Федеральное государственное образовательное бюджетное
учреждение высшего образования
«Финансовый университет при Правительстве Российской Федерации»
(Финансовый университет)

Колледж информатики и программирования

УТВЕРЖДАЮ
Директор
Колледжа информатики
и программирования
_____ Н.И. Демкина
«21» декабря 2023 г.

ПРОГРАММА ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ ВЫПУСКНИКОВ ПО СПЕЦИАЛЬНОСТИ СРЕДНЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ 10.02.05 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

2023 г.

ОДОБРЕНА
Педагогическим советом Колледжа информатики и программирования
Протокол №2 от «21» декабря 20__ г.

Разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, (утверждён приказом Министерства образования и науки Российской Федерации от 09 декабря 2016 г. №1553, зарегистрирован Министерством юстиции Российской Федерации 26 декабря 2016 г., регистрационный №44938).

Программа рассмотрена и
рекомендована к утверждению на
заседании предметной (цикловой)
комиссии Обеспечения
информационной безопасности
автоматизированных систем
Протокол № 4
от «07» декабря 2023 г.

Председатель
предметной (цикловой) комиссии
_____ А.Л. Маринич
Подпись Ф.И.О.

Составители: Демкина Н.И. к.э.н., директор Колледжа информатики и программирования, Долгова Н.Ю., заместитель директора колледжа по учебной работе, Маринич А.Л., преподаватель 1КК

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Программа государственной итоговой аттестации (далее- Программа ГИА) является частью образовательной программы подготовки специалистов среднего звена, разработанной в соответствии с Федеральным государственным образовательным стандартом среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем от 09.12.2016 №1553 (в ред. Приказа Минпросвещения России от 17.12.2020 №747), зарегистрированным в Минюсте России от 26.12.2016 №44938 (далее - ФГОС СПО).

Квалификация выпускника - Техник по защите информации.

База приема – основное общее образование.

1.2. Государственная итоговая аттестация (далее – ГИА) является завершающим этапом освоения программы подготовки специалистов среднего звена по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

К ГИА допускаются выпускники, не имеющие академической задолженности и в полном объеме выполнившие учебный план или индивидуальный учебный план по осваиваемой образовательной программе среднего профессионального образования.

1.3. Процедура государственной итоговой аттестации (далее- ГИА) в Колледже информатики и программирования Финансового университета осуществляется в соответствии с:

- Федеральным законом от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» (с изменениями и дополнениями);

- Приказом Министерства просвещения Российской Федерации от 24.08.2022 № 762 (ред. от 20.12.2022) «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам среднего профессионального образования» (Зарегистрировано в Минюсте России 21.09.2022 № 70167);

- Приказом Министерства просвещения Российской Федерации от 08.11.2021 № 800 «Об утверждении Порядка проведения государственной итоговой аттестации по образовательным программам среднего профессионального образования»;

- Федеральным государственным образовательным стандартом среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем от 09.12.2016 №1553 (в ред. Приказа Минпросвещения России от 17.12.2020 №747). (Зарегистрировано в Минюсте России от 26.12.2016 №44938);

- Порядком проведения государственной итоговой аттестации по образовательным программам среднего профессионального образования в Финансовом университете, утвержденным приказом Финансового университета от 10.10.2022 №2276/о;

- Положением о дипломном проекте (работе) по образовательным программам среднего профессионального образования в Финансовом университете, утвержденным приказом Финансового университета от 19.12.2022 №3080/о.

1.4. Государственная итоговая аттестация проводится государственной экзаменационной комиссией в целях определения соответствия результатов освоения обучающимися основной образовательной программы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем соответствующим требованиям ФГОС СПО.

Задачами государственной итоговой аттестации являются:

- оценка степени и уровня освоения обучающимися образовательной программы, характеризующая его подготовленность к самостоятельному выполнению определенных видов профессиональной деятельности;

- принятие решения о присвоении квалификации по результатам ГИА и выдаче выпускнику документа государственного образца об уровне образования и квалификации.

1.5. В процессе проведения государственной итоговой аттестации определяется уровень освоения общих и профессиональных компетенций (элементы) по следующим видам деятельности:

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.

Выполнение работ по одной или нескольким профессиям рабочих, должностям 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

Выпускник, освоивший образовательную программу, должен обладать следующими общими компетенциями (далее - ОК):

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, применять стандарты антикоррупционного поведения.

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 поддержания 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.

1.6. Формы проведения государственной итоговой аттестации**:** защита выпускной квалификационной работы (дипломной работы (проекта)) и демонстрационный экзамен профильного уровня (совокупность инвариантной и вариативной части).

1.7. Программа ГИА доводится до сведения обучающихся не позднее чем за шесть месяцев до начала ГИА.

2. ПРОЦЕДУРА ПРОВЕДЕНИЯ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

2.1. В соответствии с календарным учебным графиком образовательной программы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем определен следующий срок проведения ГИА: с 14.06.2024 по 27.06.2024.

2.2. Для проведения ГИА создается государственная экзаменационная комиссия (далее - ГЭК) в порядке, установленном приказом Финансового университета от 10 октября 2022 г. №2276/о «Об утверждении Порядка проведения государственной итоговой аттестации по образовательным программам среднего профессионального образования в Финансовом университете» (далее – Порядок).

2.3. В состав ГЭК входят председатель ГЭК, заместитель председателя ГЭК и члены ГЭК, в том числе эксперты для проведения демонстрационного экзамена.

Председатель ГЭК организует и контролирует деятельность государственной экзаменационной комиссии, обеспечивает единство требований, предъявляемых к выпускникам. Председателем ГЭК Министерством просвещения Российской Федерации по представлению Ученого совета Финансового университета утверждается лицо, не работающее в Финансовом университете из числа:

руководителей или заместителей руководителей организаций, осуществляющих образовательную деятельность, соответствующую области профессиональной деятельности, к которой готовятся выпускники;

представителей работодателей или их объединений, организаций-партнеров, включая экспертов, при условии, что направление деятельности данных представителей соответствует области профессиональной деятельности, к которой готовятся выпускники.

Заместителем председателя ГЭК является директор колледжа, членами ГЭК - педагогические работники колледжа.

Из числа лиц, относящихся к педагогическим или административным работникам колледжа, назначается секретарь ГЭК, который ведет протоколы заседаний ГЭК, представляет необходимые материалы в апелляционную комиссию.

Экспертную группу возглавляет главный эксперт, назначаемый из числа экспертов, включенных в состав ГЭК.

Главный эксперт организует и контролирует деятельность возглавляемой экспертной группы, обеспечивает соблюдение всех требований к проведению демонстрационного экзамена и не участвует в оценивании результатов ГИА.

2.4. Особенности проведения демонстрационного экзамена

2.4.1. Демонстрационный экзамен по специальности 10.02.05

Обеспечение информационной безопасности автоматизированных систем проводится в соответствии с комплектом оценочной документации КОД 10.02.05-1-2024 https://bom.firpo.ru/Public/94, разработанной оператором демонстрационного экзамена и вариативной части комплекта оценочной документации, разработанной колледжем совместно с организацией-партнером (Приложение 1).

2.4.2. Демонстрационный экзамен проводится в центре проведения демонстрационного экзамена (далее - центр проведения экзамена), представляющем собой площадку, оборудованную и оснащенную в соответствии с комплектом оценочной документации. Центр проведения экзамена располагается на территории колледжа.

2.4.3. Дата и время начала проведения демонстрационного экзамена, расписание сдачи экзаменов, планируемая продолжительность проведения демонстрационного экзамена, технические перерывы в проведении демонстрационного экзамена определяются планом проведения демонстрационного экзамена, утверждаемым ГЭК не позднее чем за двадцать календарных дней до даты проведения демонстрационного экзамена. Колледж знакомит с планом проведения демонстрационного экзамена выпускников, сдающих демонстрационный экзамен, и лиц, обеспечивающих проведение демонстрационного экзамена, в срок не позднее чем за пять рабочих дней до даты проведения экзамена.

2.4.4. Не позднее чем за один рабочий день до даты проведения демонстрационного экзамена главным экспертом проводится проверка готовности центра проведения экзамена в присутствии членов экспертной группы, выпускников, а также технического эксперта, назначаемого колледжем, ответственного за соблюдение установленных норм и правил охраны труда и техники безопасности.

Главным экспертом осуществляется осмотр центра проведения экзамена, распределение обязанностей между членами экспертной группы по оценке выполнения заданий демонстрационного экзамена, а также распределение рабочих мест между выпускниками с использованием способа случайной выборки. Результаты распределения обязанностей между членами экспертной группы и распределения рабочих мест между выпускниками фиксируются главным экспертом в соответствующих протоколах.

2.4.5. Выпускники знакомятся со своими рабочими местами, под руководством главного эксперта также повторно знакомятся с планом проведения демонстрационного экзамена, условиями оказания первичной медицинской помощи в центре проведения экзамена. Факт ознакомления отражается главным экспертом в протоколе распределения рабочих мест.

2.4.6. Технический эксперт под подпись знакомит главного эксперта, членов экспертной группы, выпускников с требованиями охраны труда и безопасности производства.

2.4.7. В день проведения демонстрационного экзамена в центре проведения экзамена присутствуют:

а) директор колледжа или представитель колледжа, назначенный директором колледжа;

б) не менее одного члена ГЭК, не считая членов экспертной группы;

в) члены экспертной группы;

г) главный эксперт;

д) представитель организаций-партнеров (по согласованию с колледжем)

е) выпускники;

ж) технический эксперт;

з) тьютор (ассистент), оказывающий необходимую помощь выпускнику из числа лиц с ограниченными возможностями здоровья, детей-инвалидов, инвалидов (далее - тьютор (ассистент);

и) организаторы, назначенные колледжем из числа педагогических работников, оказывающие содействие главному эксперту в обеспечении соблюдения всех требований к проведению демонстрационного экзамена.

Допуск выпускников в центр проведения экзамена осуществляется главным экспертом на основании документов, удостоверяющих личность.

2.4.8. В день проведения демонстрационного экзамена в центре проведения экзамена могут присутствовать:

а) должностные лица органа исполнительной власти субъекта Российской Федерации, осуществляющего управление в сфере образования (по решению указанного органа);

б) представители оператора демонстрационного экзамена (по согласованию с колледжем);

в) медицинские работники (по решению колледжа);

г) представители организаций-партнеров (по решению таких организаций по согласованию с колледжем).

Указанные в настоящем пункте лица присутствуют в центре проведения экзамена в день проведения демонстрационного экзамена на основании документов, удостоверяющих личность.

2.4.9. Члены экспертной группы осуществляют оценку выполнения заданий демонстрационного экзамена самостоятельно.

2.4.10. Главный эксперт вправе давать указания по организации и проведению демонстрационного экзамена, обязательные для выполнения лицами, привлеченными к проведению демонстрационного экзамена, и

выпускникам, удалять из центра проведения экзамена лиц, допустивших грубое нарушение требований Порядка, требований охраны труда и безопасности производства, а также останавливать, приостанавливать и возобновлять проведение демонстрационного экзамена при возникновении необходимости устранения грубых нарушений требований Порядка, требований охраны труда и производственной безопасности.

