ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ И НАУКИ ТЮМЕНСКОЙ ОБЛАСТИ

ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ТЮМЕНСКОЙ ОБЛАСТИ
«ТЮМЕНСКИЙ КОЛЛЕДЖ ПРОИЗВОДСТВЕННЫХ И СОЦИАЛЬНЫХ ТЕХНОЛОГИЙ»
(ГАПОУ ТО «ТКПСТ»)

СОГЛАСОВАНО

Генеральный директор
Общества с ограниченной
ответственностью
«Компания «мир визуальных
коммуникаций»

_____ Попов Р.В.
подпись
«19» 12 2019 г.

УТВЕРЖДЕНО

Директор Государственного автономного
профессионального образовательного
учреждения Тюменской области
«Тюменский колледж производственных и
социальных технологий»

_____ Т.Е. Шпак
подпись
«16» 12 2019 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ»

г. Тюмень, 2019 год

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ»

1. Цели реализации программы

Программа повышения квалификации направлена на обучение лиц, имеющих и (или) получающих среднее профессиональное и (или) высшее образование, различного возраста для совершенствования и (или) получения новой компетенции, необходимой для профессиональной деятельности, и (или) повышения профессионального уровня в рамках имеющейся квалификации, в том числе для работы с конкретным оборудованием, технологиями, аппаратно-программными и иными профессиональными средствами.

2. Требования к результатам повышения квалификации. Планируемые результаты повышения квалификации.

2.1. Характеристика новой компетенции, трудовых функций и (или) уровней квалификации.

Программа предназначена для совершенствования и (или) получения новой компетенции, необходимой для профессиональной деятельности, и (или) повышения профессионального уровня в рамках имеющейся квалификации и разработана в соответствии с:

– профессиональным стандартом 06.033 Специалист по защите информации в автоматизированных системах, зарегистрированный в Министерстве юстиции Российской Федерации 28 сентября 2016 года, регистрационный № 43857;

– спецификацией стандарта компетенции «Кибербезопасность».

Медицинские ограничения регламентированы Перечнем медицинских противопоказаний Министерства здравоохранения и социального развития РФ.

2.2 Требования к результатам освоения программы

В результате освоения программы слушатель должен:

Знать:

З-1 Нормативные правовые акты в области защиты информации

З-2 Организационные меры по защите информации

З-3 Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах

З-4 Принципы организации и структура систем защиты программного обеспечения автоматизированных систем

З-5 Особенности применения программных и программно-аппаратных средств защиты информации в автоматизированных системах

З-6 Технические средства контроля эффективности мер защиты информации

З-7 Организация защиты информации от «утечки» по техническим каналам на объектах информатизации

Уметь:

У-1 Устанавливать и настраивать операционные системы, системы управления базами данных, компьютерные сети и программные системы с учетом требований по обеспечению защиты информации

У-2 Применять технические средства контроля эффективности мер защиты информации

У-3 Работать со сканерами уязвимостей

У-4 Самостоятельно проверять технические средства и настройки сетевого и серверного программного обеспечение на наличие уязвимостей

У-5 Тестировать информационные системы и сервера на наличие известных и широко распространенных уязвимостей

У-6 Анализировать программный код веб-сервисов на наличие уязвимостей

У-7 Тестировать программное обеспечение, в том числе и веб-приложения, на наличие потенциальных и скрытых уязвимостей

У-8 Идентифицировать угрозы и уязвимости информационных систем и приложений.

Владеть трудовыми действиями (ТД1):

ТД-1 Ведение документов учета, обработки, хранения и передачи информации, составляющей тайну

ТД-2 Информирование персонала о правилах эксплуатации системы защиты автоматизированной системы и отдельных средств защиты информации

ТД-3 Уничтожение информации, обрабатываемой автоматизированной системой

ТД-4 Архивирование информации, обрабатываемой автоматизированной системой

ТД-5 Выявление угроз безопасности информации в автоматизированных системах

ТД-6 Принятие мер защиты информации при выявлении новых угроз безопасности информации

ТД-7 Обеспечение безопасности информации с учетом требования эффективного функционирования автоматизированной системы

Содержание программы

Категория слушателей: специалисты органов государственной власти, местного самоуправления, организаций и учреждений, осуществляющие разработку и эксплуатацию автоматизированных информационных систем, обеспечивающих обработку, хранение и передачу персональных данных.

Трудоемкость обучения: 72 ак. часов.

Форма обучения: очная.

