвержденным приказом Министерства науки и высшего образования Российской Федерации от 17 ноября 2020 г. N 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 2026 г. № 9

И.О.Зав. кафедрой  Жуковский А.Г.

1. Цели изучения дисциплины

Целями **Производственной (преддипломной) практики** является закрепление и углубление теоретической подготовки по направлению подготовки 10.03.01 Информационная безопасность, получение обучающимися практических навыков и компетенций по видам профессиональной деятельности, сбор материалов для выполнения исследования, приобретение практических навыков и компетенций в сфере профессиональной деятельности и их применение при решении научно-исследовательских и производственных задач.

Задачи производственной практики:

- изучение теоретических и экспериментальных методов получения, обработки и хранения научной информации с привлечением современных информационных технологий;
- изучение опыта проведения конкретных научных исследований в организации и лабораториях кафедры университета,
- развитие навыков сбора, обработки, анализ и систематизации научно-технической информации по теме исследования;
- выбор методик и средств решения поставленных задач;
- изучение форм и порядка составления отчетной научно-технической документации и внедрения результатов научных исследований;
- формирование навыков ведения научных исследований, как целостного процесса, в том числе навыков анализа конкретной проблемной ситуации, формулировки проблемы и выдвижения гипотезы, разработки плана эксперимента, проведения эксперимента, обработки результатов, формулировки выводов и представления итогов проделанной работы в виде научных отчетов, рефератов или статей;
- разработка плана и программы проведения научных исследований и технических разработок по выбранной теме исследования.

Вид практики: производственная

Тип практики: преддипломная практика

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:

Компетенции, формируемые у обучающегося в результате освоения дисциплины (в части, обеспечиваемой дисциплиной)
ПК-1. Администрирование подсистем защиты информации в операционных системах
Знать:
Архитектуру и принципы построения операционных систем
Программные интерфейсы операционных систем
Виды политик управления доступом и информационными потоками применительно к операционным системам
Архитектура подсистем защиты информации в операционных системах
Принципы функционирования средств защиты информации в операционных системах, в том числе использующих криптографические алгоритмы
Состав типовых конфигураций программно-аппаратных средств защиты информации
Требования по составу и характеристикам подсистем защиты информации применительно к операционным системам
Порядок реализации методов и средств антивирусной защиты в операционных системах
Программно-аппаратные средства и методы защиты информации в операционных системах
Принципы работы и правила эксплуатации программно-аппаратных средств защиты информации
Нормативные правовые акты в области защиты информации

Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации и обеспечению безопасности критической информационной инфраструктуры
Организационные меры по защите информации.

Уметь:

Формулировать политики безопасности операционных систем
Настраивать политики безопасности операционных систем
Оценивать угрозы безопасности информации операционных систем
Противодействовать угрозам безопасности информации с использованием встроенных средств защиты информации операционных систем
Выбирать режимы работы программно-аппаратных средств защиты информации в операционных системах
Настраивать антивирусные средства защиты информации в операционных системах
Устанавливать обновления программного обеспечения и средств антивирусной защиты
Проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах
Производить анализ эффективности программно-аппаратных средств защиты информации в операционных системах
Оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в операционных системах.

Владеть:

Определением состава применяемых программно-аппаратных средств защиты информации в операционных системах
Разработкой порядка применения программно-аппаратных средств защиты информации в операционных системах
Формированием шаблонов установки программно-аппаратных средств защиты информации в операционных системах
Установкой программно-аппаратных средств защиты информации в операционных системах, включая средства криптографической защиты информации
Конфигурированием программно-аппаратных средств защиты информации в операционных системах
Контролем корректности функционирования программно-аппаратных средств защиты информации в операционных системах
Управлением антивирусной защитой операционных систем в соответствии с действующими требованиями.

ПК-2. Администрирование программно-аппаратных средств защиты информации в компьютерных сетях.

Знать:

Принципы построения компьютерных сетей
Стек сетевых протоколов операционных систем
Стек протоколов сетевого оборудования
Порядок реализации методов и средств межсетевого экранирования
Принципы функционирования сетевых протоколов, включающих криптографические алгоритмы
Виды политик управления доступом и информационными потоками в компьютерных сетях
Источники угроз информационной безопасности в компьютерных сетях и меры по их предотвращению
Состав типовых конфигураций программно-аппаратных средств защиты информации и режимов их функционирования в компьютерных сетях
Методы измерений, контроля и технических расчетов характеристик программно-аппаратных средств защиты информации
Принципы работы и правила эксплуатации применяемых программно-аппаратных средств защиты информации

Программно-аппаратные средства и методы защиты информации в компьютерных сетях Нормативные правовые акты в области защиты информации Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации и обеспечению безопасности критической информационной инфраструктуры Организационные меры по защите информации
Уметь: Оценивать угрозы безопасности информации в компьютерных сетях Настраивать правила фильтрации пакетов в компьютерных сетях Обосновывать выбор используемых программно-аппаратных средств защиты информации в компьютерных сетях Конфигурировать и контролировать корректность настройки программно-аппаратных средств защиты информации в компьютерных сетях Выбирать режимы работы программно-аппаратных средств защиты информации в компьютерных сетях Проводить мониторинг функционирования программно-аппаратных средств защиты информации в компьютерных сетях Производить анализ эффективности программно-аппаратных средств защиты информации в компьютерных сетях Оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях.
Владеть: Определением состава применяемых программно-аппаратных средств защиты информации в компьютерных сетях Разработкой порядка применения программно-аппаратных средств защиты информации в компьютерных сетях Формированием шаблонов конфигурации программно-аппаратных средств защиты информации в компьютерных сетях Настройкой программных и аппаратных средств построения компьютерных сетей, использующих криптографическую защиту информации Управлением функционированием программно-аппаратных средств защиты информации в компьютерных сетях Контролем корректности функционирования программно-аппаратных средств защиты информации в компьютерных сетях Управлением средствами межсетевого экранирования в компьютерных сетях в соответствии с действующими требованиями.
ПК-3: Администрирование средств защиты информации прикладного и системного программного обеспечения
Знать: Архитектуру подсистем защиты информации в операционных системах Принципы построения систем управления базами данных Основные средства и методы анализа программных реализаций Принципы построения антивирусного программного обеспечения Виды политик управления доступом и информационными потоками применительно к прикладному программному обеспечению Источники угроз информационной безопасности программного обеспечения и меры по их предотвращению Уязвимости используемого программного обеспечения и методы их устранения Виды и формы функционирования вредоносного программного обеспечения Характерные признаки наличия вредоносного программного обеспечения Средства и методы обнаружения ранее неизвестного вредоносного программного обеспечения Принципы функционирования программных средств криптографической защиты информации Порядок обеспечения безопасности информации при эксплуатации программного обеспечения

Нормативные правовые акты в области защиты информации Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации и обеспечению безопасности критической информационной инфраструктуры Организационные меры по защите информации.	
Уметь:	
Анализировать угрозы безопасности информации программного обеспечения Формулировать правила безопасной эксплуатации программного обеспечения Обосновывать правила безопасной эксплуатации программного обеспечения Анализировать функционирование программного обеспечения с целью определения возможного вредоносного воздействия Производить проверку соответствия реальных характеристик программно-аппаратных средств защиты информации заявленным в их технической документации Осуществлять мероприятия по противодействию угрозам безопасности информации, возникающим при эксплуатации программного обеспечения Определять порядок функционирования программного обеспечения с целью обеспечения защиты информации Анализировать эффективность сформулированных требований к встроенным средствам защиты информации программного обеспечения.	
Владеть:	
Определением порядка установки программного обеспечения с целью соблюдения требований по защите информации Контролем за соблюдением требований по защите информации при установке программного обеспечения, включая антивирусное программное обеспечение Формулированием требований к параметрам средств антивирусной защиты для корректной работы программного обеспечения Выполнением работ по обнаружению вредоносного программного обеспечения Ликвидацией обнаруженного вредоносного программного обеспечения и последствий его функционирования Формулированием требований к встроенным средствам защиты информации программного обеспечения.	

