Смоленский колледж телекоммуникаций (филиал)
федерального государственного образовательного бюджетного
учреждения высшего образования
«Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича»

СОГЛАСОВАНО

Ведущий специалист-эксперт
отдела по защите
информации ГУ-ОПФ
по Смоленской области
Ефремов А.А.
«31» 08 2023г

УТВЕРЖДАЮ
Директор
СКТ(ф)СПбГУТ
А.В. Казаков
«____» _____2023г.

СМОЛЕНСК
ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 00B182C091A307CBE4CFE66639F436FFDC
Владелец: Казаков Андрей Викторович
Действителен: с 12.05.2023 до 04.08.2024

Фонд контрольно-оценочных средств по профессиональному модулю

«ПМ.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных в том числе, криптографических средств защиты»

основной образовательной программы (ООП) по специальности СПО

10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

2023г.

Утверждаю
Зам. директора по УР
_____ И.В. Иванешко
«31» 08 2023 г.

Рассмотрено
методической комиссией
компьютерных сетей и администрирование
Председатель
_____ О.С. Скряго
«31» 08 2023г.

Разработчики:
Скряго О.С. - преподаватель высшей квалификационной категории СКТ (ф) СПбГУТ

2

Содержание

Общие положения

Контрольно-оценочные средства (КОС) предназначены для контроля и оценки результатов освоения профессионального модуля «ПМ.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных в том числе, криптографических средств защиты»

В состав комплекта КОС входят паспорт, оценочные средства, задания для экзаменующегося, пакет экзаменатора, литература, критерии оценки. Количество вариантов задания для экзаменующихся - 15. В каждом задании указаны: инструкция по выполнению, оборудование, материалы, которыми можно воспользоваться (раздаточный материал, технические описания, инструкции по установке), время выполнения.

Результатом освоения профессионального модуля является готовность студента к выполнению вида профессиональной деятельности Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты и составляющих его профессиональных компетенций, а также общие компетенции, формирующиеся в процессе освоения ООП в целом.

Формой аттестации по профессиональному модулю является экзамен (квалификационный). Форма проведения экзамена - выполнение кейс-заданий.

Итогом экзамена является однозначное решение: «вид профессиональной деятельности освоен /не освоен» с выставлением оценки по пятибалльной шкале (от двух до пяти баллов).

1. Формы контроля и оценивания элементов профессионального модуля

Элемент модуля	Форма контроля и оценивания	
	Промежуточная аттестация	**Текущий контроль**
МДК02.01 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты	дифференцированный зачет	лабораторно-практические занятия, тестирование
МДК02.02 Криптографическая защита информации	дифференцированный зачет	лабораторно-практические занятия, тестирование
Учебная практика УП.02	дифференцированный зачет	Тестирование, аттестационные листы по учебной практике
Производственная практика ПП.02 (по профилю специальности)	дифференцированный зачет	аттестационные листы, дневник и отчеты по производственной практике

2. Результаты освоения модуля, подлежащие проверке на экзамене (квалификационном)

2.1 В результате аттестации по профессиональному модулю осуществляется комплексная проверка следующих профессиональных и общих компетенций:

Таблица 2.1

Код	Профессиональные и общие компетенции
ПК 2.1	Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных систем и сетей.
ПК 2.2	Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях.
ПК 2.3	Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявляемыми требованиями.
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 09.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.

2.2. Требования к курсовому проекту. Подготовка и защита проекта.

Выполнение курсового проектирования проводится в соответствии с положением о курсовом проектировании, утвержденного директором колледжа.

Темы курсового проекта:

1. Модель угроз НСД на предприятии
2. Проведение классификации АС и СВТ по требованиям ФСТЭК на предприятии
3. Проведение классификации ПО по требованиям ФСТЭК на предприятии
4. Проведение классификации МЭ по требованиям ФСТЭК на предприятии
5. Построение модели нарушителя по требованиям ФСТЭК на предприятии
6. Построение модели нарушителя по требованиям ФСБ на предприятии
7. Модель угроз безопасности ИС персональных данных на предприятии
8. Комплексная модель защиты информации на предприятии.
9. Оценка эффективности существующих программных и программно-аппаратных средств защиты информации с применением специализированных инструментов и методов (индивидуальное задание)
10. Обзор и анализ современных программно-аппаратных средств защиты информации (индивидуальное задание)
11. Выбор оптимального средства защиты информации исходя из методических рекомендаций ФСТЭК и имеющихся исходных данных (индивидуальное задание)
12. Применение программно-аппаратных средств защиты информации от различных типов угроз на предприятии (индивидуальное задание)
13. Проблема защиты информации в облачных хранилищах данных и ЦОДах
14. Защита сред виртуализации.