3.1. Учебный план

№	Наименование учебных курсов, дисциплин, модулей, практик	Всего, академических часов	В том числе			Итоговый контроль	Консультации
			Теоретические занятия	Практические занятия	Лабораторные занятия		
1	2	3	4	5	6	7	8
1.	Раздел 1. Общие вопросы технической защиты информации	38	34	4	–	–	–
2.	Раздел 2. Организация обеспечения защиты персональных данных в информационных системах персональных данных	12	12	–	–	–	–
3.	Раздел 3. Организация обеспечения защиты персональных данных с использованием криптосредств	12	4	8	–	–	–
4.	Раздел 4. Обеспечение безопасности персональных данных при их обработке без использования средств автоматизации. Биометрические персональные данные	4	4	–	–	–	–
	Демонстрационный экзамен	6	–	–	–	6	–
	ИТОГО:	72	62	12	–	6	–

3.2. Учебно-тематический план

№ п/п	Наименование учебных курсов, дисциплин, модулей, разделов и тем практик	Содержание учебного материала, практические занятия	Объем часов (аудиторно)	Формируемые умения / знания / ТД
1.	**Раздел 1 Общие вопросы технической защиты информации**			
1.1	Тема 1.1. Правовые и организационно-распорядительные документы в области технической защиты информации.	**Содержание**	8	З-1
		Стратегия национальной безопасности Российской Федерации		
		Доктрина информационной безопасности Российской Федерации. Концептуальные основы защиты информации		
		Законодательные и иные правовые акты, регулирующие вопросы защиты информации		
		Задачи и функции Федеральной службы по техническому и экспортному контролю (ФСТЭК России)		
		Сертификация средств защиты информации, аттестация объектов информатизации по безопасности информации		
1.2	Тема 1.2. Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа	**Содержание**	12	З-3, З-4
		Целостность, конфиденциальность и доступность информации.		
		Классификационная схема угроз безопасности информации и их общая характеристика.		
		Особенности проведения комплексного исследования объектов информатизации на наличие угроз безопасности информации.		
		Характеристика основных классов атак, реализуемых в сетях общего пользования		
		Порядок обеспечения защиты информации при эксплуатации автоматизированных систем		
		Практическое занятие 1 Защита информации при работе с системами управления базами данных	2	У-1
1.3	Тема 1.3. Основные	**Содержание**	14	З-7

	организационные меры, технические средства защиты информации от утечки по техническим каналам на объектах информатизации и в защищаемых помещениях.	Причины и физические явления, порождающие технические каналы утечки информации (ТКУИ) при эксплуатации объектов информатизации и защищаемых помещений.		
		Классификация ТКУИ.		
		Методы и средства выявления ТКУИ на типовом объекте информатизации и в защищаемых помещениях		
		Практическое занятие 2 Защита информации, циркулирующей в системах звукоусиления и звукового сопровождения видео-кинофильмов	2	У-2
2.	**Раздел 2 Организация обеспечения защиты персональных данных в информационных системах персональных данных**			
2.1	Тема 2.1. Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных	**Содержание**	4	3-2, 3-4, 3-6
		Принципы обработки персональных данных и права субъекта персональных данных.		
		Основные принципы обеспечения безопасности персональных данных		
		Методы и способы защиты информации в информационных системах персональных данных.		
		Общий порядок организации обеспечения безопасности персональных данных в информационных системах персональных данных.		
2.2	Тема 2.2. Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.	**Содержание**	2	3-2
		Понятие «уровня важности» информационных систем персональных данных в зависимости от характера и объема обрабатываемых в них персональных данных		
		Описание пакетов обязательных требований по обеспечению безопасности для информационных систем персональных данных		
		Перечень основных этапов при организации работ по обеспечению безопасности персональных данных		
2.3	Тема 2.3. Рекомендации по обеспечению безопасности	**Содержание**	6	3-2, 3-6
		Комплекс организационных и технических мероприятий в		

