Автономная некоммерческая организация высшего образования
Российский новый университет
Колледж

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ИТОГОВОЙ АТТЕСТАЦИИ

ВЫПУСКНИКОВ АНО ВО «РОСИЙСКИЙ НОВЫЙ УНИВЕРСИТЕТ»,

ОБУЧАЮЩИХСЯ ПО ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЕ
СРЕДНЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

10.02.05 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

код и наименование специальности

Техник по защите информации

квалификация выпускника

Москва 2021

ОДОБРЕН
предметной (цикловой) комиссией по специальности: Прикладная информатика (по отраслям)

Протокол № 09
от «10» июня 2021 г.

Председатель предметной (цикловой) комиссии

_____/ Аскерова В.И.

Разработан на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования
10.02.05 Обеспечение информационной безопасности автоматизированных систем

Заместитель директора по учебно-производственной работе

/Мальчевская И.Ю.

Составитель (автор): Батманова О.В., ст. преподаватель кафедры Телекоммуникационных систем и информационной безопасности

Рецензенты: Зайцев Д.А., генеральный директор ООО АйДи - Финансовые Технологии

ОГЛАВЛЕНИЕ

1. ПАСПОРТ ОЦЕНОЧНЫХ СРЕДСТВ ИТОГОВОЙ АТТЕСТАЦИИ

1.1. Область применения оценочных средств итоговой аттестации

1.1.1. Фонд оценочных средств итоговой аттестации (далее - ИА) является частью образовательной программы подготовки специалистов среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем (далее – ФГОС СПО) в части освоения видов профессиональной деятельности:

ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении;

ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами;

ПМ.03 Защита информации техническими средствами;

ПМ. 04 Освоение одной или нескольких профессий рабочих, должностей служащих;

и соответствующих **общих компетенций(ОК):**

Код	**Наименование результатов практики**
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 04.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами
ОК 05.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста
ОК 06.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей
ОК 07.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях
ОК 08.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности
ОК 09.	Использовать информационные технологии в профессиональной деятельности
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языках
ОК 11	Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере.

и профессиональных компетенций (ПК):

Эксплуатация автоматизированных (информационных) систем в защищенном исполнении:

ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации;

ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении;

ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации;

ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.

Защита информации в автоматизированных системах программными и программно-аппаратными средствами:

ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации;

ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами;

ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации;

ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа;

ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств;

ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

Защита информации техническими средствами:

ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации;

ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации;

ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа;

ПК 3.4. Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации;

ПК 3.5. Организовывать отдельные работы по физической защите объектов информатизации.

Освоение одной или нескольких профессий рабочих, должностей служащих:

ПК 4.1. Осуществлять подготовку оборудования компьютерной системы к работе, производить инсталляцию, настройку и обслуживание программного обеспечения;

ПК 4.2. Создавать и управлять на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работать в графических редакторах;

ПК 4.3. Использовать ресурсы локальных вычислительных сетей, ресурсы технологий и сервисов Интернета;

ПК 4.4. Обеспечивать применение средств защиты информации в компьютерной системе.

1.1.2. Фонд оценочных средств итоговой аттестации разработан в соответствии с нормативными документами:

1.1.2. Фонд оценочных средств итоговой аттестации разработан в соответствии с нормативными документами:

– Федеральным законом РФ «Об образовании в Российской Федерации» (от 29 декабря 2012 г. № 273-ФЗ);

Федеральным государственным образовательным стандартом среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем от 09.12.2016 №1553;

– Порядком организации и осуществления образовательной деятельности по образовательным программам среднего профессионального образования (утв. пр. Минобрнауки РФ от 14 июня 2013 г. № 464);

– Приказом Министерства образования и науки РФ № 968 от 16 августа 2013 г. «Об утверждении порядка проведения государственной итоговой аттестации по образовательным программам среднего профессионального образования» с учетом внесенных изменений утвержденных Приказом Минобразования и науки РФ от 31 января 2014 г. № 74, от 17 ноября 2017 г. № 1138;

– Письмом Рособрнадзора от 17 февраля 2014 г. № 02-68 «О прохождении государственной итоговой аттестации по образовательным программам среднего общего образования обучающимися по образовательным программам среднего профессионального образования»;

– Уставом АНО ВО «Российский новый университет»;

