УТВЕРЖДАЮ
Заместитель директора по
учебной работе
_____ И. В. Иванешко
«30» 08 2023 г.

Согласовано
Руководитель направления Управления безопасности Смоленского филиала
ПАО «Ростелеком» «30» 08 2023г.
_____ Петров В.А.

Контрольно-оценочные материалы для промежуточной аттестации
ОП.08 Организационно-правовое обеспечение информационной безопасности
для специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

Дифференцируемый зачет является промежуточной формой контроля, подводит итог освоения дисциплины ОП.08 Организационно-правовое обеспечение информационной безопасности.

Профессиональные компетенции:

ПК 1.4. Осуществлять контроль функционирования информационно-телекоммуникационных систем и сетей.

ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных систем и сетей.

ПК 3.2. Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в информационно-телекоммуникационных системах и сетях.

Общие компетенции:

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.

ОК 09. Использовать информационные технологии в профессиональной деятельности.

Дифференцированный зачет по МДК.01.02 Математический аппарат для построения компьютерных проводится в форме тестирования.

Тест содержит 10 вопросов (суммарно тестовых позиций и теоретических вопросов с кратким ответом), выбираемых случайным образом программой из каждого блоков (состоящих первый блок 35 вопросов, второй блок 25 вопросов) заданий по 5 вопросов. Время тестирования – 45 минут для каждой подгруппы (по 3 минуты на каждый вопрос из первого блока, по 6 минут на каждый вопрос закрытого типа).

Критерии оценивания

«5» - получают студенты, справившиеся с работой 100-90%;
«4» - ставится в том случае, если верные ответы составляют 89-75% от общего количества;
«3» - соответствует работа, содержащая 60-74% правильных ответов;
«2» - соответствует работа, содержащая менее 60% правильных ответов.

Шкала оценивания образовательных результатов:

Оценка	Критерии
«отлично»	Студент набрал 5 баллов (по весу критерия)
«хорошо»	Студент набрал 4 балла (по весу критерия)
«удовлетворительно»	Студент набрал 3 балла (по весу критерия)
«неудовлетворительно»	Студент набрал 0-2 балла (по весу критерия)

Первый блок

Формируемые компетенции ОК1, ОК2, ОК3, ОК9, ПК 1.4, ПК 2.1, ПК 3.2

№	ПК	Формулировка вопроса	Варианты ответов
1	ПК 1.4 ПК 2.1 ПК 3.2	Какой закон регулирует отношения, возникающий при: 1) осуществлении права на поиск, получение, передачу, производство и распространение информации; 2) применении информационных технологий; 3) обеспечении защиты информации?	1) Федеральный закон «Об информации, информационных технологиях и о защите информации» 2) Федеральный закон «Об информации, и о защите информационных технологиях» 3) Федеральный закон «Об информации»
2	ПК 2.1 ПК 3.2	На скольких принципах основывается правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации?	1) 6 2) 7 3) 8
3	ПК 1.4	На что подразделяется информация в зависимости от порядка ее предоставления или распространения? (выберите несколько вариантов правильных ответов)	1) информацию, свободно распространяемую; 2) информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях; 3) информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению; 4) информацию, распространение которой в Российской Федерации ограничивается или запрещается.
4	ПК 1.4 ПК 2.1 ПК 3.2	Что обязан обладатель информации при осуществлении своих прав? (выберите несколько вариантов правильных ответов)	1) соблюдать права и законные интересы иных лиц; 2) принимать меры по защите информации; 3) ограничивать доступ к информации, если такая обязанность установлена федеральными законами. 4) соблюдать правила передачи информации.
5	ПК 2.1 ПК 3.2	Защита информации, составляющей государственную тайну, осуществляется в соответствии с каким законодательством?	1) законодательством Российской Федерации о государственной тайне; 2) законодательством Российской Федерации о государственной и коммерческой тайне;