2.4.11. Технический эксперт вправе:

наблюдать за ходом проведения демонстрационного экзамена;

давать разъяснения и указания лицам, привлеченным к проведению демонстрационного экзамена, выпускникам по вопросам соблюдения требований охраны труда и производственной безопасности;

сообщать главному эксперту о выявленных случаях нарушений лицами, привлеченными к проведению демонстрационного экзамена, выпускниками требований охраны труда и требований производственной безопасности, а также невыполнения такими лицами указаний технического эксперта, направленных на обеспечение соблюдения требований охраны труда и производственной безопасности;

останавливать в случаях, требующих немедленного решения, в целях охраны жизни и здоровья лиц, привлеченных к проведению демонстрационного экзамена, выпускников действия выпускников по выполнению заданий, действия других лиц, находящихся в центре проведения экзамена с уведомлением главного эксперта.

2.4.12. Выпускники вправе:

пользоваться оборудованием центра проведения экзамена, необходимыми материалами, средствами обучения и воспитания в соответствии с требованиями комплекта оценочной документации, задания демонстрационного экзамена;

получать разъяснения технического эксперта по вопросам безопасной и бесперебойной эксплуатации оборудования центра проведения экзамена;

получить копию задания демонстрационного экзамена на бумажном носителе;

Выпускники обязаны:

во время проведения демонстрационного экзамена не пользоваться и не иметь при себе средства связи, носители информации, средства ее передачи и хранения, если это прямо не предусмотрено комплектом оценочной документации;

во время проведения демонстрационного экзамена использовать только средства обучения и воспитания, разрешенные комплектом оценочной документации;

во время проведения демонстрационного экзамена не взаимодействовать с другими выпускниками, экспертами, иными лицами, находящимися в центре проведения экзамена, если это не предусмотрено комплектом оценочной документации и заданием демонстрационного экзамена.

Выпускники могут иметь при себе лекарственные средства и питание, прием которых осуществляется в специально отведенном для этого помещении согласно плану проведения демонстрационного экзамена за пределами центра проведения экзамена.

2.4.13. Допуск выпускников к выполнению заданий осуществляется при условии обязательного их ознакомления с требованиями охраны труда и производственной безопасности.

2.4.14. В соответствии с планом проведения демонстрационного экзамена главный эксперт ознакамливает выпускников с заданиями, передает им копии заданий демонстрационного экзамена.

2.4.15. После ознакомления с заданиями демонстрационного экзамена выпускники занимают свои рабочие места в соответствии с протоколом распределения рабочих мест.

2.4.16. После того, как все выпускники и лица, привлеченные к проведению демонстрационного экзамена, займут свои рабочие места в соответствии с требованиями охраны труда и производственной безопасности, главный эксперт объявляет о начале демонстрационного экзамена.

Время начала демонстрационного экзамена фиксируется в протоколе проведения демонстрационного экзамена, составляемом главным экспертом по каждой экзаменационной группе.

После объявления главным экспертом начала демонстрационного экзамена выпускники приступают к выполнению заданий демонстрационного экзамена.

2.4.17. Демонстрационный экзамен проводится при неукоснительном соблюдении выпускниками, лицами, привлеченными к проведению демонстрационного экзамена, требований охраны труда и производственной безопасности, а также с соблюдением принципов объективности, открытости и равенства выпускников.

2.4.18. Центр проведения экзамена может быть оборудован средствами видеонаблюдения, позволяющими осуществлять видеозапись хода проведения демонстрационного экзамена.

2.4.19. Видеоматериалы о проведении демонстрационного экзамена в случае осуществления видеозаписи подлежат хранению в колледже не менее одного года с момента завершения демонстрационного экзамена.

2.4.20. Явка выпускника, его рабочее место, время завершения

выполнения задания демонстрационного экзамена подлежат фиксации главным экспертом в протоколе проведения демонстрационного экзамена.

2.4.21. В случае удаления из центра проведения экзамена выпускника, лица, привлеченного к проведению демонстрационного экзамена, или присутствующего в центре проведения экзамена, главным экспертом составляется акт об удалении. Результаты ГИА выпускника, удаленного из центра проведения экзамена, аннулируются ГЭК, и такой выпускник признается ГЭК не прошедшим ГИА по неуважительной причине.

2.4.22. Главный эксперт сообщает выпускникам о течении времени выполнения задания демонстрационного экзамена каждые 60 минут, а также за 30 и 5 минут до окончания времени выполнения задания.

2.4.23. После объявления главным экспертом окончания времени выполнения заданий выпускники прекращают любые действия по выполнению заданий демонстрационного экзамена.

Технический эксперт обеспечивает контроль за безопасным завершением работ выпускниками в соответствии с требованиями производственной безопасности и требованиями охраны труда.

2.4.24. Выпускник по собственному желанию может завершить выполнение задания досрочно, уведомив об этом главного эксперта.

2.4.25. Результаты выполнения выпускниками заданий демонстрационного экзамена подлежат фиксации экспертами экспертной группы в соответствии с требованиями комплекта оценочной документации и задания демонстрационного экзамена

2.5. Порядок защиты дипломной работы (проекта)

2.5.1. Подготовка и защита дипломной работы (проекта) осуществляется в соответствии с Положением о дипломном проекте (работе) по образовательным программам среднего профессионального образования в Финансовом университете, утвержденным приказом Финансового университета от 19 декабря 2022 г. №3080/о, и Методическими рекомендациями по подготовке к защите дипломной работы (проекта) по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденными директором колледжа (далее – Методические рекомендации).

2.5.2. Дипломная работа (проект) направлена на систематизацию и закрепление знаний студента по специальности, а также определение уровня готовности студента к самостоятельной профессиональной деятельности. Дипломный работа (проект) предполагает самостоятельную подготовку (написание) студентом работы (проекта), демонстрирующей уровень знаний студента в рамках выбранной темы, а также сформированность его профессиональных умений и навыков.

2.5.3. Дипломная работа (проект) может быть выполнена индивидуально или несколькими студентами совместно (коллективная дипломная работа (проект)).

2.5.4. Ежегодно колледжем формируется тематика дипломных работ (проектов).

2.5.5. Предметная (цикловая) комиссия колледжа «Обеспечение информационной безопасности автоматизированных систем информационной безопасности» доводит до сведения студентов перечень тем дипломных работ (проектов) до 15 сентября завершающего учебного года.

2.5.6. Закрепление темы за студентом осуществляется на основании его личного заявления на имя председателя предметной (цикловой) комиссии по форме согласно приложению № 2.

2.5.7. Студенту предоставляется право выбора темы дипломной работы (проекта), в том числе предложения своей тематики с необходимым обоснованием целесообразности ее разработки для практического применения. Тема дипломной работы (проекта) должна соответствовать содержанию одного или нескольких профессиональных модулей, входящих в соответствующую образовательную программу СПО.

2.5.8. Студент обязан выбрать тему дипломной работы (проекта), согласовать ее с потенциальным руководителем до 15 октября завершающего учебного года.

2.5.9. Закрепление тем дипломной работы (проекта), назначение руководителей дипломной работы (проекта) и консультантов (при наличии) студентов осуществляется приказом Финуниверситета не позднее 15 ноября завершающего учебного года.

2.5.10. Изменение или уточнение темы дипломной работы (проекта) в исключительных случаях возможно, но не позднее, чем за два месяца до предполагаемой даты защиты дипломной работы (проекта), на основании согласованного с руководителем дипломной работы (проекта) личного заявления, составленного на имя директора колледжа, с обоснованием причины корректировки. Изменение или уточнение темы оформляется приказом Финуниверситета.

2.5.11. Примерные темы дипломных работ (проектов) представлены в приложении №3.

2.5.12. Непосредственное руководство дипломной работой (проектом) осуществляет руководитель. В обязанности руководителя дипломных работ (проектов) входят:

разработка задания на дипломную работу (проект) по форме согласно приложению № 4;

оказание помощи студенту при составлении плана дипломной работы (проекта);

оказание помощи студенту в разработке индивидуального графика работы на весь период выполнения дипломной работы (проекта);

консультирование студента по вопросам содержания и последовательности выполнения дипломной работы (проекта);

консультирование студента по подбору литературы, информационного и фактического материала;

осуществление постоянного контроля за ходом подготовки дипломных работ (проектов) в соответствии с установленным индивидуальным графиком;

осуществление контроля за качеством подготовки дипломных работ (проектов);

своевременное информирование докладной запиской директора колледжа в случае несоблюдения студентом графика подготовки или неготовности дипломной работы (проекта);

консультирование студента в подготовке презентации и доклада для защиты дипломной работы (проекта);

предоставление письменного отзыва о работе студента в период подготовки дипломной работы (проекта)по форме согласно приложению № 5;

присутствие на защите дипломных работ (проектов), при условии его незанятости аудиторной работой со студентами.

2.5.13. Студент в рамках подготовки дипломной работы (проекта) обязан:

выбрать и согласовать с потенциальным руководителем тему дипломной работы (проекта);

разработать и согласовать с руководителем индивидуальный график работы над дипломной работой (проектом);

систематически работать над дипломной работой (проектом)в соответствии с установленными сроками и требованиями, использовать Методические рекомендации, разработанные колледжем;

регулярно общаться с руководителем дипломной работы (проекта) и информировать его о проделанной работе;

оформить дипломную работу (проект) в соответствии с установленными требованиями;

пройти процедуру предзащиты дипломной работоты (проекта);

подготовить доклад и презентацию для защиты дипломной работы (проекта), согласовать их с руководителем;

представить дипломную работу (проект)в установленные сроки.

2.5.14. Структура и содержание дипломной работы (проекта) должны соответствовать Методическим рекомендациям и отвечать следующим

требованиям:

- наличие в работе всех структурных элементов: теоретической, практической составляющих;

- иметь актуальность, практическую значимость и выполняться, по возможности, по предложениям (заказам) организаций-работодателей, инновационных компаний, высокотехнологичных производств или образовательных организаций;

- достаточность и обоснованность использованного библиографического материала.

2.5.15. Дипломная работа (проект) включает в себя следующие разделы:

титульный лист, оформленный на стандартном белом листе бумаги формата А4 по форме в соответствии с приложением № 7;

содержание;

введение;

основная часть, как правило, структурированная на главы и параграфы;

заключение;

список использованных источников;

приложения (при наличии).

2.5.16. Рекомендуемый объем дипломной работы (проекта)не менее 40 и не более 50 страниц без учета приложений.

При выполнении коллективной дипломной работы (проекта) объем может быть увеличен до 50 – 80 страниц без учета приложений.

2.5.17. Дипломная работа (проект) в распечатанном и переплетенном виде подписывается студентом, консультантом (при наличии) и передается руководителю дипломной работы (проекта) не позднее чем за 10 дней до начала ГИА согласно календарному учебному графику.

Руководитель дипломной работы (проекта) проверяет качество работы, подписывает ее, подписывает дипломную работу (проект) у председателя ПЦК и передает вместе с заданием, своим письменным отзывом ответственному сотруднику колледжа для регистрации в журнале учета дипломных работ (проектов) с указанием даты сдачи.