3. Место дисциплины в структуре образовательной программы

Требования к предварительной подготовке обучающегося (предшествующие дисциплины, модули, темы):	
1	Б1.О.33 Программно-аппаратные средства защиты информации
2	Б1.О.36.02 Криптографические протоколы
3	Б1.В.02 Комплексное обеспечение защиты информации объекта информатизации
4	Б1.О.36.06 Администрирование средств защиты информации в компьютерных системах и сетях
5	Б1.В.07 Аналитика DLP-систем
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:	
1	Б3.01 Подготовка к процедуре защиты и защита выпускной квалификационной работы

4. Структура и содержание дисциплины

4.1 Очная форма обучения, 4 года (всего 216 часов, 2 часа контактной работы)

Код зан.	Тема и краткое содержание работы	Кол. часов	Компетенции
1.1	Инструктаж по ПМБ. Изучение требований правил и мер безопасности, установленных в компании и непосредственно на рабочем месте.	4	ПК-1, ПК-2, ПК-3
1.2	Библиографический поиск	22	ПК-1, ПК-2, ПК-3
1.3	Изучение нормативно-технической документации	32	ПК-1, ПК-2, ПК-3
1.4	Участие в измерениях или отладке оборудования и программного обеспечения систем и устройств программной защиты информации	50	ПК-1, ПК-2, ПК-3
1.5	Изучение требований по размещению криптографического оборудования	20	ПК-1, ПК-2, ПК-3
1.6	Рассмотрение вопросов применения дополнительного оборудования для информационной защиты компьютерной сети предприятия	20	ПК-1, ПК-2, ПК-3
1.7	Подготовка технической документации и необходимых заявок на ремонт или замену оборудования, а также обновление или замену программного обеспечения.	26	ПК-1, ПК-2, ПК-3
1.8	Ознакомление со структурой и содержанием типовых ВКР бакалавра.	20	ПК-1, ПК-2, ПК-3
1.9	Обобщение результатов работы. Написание отчёта по производственной (преддипломной) практике и получение отзыва о работе во время практики.	20	ПК-1, ПК-2, ПК-3
	Зачёт с оценкой	2	ПК-1, ПК-2, ПК-3
Итого – 216 часов			

5. Формы отчетности по практике

Формами отчетности обучающихся по практике являются:

1) *Заполненный дневник с отзывом руководителя практики.*

Содержание дневника должно соответствовать индивидуальному заданию и плану производственной практики. Подписи представителя организации о прибытии на практику и убытии с неё, а также подпись руководителя практики от предприятия под его отзывом должны быть заверены печатью организации, в которой проводилась практика.

2) *Отчет по практике.*

Отчет по практике оформляется отдельным документом в печатном виде на бумаге формата А4. Он должен содержать:

- титульный лист (образец приведен на сайте филиала);
- содержание практики (в соответствии с Программой производственной практики);
- краткие теоретические сведения и свидетельства выполнения Плана и Программы

практики (скриншоты, фотографии оборудования, должностные инструкции.)

– перечень и обзор использованных обучающимся информационных источников и нормативных документов;

– выводы и предложения обучающегося по практике.

Отчет по практике подписывается обучающимся, проверяется и визируется руководителем практики от организации и руководителем практики от института. Защита отчетов производится в соответствии с установленным графиком защиты отчетов. Нарушение сроков прохождения практики и сроков защиты считается невыполнением учебного плана. По результатам защиты отчетов по практике в институте обучающемуся выставляется оценка.

3) Ответы на контрольные вопросы и выполнение задач.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Рекомендуемая литература				
6.1.1. Основная литература				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л1.1	Галатенко, В. А.	Основы информационной безопасности : учебное пособие	Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024.	Э1
Л1.2	Суворова, Г. М.	Информационная безопасность : учебное пособие	Саратов : Вузовское образование, 2024.	Э2
Л1.3	А.М. Голиков	Защита информации от утечки по техническим каналам	Томский Государственный университет Систем управления и радиоэлектроники, 2015	Э3
Л1.4	Бузов Г.А.	Защита информации ограниченного доступа от утечки по техническим каналам	М.: Гор. линия-Телеком, 2024. – 585 с.	Э4
Л1.5	Лапони́на О.Р., В.А. Сухомлина	Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия : учебное пособие	М.: ИНТУИТ, Ай Пи Ар Медиа, 2024— 605 с.	Э5
Л1.6	Бабаш А.В.	Криптографические методы защиты информации. Том 1: учебно-методическое пособие	М.: РИОР: ИНФРА-М, 2021. — 413 с.	Э6
Л1.7	Белоус, А. И., В. А. Солодуха	Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения	Москва: Техносфера, 2021. — 482 с.	Э7
6.1.2. Дополнительная литература				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л2.1	Кубанков А.Н., Булгакова Е.В.	Основы информационной безопасности	М.: МТУСИ, 2024.	Э8

Л2.2	Шаньгин, В. Ф.	Комплексная защита информации в корпоративных системах : учебное пособие	Москва : ФОРУМ : ИНФРА-М, 2022. — 592 с.	Э9
Л2.3	Литвинов, Р.В., К.А. Волегов, А.П. Бацула	Технические средства защиты информации. Часть 1 : курс лекций	Томск : Томский государственный университет систем управления и радиоэлектроники, 2006. — 170 с.	Э10
Л2.4	Маршаков Д.В., Д.В. Фахти	Методы и средства криптографической защиты информации. Практический курс: учебное пособие	М.: ИНФРА-М, 2022. — 76 с	Э11
Л2.5	Макаренко С.И.	Аудит безопасности критической инфраструктуры специальными информационными воздействиями: монография	Санкт-Петербург: Наукоемкие технологии, 2018	Э12
Л2.6	А. В. Терехов, В. Н. Чернышов, А. В. Платенкин, А. В. Селезнев	Информационная безопасность и правовые основы защиты персональных данных : учебное пособие	Тамбов : Тамбовский государственный технический университет, ЭБС АСВ, 2023. — 80 с.	Э13
Л2.7		Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных" (с изм. и доп.)		Э14
Л2.8		Федеральный закон от 06.04.2011 N 63-ФЗ (с изм. и доп.) "Об электронной подписи"		Э15
Л2.9		Федеральный закон от 07.07.2003 N 126-ФЗ "О связи" (с изм. и доп.)		Э16
Л2.10		Федеральный закон от 17 июля 1999 г. N 176-ФЗ "О почтовой связи" (с изм. и доп.)		Э17
Л2.11		Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изм. и доп.)		Э18
Л2.12		Закон РФ от 21 июля 1993 г. N 5485-1 "О государственной тайне" (с изм. и доп.)		Э19
Л2.13		Указ Президента РФ от 17 марта 2008 г. N 351 "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена"		Э20
Л2.14		Приказ Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. N 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах"		Э21
Л.15		ГОСТ 34.936-91 Информационная технология. Локальные вычислительные сети. Определение услуг уровня управления доступом к среде		Э22
Л2.16		ГОСТ Р 53724-2009 Качество услуг связи. Общие положения		Э23
6.1.3. Учебно-методическое обеспечение				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
ЛЗ.1	И. В. Влацкая,	Практическая подготовка обучающихся специ-	Оренбург : ОГУ,	Э24