– Положением об итоговой аттестации обучающихся по не имеющим аккредитации программам среднего профессионального образования, утвержденным приказом ректора АНО ВО «РосНОУ» от 08.06.2021г. № 249-о;

– Положением о выпускной квалификационной работе по программам среднего профессионального образования, утвержденным приказом ректора АНО ВО «РосНОУ» 31.12.2020 г. № 455-о;

– Положением об использовании пакетов программ на проверку заимствований «ВКР-ВУЗ.РФ» в образовательной и научной деятельности АНО ВО «Российский новый университет»;

– Методическими рекомендациями по выполнению выпускной квалификационной (дипломной) работы.

1.2. Цели и задачи итоговой аттестации

Целью итоговой аттестации является установление соответствия уровня освоенности компетенций, обеспечивающих соответствующую квалификацию и уровень образования обучающихся, ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем. ИА призвана способствовать систематизации и закреплению знаний и умений обучающегося по специальности при решении конкретных профессиональных задач, определить уровень подготовки выпускника к самостоятельной работе.

1.3. Количество часов, отводимое на итоговую аттестацию

Всего - 6 недель, в том числе:

- подготовка к итоговой аттестации (выполнение выпускной квалификационной работы) - 4 недели,
- проведение демонстрационного экзамена - 1 неделя,
- защита выпускной квалификационной (дипломной) работы - 1 неделя.

2. СТРУКТУРА ПРОЦЕДУР ИТОГОВОЙ АТТЕСТАЦИИ И ПОРЯДОК ЕЕ ПРОВЕДЕНИЯ

2.1. Формы и сроки проведения итоговой аттестации

Итоговая аттестация проводится в форме демонстрационного экзамена и защиты выпускной квалификационной (дипломной) работы.

Демонстрационный экзамен является первым этапом итоговой аттестации.

На втором этапе итоговой аттестации проводится защита выпускной квалификационной (дипломной) работы.

Сроки проведения каждой формы ИА регламентируются университетом в календарном графике учебного процесса на текущий учебный год.

2.2. Порядок проведения итоговой аттестации

Для проведения ИА создается Итоговая экзаменационная комиссия в порядке, предусмотренном Приказом Министерства образования и науки Российской Федерации (Минобрнауки России) от 16 августа 2013 г. № 968 г.

Москва «Об утверждении Порядка проведения государственной итоговой аттестации по образовательным программам среднего профессионального образования».

Итоговая экзаменационная комиссия формируется из педагогических работников университета, лиц, приглашенных из сторонних организаций, в том числе педагогических работников, представителей работодателей или их объединений, направление деятельности которых соответствует области профессиональной деятельности, к которой готовятся выпускники.

Состав Итоговой экзаменационной комиссии утверждается распорядительным актом университета.

Итоговую экзаменационную комиссию возглавляет председатель, который организует и контролирует деятельность Итоговой экзаменационной комиссии, обеспечивает единство требований, предъявляемых к выпускникам.

Ректор/проректор университета является заместителем председателя Итоговой экзаменационной комиссии.

Итоговая экзаменационная комиссия действует в течение одного календарного года.

3. ЗАДАНИЯ ДЛЯ ДЕМОНСТРАЦИОННОГО ЭКЗАМЕНА

3.1. Порядок оценки демонстрационного экзамена

Программа ИА предусматривает для выпускников на первом этапе демонстрационный экзамен, включающий выполнение заданий.

Задания формируются в соответствии со специфическими для специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем профессиональными компетенциями, умениями и практическим опытом с учетом трудовых функций профессиональных стандартов, а также с использованием комплекта оценочной документации по соответствующей компетенции демонстрационного экзамена по стандартам Ворлдскиллс Россия. Для обучающихся по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем демонстрационный экзамен проводится в соответствии с компетенцией № F7 «Корпоративная защита от внутренних угроз информационной безопасности».