6	ПК 1.4 ПК 2.1 ПК 3.2	Что предусматривает государственное регулирование в сфере применения информационных технологий? (выберите несколько правильных вариантов ответа)	1) регулирование отношений, связанных с поиском, получением, передачей, производством и распространением информации с применением информационных технологий (информатизации), на основании принципов, установленных настоящим Федеральным законом; 2) развитие информационных систем различного назначения для обеспечения граждан (физических лиц), организаций, государственных органов и органов местного самоуправления информацией, а также обеспечение взаимодействия таких систем; 3) создание условий для эффективного использования в Российской Федерации информационно - телекоммуникационных сетей, в том числе сети "Интернет" и иных подобных информационно-телекоммуникационных сетей; 4) обеспечение информационной безопасности детей.
7.	ПК 1.4 ПК 2.1 ПК 3.2	Что создается в целях расширения использования российских программ для электронных вычислительных машин и баз данных, подтверждения их происхождения из Российской Федерации, а также в целях оказания правообладателям программ для электронных вычислительных машин или баз данных мер государственной поддержки?	1) создается единый реестр российских программ для электронных вычислительных машин и баз данных; 2) создается единый реестр российских программ баз данных.
8.	ПК 1.4 ПК 2.1 ПК 3.2	Государственные органы, банки и иные организации в случаях, определенных федеральными законами, после проведения идентификации при личном присутствии физического лица с его согласия на безвозмездной основе, что размещают в электронной форме? (выберите несколько правильных вариантов ответа)	1) сведения, необходимые для регистрации физического лица в единой системе идентификации и аутентификации, и иные сведения, если такие сведения предусмотрены федеральными законами, - в единой системе идентификации и аутентификации; 2) биометрические персональные данные физического лица - в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица (далее - единая биометрическая система).
9	ПК 1.4 ПК 2.1	Какие меры входят в состав мер по защите персональных дан-	1) использование системы идентификации и аутентификации (авториза-

	ПК 3.2	ных согласно требованиям ФСТЭК**?** (выберите несколько правильных вариантов ответа)	ции) субъектов, имеющих доступ к ПНд, и объектов ПНд; 2) возможность ограничения и управления правами доступа к персональной информации; 3) физическая и программная защита носителей информации; 4) регистрация событий безопасности и ведение их журнала; 5) применение средств антивирусной защиты; 6) регулярный контроль защищенности ПНд; 7) обнаружение и предотвращение вторжений, несанкционированного доступа; 8) обеспечение доступности хранимых сведений, их и информационной системы, базы данных доступности; 9) соблюдение требований по защите среды виртуализации, технических средств, информационной системы (ИС), ее средств, каналов и линий связи и передачи данных.
10	ПК 1.4 ПК 2.1 ПК 3.2	Согласно ли с данным высказыванием? Согласно требованиями ФСТЭК России по защите персональных данных предусмотрено наличие возможности управления конфигурацией ИС, своевременного выявления инцидентов, способных привести к сбоям в работе ИС, возникновению угроз безопасности ПНд.	1) Да 2) Нет
11	ПК 1.4 ПК 2.1 ПК 3.2	На что распространяются требования ФСТЭК по технической защите информации? (Выберите несколько правильных ответов)	1) программное обеспечения и оборудование; 2) внешние носители; 3) средства связи и шифровки/дешифровки данных; 4) операционные системы; 5) прочие технические средства хранения, обработки, передачи сведений; 6) персональные данные; 7) специалистов по обеспечению информационной безопасности.
12	ПК 1.4 ПК 2.1	Какие меры по защите персональных данных согласно требованиям ФСТЭК Вы знаете?	1) использование системы идентификации и аутентификации (авторизации) субъектов, имеющих доступ к ПНд, и объектов ПНд; 2) возможность ограничения и управления правами доступа к персональной информации; 3) физическая и программная защита носителей информации;