Курсовой проект содержит увеличенную проектную часть, с подробным описанием технологических процессов, а также их обоснованием. Основное внимание в проектной части уделяется разработке комплекса мероприятий по теме исследования, расчет оборудования и др. позволяющих после их реализаций обеспечить технический эффект. При этом важно определить состав мероприятий, содержание, последовательность и сроки внедрения. Обязательно надлежит дать их экономическое обоснование путем сопоставления разработанного варианта с фактическим положением дела

Структура курсового проекта:

- введение
- основная часть (пояснительная записка по разделам)
- заключение (выводы и предложения)
- библиографический список (литература)
- приложения.

Во введении следует раскрыть теоретическое и практическое значение темы курсового проекта, обосновать ее актуальность, определить цель и задачи, объект и предмет проектирования, указать теоретическую основу проекта и практическую базу. Объем введения не должен превышать 1 страницу машинописного текста.

Основная часть состоит из разделов, подразделов, пунктов, подпунктов (при необходимости) в соответствии с логической структурой изложения. Объем основной части превышать 15 страниц машинописного текста. Разделы должны содержать ссылки на источники и литературу, а также ссылки на приложения.

Заключение содержит выводы и предложения с их кратким обоснованием в соответствии с поставленной целью и задачами, раскрывает значимость полученных результатов. Объем страниц заключения не должен превышать 2 страниц машинописного текста.

Библиографический список должен содержать не менее 10 источников. Библиографический список отражает перечень источников, которые использовались при написании курсового проекта, показывает глубину и широту изучаемой темы и документально подтверждает достоверность и точность приводимых в тексте заимствований (цитат, фактов, формул и других документов). При написании курсового проекта следует ориентироваться на наиболее свежие фактические данные, относящиеся к последнему году. Разрешается использование только действующих нормативных документов. Список использованных источников и литературы располагается в систематическом порядке:

- законодательные и нормативные акты: Конституция Российской Федерации; законы, указы, постановления, распоряжения высших, региональных и муниципальных органов государственной власти Российской Федерации;
- учебная и научная литература: учебники и учебные пособия; монографии; сборники статей;
- периодические издания;
- Интернет - источники.

Объем курсового проекта составляет не менее 20 страниц и не более 25 страниц машинописного текста, не включая приложения.

Информационное обеспечение

Электронные издания (электронные ресурсы)

ОИ.1 Акимова, О. Ю. Хранение и защита компьютерной информации : лабораторный практикум / О. Ю. Акимова. — Москва : Издательский Дом МИСиС, 2020. — 76 с. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/106895

ОИ.2 Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 с. — ISBN 978-5-4488-0070-2. — Текст: электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/87995

ОИ.3 Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2022. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/497433

3.2.2. Дополнительные источники

ДИ.1Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / ДИ.2 О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2022. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/495524

ДИ.3 Лапонина, О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия : учебное пособие / О. Р. Лапонина ; под редакцией В. А. Сухомлина. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 605 с. — ISBN 978-5-4497-0684-3. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование: [сайт]. — URL: https://profspo.ru/books/97571

ДИ.4 Бахаров, Л. Е. Информационная безопасность и защита информации (разделы криптография и стеганография) : практикум / Л. Е. Бахаров. — Москва : Издательский Дом МИСиС, 2019. — 59 с. — ISBN 978-5-906953-94-0. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/98171

Интернет ресурсы и источники:

1. Электронно-библиотечная система издательства «Лань» [Электронный ресурс]. – Режим доступа: e.lanbook.com
2. Электронно-библиотечная система «Ibooks.ru» [Электронный ресурс]. – Режим доступа: ibooks.ru
3. Электронно-библиотечная система «IPRbook» [Электронный ресурс]. – Режим доступа: iprbookshop.ru
4. Электронно-библиотечная система издательства « [Электронный ресурс]. – Режим доступа: profspo.ru/