	С. А. Герасименко	альности 10.05.01 Компьютерная безопасность : методические указания	2024. — 70 с.	
6.2. Электронные образовательные ресурсы				
Э1	https://www.iprbookshop.ru/142285.html			
Э2	https://www.iprbookshop.ru/142805.html			
Э3	https://www.iprbookshop.ru/72090.html			
Э4	https://elib.mtuci.ru/view.php?book_id=3168			
Э5	: https://www.iprbookshop.ru/142292.html			
Э6	https://znanium.com/catalog/product/1215714			
Э7	https://www.iprbookshop.ru/108023.html			
Э8	http://elib.mtuci.ru/view.php?book_id=3659			
Э9	https://znanium.ru/catalog/product/1843022			
Э10	https://www.iprbookshop.ru/14027.html			
Э11	https://znanium.ru/catalog/product/1891129			
Э12	https://www.iprbookshop.ru/10615.html			
Э13	https://www.iprbookshop.ru/141049.html			
Э14	https://www.consultant.ru/document/cons_doc_LAW_61801/			
Э15	https://www.consultant.ru/document/cons_doc_LAW_112701/			
Э16	https://www.consultant.ru/document/cons_doc_LAW_43224/			
Э17	https://www.consultant.ru/document/cons_doc_LAW_6719/			
Э18	https://www.consultant.ru/document/cons_doc_LAW_61798/			
Э19	https://www.consultant.ru/document/cons_doc_LAW_2481/			
Э20	https://www.consultant.ru/document/cons_doc_LAW_75586/			
Э21	https://ivo.garant.ru/#/document/70391358/paragraph/1/doclist/376/1/0/0/от%2011%20февраля%202013%20г.%20N%2017:2			
Э22	https://docs.cntd.ru/document/1200021831			
Э23	https://docs.cntd.ru/document/1200082201			
Э24	https://e.lanbook.com/book/503273			
6.3 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	Электронный ресурс http://www.securitylab.ru/			
5.3.5	Профессиональная база данных: Федеральный портал «Российское образование»: [Электронный ресурс] – Режим доступа: http://www.edu.ru/ (открытый доступ)			
5.3.6	Профессиональная база данных: Федеральный центр информационно-образовательных ресурсов: [Электронный ресурс] – Режим доступа: http://fcior.edu.ru/ (открытый доступ)			
5.3.7	Научно информационная сеть https://www.researchgate.net/			
5.3.8	Национальный открытый университет «ИНТУИТ» - https://intuit.ru/			
6.4. Программное обеспечение				
СКФ МТУСИ обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства:				
П.1	Linux (свободное ПО)			
П.2	LibreOffice (свободное ПО)			
П.3	Kaspersky Endpoint Security (лицензионное ПО)			

7. Материально-техническое обеспечение практической подготовки	
7.1	Прохождение практики обеспечивается материально-техническими средствами в организации, осуществляющей деятельность по профилю образовательной программы (в том числе в структурном подразделении профильной организации, предназначенном

	для проведения практической подготовки), и/или структурных подразделений СКФ МТУСИ, предназначенных для проведения практической подготовки, а также учебными аудиториями для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенных оборудованием и техническими средствами обучения, а так же помещениями для самостоятельной работы обучающихся, оснащенными специализированной мебелью и компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду СКФ МТУСИ. Проведение практики обеспечено материально-технической базой, соответствующей действующим противопожарным правилам и нормам.
--	---

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

9. Методические рекомендации для обучающихся по проведению практической подготовки

9.1 Организация и руководство практической подготовкой

Практическая подготовка при проведении практики организуется путем непосредственного выполнения обучающимися определенных видов работ, связанных с будущей профессиональной деятельностью.

Практическая подготовка обучающегося может быть организована:

- 1) непосредственно в филиале, в том числе в его структурном подразделении, предназначенном для проведения практической подготовки;
- 2) в организации, осуществляющей деятельность по профилю соответствующей образовательной программы (далее - профильная организация), в том числе в структурном подразделении профильной организации, предназначенном для проведения практической подготовки, на основании договора, заключаемого между университетом и профильной организацией.

В этом случае распределение на практику осуществляется только при наличии персональных договоров с профильной организацией.

При организации практической подготовки профильные организации создают условия для реализации компонентов образовательной программы, предоставляют оборудование и технические средства обучения в объеме, позволяющем выполнять определенные виды работ, связанные с будущей профессиональной деятельностью обучающихся.

При организации практической подготовки обучающиеся и работники Филиала обязаны соблюдать правила внутреннего трудового распорядка профильной организации, требования охраны труда и техники безопасности.

Выпускающая кафедра организует и методически обеспечивает практику обучающихся, разрабатывает программы практики, назначает руководителей практики из числа профессорско-преподавательского состава кафедры. Ответственный за производственную (преддипломную) практику от факультета готовит приказ о распределении обучающихся на практику.

Выпускающая кафедра и ответственный за производственную (преддипломную) практику от факультета проводят организационное собрание обучающихся и руководителей практики по разъяснению целей, содержания, порядка и контроля прохождения практики.

Руководитель от университета составляет план проведения практики, разрабатывает индивидуальные задания для обучающихся, выполняемые в период практики, участвует в распределении обучающихся по рабочим местам и видам работ в организации, осуществляет контроль за соблюдением сроков проведения практики, соответствием ее содержания требованиям, установленным ОП ВО, оказывает методическую помощь обучающимся при выполнении ими индивидуальных заданий, оценивает результаты прохождения практики обучающимися.

Руководитель практики от профильной организации (при наличии):

- согласовывает план проведения производственной (преддипломной) практики, индивидуальные задания, содержание и планируемые результаты производственной (преддипломной) практики;

- предоставляет рабочие места обучающимся. Обеспечивает безопасные условия прохождения производственной (преддипломной) практики обучающимся, отвечающие санитарным правилам и требованиям охраны труда, правил противопожарной безопасности, техники безопасности, санитарно-эпидемиологических правил и гигиенических нормативов;

- проводит инструктаж обучающихся по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, а также правилами внутреннего трудового распорядка организации.

По результатам практики оформляется характеристика на каждого обучающегося.

9.1.1 Обязанности руководителя практики от СКФ МТУСИ:

- провести организационное собрание обучающихся перед началом практики;
- обеспечить контроль своевременного начала практики, прибытия и нормативов работы обучающихся на предприятии;
- обеспечить контроль соблюдения сроков практики и ее содержания;
- оказывать методическую помощь обучающимся при сборе материалов и выполнении отчетов;
- провести итоговый контроль отчета по практике в форме зачета, которая выставляется руководителем практики на основании оценок со стороны куратора практики от предприятия, собеседования со обучающимся с учетом его личных наблюдений;
- вносить предложения по улучшению и совершенствованию проведения практики перед руководством СКФ МТУСИ.

9.1.2 Обязанности куратора практики от предприятия

Ответственность за организацию и проведение практики возлагается на руководителя подразделения, в котором обучающиеся проходят практику.

Куратор практики:

- знакомится с содержанием заданий на практику и способствует их выполнению на рабочем месте;
- знакомит практиканта с правилами внутреннего распорядка;
- предоставляет максимально возможную информацию, необходимую для выполнения заданий практики;
- в случае необходимости вносит коррективы в содержание и процесс организации практики обучающихся;
- по окончании практики дает характеристику о работе обучающегося – практиканта;
- оценивает работу практиканта во время практики.