2.5.18. Выполненные дипломные работы (проекты) подлежат обязательному рецензированию по форме согласно приложению № 6. Рецензентами являются специалисты из числа работников организаций, преподавателей колледжа и других образовательных организаций, владеющих вопросами, связанными с тематикой дипломных работ (проектов).

Рецензенты утверждаются приказом Финуниверситета не позднее чем за месяц до защиты дипломных работ (проектов).

Содержание рецензии доводится до сведения студента не позднее чем за

день до защиты работы.

Внесение изменений в дипломную работу (проект) после получения рецензии не допускается

2.5.19. С целью контроля готовности студента к защите дипломной работы (проекта) проводится предварительная защита дипломной работы (проекта).

Задачами предзащиты дипломных работ (проектов) являются оценка соответствия текста доклада заявленной теме, полноты раскрытия заявленных целей и задач, своевременное выявление недостатков и недочетов, возникших в ходе выполнение дипломной работы (проекта), а также получение рекомендаций по работе и помощь в формулировании основных положений и выводов для выступления студента на защите.

Порядок и сроки проведения предзащиты устанавливаются предметной (цикловой) комиссией колледжа «Обеспечение информационной безопасности автоматизированных систем» и доводятся до сведения студентов не позднее, чем за 7 календарных дней до даты проведения.

2.5.20. Защита является завершающим этапом выполнения студентами дипломной работы (проекта). К защите дипломной работы (проекта) допускаются студенты, завершившие полный курс обучения и представившие дипломную работу (проект) в установленный срок.

Защита дипломной работы (проекта) проводится в соответствии с расписанием государственной итоговой аттестации, утвержденным директором колледжа.

Защита дипломной работы (проекта) производится в очном формате. В исключительных случаях по решению ректора Финуниверситета защита дипломной работы (проекта) может проводиться с применением дистанционных образовательных технологий в режиме видеоконференции.

2.5.21. Процедура защиты дипломной работы (проекта) включает в себя:

открытие заседания ГЭК председателем или заместителем председателя ГЭК;

доклады студентов, на которые предусматривается не более 10 минут;

вопросы членов комиссии ГЭК по докладу студента, а также смежной тематике. При ответах студент имеет право пользоваться текстом своей дипломной работы (проекта);

заслушивание текста отзыва с обязательным отражением замечаний и мнения руководителя о рекомендации дипломной работы (проекта) к защите;

заслушивание текста рецензии.

2.5.22. ГЭК при определении результата защиты дипломной работы (проекта) принимает во внимание:

индивидуальную оценку членами ГЭК содержания работы, ее защиты,

включая доклад, ответы на вопросы членов ГЭК;

наличие практической значимости и обоснованности выводов и рекомендаций, сделанных студентом в результате проведенного исследования;

оценку руководителя работы студента в период подготовки дипломной работы (проекта), степени ее соответствия требованиям, предъявляемым к дипломным работам (проектам), количество и серьезность замечаний;

оценку рецензента за работу целом;

общую оценку членами ГЭК содержания дипломной работы (проекта), качество ответов на вопросы членов ГЭК, свободное владение материалом дипломной работы (проекта).

В случае возникновения спорной ситуации при равном числе голосов председательствующий обладает правом решающего голоса.

2.6. Оценка результатов государственной итоговой аттестации

2.6.1. Результаты любой из форм государственной итоговой аттестации определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» и объявляются в тот же день после оформления в установленном порядке протоколов заседаний ГЭК.

2.6.2. Процедура оценивания результатов выполнения заданий демонстрационного экзамена осуществляется членами экспертной группы по системе, определенной требованиями комплекта оценочной документации.

2.6.3. Баллы выставляются в протоколе проведения демонстрационного экзамена, который подписывается каждым членом экспертной группы и утверждается главным экспертом после завершения экзамена для экзаменационной группы.

При выставлении баллов присутствует член ГЭК, не входящий в экспертную группу, присутствие других лиц запрещено.

Подписанный членами экспертной группы и утвержденный главным экспертом протокол проведения демонстрационного экзамена далее передается в ГЭК для выставления оценок по итогам ГИА.

Оригинал протокола проведения демонстрационного экзамена передается на хранение в колледж.

2.6.4. Перевод баллов в оценку осуществляется в соответствии с таблицей:

Оценка ГИА	"2"	"3"	"4"	"5"
Отношение полученного количества баллов к максимально возможному (в процентах)	0,00 - 19,99	20,00 - 39,99	40,00 - 69,99	70,00 - 100,00

2.6.7. Решения ГЭК принимаются на закрытых заседаниях простым большинством голосов членов ГЭК, участвующих в заседании, при

обязательном присутствии председателя ГЭК или его заместителя. При равном числе голосов голос председательствующего на заседании ГЭК является решающим.

2.6.8. При выставлении оценки на защите дипломной работы (проекта) члены ГЭК руководствуются следующими критериями:

«Отлично» - выпускник уверенно владеет содержанием дипломной работы (проекта), показывает свою точку зрения, опираясь на соответствующие теоретические положения. Изложение материалов полное, последовательное, грамотное. Выполнена практическая и теоретическая часть работы. Приложения логично связаны с текстовой частью отчета. Успешно выполнены все задания и рекомендации, данные руководителем. Обобщенные результаты практических разработок соответствуют теме исследования, отражают реальное состояние объекта и предмета исследования. Дипломная работа имеет положительные отзывы руководителя и рецензента. При защите дипломной работы выпускник во время доклада использует наглядные пособия (таблицы, схемы, графики, раздаточный материал и т.п.) грамотно и содержательно отвечает на все поставленные вопросы. Дипломная работа (проект) оформлена в соответствии с требованиями, сдана в установленный срок.

«Хорошо» - выпускник достаточно уверенно владеет содержанием дипломной работы (проекта). Изложение материалов полное, последовательное, соответствует требованиям, предъявляемым к работам данного вида. Освоены технические приемы проектных работ. Приложения в основном связаны с текстовой частью. Обобщенные результаты практических разработок соответствуют теме исследования, отражают реальное состояние объекта и предмета исследования. Работа имеет положительный отзыв руководителя и рецензента. При защите дипломной работы выпускник использует наглядные пособия (таблицы, схемы, графики, раздаточный материал и т.п.), отвечает на поставленные вопросы, но допускает незначительные неточности при ответах. Дипломная работа сдана в установленный срок, есть некоторые недочеты в оформлении работы.

«Удовлетворительно» - выпускник, в целом, владеет содержанием дипломной работы (проекта), но при этом затрудняется в ответах на вопросы членов ГЭК. Допускает неточности и ошибки при толковании основных положений и результатов работы, не имеет собственной точки зрения на проблему исследования. Автор показал слабую ориентировку в тех понятиях, терминах, которые использует в своей работе. Текстовая часть дипломной работы (проекта) не везде связана с приложениями. Обучающийся выполнил не все

практические задания, рекомендованные руководителем, допустил большое количество ошибок в оформлении. Дипломная работа сдана с опозданием. В отзывах рецензентов имеются замечания по содержанию работы и методике исследования.

«Неудовлетворительно» - выпускник не ориентируется в терминологии дипломной работы (проекта), при ответе допускает существенные ошибки, доклад охватывает менее 50% необходимого материала, разрозненный и бессистемный, неуверенный, нечеткий. На вопросы членов ГЭК выпускник не ответил или дал неверные ответы. Изложение материалов неполное, бессистемное, допущены существенные ошибки, много нарушений правил оформления дипломной работы (проекта). Приложения отсутствуют или не соответствуют основной части дипломной работы (проекта). Дипломная работа сдана с опозданием. В отзывах руководителя и рецензента имеются серьезные критические замечания.

2.6.9. В ходе заседания ГЭК ведется протокол, в котором отражается перечень заданных выпускнику вопросов и характеристика ответов на них, мнения председателя и членов ГЭК о выявленном уровне подготовленности выпускника к решению профессиональных задач, а также о выявленных недостатках в теоретической и практической подготовке. На последнем заседании в протокол вносится решение ГЭК о присвоении квалификации выпускникам, прошедшим государственную итоговую аттестацию.

2.6.10. Выпускникам, не проходившим государственную итоговую аттестацию по уважительной причине, в том числе не явившимся для прохождения ГИА по уважительной причине (далее - выпускники, не прошедшие ГИА по уважительной причине), предоставляется возможность пройти ГИА без отчисления из Финансового университета.

Дополнительные заседания ГЭК организуются в установленные сроки, но не позднее четырех месяцев после подачи заявления выпускника, не проходившего государственную итоговую аттестацию по уважительной причине.

2.6.11. Обучающиеся, не прошедшие ГИА по неуважительной причине, в том числе не явившиеся для прохождения ГИА без уважительных причин (далее - выпускники, не прошедшие ГИА по неуважительной причине), или получившие на ГИА неудовлетворительные результаты, отчисляются из Финуниверситета и проходят ГИА не ранее чем через шесть месяцев после прохождения ГИА впервые.

Для прохождения государственной итоговой аттестации обучающийся, не прошедшие ГИА по неуважительной причине, и выпускники, получившие на

ГИА неудовлетворительные результаты, восстанавливается в Финансовый университет на период времени, установленный календарным учебным графиком для прохождения ГИА соответствующей образовательной программы среднего профессионального образования. Повторное прохождение ГИА для обучающегося назначается не более двух раз.

2.6.12. После окончания государственной итоговой аттестации ГЭК составляет ежегодный отчет о работе, который обсуждается на Педагогическом совете колледжа.

3. ПОРЯДОК ПОДАЧИ И РАССМОТРЕНИЯ АПЕЛЛЯЦИИ ПРИ ПРОВЕДЕНИИ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

3.1. По результатам государственной аттестации выпускник, имеет право подать в апелляционную комиссию письменное апелляционное заявление о нарушении, по его мнению, установленного порядка проведения государственной итоговой аттестации и (или) несогласии с ее результатами (далее - апелляция).

Для проведения апелляций по результатам ГИА в колледже создается апелляционная комиссия по соответствующей специальности.

Состав апелляционной комиссии утверждается одновременно с утверждением состава ГЭК.

3.2. Апелляционная комиссия состоит из председателя апелляционной комиссии, не менее пяти членов из числа педагогических работников колледжа и секретаря апелляционной комиссии, не входящих в данном учебном году в состав государственных экзаменационных комиссий.

Председателем апелляционной комиссии может быть назначен директор колледжа или один из заместителей директора колледжа, представитель организаций-партнеров или их объединений, включая экспертов, при условии, что данные представители не входят в состав ГЭК.

3.3. Апелляция подается лично выпускником или родителями (законными представителями) несовершеннолетнего выпускника в апелляционную комиссию.

Апелляция о нарушении порядка проведения государственной итоговой аттестации подается непосредственно в день проведения ГИА, в том числе до выхода из центра проведения экзамена.

Апелляция о несогласии с результатами ГИА подается не позднее следующего рабочего дня после объявления результатов государственной итоговой аттестации.

3.4. Апелляция рассматривается апелляционной комиссией не позднее

трех рабочих дней с момента ее поступления.

3.5. Апелляция рассматривается на заседании апелляционной комиссии с участием не менее двух третей ее состава.