Оценка проекта (включая структуру и оформление)

Предмет(ы) оценивания	Показатели оценки	Критерии оценки	Вес критерия
ПК 2.1 Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных систем и сетей. ПК 2.2 Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях. ПК 2.3 Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно-	Разработка и оформление проекта Использование современных источников информации Выполнение расчетов с применением программных продуктов Результативность и своевременность выполнения текущих заданий по курсовому проекту Обоснованность и	Соответствие содержания курсового проекта выбранной теме Соответствие требованиям ГОСТ и ЕСКД оформления Сроки выполнения проекта Правильность выполнения расчетов	6 баллов 5 баллов 5 баллов 5 баллов

телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявляемыми требованиями. 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 09. Использовать информационные технологии в профессиональной деятельности. ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.	правильность выбора оборудования Соответствие комплектации оборудования выполненным расчетам		

Оценка защиты проекта

Предмет(ы) оценивания	Показатели оценки	Критерии оценки	Вес критерия
ОК3. Планировать и реализовывать собственное профессиональное и личностное развитие. ОК 09. Использовать информационные технологии в профессиональной деятельности.	Формат защиты	Время защиты – 10 минут, аргументированность и четкость изложения	5 баллов
	Презентация	Выполнение в соответствии с требованиями	2 балла
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	Ответы на вопросы	Полнота ответа	3 балла

Курсовой проект представляется и защищается в сроки, предусмотренные графиком выполнения курсовых проектов по МДК. Курсовой проект должен быть сдан преподавателю - руководителю не позднее, чем за 5 дней до назначенного срока защиты. Если курсовой проект не представлен в назначенный срок по уважительной причине, студенту определяется новый срок представления проекта. Если курсовой проект был представлен в срок, но при этом не соответствовал требованиям по содержанию и (или) оформлению, то такой проект возвращается студенту для доработки.

Критерии формирования оценки за курсовой проект:

Шкала перевода баллов в оценки:

оценки за курсовой проект	**Количество баллов**
«5» (отлично)	31-27
«4» (хорошо)	26-21
«3» (удовлетворительно)	20-15
«2» (не удовлетворительно)	менее 14

Студент, не защитивший проект, допускается к повторной защите не ранее чем через два дня.

Итоговая оценка по курсовому проекту выставляется непосредственно после защиты курсового проекта.

3. Оценка освоения теоретического курса профессионального модуля

Междисциплинарные курсы МДК для проведения промежуточной аттестации применяется тестирование. Кос промежуточной аттестации МДК 02.01 и МДК 02.02 прилагаются отдельным документом.

Итоговая ведомость успеваемости дифференцированного зачета
МДК 02.01 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты
Группа _____ Курс ____ Специальность

ФИО студента	Тест (оценка 3-5) **ДЗ**

Итоговая ведомость успеваемости дифференцированного зачета
МДК 02.02 Криптографическая защита информации
Группа _____ Курс ____ Специальность

ФИО студента	Тест (оценка 3-5) **ДЗ**

4. Требования к аттестации по учебной и производственной практике

КОС по учебной практики УП.02, КОС по производственной практики ПП.02 прилагаются отдельным документом.

5. Оценочные средства для проведения промежуточной аттестации – экзамена квалификационного

Прилагается отдельным документом

Приложение 1

Матрица оценок КОС экзамена квалификационного по ПМ

ПМ.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты

Коды проверяемых компетенций	**Результаты (освоенные профессиональные компетенции)**	**Основные показатели оценки результата** (ОПОР)	**Формы и методы контроля и оценки**	**Оценка выполнения работ (положительная – 3,4,5 - освоена / отрицательная – 2)*, не освоена**
ПК 2.1 ОК 1 ОК 2	Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных систем и сетей. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	ОПОР1 выявлять и оценивать угрозы безопасности информации в ИТКС; ОПОР2 настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; ОПОР3 проводить установку и настройку программных и программно-аппаратных (в том числе криптографических) средств защиты информации; ОПОР 4 проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации;	Правильное выявление и оценивание угрозы безопасности информации в ИТКС; Правильная настройка и применения средства защиты информации в операционных системах, в том числе средства антивирусной защиты; Правильная проведена установка и настройка программных и программно-аппаратных (в том числе криптографических) средств защиты информации; Правильное проведение конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации;	*2,3,4,5*