9.2 Методические рекомендации обучающимся

Перед прохождением практики обучающийся должен изучить программу, представленную учебно-методическую документацию по практике и обратиться к соответствующим нормативным материалам, литературе с тем, чтобы быть подготовленным к выполнению поручений, данных руководителем практики, к решению задач практики, конкретных практических вопросов.

При прохождении практики на предприятиях обучающиеся при необходимости должны подготовить необходимые документы (получить медицинскую справку по форме, требуемой предприятием-базой практики, подготовить фотографии и паспортные данные (ксерокопии разворотов с фотографией и регистрацией места жительства для оформления пропусков на предприятии и т.д.).

В рамках самостоятельной работы обучающимся рекомендуется просмотреть конспекты лекций, учебники и другие учебные издания.

При прохождении практики обучающиеся обязаны: своевременно прибыть на место прохождения практики, иметь при себе все необходимые документы: индивидуальное задание, план (график) практики; подчиняться действующим правилам внутреннего трудового распорядка организации

- места прохождения практики; изучить и строго соблюдать правила охраны труда, техники безопасности, пожарной безопасности; выполнять задания, предусмотренные программой практики; быть вежливым, внимательным в общении с работниками; вести записи о проделанной работе, чтобы в дальнейшем в отчете описать содержание проделанной работы; в установленный срок отчитаться о прохождении практики руководителю практики от университета, подготовить и сдать отчет и другие документы по практике на кафедру.

При подготовке к практике и во время прохождения практики рекомендуется по возникшим вопросам обращаться к учебной литературе, методическим материалам. При возникновении затруднений в процессе практики обучающийся может обратиться к руководителю практики от университета либо от организации-базы практики и получить необходимые разъяснения.

В результате практики бакалавра готовит краткий отчет (рекомендуемый объем – 15-25 страниц). В отчет следует помещать информацию об использованной литературе по теме дисциплины исследования, результаты исследований.

По окончании практики в дневнике делаются отметки, заверенные печатью, о сроках пребывания бакалавра на практике и дается отзыв научного руководителя.

Контроль качества самостоятельной работы обучающихся производится при защите отчета по практике.

10. Особенности прохождения практики для инвалидов и лиц с ограниченными возможностями здоровья

Выбор мест прохождения практики для обучающихся с ограниченными возможностями здоровья осуществляется с учетом рекомендаций медико-социальной экспертизы, отраженных в индивидуальной программе реабилитации, доступности рекомендованных условий труда для данной категории обучающихся (сюда относятся профильные доступные организации, готовые принять обучающихся, кафедры Филиала).

Обучающимся с ограниченными возможностями здоровья и инвалидам необходимо не позже чем за 2 месяца до начала практики написать заявление с приложением документов, подтверждающих необходимость подбора места практики с учетом их индивидуальных особенностей.

Содержание индивидуального задания для практики обсуждается обучающимся совместно с руководителем практики от организации, учитывая специфику организации и возможности в предоставлении материалов по отдельным аспектам организационной работы.

Обучающиеся должны проходить практику в соответствии с планом, выполняя все задания и по возникающим вопросам обращаться к руководителю практики от кафедры, сообщая о результатах проведенной работы не реже, чем два раза в неделю, при личном посещении или по электронной почте.

11. Дополнения и изменения в Рабочей программе

Лист актуализации рабочей программы практики «Производственная (преддипломная) практика Б2.О.02(Пд)» для использования в 20___/20___ учебном году

Утверждаю

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

Направление: 10.03.01 Информационная безопасность

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

Форма обучения: очная, заочная, очно-заочная

(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

ПК-1: Администрирование подсистем защиты информации в операционных системах		
Знать:		
- архитектуру и принципы построения операционных систем; - программные интерфейсы операционных систем; - виды политик управления доступом и информационными потоками применительно к операционным системам; - архитектуру подсистем защиты информации в операционных системах; - принципы функционирования средств защиты информации в операционных системах, в том числе использующих криптографические алгоритмы; - состав типовых конфигураций программно-аппаратных средств защиты информации; - требования по составу и характеристикам подсистем защиты информации применительно к операционным системам; - порядок реализации методов и средств антивирусной защиты в операционных системах; - программно-аппаратные средства и методы защиты информации в операционных системах; - принципы работы и правила эксплуатации программно-аппаратных средств защиты информации; - нормативные правовые акты в области защиты информации; - руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; - организационные меры по защите информации.	Индивидуальное задание	Модуль 1 0-20 «Неудовлетворительно» - 0-8 «Удовлетворительно» - 9-12 «Хорошо» - 13-16 «Отлично» -17-20
Уметь:		
- формулировать политики безопасности операционных систем; - настраивать политики безопасности операционных систем; - оценивать угрозы безопасности информации операционных систем; - противодействовать угрозам безопасности информации с использованием встроенных средств защиты информации операционных систем; - выбирать режимы работы программно-аппаратных средств защиты информации в операционных системах;	Индивидуальное задание	Модуль 1 0-10 «Неудовлетворительно» - 0-3 «Удовлетворительно» - 4-5 «Хорошо» - 6-7 «Отлично» -8-10

- настраивать антивирусные средства защиты информации в операционных системах; - устанавливать обновления программного обеспечения и средств антивирусной защиты; - проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах; - производить анализ эффективности программно-аппаратных средств защиты информации в операционных системах; - оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в операционных системах.		
Владеть:		
- определением состава применяемых программно-аппаратных средств защиты информации в операционных системах; - разработкой порядка применения программно-аппаратных средств защиты информации в операционных системах; - формированием шаблонов установки программно-аппаратных средств защиты информации в операционных системах; - установкой программно-аппаратных средств защиты информации в операционных системах, включая средства криптографической защиты информации; - конфигурированием программно-аппаратных средств защиты информации в операционных системах; - контролем корректности функционирования программно-аппаратных средств защиты информации в операционных системах; - управлением антивирусной защитой операционных систем в соответствии с действующими требованиями.	Индивидуальное задание	Модуль 1 0-10 «Неудовлетворительно» - 0-3 «Удовлетворительно» - 4-5 «Хорошо» - 6-7 «Отлично» -8-10
ПК-2: Администрирование программно-аппаратных средств защиты информации в компьютерных сетях		
Знать:		
- принципы построения компьютерных сетей; - стек сетевых протоколов операционных систем; - стек протоколов сетевого оборудования; - порядок реализации методов и средств межсетевого экранирования; - принципы функционирования сете-	Индивидуальное задание	Модуль 1 0-20 «Неудовлетворительно» - 0-8 «Удовлетворительно» – 9-12 «Хорошо» – 13-16 «Отлично» –17-20

вых протоколов, включающих криптографические алгоритмы; - виды политик управления доступом и информационными потоками в компьютерных сетях; - источники угроз информационной безопасности в компьютерных сетях и меры по их предотвращению; - состав типовых конфигураций программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях; - методы измерений, контроля и технических расчетов характеристик программно-аппаратных средств защиты информации; - принципы работы и правила эксплуатации эксплуатируемых программно-аппаратных средств защиты информации; - программно-аппаратные средства и методы защиты информации в компьютерных сетях; - нормативные правовые акты в области защиты информации; - руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; - организационные меры по защите информации.		
Уметь:		
- оценивать угрозы безопасности информации в компьютерных сетях; - настраивать правила фильтрации пакетов в компьютерных сетях; - обосновывать выбор используемых программно-аппаратных средств защиты информации в компьютерных сетях; - конфигурировать и контролировать корректность настройки программно-аппаратных средств защиты информации в компьютерных сетях; - выбирать режимы работы программно-аппаратных средств защиты информации в компьютерных сетях; - проводить мониторинг функционирования программно-аппаратных средств защиты информации в компьютерных сетях; - производить анализ эффективности программно-аппаратных средств защиты информации в компьютерных сетях;	Индивидуальное задание	Модуль 1 0-15 «Неудовлетворительно» - 0-5 «Удовлетворительно» – 6-9 «Хорошо» – 9-12 «Отлично» –12-15