	и контролю безопасности персональных данных при их обработке в информационных системах персональных данных	рамках подсистемы защиты персональных данных		
		Возможные варианты реализации мероприятий по защите персональных данных с использованием существующих сертифицированных средств защиты информации		
		Виды, формы и способы контроля защиты персональных данных в информационных системах обработки персональных данных		
3.	**Раздел 3 Организация обеспечения защиты персональных данных с использованием криптосредств**			
3.1	Тема 3.1. Рекомендации по обеспечению с помощью криптосредств безопасности персональных данных	**Содержание**	2	3-5
		Общие положения и организация обеспечения безопасности обработки персональных данных с использованием шифровальных (криптографических) средств		
3.2	Тема 3.2. Требования по организации и обеспечению функционирования шифровальных (криптографических) средств в случае их использования для обеспечения безопасности персональных данных.	**Содержание**	2	3-5
		Порядок обращения с криптосредствами и криптоключами к ним		
		Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены криптосредства или хранятся ключевые документы к ним.		
		Мероприятия при компрометации криптоключей		
		Практическое занятие 3	8	У-3 – У-8, ТД1 – ТД7
		Проведение аудита безопасности WEB-портала		
4.	**Раздел 4 Обеспечение безопасности персональных данных при их обработке без использования средств автоматизации. Биометрические персональные данные**			
4.1	Тема 4.1. Обеспечение безопасности персональных данных при их обработке без использования средств автоматизации	**Содержание**	2	3-2, 3-6
		Условия использования .типовых форм документов.		
		Меры по обеспечению безопасности персональных данных при обработке, осуществляемой без использования средств автоматизации		
4.2	Тема 4.2. Биометрические персональные данные	**Содержание**	2	3-1
		Требования к материальным носителям биометрических		

		персональных данных		
		Порядок передачи материальных носителей уполномоченным лицам		
		Обязанности операторов при использовании и хранении материальных носителей биометрических персональных данных.		
	Демонстрационный экзамен		**6**	ТД1 – ТД7
		Всего	**72**	

3.3. Календарный учебный график
(порядок освоения модулей, разделов, дисциплин)

Период обучения (дни, недели)*	Наименование раздела, модуля
1-5 день	Раздел 1. Общие вопросы технической защиты информации
6-8 день	Раздел 2 Организация обеспечения защиты персональных данных в информационных системах персональных данных
8 день	Раздел 3 Организация обеспечения защиты персональных данных с использованием криптосредств
9 день	Раздел 4. Обеспечение безопасности персональных данных при их обработке без использования средств автоматизации. Биометрические персональные данные Итоговая аттестация
* Точный порядок реализации разделов, модулей (дисциплин) обучения определяется в расписании занятий.	

4. Условия реализации программы

4.1. Материально-технические условия реализации программы

Наименование помещения	Вид занятий	Наименование оборудования, программного обеспечения
1	2	3
Лаборатория «3D моделирование»	Теоретические занятия	- Рабочее место преподавателя -1 (компьютер (Системный блок (i7-3.6-4,2GHz\H110\DDR4 2x16Gb\1000Gb+SSD250Gb\NV GTX1660-6GB\DVD±RW\Audio 8ch\Lan-Gbt\600W\Win10Pro)+Монитор 24» Samsung S24D300H, Клавиатура Logitech Keyboard K120, Мышь Logitech B100), МФУ (Kyocera ECOSYS M2235dn (A4, 35стр, 600 x600 dpi, 512Mb, ADF, Duplex, USB 2.0 (Hi-Speed), USB Host, Gigabit Ethernet)); - рабочие места обучающихся – 15 шт.; маркерная доска
Лаборатория «3D моделирование»	Практические занятия, итоговая аттестация	**Общее оснащение рабочих мест** **Оборудование:** **Рабочее место обучающегося:** – персональный компьютер с монитором, клавиатурой, колонками, мышь: (Процессор Intel Core i7-8700 S1151, 3.2-4.6GHz, 12MB, 6 core/12 thread, UHD 630, 65W Oem (SR3QS) – Кулер процессора S-1156/1155/1150/1151 Deepcool THETA 15 PWM 95W, 4pin, 28dB, 2000rpm, гидродинамический подшипник, вент. 100 мм – Материнская плата Gigabyte H310M H 2.0 (S-1151, Intel H310, 2*DDR4, PCI-Ex16, 2*PCI-Ex1, 4xSATA3, 7.1 Audio, D-sub/HDMI, GbE, mATX)