На заседание апелляционной комиссии приглашается председатель соответствующей ГЭК.

При проведении ГИА в форме демонстрационного экзамена по решению председателя апелляционной комиссии к участию в заседании комиссии могут быть также привлечены члены экспертной группы, технический эксперт.

По решению председателя апелляционной комиссии заседание апелляционной комиссии может пройти с применением средств видео, конференц-связи, а равно посредством предоставления письменных пояснений по поставленным апелляционной комиссией вопросам.

Выпускник, подавший апелляцию, имеет право присутствовать при рассмотрении апелляции. С несовершеннолетним выпускником имеет право присутствовать один из родителей (законных представителей). Указанные лица должны при себе иметь документы, удостоверяющие личность.

3.6. Рассмотрение апелляции не является пересдачей государственной итоговой аттестации.

3.7. При рассмотрении апелляции о нарушении порядка проведения ГИА апелляционная комиссия устанавливает достоверность изложенных в ней сведений и выносит одно из решений:

об отклонении апелляции, если изложенные в ней сведения о нарушениях порядка проведения ГИА выпускника не подтвердились и (или) не повлияли на результат государственной итоговой аттестации;

об удовлетворении апелляции, если изложенные в ней сведения о допущенных нарушениях порядка проведения ГИА выпускника подтвердились и повлияли на результат государственной итоговой аттестации.

В последнем случае результат проведения ГИА подлежит аннулированию, в связи с чем протокол о рассмотрении апелляции не позднее следующего рабочего дня передается в ГЭК для реализации решения апелляционной комиссии. Выпускнику предоставляется возможность пройти государственную итоговую аттестацию в дополнительные сроки, установленные колледжем без отчисления такого выпускника из Финуниверситета в срок не более четырех месяцев после подачи апелляции.

3.8. В случае рассмотрения апелляции о несогласии с результатами ГИА, полученными при прохождении демонстрационного экзамена, секретарь ГЭК не позднее следующего рабочего дня с момента поступления апелляции направляет в апелляционную комиссию протокол заседания ГЭК, протокол проведения демонстрационного экзамена, результаты работ выпускника, подавшего

апелляцию, видеозаписи хода проведения демонстрационного экзамена (при наличии).

3.9. В случае рассмотрения апелляции о несогласии с результатами ГИА, полученными при защите дипломного проекта (работы), секретарь ГЭК не позднее следующего рабочего дня с момента поступления апелляции направляет в апелляционную комиссию дипломный проект(работу), протокол заседания ГЭК.

3.10. В результате рассмотрения апелляции о несогласии с результатами ГИА апелляционная комиссия принимает решение об отклонении апелляции и сохранении результата ГИА либо об удовлетворении апелляции и выставлении иного результата государственной итоговой аттестации. Решение апелляционной комиссии не позднее следующего рабочего дня передается в ГЭК. Решение апелляционной комиссии является основанием для аннулирования ранее выставленных результатов ГИА выпускника и выставления новых.

3.11. Решение апелляционной комиссии принимается простым большинством голосов. При равном числе голосов голос председательствующего на заседании апелляционной комиссии является решающим.

Решение апелляционной комиссии доводится до сведения подавшего апелляцию выпускника (под роспись) в течение трех рабочих дней со дня заседания апелляционной комиссии.

3.12. Решение апелляционной комиссии является окончательным и пересмотру не подлежит.

3.13. Решение апелляционной комиссии оформляется протоколом, который подписывается председателем (заместителем председателя) и секретарем апелляционной комиссии и хранится в колледже.

4. ПОРЯДОК ПРОВЕДЕНИЯ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ ДЛЯ ВЫПУСКНИКОВ ИЗ ЧИСЛА ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

4.1. Для выпускников из числа лиц с ограниченными возможностями здоровья и выпускников из числа детей-инвалидов и инвалидов проводится ГИА с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких выпускников (далее - индивидуальные особенности). При проведении ГИА обеспечивается соблюдение следующих общих требований:

- проведение ГИА для выпускников с ограниченными возможностями здоровья, выпускников из числа детей-инвалидов и инвалидов в одной аудитории совместно с выпускниками, не имеющими ограниченных возможностей здоровья, если это не создает трудностей для выпускников при прохождении ГИА;

- присутствие в аудитории, центре проведения экзамена тьютора, ассистента, оказывающих выпускникам необходимую техническую помощь с учетом их индивидуальных особенностей (занять рабочее место, передвигаться, прочитать и оформить задание, общаться с членами ГЭК, членами экспертной группы);

- пользование необходимыми выпускникам техническими средствами при прохождении ГИА с учетом их индивидуальных особенностей;

- обеспечение возможности беспрепятственного доступа выпускников в аудитории, туалетные и другие помещения, а также их пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных проемов, лифтов, при отсутствии лифтов аудитория должна располагаться на первом этаже, наличие специальных кресел и других приспособлений).

4.2. Дополнительно при проведении ГИА обеспечивается соблюдение следующих требований в зависимости от категорий выпускников с ограниченными возможностями здоровья, выпускников из числа детей-инвалидов и инвалидов:

а) для слепых:

- задания для выполнения, а также инструкция о порядке ГИА, комплект оценочной документации, задания демонстрационного экзамена оформляются рельефно-точечным шрифтом по системе Брайля или в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением для слепых, или зачитываются ассистентом;

- письменные задания выполняются на бумаге рельефно-точечным шрифтом по системе Брайля или на компьютере со специализированным программным обеспечением для слепых, или надиктовываются ассистенту;

- выпускникам для выполнения задания при необходимости предоставляется комплект письменных принадлежностей и бумага для письма рельефно-точечным шрифтом Брайля, компьютер со специализированным программным обеспечением для слепых;

б) для слабовидящих:

- обеспечивается индивидуальное равномерное освещение не менее 300 люкс;

выпускникам для выполнения задания при необходимости предоставляется увеличивающее устройство;

- задания для выполнения, а также инструкция о порядке проведения государственной аттестации оформляются увеличенным шрифтом;

в) для глухих и слабослышащих, с тяжелыми нарушениями речи:

- обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости предоставляется звукоусиливающая аппаратура индивидуального пользования;

- по их желанию государственный экзамен может проводиться в письменной форме;

г) для лиц с нарушениями опорно-двигательного аппарата (с тяжелыми нарушениями двигательных функций верхних конечностей или отсутствием верхних конечностей):

- письменные задания выполняются на компьютере со специализированным программным обеспечением или надиктовываются ассистенту;

по их желанию государственный экзамен может проводиться в устной форме;

д) также для выпускников из числа лиц с ограниченными возможностями здоровья и выпускников из числа детей-инвалидов и инвалидов создаются иные специальные условия проведения ГИА в соответствии с рекомендациями психолого-медико-педагогической комиссии (далее - ПМПК), справкой, подтверждающей факт установления инвалидности, выданной федеральным

государственным учреждением медико-социальной экспертизы (далее - справка).

4.3. Выпускники или родители (законные представители) несовершеннолетних выпускников не позднее чем за 3 месяца до начала ГИА подают в колледж письменное заявление о необходимости создания для них специальных условий при проведении ГИА с приложением копии рекомендаций ПМПК, а дети-инвалиды, инвалиды - оригинала или заверенной копии справки, а также копии рекомендаций ПМПК при наличии.

Приложение №1

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ДЕМОНСТРАЦИОННОГО ЭКЗАМЕНА ПРОФИЛЬНОГО УРОВНЯ (выписка)

Код и наименование специальности среднего профессионального образования	10.02.05 Обеспечение информационной безопасности автоматизированных систем
Наименование квалификации	Техник по защите информации

Федеральный государственный образовательный стандарт среднего профессионального образования по профессии (специальности) среднего профессионального образования (ФГОС СПО):	ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденный приказом Минобрнауки РФ от 09.12.2016 № 1553.
Виды аттестации:	Государственная итоговая аттестация
Уровни демонстрационного экзамена:	Профильный (совокупность инвариантной и вариативной частей)
Шифр комплекта оценочной документации:	КОД 10.02.05-1-2024

Общие организационные требования:

1. ДЭ направлен на определение уровня освоения выпускником материала, предусмотренного образовательной программой, и степени сформированности профессиональных умений и навыков путем проведения независимой экспертной оценки выполненных выпускником практических заданий в условиях реальных или смоделированных производственных процессов.
2. ДЭ в рамках ГИА проводится с использованием КОД, включенных образовательными организациями в программу ГИА.
3. Задания ДЭ доводятся до главного эксперта в день, предшествующий дню начала ДЭ.
4. Образовательная организация обеспечивает необходимые технические условия для обеспечения заданиями во время ДЭ обучающихся, членов ГЭК, членов экспертной группы.
5. ДЭ проводится в Центре проведения демонстрационного экзамена (ЦПДЭ), представляющем собой площадку, оборудованную и оснащенную в соответствии с КОД.
6. Обучающиеся проходят ДЭ в ЦПДЭ в составе экзаменационных групп.
7. Образовательная организация знакомит с планом проведения ДЭ обучающихся, сдающих ДЭ, и лиц, обеспечивающих проведение ДЭ, в срок не позднее чем за 5 рабочих дней до даты проведения экзамена.
8. Количество, общая площадь и состояние помещений, предоставляемых для проведения ДЭ, должны обеспечивать проведение ДЭ в соответствии с КОД.
9. Не позднее чем за один рабочий день до даты проведения ДЭ главным экспертом проводится проверка готовности ЦПДЭ в присутствии членов экспертной группы, обучающихся, а также технического эксперта, назначаемого организацией, на территории которой расположен ЦПДЭ, ответственного за соблюдение установленных норм и правил охраны труда и техники безопасности.
10. Главным экспертом осуществляется осмотр ЦПДЭ, распределение обязанностей между членами экспертной группы по оценке выполнения заданий ДЭ, а также распределение рабочих мест между обучающимися с использованием способа случайной выборки. Результаты распределения обязанностей между членами экспертной группы и распределения рабочих мест между обучающимися фиксируются главным экспертом в соответствующих протоколах.
11. Обучающиеся знакомятся со своими рабочими местами, под руководством главного эксперта также повторно знакомятся с планом проведения ДЭ, условиями оказания первичной медицинской помощи в ЦПДЭ. Факт ознакомления отражается главным экспертом в протоколе распределения рабочих мест.

12. Допуск обучающихся в ЦПДЭ осуществляется главным экспертом на основании документов, удостоверяющих личность.

13. Образовательная организация обязана не позднее чем за один рабочий день до дня проведения ДЭ уведомить главного эксперта об участии в проведении ДЭ тьютора (ассистента).

Требование к продолжительности ДЭ. Продолжительность ДЭ зависит от вида аттестации, уровня ДЭ (таблица № 2)

Таблица № 2

Вид аттестации	**Уровень ДЭ**	**Составная часть КОД (инвариантная/ вариативная)**	**Продолжительность ДЭ**
ГИА	профильный	Совокупность инвариантной и вариативной частей	**4 ч. 30 мин.**

Требования к содержанию КОД. Единое базовое ядро содержания КОД (таблица № 3) сформировано на основе вида деятельности (вида профессиональной деятельности) в соответствии с ФГОС СПО и является общей содержательной основой заданий ДЭ вне зависимости от вида аттестации и уровня ДЭ.