сетях; - оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях.		
Владеть:		
- определением состава применяемых программно-аппаратных средств защиты информации в компьютерных сетях; - разработкой порядка применения программно-аппаратных средств защиты информации в компьютерных сетях; - формированием шаблонов конфигурации программно-аппаратных средств защиты информации в компьютерных сетях; - настройкой программных и аппаратных средств построения компьютерных сетей, использующих криптографическую защиту информации; - управлением функционированием программно-аппаратных средств защиты информации в компьютерных сетях; - контролем корректности функционирования программно-аппаратных средств защиты информации в компьютерных сетях; - управлением средствами межсетевого экранирования в компьютерных сетях в соответствии с действующими требованиями	Индивидуальное задание	Модуль 1 0-15 «Неудовлетворительно» - 0-5 «Удовлетворительно» – 6-9 «Хорошо» – 9-12 «Отлично» –12-15
ПК-3: Администрирование средств защиты информации прикладного и системного программного обеспечения		
Знать:		
- архитектуру подсистем защиты информации в операционных системах; - принципы построения систем управления базами данных; - основные средства и методы анализа программных реализаций; - принципы построения антивирусного программного обеспечения; - виды политик управления доступом и информационными потоками применительно к прикладному программному обеспечению; - источники угроз информационной безопасности программного обеспе-	Индивидуальное задание	Модуль 1 0-20 «Неудовлетворительно» - 0-7 «Удовлетворительно» – 8-12 «Хорошо» – 12-16 «Отлично» –16-20

чения и меры по их предотвращению; - уязвимости используемого программного обеспечения и методы их эксплуатации; - виды и формы функционирования вредоносного программного обеспечения; - характерные признаки наличия вредоносного программного обеспечения; - средства и методы обнаружения ранее неизвестного вредоносного программного обеспечения; - принципы функционирования программных средств криптографической защиты информации; - порядок обеспечения безопасности информации при эксплуатации программного обеспечения; - нормативные правовые акты в области защиты информации; - руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; - организационные меры по защите информации.		
Уметь:		
- анализировать угрозы безопасности информации программного обеспечения; - формулировать правила безопасной эксплуатации программного обеспечения; - обосновывать правила безопасной эксплуатации программного обеспечения; - анализировать функционирование программного обеспечения с целью определения возможного вредоносного воздействия; - производить проверку соответствия реальных характеристик программно-аппаратных средств защиты информации заявленным в их технической документации; - осуществлять мероприятия по противодействию угрозам безопасности информации, возникающим при эксплуатации программного обеспечения; - определять порядок функционирования программного обеспечения с	Индивидуальное задание	Модуль 1 0-15 «Неудовлетворительно» - 0-5 «Удовлетворительно» – 6-9 «Хорошо» – 9-12 «Отлично» –12-15

целью обеспечения защиты информации; - анализировать эффективность сформулированных требований к встроенным средствам защиты информации программного обеспечения.		
Владеть:		
- определением порядка установки программного обеспечения с целью соблюдения требований по защите информации; - контролем над соблюдением требований по защите информации при установке программного обеспечения, включая антивирусное программное обеспечение; - формулированием требований к параметрам средств антивирусной защиты для корректной работы программного обеспечения; - выполнением работ по обнаружению вредоносного программного обеспечения; - ликвидацией обнаруженного вредоносного программного обеспечения и последствий его функционирования; - формулированием требований к встроенным средствам защиты информации программного обеспечения.	Индивидуальное задание	Модуль 1 0-15 «Неудовлетворительно» - 0-5 «Удовлетворительно» – 6-9 «Хорошо» – 9-12 «Отлично» –12-15
	Зачет с оценкой	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

Модуль 1 (100 баллов):

Модуль содержит 216 часов самостоятельной работы в форме практической подготовки в организации, выбранной в качестве места практики, по итогам которой проводится зачет с оценкой – 2 часа. Максимальное количество баллов за модуль 1 составляет 100.

Типовой план проведения практики должен содержать следующие пункты:

- 1 Прохождение инструктажа по правилам и мерам безопасности.
- 2 Изучение требований безопасности на рабочем месте.
- 3 Проведение поиска и изучение нормативной и правовой документации в соответствии со списком рекомендованных источников.
- 5 Выполнение индивидуального задания.

6 Оформление дневника и отчета по практике.

7. Предоставление дневника и отчета о прохождении практики руководителю, защита отчета.

Все пункты плана практики устанавливаются руководителем практики. Данные пункты являются базовыми, но они могут быть дополнены или изменены исходя из индивидуальных особенностей обучающегося или в целях научно-исследовательской работы в филиале.

В индивидуальное задание выносятся вопросы, которые должны быть отражены в отчете по практике.

Типовой вариант индивидуального задания для прохождения практики:

1 Пройти инструктажа по правилам и мерам безопасности.

2 Изучить требования безопасности на рабочем месте.

4. Изучить правила организации рабочего места.

5. Выполнять обязанности должностного лица. Получить умения и навыки выполнения обязанностей, соответствующих должности, на которой проходит практика.

6. Вопросы, раскрываемые обучающимся в отчете о прохождении практики:

7. Оформить дневник и отчёт по практике.

8. Отчитаться о прохождении практики перед руководителем от предприятия и получить от него отзыв о работе.

Типовое индивидуальное задание

Тематика индивидуального задания может быть определена на основе текущих задач автоматизации подразделений профильной организации, согласованная предварительно с руководителем практики от образовательной организации.

Выполнение индивидуального задания состоит из пяти этапов.

-Первый этап. Руководителем практики определяются цели, задачи, структура, содержание практики; способы обработки и презентации результатов и отчетность по практике; правила техники безопасности.

-Второй этап. Практикант самостоятельно изучает структуру, организацию и основные виды деятельности в организации; технические средства сбора, обработки и передачи информации, используемые в организации; состояние и оборудование локальной сети организации. Ведет дневник по практике. При возникновении затруднений консультируется с руководителем практики.

-Третий этап. Практикант самостоятельно знакомится с программными средствами сбора, обработки и передачи информации, используемыми в организации. Получает опыт и навыки работы с профессиональным ПО организации. Изучает обобщенные технологические процессы сбора, передачи, обработки и выдачи информации, применяемые в организации. Ведет дневник по практике. При возникновении затруднений консультируется с руководителем практики.

- Четвёртый этап. Практикант под руководством руководителя выполняет индивидуальное задание. Ведет дневник по практике. При возникновении затруднений консультируется с руководителем практики.

-Пятый этап. Практикант оформляет дневник и подготавливает отчет по практике.

1.3.2 Оценочные материалы промежуточной аттестации для очной формы обучения

По результатам освоения программы практики обучающиеся представляют письменный отчёт с промежуточной аттестацией в форме зачета с оценкой.

Отчёт о прохождении практики должен содержать текстовую часть и приложения. В нём излагаются результаты прохождения практической подготовки в соответствии с индивидуальным заданием.