13	ПК 1.4 ПК 2.1 ПК 3.2	Согласны ли Вы с данным утверждением? Существует регламентация разработки систем и введения их в эксплуатацию, разграничения уровней доступности, проведения проверок и анализ реакций, ответственных за организацию защиты специалистов. Лишь после проведения совокупности мероприятий информационная система аттестуется, вводясь в эксплуатацию.	1) Да 2) Нет
14	ПК 2.1 ПК 3.2	Верно ли данное утверждение? ФСТЭК не рекомендует использовать такие методы по защите информации как контроль доступа к носителям данных и ИС (физический, аппаратный, программный и т.д.), шифрование передаваемых сведений.	1) Да 2) Нет
15	ПК 2.1 ПК 3.2	На каких основополагающих элементах строиться система документов по технической защите информации? (Выберите несколько правильных ответов.)	1) федеральное законодательство; 2) устав документов; 3) распоряжения и указы Президента РФ; 4) постановления правительства РФ; 5) документация ФСБ, ФСТЭК, Роскомнадзора; 6) общероссийские стандарты; 7) документы руководящие, нормативно-методические.
16	ПК 1.4 ПК 2.1 ПК 3.2	Сколько классов средств защиты информации ФСТЭК существует?	1) 8 2) 5 3) 7
17.	ПК 1.4 ПК 2.1 ПК 3.2	Какие задачи решает система защиты информации? (Выберите несколько парильных ответов.)	1) исключение неправомерных действий: доступа, копирования, предоставления или распространения информации (обеспечение конфиденциальности информации); 2) исключение неправомерных вторжений на территорию организации; 3) исключение неправомерного уничтожения или модифицирования информации (обеспечение целостности информации); 4) исключение неправомерного блокирования информации (обеспечение доступности информации).
18	ПК 3.2	Поставьте в соответствие номер этапа стадии создания системы защиты информации и его название.	1. Этап 1. 2. Этап 2. 3. Этап 3 4. Этап 4.

			А) Разработка системы защиты информации (этап проектирования). Б) Формирование требований к системе защиты информации (предпроектный этап). В) Внедрение системы защиты информации (этап установки, настройки, испытаний). С) Подтверждение соответствия системы защиты информации (этап оценки).
19	ПК 1.4 ПК 2.1 ПК 3.2	Каким бывает контроль состояния системы защиты информации?	1) Внешний контроль; 2) Соседский контроль; 3) Внутренний контроль.
20	ПК 2.1 ПК 3.2	Какое средство вычислительной техники, осуществляющее криптографическое преобразование информации для обеспечения ее безопасности?	1) Средство криптографической защиты информации (СКЗИ); 2) Средство биометрической защиты информации.
21	ПК 1.4 ПК 2.1 ПК 3.2	Как Вы считаете верно ли данное высказывание? На технических средствах АРМ с установленным СКЗИ необходимо использовать только лицензионное программное обеспечение фирм-изготовителей, полученное из доверенных источников.	1) Нет 2) да
22	ПК 1.4 ПК 2.1 ПК 3.2	Какие самые распространенные виды информационно-телекоммуникационных сетей Вы знаете? (Выберите несколько правильных ответов)	1) Корпоративные информационные сети; 2) Локальная сеть; 3) Сеть международного обмена «Интернет».
23	ПК 1.4 ПК 2.1	Согласны ли Вы с утверждением? Централизованное управление сетью связи общего пользования осуществляется путем управления техническими средствами противодействия угрозам и (или) путем передачи обязательных к выполнению указаний операторам связи, собственникам или иным владельцам технологических сетей связи, собственникам или иным владельцам точек обмена трафиком, собственникам или иным владельцам линий связи, пересекающих Государственную границу Российской Федерации, иным лицам, если такие лица имеют номер автономной системы (далее также - лица, участвующие в централизованном управлении).	1) Да 2) Нет