Таблица № 3

ЕДИНОЕ БАЗОВОЕ ЯДРО СОДЕРЖАНИЯ КОД[1]		
Вид деятельности/ Вид профессиональной деятельности	**Перечень оцениваемых ОК/ПК**	**Перечень оцениваемых умений, навыков (практического опыта)**
Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	ПК: Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении	Умение: организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней
		Умение: производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы
Защита информации в автоматизированных системах программными и программно-аппаратными средствами	ПК: Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации	Умение: устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;
	ПК: Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами	Умение: устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации
		Практический опыт: в использовании программных и программно-аппаратных средств для защиты информации в сети
	ПК: Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации	Практический опыт: в тестировании функций, диагностике, устранении отказов и восстановлении работоспособности программных и программно-аппаратных средств защиты информации

[1] Единое базовое ядро содержания КОД – общая (сквозная) часть единого КОД, относящаяся ко всем видам аттестации (ГИА, ПА) вне зависимости от уровня ДЭ.

Содержательная структура КОД представлена в таблице № 4.

Таблица № 4

Вид деятельности (вид профессиональной деятельности)	**Перечень оцениваемых ОК, ПК**	**Перечень оцениваемых умений, навыков (практического опыта)**	**ГИА ДЭ ПУ**
Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	ПК: Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении	Умение: производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы	■
		Умение: организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней	■
		Умение: осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем	■
		Практический опыт: в администрировании автоматизированных систем в защищенном исполнении	■
	ПК: Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями	Практический опыт: в установке компонентов систем защиты информации автоматизированных (информационных) систем	■

	эксплуатационной документации		
	ПК: Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	Умение: настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам	■
		Практический опыт: в эксплуатации компонентов систем защиты информации автоматизированных систем	■
Защита информации в автоматизированных системах программными и программно-аппаратными средствами	ПК: Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами	Умение: устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации	■
		Практический опыт: в использовании программных и программно-аппаратных средств для защиты информации в сети	■
	ПК: Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации	Умение: устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации	■
		Практический опыт: в установке, настройке программных средств защиты информации в автоматизированной системе	■
	ПК: Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации	Практический опыт: в тестировании функций, диагностике, устранении отказов и восстановлении работоспособности программных и программно-аппаратных средств защиты информации	■
		Умение: диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации	■

	ПК: Осуществлять обработку, хранение и передачу информации ограниченного доступа	Умение: использовать типовые программные криптографические средства, в том числе электронную подпись	■
		Практический опыт: в решении задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации	■
		Практический опыт: в применении электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных	■
Вариативная часть КОД			
Защита информации в автоматизированных системах программными и программно-аппаратными средствами	ПК: Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации	Умение: устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации Практический опыт: в установке, настройке программных средств защиты информации в автоматизированной системе	■
	ПК: Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами	Умение: устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации	■

	ПК: Осуществлять обработку, хранение и передачу информации ограниченного доступа	Практический опыт: в решении задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации	■
	ПК : 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	Практический опыт: работа с подсистемами регистрации событий	■

Требования к оцениванию.

Распределение баллов по критериям оценивания для ДЭ ПУ (инвариантная и вариативная части КОД) в рамках ГИА представлена в таблице № 9.

Таблица № 9

№ п/п	**Модуль задания** (вид деятельности, вид профессиональной деятельности)	**Критерий оценивания**[6]	**Баллы**
1	Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	Установка и настройка компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	3,00
		Администрирование программных и программно-аппаратных компонентов автоматизированной (информационной) системы в защищенном исполнении	17,00
		Обеспечение бесперебойной работы автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиямиэксплуатационной документации	10,00
2	Защита информации в автоматизированных системах программными и программно-аппаратными средствами	Осуществление установки и настройки отдельных программных, программно- аппаратных средств защиты информации	12,00
		Обеспечение защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами	12,00
		Осуществление тестирования функций отдельных программных и программно- аппаратных средств защиты информации	12,00
		Осуществление обработки, хранения ипередачи информации ограниченного доступа	14,00
ИТОГО (инвариантная часть)			**80,00**
3	Защита информации в автоматизированных системах программными и программно-аппаратными средствами	Осуществление установки и настройки отдельных программных, программно-аппаратных средств защиты информации	10
		Обеспечение защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами	6
		Осуществление обработки, хранения и передачи информации ограниченного доступа	2
		Осуществление регистрации основных событий в автоматизированных (информационных) системах	2
ВСЕГО (вариативная часть)			**20,00**
ИТОГО (совокупность инвариантной и вариативной частей)			**100,00**

3.1 Инструкция по технике безопасности

1. Технический эксперт под подпись знакомит главного эксперта, членов экспертной группы, обучающихся с требованиями охраны труда и безопасности производства.

2. Все участники ДЭ должны соблюдать установленные требования по охране труда и производственной безопасности, выполнять указания технического эксперта по соблюдению указанных требований.

Инструкция:

Перед началом выполнения работ участнику ДЭ необходимо подготовить рабочее место:

- Осмотреть и привести в порядок рабочее место, убрать все посторонние предметы, которые могут отвлекать внимание и затруднять работу.
- Проверить правильность установки стола, стула, подставки под ноги, угол наклона экрана монитора, положения клавиатуры в целях исключения неудобных поз и длительных напряжений тела. Особо обратить внимание на то, что дисплей должен находиться на расстоянии не менее 50 см от глаз (оптимально 60-70 см).
- Проверить правильность расположения оборудования.
- Кабели электропитания, удлинители, сетевые фильтры должны находиться с тыльной стороны рабочего места, сетевые фильтры не должны лежать на полу.
- Убедиться в отсутствии засветок, отражений и бликов на экране монитора.
- Убедиться в том, что на устройствах ПК (системный блок, монитор, клавиатура) не располагаются сосуды с жидкостями, сыпучими материалами (чай, кофе, сок, вода и пр.).
- Включить электропитание в последовательности, установленной инструкцией по эксплуатации на оборудование; убедиться в правильном выполнении процедуры загрузки оборудования, правильных настройках.

Участнику запрещается приступать к выполнению задания при обнаружении неисправности оборудования. О замеченных недостатках и неисправностях немедленно сообщить Эксперту и до устранения неполадок к заданию не приступать.

Требования охраны труда во время выполнения работ

В течение всего времени выполнения задания со средствами компьютерной и оргтехники участник экзамена обязан:

- содержать в порядке и чистоте рабочее место;
- следить за тем, чтобы вентиляционные отверстия устройств ничем не были закрыты;

- выполнять требования инструкции по эксплуатации оборудования;
- соблюдать, установленные расписанием, перерывы в выполнении задания, выполнять рекомендованные физические упражнения.

Участнику запрещается во время выполнения задания:

- отключать и подключать интерфейсные кабели периферийных устройств если это не указано в задании;
- класть на устройства средств компьютерной и оргтехники бумаги, папки и прочие посторонние предметы;
- прикасаться к задней панели системного блока (процессора) при включенном питании;
- отключать электропитание во время выполнения программы, процесса;
- допускать попадание влаги, грязи, сыпучих веществ на устройства средств компьютерной и оргтехники;
- производить самостоятельно вскрытие и ремонт оборудования;
- работать со снятыми кожухами устройств компьютерной и оргтехники;
- располагаться при работе на расстоянии менее 50 см от экрана монитора.

Рабочие столы следует размещать таким образом, чтобы экран монитора был ориентирован боковой стороной к световым проемам, чтобы естественный свет падал преимущественно слева. Освещение не должно создавать бликов на поверхности экрана.

Продолжительность работы на ПК без регламентированных перерывов не должна превышать 1-го часа. Во время регламентированного перерыва с целью снижения нервно-эмоционального напряжения, утомления зрительного аппарата, необходимо выполнять комплексы физических упражнений.

При неисправности инструмента и оборудования – прекратить выполнение задания и сообщить об этом Эксперту, а в его отсутствие заместителю главного Эксперта.

3.2 Образцы задания

Наименование модуля задания	**Вид аттестации/уровень ДЭ** (ГИА/ДЭ ПУ)
Модуль 1: Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	
С помощью технологии виртуальных машин для выполнения задания смоделирована корпоративная сеть организации. В ходе выполнения данного задания нужно установить основное ПО на рабочие станции будущей защищенной сети. Доступ на все машины указан в дополнительной карточке задания В случае изменения каких-либо логинов или паролей необходимо отобразить это в отчете. Настройки сетевого окружения Для правильной работы сети надо создать или убедиться в наличии сетей: – Host only или внутренняя сеть адаптер для сети центрального офиса – Host only или внутренняя сеть адаптер для сети филиала – Host only адаптер, NAT или Bridge для виртуального «Интернета» (в соответствии с инфраструктурой площадки, для связи всех координаторов между собой) IP адреса защищенных сетей – Центральный офис «Сеть 1 ЦО»: 1.2.3.0/28 – Офис филиал «Сеть 1 Филиал»: 2.3.4.0/27 – Офис сеть 2 «Сеть 2 Офис»: 5.6.7.0/26 – «Интернет» для всех координаторов: 8.9.10.0/24 Адреса выбираются самостоятельно из указанного диапазона. Необходимо записать все IP адреса, логины и пароли в текстовый файл VPN.txt на рабочем столе компьютера. В связи с особенностями работы системы на серверных версиях необходимо устанавливать компоненты системы вручную (например, БД, сервер ЦУС, клиент ЦУС) используя пакеты MSI в подпапках дистрибутивов. Необходимо произвести установку и настройку основных компонентовVPN-сети.	ГИА/ДЭ ПУ

