Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Вятский государственный университет»

УТВЕРЖДАЮ
Начальник Управления
дополнительного образования
_____О.В. Золотарева
«23» октября 2023 г.

ПРОГРАММА ИТОГОВОЙ АТТЕСТАЦИИ

дополнительной профессиональной программы – программы повышения квалификации

«Правоприменительная практика по организационно-правовым и техническим мерам защиты информации»

Киров, 2023

Итоговая аттестация проводится в форме зачета.

Зачет представляет собой итоговое испытание по профессионально-ориентированным проблемам, устанавливающим соответствие подготовленности выпускников требованиям ДПП.

Зачет проводится с целью проверки уровня и качества профессиональной подготовки слушателей, предусмотренных профессиональным стандартом и квалификационными характеристиками.

Зачет позволяет выявить и оценить уровень сформированности компетенций у выпускника для решения профессиональных задач, готовность к новым видам профессиональной деятельности.

Перечень проверяемых результатов обучения

Виды деятельности	Профессиональные компетенции	Практический опыт	Умения	Знания
62.09 Деятельность, связанная с использованием вычислительной техники и информационных технологий	**ПК 1 -** Способность осуществлять профессиональную деятельность по защите информации организационно-правовыми и техническими мерами в рамках законодательства РФ в сфере информационной безопасности.	Владеть навыками - ознакомления с изменениями нормативных правовых актов и методических документов в области информационной безопасности; - ознакомления с практикой применения основ информационной безопасности.	Уметь - анализировать нормативные правовые акты в области информационной безопасности; - применять методы формирования личной информационной безопасности; - осуществлять выбор организационно-правовых и технических мер защиты информации в соответствии с потребностями организации	Знать -базовые и специальные принципы организационного и технического обеспечения информационной безопасности

Примерный перечень вопросов к итоговому зачету

1 Какая информация относится к государственному информационному ресурсу? Какими нормативными документами это определено?

2 Какая информация относится к категории «ограниченного доступа»? Приведите примеры такой информации. Назовите нормативные правовые акты Российской Федерации, относящие информацию к категории ограниченного доступа.
3 Назовите основные статьи Кодекса Российской Федерации об административных правонарушениях, предусматривающих ответственность за нарушения в области защиты информации. Приведите пример административного правонарушения в области защиты информации.
4 Каким документом определена структура государственной системы защиты информации в РФ. Какой федеральный орган исполнительной власти возглавляет государственную систему защиты информации.
5 Назовите основные нормативные правовые акты, предусматривающие необходимость наличия в организациях подразделений (специалистов) по ЗИ.
6 Нормативные и методические документы, содержащие требования по защите от компьютерных вирусов.
7 Какие нормативные документы определяют требования к средствам электронной подписи и Требования к средствам удостоверяющего центра и к форме квалифицированного сертификата ключа проверки электронной подписи? Их основные положения. Сколько классов защиты определено для средств электронной подписи?
8 Какой документ определяет состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (далее - информационная система) с использованием средств криптографической защиты информации? Его основные требования.
9 Какой документ утверждает «Инструкцию об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»? Его основные требования.
10 В каких случаях обязательно использование сертифицированных средств криптографической защиты информации? Назовите нормативные документы.
11 Положение о порядке организации и проведения работ по защите конфиденциальной информации.
12 Каким документом определяется структура и содержание Руководства по защите информации в организации. Каков порядок разработки, утверждения и согласования документа.
13 Перечислите основные локальные организационно-распорядительные документы по защите информации в организации, определяющие порядок и правила функционирования объектовой системы защиты информации.

14 Перечислите базовые и специальные принципы организационного обеспечения информационной безопасности.
15 Перечислите базовые и специальные принципы технического обеспечения информационной безопасности.
16 Понятие критическая информационной инфраструктуры (КИИ). Какие нормативные документы приняты в последнее время по защите информации в КИИ?
17 Что понимается под компьютерной преступность?
18 Какова ответственность за применение методов компьютерной преступности в соответствии с КоАП и УК РФ Приведите примеры построения систем комплексной безопасности организаций и предприятий
19 Что представляет из себя «триада информационной безопасности»? Каким образом вы могли бы ее применить при подходе к построению систем защиты информации?
20 Назовите виды охраняемой законом информации? Каким федеральным законом или иным нормативным правовым актом она регламентируется?
21 Принцип необходимости и достаточности обеспечения информационной безопасности. Что подразумевается под ним. Приведите пример необходимых и достаточных мер по обеспечению безопасности информации на примере любого из видов охраняемой законом компьютерной информации.
22 Смоделируйте пример компании (организации) с наличием многоранговой ЛВС, сервисами, имеющими доступ из сети Интернет для клиентов компании и минимум двумя видами хранящейся и обрабатываемой охраняемой законом компьютерной информации. Какие основные организационные и технические меры вы предпримете для обеспечения ее защиты.
23 Какими статьями УК РФ предусмотрена ответственность за противоправную деятельность в сфере компьютерной информации. Назовите примеры за что может наступить уголовная ответственность за противоправную деятельность в сфере компьютерной информации.
24 Основные методы неправомерного доступа к охраняемой законом компьютерной информации, хранящейся и обрабатываемой в информационных системах РФ. Какие Вам известны аппаратно-программные и программные средства нейтрализации угроз информационной безопасности.

Критерии оценивания

Оценка за зачет является интегрированной и включает в себя оценку уровня освоения всех компетенций, формируемых в ходе изучения ДПП. Оценка соответствует уровню освоения компетенций: пороговый,

продвинутый, высокий. Результаты итоговой аттестации определяются по системе: «зачтено», «не зачтено».

Оценки «зачтено» заслуживает ответ слушателя, в котором полностью раскрыто теоретическое содержание заявленных в экзаменационном билете вопросов. Представлен анализ практической составляющей вопроса, слушатель приводит примеры, аргументирует и соотносит теоретические знания с профессиональной сферой; использует творческий подход к решению проблемных вопросов; владеет навыками обобщения, систематизации и обоснования выводов, предложений по конкретному вопросу; использует аргументацию в ответах на вопросы членов аттестационной комиссии, что позволяет сделать вывод о понимании, готовности к дискуссии по данной проблеме, теоретическому вопросу. Практическое задание выполнено в полном соответствии с требованиями ДПП. Слушатель демонстрирует сформированность компетенций в сфере профессиональной деятельности

Оценки «не зачтено» заслуживает слушатель, который обнаруживает существенные пробелы в знании основного учебного материала, допустивший принципиальные ошибки; если слушатель не дал правильных ответов на большинство заданных вопросов членов аттестационной комиссии. Выполнение практического задания не соответствует требованиям ДПП. Слушатель демонстрирует несформированность компетенций в сфере профессиональной деятельности.