24	ПК 1.4 ПК 2.1 ПК 3.2	Какие категорий риска причинения вреда (ущерба) (далее - категории риска) информационно-телекоммуникационных систем и сетей Вы знаете?	1) значительный риск; 2) умеренный риск; 3) низкий риск; 4) высокий риск.
25	ПК 1.4 ПК 2.1 ПК 3.2	Верно ли данное высказывание? Использование на территории Российской Федерации информационно-телекоммуникационных сетей в хозяйственной или иной деятельности может служить основанием для установления дополнительных требований или ограничений, касающихся регулирования указанной деятельности, осуществляемой без использования таких сетей, а также для несоблюдения требований, установленных федеральными законами.	1) Да 2) Нет
26	ПК 1.4 ПК 2.1	В соответствии с Федеральным законом «О связи», различают какие категории сетей?	1) сеть связи общего пользования; 2) выделенные сети связи; 3) технологические сети связи, присоединенные к сети связи общего пользования; 4) сети связи специального назначения и другие сети связи для передачи информации при помощи электромагнитных систем.
27	ПК 1.4 ПК 2.1	Что называют совокупностью программ для электронных вычислительных машин и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет") по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в сети "Интернет"?	1) Интернет 2) сайт в сети "Интернет" 3) электронная почта
28	ПК 1.4 ПК 2.1 ПК 3.2	На каких стадиях и этапах создания АСЗИ с учетом применимых (исходя из предназначения АСЗИ) требований нормативных правовых актов и методических документов уполномоченных федеральных органов исполнительной власти и национальных стандартов в области ЗИ, должны проводится мероприятиях по ЗИ?	1) На первых; 2) На последних; 3) На всех.

29	ПК 1.4 ПК 2.1 ПК 3.2	Какие нарушения требований по обеспечению персональных данных Вы знаете? (Выберите несколько правильных ответов).	1) Отсутствие актуального сертификата соответствия СКЗИ; 2) Отсутствие журналов учета или нерегулярное их заполнение; 3) Отсутствие дистрибутивов СКЗИ, формуляров, документов; 4) Недостаточные меры по обеспечению физической защиты; 5) Использование СКЗИ класса ниже необходимого. 6) Некорректно разработанная модель угроз.
30	ПК 1.4 ПК 2.1 ПК 3.2	Для оценки степени негативных последствий централизованных информационных систем рекомендуется использовать методики, определенные в каких ГОСТ?	1) ГОСТ 13335-3: 2007 2) ГОСТ 13569: 2007 3) ГОСТ 13588: 2007
31	ПК 1.4 ПК 2.1 ПК 3.2	Согласны ли Вы с утверждением? Все СЗИ, применяемые для защиты ЦИС, должны использовать встроенные механизмы защиты от НСД.	1) Да 2) Нет
32	ПК 1.4 ПК 2.1 ПК 3.2	Для защиты компонентов ЦИС категорий 2 и 2F допускается использовать только сертифицированные программные или аппаратно - программные компоненты, выполняющие функции защиты информации, а также какие специальные средства защиты информации? (Выберите несколько правильный ответ).	1) МЭ, не ниже чем по 4 классу защищенности 2) МЭ, не ниже чем по 5 классу защищенности; 3) средства обнаружения вторжений по 6 - 4 классу защиты в зависимости от требуемой защищенности ЦИС ; 4) СЗИ, предназначенные для использования в АС класса не ниже 1Г;
33	ПК 1.4 ПК 2.1 ПК 3.2	Для защиты компонентов ЦИС категорий 1 и 1F допускается использовать только сертифицированные программные или аппаратно - программные компоненты, выполняющие функции защиты информации, а также какие специальные средства защиты информации? (Выберите несколько правильный ответ).	1) межсетевые экраны не ниже чем по 3 классу защищенности; 2) средства обнаружения вторжений не ниже чем по 4 классу защиты; 3) СЗИ (программные части) не ниже чем по 4 уровню отсутствия НДВ; 4) СЗИ предназначенные для использования в АС класса не ниже 1Г.
34	ПК 1.4 ПК 2.1 ПК 3.2	Требования по защите информации определены в руководящих документах ФСТЭК и ФСБ России. На какие направления распределены документы? (Выберите несколько правильный ответ).	1. Защита конфиденциальной информации (в том числе персональных данных); 2. Защита коммерческой тайны; 3. Защита государственной тайны; 4. Защита информации в ключевых системах информационной инфраструктуры (защита информации криптографическими методами)
35	ПК 1.4	Какие моменты должен обязательно знать администратор ИС при сканировании защищенности ИС общего пользования подразделением ФСБ России?	1) Время; 2) ФИО, кто сканирует ИС; 3) С каких адресов проводиться сканирование.