ПК 2.2 ОК 03 ОК 04	Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях. Планировать и реализовывать собственное профессиональное и личностное развитие. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	ОПОР 1 выявлять и оценивать угрозы безопасности информации в ИТКС; ОПОР 5 проводить контроль показателей и процесса функционирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации; ОПОР 6 проводить восстановление процесса и параметров функционирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации; ОПОР 7 проводить техническое обслуживание и ремонт программно-аппаратных (в том числе криптографических) средств защиты информации;	Правильное выявление и оценивание угрозы безопасности информации в ИТКС; Правильно проведен контроль показателей и процесса функционирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации; Правильно проведено восстановление процесса и параметров функционирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации; Правильно проведено техническое обслуживание и ремонт программно-аппаратных (в том числе криптографических) средств защиты информации;	*2,3,4,5*
ПК 2.3	Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявляемыми требованиями.	ОПОР 1 выявлять и оценивать угрозы безопасности информации в ИТКС; ОПОР2 настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; ОПОР4 проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации;	Правильное выявление и оценивание угрозы безопасности информации в ИТКС; Правильная настройка и применения средства защиты информации в операционных системах, в том числе средства антивирусной защиты; Правильное проведение конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации;	

Приложение 2

Матрица оценок КОС курсового проектирования по ПМ

ПМ.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты

Коды проверяемых компетенций	**Результаты (освоенные профессиональные компетенции)**	**Основные показатели оценки результата** (ОПОР)	**Формы и методы контроля и оценки**	**Оценка выполнения работ (положительная – 3,4,5, освоена / отрицательная – 2)*, не освоена**
ПК 2.1 ПК 2.2 ПК 2.3	Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных систем и сетей. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно-телекоммуникационных системах и сетях с	ОПОР 1 Соответствие содержания курсового проекта выбранной теме	Правильность исходных данных, соответствие темы	2,3,4,5
		ОПОР 2 Соблюдение требований к выполнению текстовых документов	Выполнение требований в соответствии с положением об организации выполнения и защиты курсовых проектов	2,3,4,5
		ОПОР 3 Соответствие оформления графической части	Выполнение требований в соответствии с положением об организации выполнения и защиты курсовых проектов	2,3,4,5
		ОПОР 4 Использование современных источников информации	Список используемой литературы содержит нормативные документы, литературу не старше 5 лет, электронные ресурсы с современным материалом по теме.	2,3,4,5
		ОПОР 5 Выполнение расчетов с применением программных продуктов	Корректный расчет, построение с помощью MS Office	2,3,4,5
		ОПОР 6 Результативность и своевременность выполнения текущих заданий по курсовому проекту	Приведен правильный анализ согласно теме проекта Приведен правильный вывод согласно теме проекта	2,3,4,5
		ОПОР 7 Правильность выполнения расчетов	Правильное выполнение расчетов оборудование, программного обеспечения, технических средств защиты, рисков.	2,3,4,5
		ОПОР 8 Обоснованность и правильность выбора программного обеспечения и технических средств защиты	Убедительно аргументирован выбор программного обеспечения, технические средства защиты	2,3,4,5

ОК 01 ОК 02 ОК03 ОК04 ОК09 ОК 10	использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявляемыми требованиями. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности. Планировать и реализовывать собственное профессиональное и личностное развитие. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами. Использовать информационные технологии в профессиональной деятельности. Пользоваться профессиональной документацией на государственном и иностранном языках.	ОПОР 9 Своевременность выполнения курсового проекта	График выполнения курсового проекта не нарушен, сроки защиты соответствуют учебному плану	2,3,4,5
		ОПОР 10 Убедительная защита курсового проекта.	Грамотная, убедительная защита. Поддержание диалога с аудиторией. Корректные ответы на вопросы, аргументированная точка зрения	2,3,4,5
		ОПОР 11 Демонстрация результатов работы с помощью презентации	Правильная структура презентации, отражение на ней всех этапов работы, полученных результатов; используется анимация для лучшей наглядности	2,3,4,5

Приложение 3

Итоги КУРСОВОГО ПРОЕКТА по профессиональному модулю

ПМ.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты

Группа _____ Курс____ Специальность 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

Коды проверяемых компетенций	ПК 2.1, ПК2.2, ПК 2.3 ОК 3, ОК 4, ОК9												
ФИО студентов	**Коды основных показателей оценки результата** (ОПОР)											**Интегральная оценка (медиана)**	**Примечание**
	ОПОР 1	ОПОР 2	ОПОР 3	ОПОР 4	ОПОР 5	ОПОР 6	ОПОР 7	ОПОР 8	ОПОР 9	ОПОР 10	ОПОР 11	**ОПОР***	*При равном количестве интегральных оценок, например 3,4,3,4, выставляется оценка 4.