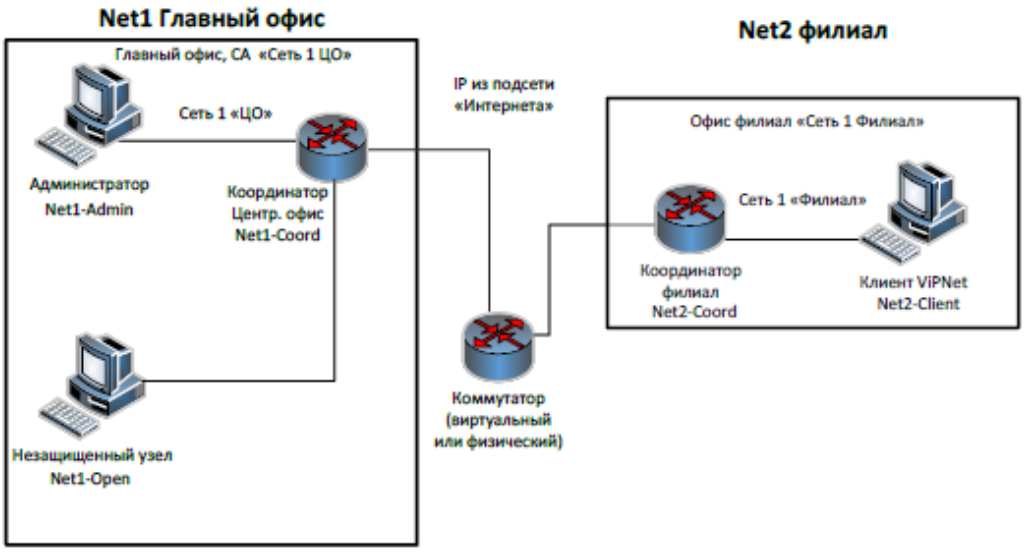
Задача. Развертывание ПК Administrator в качестве центра сертификации Установить базу данных на ВМ Net1-DB (незащищенный узел)	
Модуль 2: Защита информации в автоматизированных системах программными и программно-аппаратными средствами	
Установить и настроить рабочее место администратора (на базе виртуальной машины Net1-Admin (ЦО)): Центр управления сетью (серверное приложение ЦУС), Удостоверяющий и ключевой центр (УКЦ); использовать ранее установленную БД. Установить клиент ЦУС на ВМ Net1-DB (незащищенный узел) Если были произведены изменения паролей, IP-адресов и так далее, необходимо отразить это в отчете. Задача. Инициализация VPN Coordinator и установка ПО VPN Client – установить ПО Client, рабочее место администратора; – инициализировать Coordinator HW-VA; Задача. Инициализация VPN Coordinator и установка ПО Client для организации сети филиала – инициализировать Coordinator HW-VA. – установить ПО Client, рабочее место пользователя. Необходимо зафиксировать процесс установки скриншотами форм + сделать скриншот директории, в которую установлено ПО, и скриншот первого запуска приложения. Задача. Развертывание удостоверяющего и ключевого центра в составе сети. Необходимо использовать рабочее место администратора (созданное ранее) для создания структуры защищенной сети, развернуть с помощью технологии виртуальных машин сеть предприятия и настроить необходимые АРМ в соответствии с заданными ролями. Схема сети, которую требуется создать, приведена далее. IP адреса сетей перечислены в начале задания (по названию сетей).  Рисунок 1 Схема защищенной сети В итоге выполнения задания должны быть развернуты и настроены следующие сетевые узлы защищенной сети (см. таблицу).	ГИА/ДЭ ПУ

Таблица 1 Узлы защищенной сети если УКЦ и ЦУС на одной машине

Вирт. машина	Название сетевого узла	ПО	ОС сетевого узла	Имя пользователя сетевого узла, уровень полномочий
Net1- Admin (ЦО)	Главный администратор (VM)	Administrator (ЦУС клиент и сервер + УКЦ),Client	ОС пользовательская или серверная	Admin
Net1-Coord (ЦО)	Координатор Центр Офис (VM)	Coordinator	Координатор HW-VA	Coordinator
Net2-Coord (Филиал)	Координатор Филиал (VM)	Coordinator	Координатор HW-VA	CoordinatorSub
Net2-Client (филиал)	Пользователь_2 Филиал (VM)	Client	ОС пользовательская или серверная	User

Связи между узлами необходимо настроить самостоятельно.

Таблица 2. Схема связей пользователей

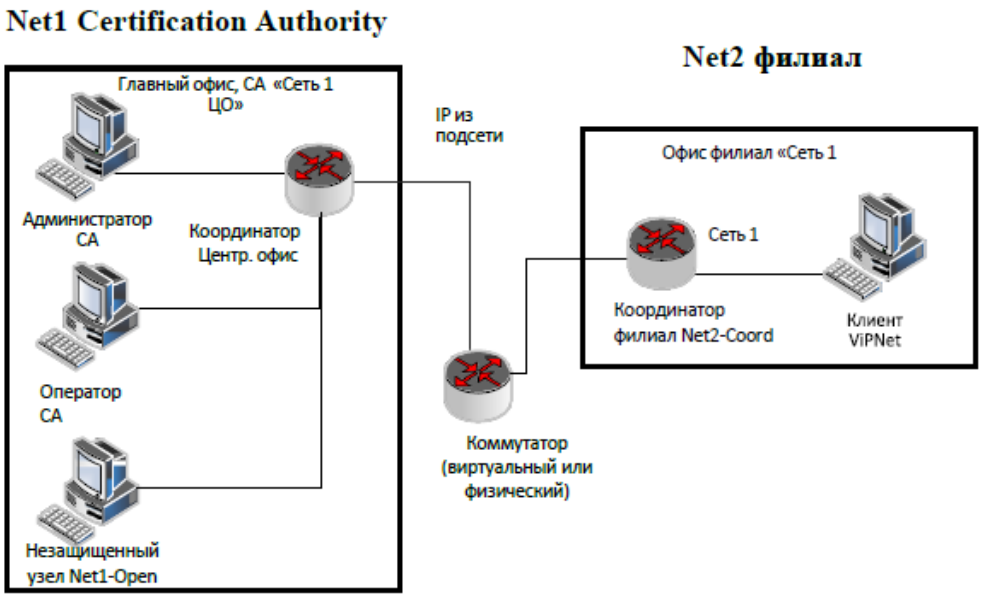
Схема связей пользователей	Coordinator	Admin	Coordinator Sub	User
Coordinator	×	*	*	
Admin	*	×		*
CoordinatorSub	*		×	*
User		*	*	×

Задача. Создание структуры защищенной сети

ЦУС. Необходимо создать в ЦУС структуру защищенной сети в соответствии с заданной схемой (выгрузить отчет в HTML). Создать пользователей узлов, настроить полномочия пользователей и их связи в соответствии со схемой.

УКЦ. Провести инициализацию УКЦ, сохранить контейнер ключей администратора в общей папке (создать подпапку Задача 1.5), поменять тип паролей для пользователей («собственный»). Задать пароли пользователей и сохранить в текстовый файл. Сформировать дистрибутивы ключей для всех сетевых узлов (сохранить на жесткий диск). Создать группы узлов для центрального офиса и филиала, настроить пароль администратора группы сетевых узлов для каждой из групп (проверить, что пароль работает).

На всех узлах сети корректно настроить или проверить корректность настройки сетевых интерфейсов в соответствии со схемой, проверить доступность соседних узлов. Разнести DST файлы по АРМ, провести первичную инициализацию узлов защищенной сети (координаторов и клиентов), проверить доступность узлов защищенной сети и сделать скриншоты работоспособности узлов. Отправить письмо по Деловой почте и текстовое сообщение пользователю User с Admin (зафиксировать скриншотом). Необходимо зафиксировать процесс настройки скриншотами ключевых моментов и заполненных форм: – скриншоты деловой почты на отправителе и получателе (при отправке письма); – скриншоты текстового сообщения на отправителе и получателе; – скриншоты журнала IP-пакетов на координаторах, подтверждающие прохождение письма через координаторы. Необходимо сохранить файл HTML с структурой защищенной сети, выгруженный из ЦУС.	
Модуль 1: Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	

Задача. Установка центра регистрации, сервиса публикации и сервиса информирования Certification Authority на соответствующие виртуальные машины – установить ПО Client; – установить ПО Publication Service; – установить ПО Registration Point; – установить ПО CA Informing. Задача. Развертывание удостоверяющего центра в составе сети Необходимо использовать рабочее место администратора (созданное ранее) для создания структуры защищенной сети, развернуть с помощью технологии виртуальных машин сеть предприятия и настроить необходимые АРМ в соответствии с заданными ролями. Схема сети, которую требуется создать, приведена далее. IP адреса сетей перечислены в начале задания (по названию сетей).  Рисунок 1 Схема защищенной сети	ГИА/ДЭ ПУ

В итоге выполнения задания должны быть развернуты и настроены следующие сетевые узлы защищенной сети (см. таблицу).

Таблица 1 Узлы защищенной сети если УКЦ и ЦУС на одной машине.

Вирт. машина	Название сетевого узла	ПО	ОС сетевого узла	Имя пользователясетевого узла, уровень полномочий
Net1-AdminCA (ЦО)	Главный администратор (VM)	Administrator (ЦУС клиент и сервер + УКЦ),Client, CA Informing	ОС пользовательская или серверная	AdminCA
Net1-CoordCA (ЦО)	Координатор Центр Офис (VM)	Coordinator	Координатор HW-VA	CoordinatorCA
Net1-OperCA (ЦО)	Оператор УЦ (VM)	Client, Publication Service, Registration Point	ОС пользовательская или серверная	OperCA
Net2-Coord (Филиал)	Координатор Филиал (VM)	Coordinator	Координатор HW-VA	CoordinatorSub
Net2-Client (филиал)	Пользователь_2 Филиал(VM)	Client	ОС пользовательск ая или серверная	User

Связи между узлами необходимо настроить самостоятельно.

Таблица 2. Схема связей пользователей

Схема связей пользователей	CoordinatorOffice	Admin	OperCA	CoordinatorSub	User
CoordinatorOffice	×	*	*	*	
Admin	*	×	*		*
OperCA	*	*	×	*	
CoordinatorSub	*		*	×	*
User		*		*	×

Задача. Настройка работы удостоверяющего центра в аккредитованном режиме

Необходимо перевести УКЦ в режим аккредитованного удостоверяющего центра, настроить параметры издания квалифицированныхсертификатов, указав:

- сведения о средствах УЦ,
- средство электронной подписи издателя,
- средства удостоверяющего центра,
- сертификат на средство электронной подписи издателя,
- сертификат на средство удостоверяющего центра,
- класс защищенности, которому соответствуют программные средства УЦ,
- место хранения контейнеров ключа ЭП и ключа защиты УКЦ.

После перевода УКЦ в аккредитованный режим необходимо выпустить:

- корневой квалифицированный сертификат,
- квалифицированные электронные подписи для пользователей.

При формировании сертификатов необходимо заполнить следующие поля:

Имя: <Имя пользователя или узла>
Электронная почта
Город
Область
Организация
Подразделение
Почтовый индекс

Создать квалифицированные ключи ЭП и ключи проверки ЭП для пользователей сети. Настроить схему обмена файлами между УКЦ посредством Сервиса Публикации (Publication Service).

Реализовать автоматическую публикацию сертификатов.Посредством Центра Регистрации (Registration Point):

- зарегистрировать пользователя;
- отправить запрос в УКЦ на выпуск сертификата, удовлетворить запрос;
- отправить запрос в УКЦ на аннулирование ранее выпущенного сертификата, удовлетворить запрос.