Примерный перечень вопросов, выносимых на защиту отчета о практике:

1. Архитектура и принципы построения операционных систем (ПК-1);

2. Программные интерфейсы операционных систем (ПК-1);

3. Виды политик управления доступом и информационными потоками применительно к операционным системам (ПК-1);

4. Архитектура подсистем защиты информации в операционных системах (ПК-1);

5. Принципы функционирования средств защиты информации в операционных системах, в том

числе использующих криптографические алгоритмы (ПК-1);

6. Состав типовых конфигураций программно-аппаратных средств защиты информации (ПК-1);
7. Порядок реализации методов и средств антивирусной защиты в операционных системах (ПК-1);
8. Программно-аппаратные средства и методы защиты информации в операционных системах (ПК-1);
9. Нормативные правовые акты в области защиты информации (ПК-1);
10. Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации (ПК-1);
11. Организационные меры по защите информации (ПК-1);
12. Виды политик управления доступом и информационными потоками в компьютерных сетях (ПК-2);
13. Источники угроз информационной безопасности в компьютерных сетях и меры по их предотвращению (ПК-2);
14. Методы измерений, контроля и технических расчетов характеристик программно-аппаратных средств защиты информации (ПК-2);
15. Принципы работы и правила эксплуатации эксплуатируемых программно-аппаратных средств защиты информации (ПК-2);
16. Программно-аппаратные средства и методы защиты информации в компьютерных сетях (ПК-2);
17. Принципы построения систем управления базами данных (ПК-3);
18. Основные средства и методы анализа программных реализаций (ПК-3);
19. Принципы построения антивирусного программного обеспечения (ПК-3);
20. Виды политик управления доступом и информационными потоками применительно к прикладному программному обеспечению (ПК-3);
21. Источники угроз информационной безопасности программного обеспечения и меры по их предотвращению (ПК-3);
22. Уязвимости используемого программного обеспечения и методы их эксплуатации (ПК-3);
23. Виды и формы функционирования вредоносного программного обеспечения (ПК-3);
24. Средства и методы обнаружения ранее неизвестного вредоносного программного обеспечения (ПК-3);
25. Принципы функционирования программных средств криптографической защиты информации (ПК-3);
26. Порядок обеспечения безопасности информации при эксплуатации программного обеспечения (ПК-3);
27. Нормативные правовые акты в области защиты информации (ПК-3);

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 – проводится в форме контроля на каждом этапе практической подготовки в соответствии с планом практики в процессе работы обучающегося в рамках его индивидуального задания.

- промежуточная аттестация – проводится в форме зачета с оценкой.

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

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

Правила ее использования прописаны в «Положении об МРС».

Набранные обучающимся 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 обучающимся по блокам модулей, показаны в Таблице.

Таблица - Распределение баллов по блокам модулей Производственная (преддипломная) практика

Модуль	Всего баллов (Максимальное значение)	Теоретический блок	Практический блок (контрольные вопросы)
Модуль 1	100	0	100
Зачет с оценкой	100	100	

3 Промежуточная аттестация

Промежуточная аттестация проводится в форме зачета с оценкой. Аттестацию обучающихся по итогам практики проводит руководитель практики от СКФ МТУСИ на основании оформленного отчета. Защита отчета проводится в форме индивидуального собеседования.

Результаты аттестации заносятся в ведомость и зачетную книжку обучающегося.

4 Тестовые задания по дисциплине Б2.В.03(Пд) Производственная (преддипломная) практика

Тестовые задания позволяют оценить уровень сформированности 3-х компетенций:

ПК-1 Администрирование подсистем защиты информации в операционных системах;

ПК-2 - Администрирование программно-аппаратных средств защиты информации в компьютерных сетях;

ПК-3 - Администрирование средств защиты информации прикладного и системного программного обеспечения

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

Базовый уровень (Блок А) 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 (Блок Б) в среднем составляет 35 % заданий.

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

Высокий уровень (Блок В) 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 из компетенции равно 20, Всего 60 заданий.

Комплект тестовых вопросов с указанием правильных ответов хранится у заведующего кафедрой.

ПК-1 Администрирование подсистем защиты информации в операционных системах

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	Библиографический список означает: 1. Список авторов и соавторов; 2. Список использованных источников; 3. Список биографии; 4. Список печатных изданий.
2	К нормативно-технической документации относятся: 1. Технический паспорт 2. Инструкция по эксплуатации 3. Формуляр 4. Параграф 5. Рецепт
3	К поисковым системам относятся: 1. Ali Express 2. Yandex 3. Rambler 4. Google
4	К локальным нормативным актам относятся: 1. Распорядок дня 2. Должностные инструкции 3. Приказы Министерств и ведомств 4. Методические указания 5. Постановления Правительства
5	Выпускная квалификационная работа в комплекте и рецензия, приложенная к ней, передаются в государственную экзаменационную комиссию не позднее, чем 1. За 5 календарных дней до дня защиты выпускной квалификационной работы. 2. За 3 календарных дня до дня защиты выпускной квалификационной работы. 3. За 2 календарных дня до дня защиты выпускной квалификационной работы.

№ задания	Тексты заданий
6	Предварительная защита выпускной квалификационной работы проводится не позднее, чем 1. За 5 дней до назначенного срока защиты. 2. За 7 дней до назначенного срока защиты. 3. За 3 дня до назначенного срока защиты.
7	В течение какого количества дней после утверждения перечень объектов КИИ в печатном и электронном виде направляется в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры. 1. 5 2. 7 3. 10 4. 30
8	Непредставление или нарушение порядка либо сроков представления в ФСТЭК РФ, сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий, предусмотренных законодательством в области обеспечения безопасности КИИ РФ, влечет наложение административного штрафа: 1. На должностных лиц - от десяти тысяч до пятидесяти тысяч рублей; 2. На должностных лиц - от 100 тысяч до пятисот тысяч рублей; 3. На должностных лиц - от одной тысячи до пяти тысяч рублей.
9	К инженерно-техническим средствам защиты относятся 1. Системы шифрования информации 2. Применение звукоизолирующих материалов 3. Подготовка документации на состав компьютеров 4. Прием на работу сотрудников на должность системных администраторов 5. Установка на компьютер антивирусной программы.
10	Приказ ФСТЭК России от 22 декабря 2017 г. № 236 называется 1. «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» 2. «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий». 3. «О безопасности критической информационной инфраструктуры Российской Федерации».

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

Инструкция: Прочитайте текст и установите соответствие

№ задания	Тексты заданий
11	Установите соответствие систем их назначению 1. DLP; 2. IRP; 3. SIEM; 4. SOC; 5. Deception. А. Централизованная система управления ложными сетевыми объектами, которые принято называть ловушками; Б. Центр мониторинга и реагирования на инциденты информационной безопасности. Специальное подразделение, которое круглосуточно следит за ИТ-инфраструктурой компании; В. Система управления информационной безопасностью и событиями безопасности. Г. Платформа реагирования на инциденты Д. Система предотвращения утечек информации
12	Объектам критической информационной инфраструктуры (КИИ) присваивают одну из трёх категорий значимости: 1. Первая категория; 2. Вторая категория; 3. Третья категория. Расставьте в соответствии тем последствиям, которые характеризуют данные категории А. Локальные последствия, затрагивающие отдельные подразделения, организации, процессы; Б. Серьёзные последствия на уровне отрасли, региона, крупных экономических потерь; В. Массовые сбои, угроза жизни, национальной безопасности.
13	Поставьте в соответствие названия различных устройств в составе компьютера единицам измерения их