Система оценивания выполнения заданий демонстрационного экзамена

Оценивание выполнения заданий осуществляется на основе следующих принципов:

- соответствия содержания заданий ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, учёта требований профессиональных стандартов и работодателей;

- достоверности оценки – оценка выполнения заданий должна базироваться на общих и профессиональных компетенциях экзаменующихся, реально продемонстрированных в моделируемых профессиональных ситуациях в ходе выполнения практико-ориентированного профессионального задания;

- адекватности оценки – оценка выполнения заданий должна проводиться в отношении тех компетенций, которые необходимы для эффективного выполнения задания;

- надежности оценки – система оценивания выполнения заданий должна обладать высокой степенью устойчивости при неоднократных (в рамках различных этапов) оценках компетенций экзаменующихся;

- комплексности оценки – система оценивания выполнения заданий должна позволять интегративно оценивать общие и профессиональные компетенции экзаменующихся;

- объективности оценки – оценка выполнения конкурсных заданий должна быть независимой от особенностей профессиональной ориентации или предпочтений членов Итоговой экзаменационной комиссии.

При выполнении процедур оценки заданий используются следующие основные методы:

– метод экспертной оценки;
– метод расчета первичных баллов;
– метод расчета сводных баллов;
– метод перевода сводных баллов в оценку.

Результаты выполнения практических заданий оцениваются с использованием следующих групп целевых индикаторов: основных и штрафных.

При оценке заданий используются следующие основные процедуры:

– процедура начисления основных баллов за выполнение заданий;
– процедура начисления штрафных баллов за нарушения при выполнении заданий;
– процедура формирования сводных результатов;
– процедура перевода результатов в оценку.

Эксперты, оценивающие выполнения задания

Оценку выполнения заданий осуществляет экспертная группа, состоящая из педагогических работников университета, имеющих опыт в подготовке обучающихся по специальности, представителя работодателей. Эксперты группы являются членами Итоговой экзаменационной комиссии.

Минимальное количество экспертов, участвующих в оценке демонстрационного экзамена – 5 человек.

Каждый эксперт выставляет объективную или субъективную оценку.

Набор заданий для демонстрационного экзамена

Задания для демонстрационного экзамена представляют собой комплекс заданий для демонстрации выпускниками общих и профессиональных компетенций в соответствии с требованиями ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем. В процессе подготовки к демонстрационному экзамену рабочая группа отбирает ряд базовых заданий. Вариативность заданий обусловлена материально-технической базой колледжа АНО ВО «Российский новый университет» и исходит из потребностей регионального рынка труда.

Конкурсное задание демонстрационного экзамена состоит из следующих модулей (в соответствии с компетенцией № F7 «Корпоративная защита от внутренних угроз информационной безопасности» Ворлдскиллс Россия)**:**

1. Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз:

- Конфигурация сетевой инфраструктуры: настройка хостмашины, сетевого окружения, виртуальных машин, и т.п.;
- Установка и настройка системы корпоративной защиты от внутренних угроз;
- Самостоятельный поиск и устранение неисправностей при развёртывании и настройке;
- Установка и настройка агентского мониторинга;
- Проведена синхронизация с LDAP-сервером, раздел персоны заполнен корректно;
- Запустить систему корпоративной защиты от внутренних угроз, проверить работоспособность. Провести имитацию процесса утечки конфиденциальной информации в системе;

2. Исследование (аудит) организации с целью защиты от внутренних угроз:

- Самостоятельно изучить структуру организации на основании полученных материалов («модели организации»), провести обследование корпоративных информационных систем;
- Определить объекты защиты;
- Перечень субъектов/персон сформулирован верно, роли пользователей, права доступа;
- Определить каналы передачи данных и потенциальных утечек;
- Типы циркулирующих данных определены верно;
- Выявить потоки передачи данных и возможные каналы утечки информации; Заполнить шаблон модели угроз;
- Подготовить отчёт о результатах аудита, включая потоки данных, потенциальные каналы утечек, уровни рисков роли пользователей, объекты защиты

(с привязкой к нормативной базе и методикам оценки последствий), ролями пользователей и т.п.