Второй блок

Формируемые компетенции ОК1, ОК2, ОК9, ОК9, ПК 1.4, ПК 2.1 , ПК 3.2

№	Профессиональные компетенции	Вопрос	Ответ
1	ПК 1.4 ПК 2.1	На что подразделяется информация в зависимости от категории доступа?	общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа).
2	ПК 1.4 ПК 2.1 ПК 3.2	Для чего необходим реестр российского программного обеспечения?	Для расширения использования российских программ для электронных вычислительных машин и баз данных, подтверждения их происхождения из Российской Федерации, а также в целях оказания правообладателям программ для электронных вычислительных машин или баз данных мер государственной поддержки
3	ПК 1.4 ПК 2.1	Какие информационные системы называются государственными?	Федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов.
4	ПК 1.4 ПК 2.1 ПК 3.2	На, что направлены требования ФСТЭК по защите конфиденциальной информации?	Направлены на исключение неправомерного доступа, копирования, передачи или распространения сведений
5	ПК 1.4 ПК 2.1 ПК 3.2	Для обеспечения требований по безопасности конфиденциальной информации проводится оценка возможных уязвимостей ИС для каких видов нарушителей?	Внешних и внутренних нарушителей
6	ПК 1.4 ПК 2.1 ПК 3.2	Что за Вид рекомендаций и для чего, перечислены ниже? ✓ межсетевых экранов, фильтрующих информацию по установленным критериям; ✓ средств, направленных на обнаружение, нейтрализацию и анализ вторжений; ✓ антивирусных программ, выявляющих, блокирующих и нейтрализующих несанкционированные действия; ✓ доверенной загрузки; ✓ контроля за съемными носителями.	Методические рекомендации ФСТЭК по защите данных
7	ПК 1.4 ПК 2.1 ПК 3.2	Что включает в себя лицензия ФСТЭК на техническую защиту конфиденциальной информации?	Включает средства информационной защиты, их установку и эксплуатацию.

8	ПК 1.4 ПК 2.1 ПК 3.2	Что называют системой защиты информации (применительно к объекту обработки информации)?	Совокупность организационных мероприятий, технических, программных и программно-технических средств защиты информации и средств контроля эффективности защиты информации
9	ПК 1.4 ПК 2.1	Из чего состоит жизненный цикл системы защиты информации (СЗИ) объекта обработки информации?	Состоит из стадии создания системы и стадии эксплуатации.
10	ПК 1.4 ПК 2.1 ПК 3.2	Что называют совокупностью взаимоувязанных процессов последовательного изменения состояния системы защиты информации конкретного объекта от принятия решения о необходимости защиты обрабатываемой на нем информации до окончания его эксплуатации?	Жизненный цикл системы защиты информации объекта информатизации
11	ПК 1.4 ПК 2.1 ПК 3.2	Что является оценкой безопасности информационной системы или компьютерных сетей средствами моделирования злоумышленника (нарушителя)?	Тестирование на проникновение
12	ПК 1.4 ПК 2.1 ПК 3.2	Сформулируйте определение информационно-телекоммуникационная Сеть.	Технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники (статья 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»).
13	ПК 1.4 ПК 2.1 ПК 3.2	Как переводиться ИТКС?	Информационно- телекоммуникационная Сеть.
14	ПК 1.4 ПК 2.1 ПК 3.2	Какие принципы обеспечения безопасности критической информационной инфраструктуры Вы знаете?	1) законность; 2) непрерывность и комплексность обеспечения безопасности критической информационной инфраструктуры, достигаемые в взаимодействия уполномоченных федеральных органов исполнительной власти и субъектов критической информационной инфраструктуры; 3) приоритет предотвращения компьютерных атак.