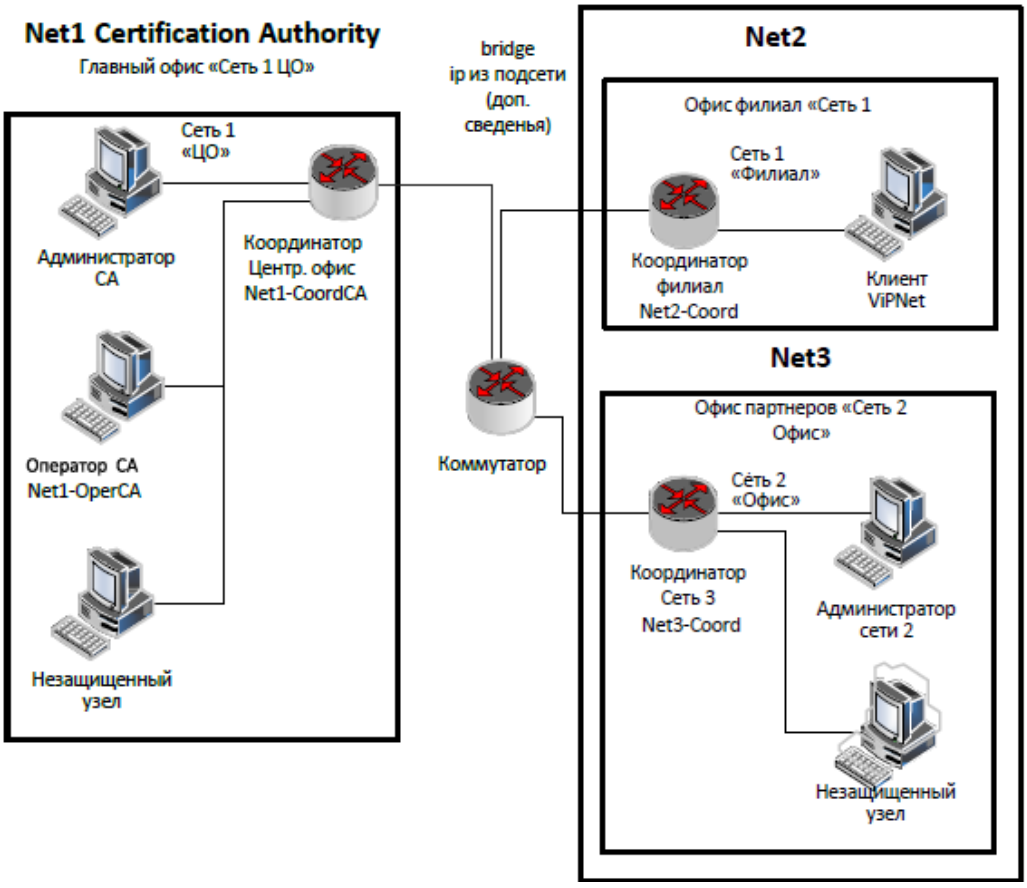
Посредством Сервиса Информирования (CA Informing): настроить способ выдачи уведомлений и сформировать отчет о выданных за текущие сутки сертификатах,предварительно в настройках указав место хранения отчетов.

Задача. Модификация структуры защищенной сети

Перед началом выполнения сделать HTML выгрузку структуры сети и сделать скриншот ЦУС окна с пользователями.

Модификация структуры сети:

1. добавить новый сетевой узел и пользователя за координатором (без фактического развертывания его на виртуальной машине). Добавить связь пользователя нового узла с пользователем. На указанных узлах проверить появление нового узла;
2. добавить пользователя на узле Филиал (Net2-Client филиала 2), связать его со всеми пользователями группы узлов центральный офис.

Модуль 2: Защита информации в автоматизированных системах программными и программно-аппаратными средствами	
По результатам проведенной модификации сети для указанного пользователя проверить появление новых связей, отправить письмо по Деловой почте пользователю, отправить текстовое сообщение пользователю. Необходимо зафиксировать процесс настройки скриншотами ключевых моментов и заполненных форм: – скриншоты деловой почты на отправителе и получателе (при отправке письма); – скриншоты текстового сообщения на отправителе и получателе; – скриншоты журнала IP-пакетов на координаторах, подтверждающие прохождение письма через координаторы, – скриншот Удостоверяющего центра со списком изданных сертификатов. Кроме того, необходимо сохранить файл HTML с обновленной структурой защищенной сети, выгруженный из ЦУС.	ГИА/ДЭ ПУ
Модуль 2: Защита информации в автоматизированных системах программными и программно-аппаратными средствами	
Задача. Межсетевое взаимодействие защищённых сетей (со связями «все со всеми»)  Рисунок 2. Схема межсетевого взаимодействия Развернуть на Net3-Admin (Сеть 3 межсеть) на ПК рабочее место Администратора партнёрской сети, создать структуру второй сети: Рабочее место администратора (БД, ЦУС, УКЦ, Client) – 1 координатор (HW-VA или координатор Linux),	ГИА/ДЭ ПУ

– 1 узел Admin, – установите координатор. Установить и настроить необходимое ПО. Настроить межсетевое взаимодействие между двумя защищёнными сетями, сделать скриншоты всех этапов установки межсетевоговзаимодействия. Проверить взаимодействие узлов, отправив сообщение деловой почты.	
Модуль 1: Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	
Задача. Туннелирование в рамках межсетевого взаимодействия Подключить незащищенную машину в сети 3. Настроить туннелирование таким образом, чтобы взаимодействие между открытыми узлами из разных сетей осуществлялось по шифрованному каналу. Проверить доступность незащищённых машин друг другу любым другим протоколом; проанализировать журналы IP-пакетов на координаторах. Скриншоты: – настройка максимального количества туннелей на координаторах; – скриншоты прохождения ICMP пакетов (ping) и любого другого трафика с незащищенного узла; скриншоты журнала IP-пакетов координатора с установленным фильтром «Туннелирование» для проверки прохождения ICMP-пакетов и любого другого трафика с помощью туннелирования.	ГИА/ДЭ ПУ
ВАРИАТИВНАЯ ЧАСТЬ	
Модуль 1: Защита информации в автоматизированных системах программными и программно-аппаратными средствами	
Задание модуля 1: Работа с защищенным служебным носителем информации. (Продукт компании ОКБ «САПР», универсальная защищенная флешка «Секрет особого назначения». Осуществить первоначальную инициализацию носителя: задать имя Секрета Особого Назначения по шаблону: SECRET_*ФАМИЛИЯ* и пароль администратора, который соответствует паролю Администратора Удостоверяющего и ключевого центра От лица Администратора задать политики доступа Установить политику при заполнении журнала: Блокировать при переполнении Установить политики использования кода авторизации: Длина кода авторизации от 6 до 10 Число ошибок авторизации пользователя до блокировки - 5 Установить размеры журнала и скрытого раздела диска Размер раздела для журнала: Мб Размер раздела для данных: Мб Задать пароль пользователя Секрета Особого Назначения по шаблону: *ФАМИЛИЯ* Сохранить регистрационную информацию (S/N, Имя Секрета, Код авторизации, PUK-код) в отчет. Записать дистрибутивы ключей на служебный носитель Выгрузить журнал событий Секрета Особого Назначения, сделать скриншоты журнала событий Зафиксировать выполнение работы скриншотами, сделать отчет	ГИА/ДЭ ПУ (вариативная часть)

Приложение №2

Форма заявления о закреплении темы дипломной работы (проекта)

Председателю предметной
(цикловой) комиссии
_____
(И.О. Фамилия)
_____
(фамилия, имя, отчество студента)
_____
(специальность)
_____
(номер учебной группы)
тел. студента _____
e-mail студента _____

Заявление

Прошу закрепить тему дипломной работы
«_____»

Участниками коллективной выпускной квалификационной работы являются студенты*: _____
(Фамилия И.О, номер учебной группы)

«____»_____ 20 __ г.
_____
(подпись студента)

Согласовано:

Руководитель ВКР
_____ _____
(подпись) (И.О. Фамилия)
«___»_____20__ г.

Председатель предметной (цикловой)
комиссии _____ _____
(подпись) (И.О. Фамилия)
*Раздел включается в заявление в случае выполнения коллективной ВКР

Приложение №3

Примерная тематика дипломных работ (проектов)

Примерный перечень тем дипломных работ на 2023-2024 годы.

1. Совершенствование комплексной системы безопасности СОТ предприятия в банковской сфере.
2. Совершенствование системы информационной безопасности госбюджетной организации.
3. Разработка периметрической СОС гос. бюджетных организаций. обнаружения нарушителя на основе радиочастотной технологии.
4. Разработка рекомендаций по организации технической защиты информационных системы гос. предприятия.
5. Разработка комплексной системы безопасности Бизнес-Центра.
6. Разработка инженерно-технической системы защиты ювелирного предприятия.
7. Разработка интегрированной системы защиты информации офисного здания коммерческого предприятия.
8. Модернизация системы СКУД на предприятии.
9. Разработка СОТС для дополнительного офиса банка и ее интеграция с другими системами инженерно-технической защиты информации
10. Модернизация системы видеонаблюдения офисного здания предприятия банковского сектора.
11. Разработка инженерно-технической защиты ЦОД промышленного предприятия.
12. Разработка системы защиты помещений Vip-этажа коммерческой организации.
13. Реализация проектно-технологических решений по внедрению DLP-системы в доменную среду
14. Анализ требований ГОСТ Р 56939-2016 к разработке безопасного программного обеспечения на примере программной платформы .NET Framework
15. Разработка лабораторного комплекса по формированию подсистемы управления распределенной СЗИ
16. Разработка лабораторного комплекса по формированию распределенной системы защиты информации
17. Анализ синергетических эффектов взаимодействия в сложных системах безопасности
18. Разработка онтологии информационной безопасности как основы для системы реагирования на инциденты

19. Исследование возможностей IBM QRadar Security Intelligence как платформы для SIEM системы в корпоративной сети
20. Разработка частной модели угроз безопасности информационной системы персональных данных «Деканат»
21. Выявление событий информационной безопасности с помощью индикаторов компрометации
22. Разработка методики категорирования объектов критической информационной инфраструктуры на примере железнодорожного узла
23. Разработка программного модуля автоматического определения тональности текста для обнаружения запрещённой информации на веб-ресурсах
24. Разработка рекомендаций по совершенствованию системы информационной безопасности бюджетного предприятия на основе аудита
25. Разработка программно-аппаратного комплекса для аудита безопасности беспроводных сетей
26. Разработка программных модулей оформления и контроля допуска в системе защищенного делопроизводства
27. Разработка программного обеспечения для аудита информационной безопасности с использованием контейнеризации приложений
28. Программный комплекс для проверки исходных текстов языка Go по требованиям приказа ФСТЭК России от 2 июня 2020 г. №76
29. Разработка динамического упаковщика для безопасного исполнения бинарных файлов
30. Разработка системы менеджмента информационной безопасности для предприятия -лицензиата ФСТЭК РФ
31. Разработка лабораторного практикума для изучения угроз безопасности блокчейн-сетей
32. Разработка учебного практикума по изучению системы обнаружения вторжений на базе нейронной сети
33. Разработка лабораторного практикума для проведения инструментального аудита безопасности информации
34. Использование технологии фаззинга для повышения безопасности информации, содержащейся в приложениях
35. Разработка модели компании занимающийся аутсорсингом информационной безопасности
36. Реализация аудита информационной безопасности организации с помощью методов социальной инженерии
37. Некоторые тренды обеспечения информационной безопасности в научной/образовательной организации
38. Обеспечение информационной безопасности с помощью квантовых технологий: КРК (QKD) и др.