- Определить перечень нормативных актов РФ, задействованных в рамках модели угроз;
- Разработать перечень, описание и шаблоны нормативно-правовых документов организации по легальному применению корпоративной защиты от внутренних угроз информационной безопасности;

3. Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз:

- Разработать новые и/или модифицировать существующие политики безопасности, перекрывающие каналы передачи данных и возможные инциденты согласно конкурсного задания;
- Разработать или/и модифицировать объекты защиты, категории, технологии защиты в DLP-системе и т.п.;
- Использовать различные технологии защиты: печатей, бланков, графических объектов, баз данных и т.п.;
- Занести политики информационной безопасности в DLP-систему;
- Модифицировать политики безопасности в системе IWTM в соответствие с получаемыми на практике данными перехвата;
- Применить политики для контроля трафика, выявления и/или блокирования инцидентов безопасности, создаваемых внешним Генератором угроз. Максимизировать число выявленных инцидентов безопасности;
- Работа с интерфейсом управления системы корпоративной защиты информации;

4. Технологии анализа и защиты сетевого трафика:

- Развёртывание, настройка и проверка работоспособности VPN-сети на существующей и вычислительной инфраструктуре;
- Развёртывание, настройка и проверка работоспособности IDS-системы на существующей и вычислительной инфраструктуре;
- VPN. Работа с узлами и пользователями;
- VPN. Компрометация узлов, ключей, пользователей. Восстановление связи. Обновление ключевой информации;
- VPN. Межсетевое взаимодействие и туннелированные;
- VPN. Централизованные политики безопасности. Защита рабочих мест;
- IDS. Выявление большей части инцидентов безопасности за ограниченное время и/или с учётом неожиданно меняющихся условий;
- IDS. Разработать и применить политики, использующие различные технологии анализа траффика;

5. Технологии агентского мониторинга:

- Продемонстрировать знание механизмов работы агентского мониторинга;

- Разработать и применить политики агентского мониторинга для работы с носителями и устройствами;
- Разработать и применить политики агентского мониторинга для работы с файлами;
- Работа с исключениями из перехвата;

6. Анализ выявленных инцидентов:

- Подготовка отчётов о нарушениях;
- Применение механизмов создания фильтров для анализа перехваченного трафика и выявленных инцидентов;
- Проведение классификацию уровня угроз инцидентов; Оценка ущерба;
- Использование дополнительных модули анализа информационных потоков, если это продиктовано особенностями условий ведения бизнеса;
- Разработка план по дальнейшему расследованию выявленных инцидентов и противодействию нарушителям с опорой на нормативную базу.

Критерии оценки

Критерии оценки выполнения каждого вида заданий по основным видам деятельности разрабатываются рабочей группой в соответствии:

- с компетенциями ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем и показателями освоения компетенций;
- с заданиями для демонстрационного экзамена.

Общее количество баллов по всем модулям конкурсного задания составляет 100.

Модуль (критерий)	**Максимальный балл**
Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз	16,00
Исследование (аудит) организации с целью защиты от внутренних угроз	12,00
Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз	20,00
Технологии анализа и защиты сетевого трафика	27,00
Технологии агентского мониторинга	15,00
Анализ выявленных инцидентов	10,00
Итого:	**100,00**

Оценка конкурсного задания базируется на следующих критериях:

1. Установка, конфигурирование и устранение неисправностей в системах корпоративной защиты от внутренних угроз:

В ходе проверки последовательно сравнивается факт установки систем и отдельных модулей согласно конкурсному заданию, проверяется корректность их функционирования.

2. Исследование (аудит) организации с целью защиты от внутренних угроз:

Проверке подлежит комплект документов, разработанный участником, на соответствие заданному эталону. Допустимые отклонения от эталона указаны в задании.

3. Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз:

Процедура проверки заключается в последовательной оценке соответствия результатов выполнения сетевых политик, созданных и применённых участником, в системах защиты от внутренних угроз информационной безопасности. Политики должны отработать корректно (с учётом требований задания в части выставления уровня угрозы, приоритета и т.п.) выявив все инциденты безопасности, без ложных срабатываний. За ошибки (ложные срабатывания, пропуски инцидентов и т.п.) максимальный балл может быть снижен.

4. Технологии анализа и защиты сетевого трафика:

Процедура проверки заключается в последовательной оценке факта успешного использования участником различных технологий VPN-систем для защиты сетевого трафика и/или IDS-систем для выявления факта атаки на корпоративные информационные системы, умения применить эти технологии для достижения целей защиты. Проверка заключается в последовательной оценке результатов работы конкурсантов по развёртыванию, настройке и применения соответствующих систем.

5. Технологии агентского мониторинга:

Процедура проверки заключается в последовательной оценке соответствия результатов выполнения агентских политик, созданных и применённых участником, в системах защиты от внутренних угроз информационной безопасности. Политики должны отработать корректно (с учётом требований задания в части выставления уровня угрозы, приоритета и т.п.) выявив все инциденты безопасности, без ложных срабатываний.