15	ПК 1.4 ПК 2.1 ПК 3.2	С помощью чего должен осуществляется контроль функционирования ИТК ИС?	Программно-информационного комплекса (ПИК).
16	ПК 1.4 ПК 2.1 ПК 3.2	Продолжите данное предложение. На территории Российской Федерации использование информационно-телекоммуникационных сетей осуществляется с соблюдением требований законодательства Российской Федерации в какой области?	связи и иных нормативных правовых актов Российской Федерации.
17	ПК 1.4 ПК 2.1 ПК 3.2	Подключение информационных систем, информационно-телекоммуникационных сетей и средств вычислительной техники, применяемых для хранения, обработки или передачи информации, содержащей сведения, составляющие государственную тайну, либо информации, обладателями которой являются государственные органы и которая содержит сведения, составляющие служебную тайну, к информационно-телекоммуникационным сетям, позволяющим осуществлять передачу информации через государственную границу Российской Федерации, в том числе к международной компьютерной сети «Интернет» (далее - информационно-телекоммуникационные сети международного информационного обмена) допускается или нет?	Допускается.
18	ПК 1.4 ПК 2.1 ПК 3.2	С использованием, каких средств происходит подключения информационных систем, информационно-телекоммуникационных сетей и средств вычислительной техники, к информационно-телекоммуникационным сетям международного информационного обмена?	Такое подключение производится только с использованием специально предназначенных для этого средств защиты информации, в том числе шифровальных (криптографических) средств, прошедших в установленном законодательством Российской Федерации порядке сертификацию в Федеральной службе безопасности Российской Федерации и (или) получивших подтверждение соответствия в Федеральной службе по техническому и экспортному контролю.

19	ПК 2.1 ПК 3.2	Что такое информационная безопасность ?	это свойство сетей связи общего пользования противостоять возможности реализации нарушителем угрозы информационной безопасности.
20	ПК 1.4 ПК 2.1 ПК 3.2	Что означает правовая защита информации?	Защита информации правовыми методами законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением.
21	ПК 2.1 ПК 3.2	Что означает техническая защита информации?	Защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств.
22	ПК 2.1 ПК 3.2	Что означает криптографическая защита информации?	Защита информации с помощью ее криптографического преобразования.
23	ПК 1.4 ПК 2.1 ПК 3.2	Что относиться к технике защиты информации?	Средства защиты информации, в том числе средства физической защиты информации, криптографические средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации.
24	ПК 1.4 ПК 2.1 ПК 3.2	Что относиться к средствам защиты информации?	Техническое, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

25	ПК 1.4 ПК 2.1 ПК 3.2	Можно ли использовать государственными организациями и предприятиями в информационно — телекоммуникационных системах шифровальных средств, включая криптографические средства обеспечения подлинности информации (электронная подпись), и защищенных технических средств хранения, обработки и передачи информации**,** не имеющих сертификата Федерального агентства правительственной связи и информации при Президенте Российской Федерации**,** а также размещение государственных заказов на предприятиях, в организациях, использующих указанные технические и шифровальные средства, не имеющие сертификата Федерального агентства правительственной связи и информации при Президенте Российской Федерации?	Нельзя

Составил преподаватель Скряго О.С.