№ задания	Тексты заданий
	параметров 1. Разрешение 2. Количество операций в секунду 3. Скорость передачи информации 4. Скорость чтения-записи 5. Наличие различных портов А. Жесткий диск Б. Системная плата В. Графический адаптер Г. Сетевой адаптер Д. Процессор
14	К классам критических процессов организации могут относиться: 1. Управленческие 2. Технологические 3. Производственные 4. Финансово-экономические Поставьте в соответствие классам процессов виды деятельности А. Экспертно-аналитическая деятельность Б. Эксплуатация информационно-вычислительной системы В. Создание и сопровождение информационных ресурсов Г. Планирование поставок комплектующих для производства 1-А 2-Б 3-В 4-Г

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

Инструкция: Прочитайте текст и установите правильную последовательность

№ задания	Тексты заданий
15	Расставьте в правильном порядке наименования разделов ВКР 1. Список использованных источников 2. Введение 3. Аннотация 4. Приложения 5. Основные разделы 6. Заключение
16	Расставьте правильный порядок действий при подготовке ВКР 1. Подготовка пояснительной записки 2. Получение задания от руководителя ВКР 3. Определение тематики и выбор руководителя ВКР 4. Написание заявления на утверждение темы ВКР 5. Защита ВКР
17	Основные этапы реагирования на инциденты включают: 1. Предотвращение повторения 2. Анализ и документирование инцидента 3. Восстановление системы 4. Изоляция и устранение угрозы 5. Оценка инцидента 6. Обнаружение инцидента

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

Инструкция: Прочитайте текст и запишите обоснованный ответ

№ задания	Тексты заданий
18	_____ ВКР должна содержать краткие сведения о содержании работы и итогах ее проведения
19	В тексте пояснительной записки ВКР, за исключением формул, _____, не допускается применять без числовых значений следующие математические знаки: > (больше); < (меньше); = (равно); ≥ (больше или равно); ≠ (не равно); ≤ (меньше или равно), а также знаки: % (процент), № (номер)
20	Микроконтроллер имеет _____ архитектуру, которая отделяет память программ от пространства данных. Все компоненты (процессор, память, ввод-вывод) интегрированы на одном чипе.

Система оценивания выполнения тестовых заданий по компетенции ПК-1, формируемой дисциплиной Б2.В.03(Пд) Производственная (преддипломная) практика

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.

ПК-2 - Администрирование программно-аппаратных средств защиты информации в компьютерных сетях;

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	Какими русскими буквами нельзя обозначать Приложения в ВКР? 1. Ё 2. Ъ 3. Ь 4. Й 5. Ю 6. Э
2	Межгосударственный стандарт «Единая система конструкторской документации ОБЩИЕ ТРЕБОВАНИЯ К ТЕКСТОВЫМ ДОКУМЕНТАМ» является: 1. ГОСТ 7.32–2001 2. ГОСТ 7.9–95 3. ГОСТ 2.105-95 4. ГОСТ 2.104–2006
3	Какой может быть нумерация рисунков и таблиц в пояснительной записке ВКР? 1. Сквозная 2. По отдельная 3. Сокращенная 4. Обратная
4	Рекомендуемое количество слайдов при защите ВКР должно составлять: 1. Не менее 5 и не более 12 2. Не менее 8 и не более 18 3. Не менее 10 и не более 20
5	При проведении нормоконтроля проверяется: 1. Правильность оформления таблиц, иллюстраций, приложений 2. Наличие и правильность ссылок на стандарты и другие нормативные документы 3. Правильность нумерации и оформления наименований разделов и подразделов, иллюстраций и таблиц, списка использованных источников и соответствие их содержанию 4. Правильность проведенных в работе расчетов
6	Продолжительность доклада при защите ВКР должна составлять: 1. 8-10 мин 2. 10-15 мин 3. 4-6 мин 4. Время не ограничено
7	Обучающиеся, не прошедшие государственной итоговой аттестации в связи с неявкой на государственное аттестационное испытание по уважительной причине, вправе пройти ее в течение: 1. 1 месяца после завершения государственной итоговой аттестации 2. 1 года после завершения государственной итоговой аттестации 3. 6 месяцев после завершения государственной итоговой аттестации
8	Комиссию по категорированию может возглавлять 1. Руководитель субъекта критической информационной инфраструктуры 2. Уполномоченное руководителем критической информационной инфраструктуры лицо. 3. Представитель государственных органов 4. Представитель российских юридических лиц
9	Порт компьютера это 1. Число, определяющее программу, для которой адресован сетевой пакет. 2. Один из многочисленных разъёмов компьютера 3. Игровая приставка 4. Специальная программа для организации сети
10	В качестве возможных последствий нарушений ИБ КИИ определяются следующие: 1) причинение ущерба жизни и здоровью людей; 2) прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения, в том числе объектов обеспечивающие водо-, тепло-, газо- и электроснабжение населения; 3) прекращение или нарушение функционирования объектов транспортной инфраструктуры, в том числе

№ задания	Тексты заданий
	высокоавтоматизированных транспортных средств; 4) прекращение или нарушение функционирования сети связи, оцениваемые по количеству абонентов, для которых могут быть недоступны услуги связи; 5) отсутствие доступа к государственной услуге;

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

Инструкция: Прочитайте текст и установите соответствие

№ задания	Тексты заданий
11	Расставьте в соответствии - ГОСТ Р 7.0.5–2008 - ГОСТ 2.105–95 - ГОСТ 19.201-78 - ГОСТ 19.701-90 А. Схемы алгоритмов, программ, данных и систем. Условные обозначения и правила выполнения Б. Техническое задание. Требования к содержанию и оформлению В. Общие требования к текстовым документам Г. Библиографическая ссылка. Общие требования и правила составления
12	Существуют 3 категории значимости объектов критической информационной инфраструктуры Российской Федерации и их значений - категория - категория - категория Расставьте в соответствие номеру категории количество человек, которому может быть причинен ущерб по социальной значимости: - Более 500 - Более или равно 1, но менее или равно 50 - более 50, но менее или равно 500
13	Наиболее известные антивирусные комплексы - Доктор Веб - ESET - Avira - Avast Software - Symantec Расставьте антивирусные комплексы в соответствии со страной-производителем - США - Чехия - Германия - Россия - Словакия
14	Для обнаружения и нейтрализации информационных инцидентов используются системы: - Deception - DLP - SOC - SIEM - IDS/IPS Расставьте их по их основному функционалу - Система предотвращения утечек - Центр реагирования на инциденты - Система управления событиями безопасности - Системы обнаружения и предотвращения вторжений - Система организации киберобмана

БЛОК Б (повышенный уровень) – Задание закрытого типа на установление последовательности
Инструкция: Прочитайте текст и установите правильную последовательность

№ задания	Тексты заданий
15	Расставьте в правильном порядке последовательность разделов технического задания на создание программного продукта 1. Требования к программе 2. Функциональное назначение разработки 3. Основания для разработки 4. Введение 5. Требования к программной документации 6. Стадии и этапы разработки
16	Расставьте в порядке повышения эффективности поисковые устройства для обнаружения закладных электронных устройств – 1. Нелинейные локаторы, 2. Индикаторы поля, 3. Досмотровые зеркала, 4. Анализаторы спектра.
17	Расставьте в порядке увеличения значимости нормативные акты, регламентирующие вопросы информационной безопасности: 1. Локальные нормативные акты; 2. Приказы соответствующих Министерств и Ведомств; 3. Законы РФ; 4. Указы Президента РФ; 5. Конституция РФ; 6. Постановления Правительства РФ.