6. Анализ выявленных инцидентов:

Проверке подлежит факт соответствия созданных в рамках задания отчётов и документов конкурсному заданию.

Методика перевода баллов демонстрационного экзамена в экзаменационную оценку:

Компетенция	Максимальный балл	Оценка «неудовлетворительно»	Оценка «удовлетворительно»	Оценка «хорошо»	Оценка «отлично»
Корпоративная защита от внутренних угроз информационной безопасности	100	0,00 – 9,99	10,00-29,99	30,00-54,99	55,00-100,00

4. ОРГАНИЗАЦИЯ ПОДГОТОВКИ И ЗАЩИТЫ ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ

4.1. Порядок оценки выпускных квалификационных работ

На втором этапе итоговой аттестации проводится защита выпускной квалификационной (дипломной) работы.

Работа по подготовке и написанию выпускной квалификационной (дипломной) работы ведутся обучающимся под руководством назначенного руководителя в течение последнего года обучения. Темы выпускной квалификационной (дипломной) работы должны иметь практико-ориентированный характер и соответствовать содержанию одного или нескольких профессиональных модулей.

Структура выпускной квалификационной (дипломной)

- титульный лист;
- содержание (оглавление)
- введение;
- основная часть;
- заключение;
- список используемых источников информации;
- приложения (по необходимости).

Примерный перечень тем ВКР:

№ п/п	Тема выпускной квалификационной работы	Соответствие темы ОП (наименование или шифр профессионального модуля)
1	Разработка информационно-поисковой системы, приложения баз данных: - складской учет, - библиотечные системы - кадровый состав, - системы хранения и обработки информации,	ПМ.02. Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах

	- создание комментариев, руководств пользователей для новых программных средств, адаптация их для конкретной организации, - разработка программных средств защиты информационных систем	
2	Программирование расчетных задач: - задачи моделирования и расчета производственных процессов, - разработка программных модулей для бухгалтерских пакетов, корпоративных систем	ПМ.01. Эксплуатация подсистем безопасности автоматизированных систем, ПМ.03. Применение инженерно-технических средств обеспечения информационной безопасности
3	Создание WEB-сайтов, средств дистанционного обучения: - создание сайтов организации, - создание тематических сайтов, - разработка электронных учебников, - разработка обучающих игр	ПМ.01. Эксплуатация подсистем безопасности автоматизированных систем, ПМ.03. Применение инженерно-технических средств обеспечения информационной безопасности
4	Проектирование компьютерной сети в соответствии с заданными параметрами	ПМ.02. Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах
5	Разработка программных средств по защите информации	ПМ.02. Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах, ПМ.03. Применение инженерно-технических средств обеспечения информационной безопасности

Примерный перечень тем выпускной квалификационной (дипломной) работы может быть расширен за счет конкретных тем, определенных на базах практики.

Выпускная квалификационная работа оценивается в баллах.

Оценка **«отлично»** выставляется в случаях, когда выпускная квалификационная работа:

− носит исследовательский характер, содержит грамотно изложенные теоретические положения, глубокий анализ, критический разбор практиче-

ского опыта по исследуемой проблеме, характеризуется логичным, последовательным изложением материала с соответствующими выводами и обоснованными предложениями;

− имеет положительные отзывы руководителя выпускной квалификационной работы и рецензента;

− при защите работы обучающийся показывает глубокое знание вопросов темы, свободно оперирует данными исследования, во время доклада использует иллюстративный (таблицы, схемы, графики) или презентационный материал, легко отвечает на поставленные вопросы.

Оценка **«хорошо»** выставляется в случаях, когда выпускная квалификационная работа:

− носит исследовательский характер, содержит грамотно изложенные теоретические положения, глубокий анализ, критический разбор практического опыта по исследуемой проблеме, характеризуется логичным, последовательным изложением материала с соответствующими выводами, но не вполне обоснованными предложениями;

− имеет положительные отзывы руководителя выпускной квалификационной работы и рецензента;

− при защите работы обучающийся показывает глубокое знание вопросов темы, свободно оперирует данными исследования, во время доклада использует иллюстративный (таблицы, схемы, графики) или презентационный материал, без особых затруднений отвечает на поставленные вопросы.