39. Перспективные направления защиты информации от разведывательных БЛА
40. Разработка алгоритма и программного обеспечения подбора оборудования для безопасного хранения данных в автоматизированной системе
41. Построение и исследование СЗИ предприятия с помощью программно-аппаратные средств компании "ИнфоТеКС"
42. Построение и исследование механизмов мониторинга регистрации событий в информационной системе предприятия
43. Анализ и обеспечение безопасности веб-приложений, разработанных на основе JavaScript
44. Защита информации при использовании облачных сервисов
45. Анализ современных подходов к информационной безопасности веб-ресурсов
46. Применение принципов информационной безопасности к защите платформы «ИТ-ЦНТИ»
47. Разработка учебного стенда по дисциплине МДК.02.01 по реализации задач пентестинга информационных систем
48. Проектирование и разработка системы распознавания опасных объектов на базе нейронных сетей
49. Разработка рекомендаций по защите информации от атак социальной инженерии применительно к организации банковского сектора.
50. Выявление психологического профиля оператора АСУ для защиты объекта критической инфраструктуры
51. Исследование Bug Bounty программ и анализ их эффективности в устранении веб-уязвимостей
52. Обеспечение аппаратно-программной защиты корпоративных систем документооборота от утечки данных
53. Анализ программного обеспечения для фильтрации корпоративного почтового трафика
54. Анализ возможностей квантовой криптографической системаы ViPNet QTS для обеспечения безопасности инфраструктуры предприятия
55. Особенности использования квантовой криптографической системы выработки и распределения ключей (ККС ВРК) ViPNet QTS Lite для защиты предприятия
56. Исследование квантовых алгоритмов Шора
57. Исследование уязвимостей сети 5G применяющей технологию "Network slicing"
58. Система безопасного входа в информационных системах при помощи биометрических данных человека
59. Анализ и исследование энергопотребления и защищенности в беспроводных сенсорных сетях

60. Структура и функции системы обеспечения безопасности компьютерной сети
61. Риск-анализ исследуемых систем, в отношении которых реализуются выявленные угроз информационной безопасности
62. Проект защищенной мультисервисной корпоративной сети транспортного предприятия
63. Разработка математической модели злоумышленника/выявленной атаки информационной безопасности
64. Разработка комплекса защитных мер по обеспечению информационной безопасности баз данных
65. Автоматизация и обеспечение информационной безопасности системы Service Desk
66. Разработка системы информационной безопасности ЛВС SEO-компании
67. Разработка киберучений для персонала в области ИБ
68. Разработка системы менеджмента ИБ для предприятия
69. Анализ и выбор коммутационного оборудования для системы ИБ на предприятии
70. Разработка схемы защищенного взаимодействия с клиентами
71. Разработка и настройка защищенной сетевой инфраструктуры в процессе перехода на импортозамещение
72. Исследование векторов атак на ПО
73. Построение адаптивной виртуальной защищённой среды
74. Разработка менеджера паролей с функцией управления ключами аутентификации с использованием фреймворка React
75. Алгоритмы выявления финансовых махинаций в социальных сетях
76. Защита банковской информации в автоматизированной системе обслуживания клиентов банка
77. Анализ применение технологий OSINT для анализа социальных сетей
78. Программно-аппаратный комплекс голосования с использованием специализированного QR-кода
79. Защищенная волоконно-оптическая система передачи информации на основе технологии GPON
80. Беспроводной модуль управления системы «Умный офис» с защищенным каналом связи
81. Проектирование и разработка защищённой системы видеонаблюдения режимного объекта
82. Разработка системы охранно-пожарной сигнализации на основе комбинированного извещателя с защищенным каналом связи
83. Анализ использования легковесного модуля защиты информации для Ethernet устройства
84. Радиорелейная система передачи конфиденциальной информации

85. Обеспечение защищенного документооборота между компанией-налогоплательщиком и государственными контролирующими органами
86. Организация защищенного сегмента сети научно-исследовательского центра для обработки информации с ограниченным доступом
87. Применение программных средств обеспечения безопасности веб-сайтов на примере обеспечения защиты от XSS атак
88. Разработка автоматизированной системы динамического анализа вредоносных файлов на основе технологии «Песочница»
89. Разработка проекта единой системы идентификации и аутентификации на предприятии
90. Блок защиты информации каналов управления автоматизированной системы спутниковой связи
91. Анализ современных средств защиты от SQL атак
92. Анализ средств обеспечения безопасности движения беспилотных автомобилей с использованием беспроводных сетей 5G
93. Разработка корпоративной сети образовательной организации с подключением удаленных филиалов по каналам VPN
94. Разработка рекомендаций по поиску и нейтрализации специальных технических средств (стс) несанкционированного съёма информации в компании по разработке ПО
95. Совершенствование системы защиты персональных данных в бюджетной организации
96. Анализ уязвимостей протокола ОКС-7 в мобильной среде
97. Использование экосистемного подхода при разработке системы обеспечения кибербезопасности
98. Создание модульной обучающей системы по изучению продуктов компании «Инфотекс»
99. Расследование инцидента информационной безопасности, связанного с уязвимостью libssh
100. Расследование инцидента информационной безопасности связанного с эксплуатацией уязвимости токенов доступа j-son web token
101. Изучение безопасности приложения для мобильной операционной системы «Аврора»
102. Исследование возможности использования персонального компьютера как подслушивающего устройства
103. Исследование механизма формирования временных меток файлов в ReFS
104. Исследование надежности механизма безопасности ASLR операционной системы Windows 10
105. Анализ возможностей безопасности ОС Android при разблокированной возможности получения прав суперпользователя

106. Исследование механизмов работы и поиск уязвимостей DLP-системы Falcongaze Secure Tower
107. Исследование защитных механизмов Libre Office Writer
108. Исследование уязвимостей в беконтактных смарт-картах с помощью приложений, использующих модуль NFC на ОС Android
109. Разработка модуля авторизации для HTTP-сервера под управлением Node.js на базе протокола OAuth 2.0
110. Исследование возможностей модернизации файловых утилит Linux для современных задач компьютерной безопасности
111. Построение защищенной сети для предприятия на базе технологий
112. Анализ возможностей интеграции API с механизмами защиты от ботов с помощью решений класса RASP
113. Разработка рекомендаций по организации разграничения доступа к информационным ресурсам организации на основе Astra Linux
114. Разработка метода защиты информации в телекоммуникационных системах с кодовым разделением каналов
115. Разработка способа оценки системы защиты информации по критерию оптимальной защищенности
116. Разработка подсистемы защиты персональных данных предприятия на базе операционной системы специального назначения LINUX
117. Исследование стойкости биометрических систем к имитации биометрических характеристик
118. Локализация рисков от внутреннего злоумышленника и их оценка для бизнес-процесса фирмы с использованием API (application programming interface)-подхода
119. Разработка рекомендаций по биометрической аутентификации клиентов банка при их обслуживании
120. Разработка рекомендаций по внедрению мобильных устройств на базе операционной системы Аврора в государственных учреждениях
121. Разработка рекомендаций по защите информации, циркулирующей в сегментах беспроводной сети организации на базе стандарта ШЕЕ 802.11п
122. Исследование алгоритмов аутентификации с нулевым разглашением секрета для RFID-метки на основе системы остаточных классов
123. Исследование алгоритмов защиты CMS системы управления веб сайтом на основе Wordpress
124. Разработка алгоритма обнаружения сетевых атак с применением нейронной сети
125. Разработка алгоритма повышения помехоустойчивости протокола аутентификации Фейге-Фиата-Шамира на основе модулярных кодов

126. Разработка алгоритма поиска и коррекции ошибок, возникающих в работе ключевой системы SPN-шифратора
127. Анализ возможностей аппаратно-программного комплекса контроля асимметричного трафика пограничных устройств в корпоративной сети
128. Разработка базы знаний для SIEM-систем на основе информации из открытых источников
129. Разработка метода аутентификации и идентификации на основе графического пароля
130. Разработка модуля распознавания эмоций разговора колл-центра с использованием рекуррентных искусственных нейронных сетей, для выявления нежелательного контента

Приложение №4

Форма задания на дипломную работу (проект)

ФИНУНИВЕРСИТЕТ
Колледж информатики
и программирования

УТВЕРЖДАЮ
Руководитель
дипломной работы (проекта)
_____
(наименование должности)
_____ _____
(подпись) (инициалы, фамилия)
«____»_____ 20 __ г.

ЗАДАНИЕ
на дипломную работу (проект)

студенту _____
(фамилия, имя, отчество)

1. Тема дипломной работы
   «_____»
2. Срок сдачи дипломной работы (проекта) «__»_____ 20 __ г.
3. Исходные данные
   _____
4. Перечень вопросов/задач, подлежащих разработке и изложению в дипломной работе (проекте):
   _____
   _____
5. Перечень графического/ иллюстративного/ практического материала:
   _____
   _____
6. Консультант (при наличии) дипломной работы (проекта) с указанием относящихся к ним разделов работы
   _____

Дата выдачи задания «___» _____ 20__г.

Задание принял к исполнению «___» _____ 20 __г. _____
(подпись студента)

Приложение №5

Форма отзыва руководителя на дипломную работу (проект)

Федеральное государственное образовательное бюджетное
учреждение высшего образования
«Финансовый университет при Правительстве Российской Федерации»
(Финансовый университет)

_____
(наименование структурного подразделения)

ОТЗЫВ
на дипломную работу
«_____»
(тема дипломной работы)
Студент _____
(фамилия, имя, отчество)
Специальность _____

1. Актуальность работы _____
2. Отличительные положительные стороны работы _____
3. Практическое значение _____
4. Уровень сформированности компетенций, продемонстрированный в ходе работы над дипломной работой (высокий, средний, низкий) _____
5. Отношение студента к выполнению дипломной работы, проявленные/не проявленные им способности _____
6. Степень самостоятельности студента и его личный вклад в раскрытие проблемы, разработку предложений по их решению _____
7. Доля (%) заимствований в дипломной работе_____
8. Недостатки и замечания по дипломной работе_____
9. Дипломная работа соответствует/не соответствует требованиям, предъявляемые к дипломным работам, может/не может быть рекомендована к защите на заседании ГЭК _____

Руководитель
дипломной работы _____ _____
(подпись) (инициалы, фамилии)
«___»_____ 20__ г.

Приложение №6

Форма рецензии на дипломную работу (проект)

РЕЦЕНЗИЯ
на дипломную работу (проект)

«_____»
(тема дипломной работы)

Студент (ка) _____
(фамилия, имя, отчество)

1. Соответствие дипломной работы заявленной теме и заданию на нее
   _____
2. Оценка качества выполнения каждого раздела
   _____
3. Оценка степени разработки поставленных вопросов и практической значимости дипломной работы_____
4. Общая оценка качества дипломной работы _____

_____ _____ _____
(ученое звание, степень, должность) (подпись) (инициалы,фамилия)

«___»_____ 20__ г. М.П.

Приложение №7

Форма титульного листа дипломной работы (проекта)

Федеральное государственное образовательное бюджетное учреждение высшего образования
«Финансовый университет при Правительстве Российской Федерации»
(Финансовый университет)

_____
(наименование структурного подразделения)

Дипломная работа

Тема: «_____»

Студент (ка) _____
(фамилия, имя, отчество полностью)

Специальность _____
(код и наименование специальности)

Руководитель
дипломной работы _____ _____
(подпись) (инициалы, фамилия)

Консультант
дипломной работы _____ _____
(при наличии) (подпись) (инициалы, фамилия)

Председатель предметной
(цикловой) комиссии _____ _____
(подпись) (инициалы, фамилия)

_____- 202_ г.
(город)