БЛОК В (высокий уровень) – Задание открытого типа с развернутым ответом
Инструкция: Прочитайте текст и запишите обоснованный ответ

№ задания	Тексты заданий
18	В разделе _____ выпускной квалификационной работы должны содержаться: анализ результатов выполненной работы, оценка полноты решения поставленных задач, рекомендации по конкретному использованию результатов работы, ее экономическая, научная, социальная значимость.
19	Лицо, не прошедшее государственную итоговую аттестацию, может повторно пройти государственную итоговую аттестацию не ранее чем через _____ и не позднее чем через _____ после срока проведения государственной итоговой аттестации, которая не пройдена обучающимся.
20	К _____ средствам ИС относятся: - средства вычислительной техники общего назначения, - защищенные средства вычислительной техники, - средства связи и периферийные устройства, - локальные вычислительные сети, - глобальные вычислительные сети.

Система оценивания выполнения тестовых заданий по компетенции ПК-2, формируемой дисциплиной Б2.В.03(Пд) Производственная (преддипломная) практика

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.

ПК-3 - Администрирование средств защиты информации прикладного и системного программного обеспечения

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	Минимальный и максимальный объем пояснительной записки ВКР должен составлять: 1. 40 и 80 2. 50 и 100 3. 30 и 120 4. 70 и 150
2	Количество оригинального текста в ВКР должно быть не менее: 1. 30% 2. 50% 3. 70%
3	В состав пояснительной записки ВКР входят: 1. Титульный лист. 2. Реферат. 3. Введение. 4. Рецензия. 5. Заключение 6. Список использованных источников
4	Выберите правильную подрисуночную подпись 1. Рисунок 1.1– Алгоритм работы программы 2. Рис. 1.1– Алгоритм работы программы 3. Рис. 1.1
5	Формулы в пояснительной записке ВКР могут нумероваться 1. Сквозной нумерацией 2. В пределах раздела 3. Обратной нумерацией 4. В пределах пункта
6	С какой периодичностью осуществляется пересмотр установленных категорий значимости или решений об отсутствии необходимости присвоения объектам таких категорий 1. 1 раз в 3 года 2. 1 раз в 5 лет 3. 1 раз в 10 лет 4. 1 раз в 15 лет
7	К нормативным правовым актам, посвященным критической информационной инфраструктуре относятся: 1. Федеральный закон от 26 июля 2017 г. N 187-ФЗ 2. Постановление Правительства Российской Федерации от 17 февраля 2018 г. N 162 3. Постановление Правительства Российской Федерации от 8 февраля 2018 г. N 127 4. Приказ ФСТЭК России от 20 апреля 2023 г. N 69 5. Приказ ФСТЭК России от 21 декабря 2017 г. N 235 6. Приказ ФСТЭК России от 22 декабря 2017 г. N 236 7. Приказ ФСТЭК России от 25 декабря 2017 г. N 239 8. Все перечисленные
8	ГОССОПКА это 1. Государственная система по охране окружающей среды 2. Государственная система по разработке полезных ископаемых на холмах и сопках. 3. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы. 4. Государственная система передачи информации об информационных инцидентах.
9	Организовав взаимодействие с ГосСОПКА, любой участник ГосСОПКА сможет получать от Национального координационного центра по компьютерным инцидентам (НКЦКИ): 1. Сведения об актуальных угрозах и уязвимостях; 2. Сведения о признаках компьютерных инцидентов;

№ задания	Тексты заданий
	3. Индикаторы вредоносной активности; 4. Сведения о способах и средствах проведения компьютерных атак; 5. Адресные рекомендации по защите; 6. Дополнительное оборудование.
10	К критической информационной инфраструктуре (КИИ) могут относиться: 1. Информационные системы; 2. Информационно-телекоммуникационные сети; 3. Автоматизированные системы управления; 4. Сети электросвязи; 5. Домашние компьютеры; 6. Компьютерные классы.

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

Инструкция: Прочитайте текст и установите соответствие

№ задания	Тексты заданий
11	Объектам критической информационной инфраструктуры (КИИ) присваивают одну из трёх категорий значимости: 1. Первая категория; 2. Вторая категория; 3. Третья категория. Расставьте в соответствии тем последствиям, которые характеризуют данные категории А. Локальные последствия, затрагивающие отдельные подразделения, организации, процессы; Б. Серьёзные последствия на уровне отрасли, региона, крупных экономических потерь; В. Массовые сбои, угроза жизни, национальной безопасности.
12	Заголовки определенных разделов ВКР оформляются по разному. Поставьте в соответствие название заголовка его правилу оформления 1. Введение 2. Заголовок раздела 3. Заголовок подраздела 4. Пункт подраздела А. Размещается в тексте Б. С абзацного отступа таким же шрифтом и выравниванием по ширине страницы, как и последующий текст. Отделяется от последующего текста пустой строкой В. С абзацного отступа, шрифтом несколько большего размера и выравниванием по ширине страницы, как и последующий текст Г. Прописными буквами в начале страницы с выравниванием по центру
13	Критерии значимости объектов критической информационной инфраструктуры подразделяются на 1. Социальная 2. Политическая 3. Экономическая 4. Экологическая 5. Значимость для обеспечения обороны страны, безопасности государства и правопорядка Установите соответствие критерия значимости его содержанию А. Прекращение или нарушение проведения учетно-расчетных операций Б. Причинение ущерба жизни и здоровью людей В. Прекращение или нарушение функционирования государственного органа Г. Снижение показателей государственного оборонного заказа, Д. Вредные воздействия на окружающую среду
14	Киберполигоны предназначены для отработки практических навыков выявления и реагирования на инциденты информационной безопасности. Расставьте в соответствии названия киберполигона и страны-разработчика 1. Ampire 2. Cyberbit 3. Pengcheng 4. National Cyber Range А. США Б. Китай В. Россия Г. Израиль

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

Инструкция: Прочитайте текст и установите правильную последовательность

№ задания	Тексты заданий
15	Установить правильный порядок действий при управлении инцидентами 1. Выработка рекомендации для совершенствования системы ИБ 2. Реализация превентивных мер 3. Расследование 4. Меры реагирования на инциденты 5. Устранение причин и последствий 6. Регистрация инцидента 7. Оповещение о возникновении 8. Выявление и классификация инцидента
16	Установить правильный порядок действий по категорированию объектов критической информационной инфраструктуры (КИИ) 1. Направление сведений о результатах категорирования в ФСТЭК России; 2. Подготовка акта категорирования объекта КИИ; 3. Категорирование объектов КИИ; 4. Определение перечня объектов КИИ, подлежащих категорированию; 5. Формирование исходных данных для категорирования; 6. Создание комиссии по категорированию.
17	Категорирование объектов КИИ регулируется Федеральным законом №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и Постановлением Правительства РФ №127. Процесс включает несколько этапов: 1. Утверждение и регистрация — результаты категорирования утверждаются в установленном порядке, данные о категорированных объектах заносятся в реестр значимых объектов КИИ РФ. 2. Идентификация объектов — определение информационных систем, сетей и систем управления, которые могут быть отнесены к критическим; 3. Присвоение категории — комиссия присваивает категорию на основе оценки; 4. Оценка значимости — анализ возможных последствий утраты конфиденциальности, целостности или доступности информации; Расставьте эти этапы в правильном порядке

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

Инструкция: Прочитайте текст и запишите обоснованный ответ

№ задания	Тексты заданий
18	Буквы русского и греческого алфавитов, а также цифры набираются _____ шрифтом.
19	_____ на создание программного продукта включает в себя: 1 Введение 2 Основания для разработки 3 Функциональное назначение разработки 4 Требования к программе 5 Требования к программной документации 6 Стадии и этапы разработки
20	Рекомендуемый для текста ВКР размер шрифта равен _____

Система оценивания выполнения тестовых заданий по компетенции ПК-3, формируемой дисциплиной Б2.В.03(Пд) Производственная (преддипломная) практика

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.