Оценка **«удовлетворительно»** выставляется в случаях, когда выпускная квалификационная работа:

− носит исследовательский характер, содержит грамотно изложенные теоретические положения, базируется на практическом материале, но отличается поверхностным анализом практического опыта по исследуемой проблеме, характеризуется непоследовательным изложением материала и необоснованными предложениями;

− в отзывах руководителя выпускной квалификационной работы и рецензента имеются замечания по содержанию работы и методам исследования;

− при защите работы обучающийся проявляет неуверенность, показывает слабое знание вопросов темы, не дает полного, аргументированного ответа на заданные вопросы, иллюстративный материал подготовлен не качественно.

Оценка **«неудовлетворительно»** выставляется в случаях, когда выпускная квалификационная работа:

− не носит исследовательский характер, не содержит анализа практического опыта по исследуемой проблеме, характеризуется непоследовательным изложением материала, не имеет выводов либо они носят декларативный порядок;

− в отзывах руководителя выпускной квалификационной работы и рецензента имеются критические замечания;

− при защите работы обучающийся затрудняется отвечать на поставленные по теме вопросы, не знает теории вопроса, при ответе допускает существенные ошибки, иллюстрационный материал к защите не подготовлен.

При определении окончательной оценки по защите дипломных работ учитываются:

- доклад обучающегося, культура речи, логика мышления и ясность изложения;
- умение слушать вопросы членов комиссии и отвечать на них;
- умение научно обосновывать свою точку зрения;
- оценка рецензента;
- отзыв руководителя;
- содержание введения;
- содержание теоретической части;
- содержание практической части;
- выводы и предложения (заключение);
- источники информации;
- объем выполненной работы в листах.

Критерии оценки дипломной работы и ее защиты

Критерии	Показатели			
	неудовлетворительно	удовлетворительно	хорошо	отлично
1	2	3	4	5

Защита	обучающийся не ориентируется в используемой в работе терминологии. Не может сформулировать ответ на вопросы членов ИЭК как по теме работы, так и на дополнительные вопросы. Не ориентируется в тексте своей работы. Не может продемонстрировать полученные теоретические и практические знания и навыки. Допускает грубые ошибки при толковании основных положений и результатов работы, не имеет соб-	обучающийся, в целом, владеет содержанием работы, но при этом затрудняется в ответах на вопросы членов ИЭК. Допускает неточности и ошибки при толковании основных положений и результатов работы, не имеет собственной точки зрения на проблему исследования. Автор показывает слабую ориентировку в понятиях, терминах, которые использует в своей работе	обучающийся, достаточно уверенно владеет содержанием работы, в основном, отвечает на поставленные вопросы, но допускает незначительные неточности при ответах. Использует наглядный материал.	обучающийся уверенно владеет содержанием работы, убежденно обосновывает свою точку зрения, опираясь на соответствующие теоретические положения, грамотно и содержательно отвечает на поставленные вопросы. Использует наглядный материал:
Актуальность	не сформулирована и не обосновывается	сформулирована в самых общих чертах	сформулирована, обоснована недоста-	сформулирована обоснована в полном
Рецензия	неудовлетворительная	удовлетворительная	хорошая	отличная
Отзыв руководителя	неудовлетворительный	удовлетворительный	хороший	отличный
Оформление	допущены многочисленные нарушения требований оформления	допущены нарушения требований оформления	допущены незначительные нарушения требований оформления	требования оформления соблюдены в полном объеме

Итоговая оценка	обучающийся обнаруживает непонимание содержательных основ исследования и неумение применять полученные знания на практике, защиту строит не связно, допускает существенные ошибки в теоретическом обосновании, которые не может исправить даже с помощью членов комиссии	обучающийся обнаруживает низкий уровень владения методологическим аппаратом исследования, допускает неточности при формулировке теоретических положений выпускной квалификационной работы, материал излагается не связно	обучающийся обнаруживает достаточно высокий уровень владения методологическим аппаратом исследования, осуществляет содержательный анализ теоретических источников, но допускает отдельные неточности в теоретическом обосновании	обучающийся обнаруживает высокий уровень владения методологическим аппаратом исследования, осуществляет сравнительно - сопоставительный анализ разных теоретических подходов.