Преподаватель _____

Председатель методической комиссии компьютерных сетей и администрированияи _____ Скряго О.С.

Дата «___»__20__г.

Приложение 4

Итоговая ведомость успеваемости

ПМ.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты

Группа _____ Курс____ Специальность 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

ФИО студента	**Результаты промежуточной аттестации по ПМ**				**№ билета**	**Результаты экзамена квалификационного по ПМ*** (экспертные оценки)				**ВПД** Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты	Примечание
	Итоговая оценка по МДК.02.01 (оценки 2-5)	Итоговая оценка по МДК.02.02 (оценки 2-5)	Итоговая оценка по УП.02 (оценки 2-5)	Итоговая оценка по ПП.02 (оценки 2-5)		ПК 2.1 (оценки 2-5)	ПК 2.2 (оценки 2-5)	ПК 2.3 (оценки 2-5)	ОК 1-4, 9,10 (оценки 2-5)	Итоговая оценка (медиана)	Экспертные оценки качества выполнения заданий выставляются по пятибалльной шкале * при одинаковом количестве экспертных оценок, например 4,3,4,3, выставляется оценка - 4
1.											
2.											
3.											
4.											
5.											
6.											
7.											
8.											
9.											
10.											

Председатель комиссии _____

Члены комиссии _____ _____

«___»_____20___г.

Приложение 5

Оценочная ведомость по профессиональному модулю

ОЦЕНОЧНАЯ ВЕДОМОСТЬ ПО ПРОФЕССИОНАЛЬНОМУ МОДУЛЮ

ПМ.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты

код и наименование профессионального модуля

ФИО _____

обучающийся на ___ курсе по специальности СПО 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

наименование

освоил(а) программу профессионального модуля **Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты**

наименование профессионального модуля

в объеме ____ академических часа с «___» _____20___г. по «___»_____20___г.

Результаты промежуточной аттестации по элементам профессионального модуля

Элементы модуля (код и наименование МДК, код практик)	**Формы промежуточной аттестации**	**Оценка**	**Примечание**
МДК 02.01 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты	Дифференцированный зачёт		тестирование, лабораторно-практические занятия
МДК 02.02 Криптографическая защита информации	Дифференцированный зачёт		тестирование, практические занятия
УП.02 Учебная практика	Дифференцированный зачёт		Аттестационные листы по учебной практике, тестирование
ПП. 02 Производственная практика (по профилю специальности)	Дифференцированный зачёт		аттестационный лист, отчет и дневник прохождения производственной практике

Заведующий учебной частью _____ Дроздович С.Н.

Приложение 6

Итоги экзамена (квалификационного) по профессиональному модулю
ПМ.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты

Студент _____ Группа _____ Курс ___
Специальность 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем
Билет № __

Коды проверяемых компетенций	**Коды основных показателей оценки результата** (ОПОР)	**Оценка выполнения работ** (положительная – 3,4,5 / отрицательная – 2)				**Интегральная оценка** (медиана)		**Итоговая оценка**	**Примечание**
						ОПОР	ПК*		* при одинаковом количестве интегральных оценок, например 4,3,4,3, выставляется оценка - 4 .
ПК 2.1 ОК 1 ОК 2	ОПОР 1								
	ОПОР 2								
	ОПОР 3								
	ОПОР 4								
ПК 2.2 ОК 3 ОК 4	ОПОР 1								
	ОПОР 5								
	ОПОР 6								
	ОПОР 7								
ПК 2.3 ОК 9 ОК 10	ОПОР 1								
	ОПОР 2								
	ОПОР 4								

Председатель комиссии _____
Члены комиссии _____
_____
_____

«___»_____20___г.