		– Память DDR4 16G Kingston HyperX Fury HX426C16FB/16 2666MHz CL16, 1.2V HX426C16FB3/16 – 2 шт – Блок питания 600W FSP QDION QD-600PNR 20+4/4+4/2*(6+2)pin, 6*SATA, 2*PATA (molex), 1*FDD, 120мм вентилятор, выключатель, 80+ – Видеокарта Asus TUF-GTX1660-O6G-GAMING nVidia GeForce GTX 1660 6144Mb 192bit GDDR5 1530, 8002 DVIx1, HDMIx1, DPx1, HDCP Ret – Твердотельный накопитель 250Gb Samsung 860 EVO MZ-76E250BW w520/r550, 90000/98000 IOPS – Жесткий диск 1Tb WD Blue WD10EZEX, 7200rpm, 64MB – Привод DVD±RW Lite-On iHAS122 SATA, черный – Операционная система Windows 10 Pro Rus 64bit DVD 1pk DSP OEI (право пользования) (FQC-08909-L), необходим FQC-08909-D – Операционная система Windows 10 Pro Rus 64bit DVD 1pk DSP OEI (установочный комплект) (FQC-08909-D), необходим FQC-08909-L – Монитор 24» Samsung S24D300H 1920x1080, 250 cd/m2, 1000:1, 170 /160 , 2ms, D-Sub/HDMI, черный (LS24D300HSI/RU) – Клавиатура Logitech Keyboard K120, USB, black, Rtl, [920-002522] – Мышь Logitech B100 Optical Mouse, USB, 800dpi, Black, [910-003357]) - личные мобильные устройства обучающихся и/или наставника с операционной системой Android - презентационное оборудование с возможностью подключения к компьютеру **Программное обеспечение:** - офисное программное обеспечение; **Расходные материалы:** – бумага А4 для рисования и распечатки – минимум 1 упаковка 200 листов; – бумага А3 для рисования – минимум по 3 листа на одного обучающегося; – набор простых карандашей – по количеству обучающихся; – набор чёрных шариковых ручек – по количеству обучающихся; – клей ПВА – 2 шт.; – клей-карандаш – по количеству обучающихся; – скотч прозрачный/матовый – 2 шт.; – скотч двусторонний – 2 шт.; – картон/гофрокартон для макетирования – 1200*800 мм, по одному листу на двух обучающихся;

		– нож макетный – по количеству обучающихся; – лезвия для ножа сменные 18 мм – 2 шт.; – ножницы – по количеству обучающихся; – коврик для резки картона – по количеству обучающихся; – линзы 25 мм или 34 мм – комплект, по количеству обучающихся; дополнительно – PLA-пластик 1,75 REC нескольких цветов.

4.2. Учебно-методическое обеспечение программы

Законодательные и нормативные документы:

1. Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании» (с изменениями на 28 ноября 2018 года)
2. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями на 1 мая 2019 года)
3. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (с изменениями на 31 декабря 2017 года)
4. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ (ТК РФ) (с изменениями на 02 августа 2019 года), гл. 14. Защита персональных данных работника (ст.ст. 85-90) / Раздел Ш. Трудовой договор (ст.ст. 5690). Часть третья (ст.ст. 55-250)
5. ГОСТ Р ИСО/МЭК 27001-2006 «Информационные технологии. Методы и средства обеспечения безопасности. Система менеджмента информационной безопасности. требования».
6. ГОСТ Р 52447-2005 «Защита информации. Техника защиты информации. Номенклатура показателей качества».
7. ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения».
8. ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» (взамен ГОСТ Р 51275-96).
9. ГОСТ Р 52863-2007 «Защита информации. Автоматизированные системы в защищенном исполнении. Испытания на устойчивость к намеренным силовым электромагнитным воздействиям. Общие требования».

Основная литература:

1. Бабаш А.В. Информационная безопасность: Лабораторный практикум / А.В. Бабаш Е.К. Баранова, Ю.Н. Мельников. – М.: КноРус, 2019. – 432 с.
2. Баранова Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. – М.: Риор, 2018. – 400 с.
3. Гришина, Н.В. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. – М.: Форум, 2018. - 118 с.
4. Нестеров С. А. Информационная безопасность – М.: Издательство Юрайт, 2017. – 321 с.

Дополнительная литература:

1. Кузнецова А.В. Искусственный интеллект и информационная безопасность общества / А.В. Кузнецова, С.И. Самыгин, М.В. Радионов. – М.: Русайнс, 2017. – 64 с.

Электронные ресурсы:

1. Консорциум «Кодекс» (электронный ресурс) режим доступа: https://kodeks.ru/

5. Оценка качества освоения программы

Итоговая аттестация по программе предназначена для оценки результатов освоения слушателем разделов программы. По результатам аттестации, выставляются отметки по двухбалльной системе «зачтено», «не зачтено». Итоговая аттестация включает в себя:

1) демонстрационный экзамен по компетенции «Кибербезопасность»;
2) тестирование.

Типовое задание демонстрационного экзамена по компетенции «Кибербезопасность» включает в себя:

Модуль № 1 Аудит безопасности

Задания для проведения демонстрационного экзамена:

– Время выполнения – 5 часов.

Обучающемуся необходимо провести исследование уязвимостей WEB-портала. В процессе выполнения задания потребуется провести анализ исходного кода приложения с целью повышения привилегий, извлечения ключа продукта или кодовой фразы. В заданиях на обратную разработку программного обеспечения флагом может являться парольная строка, ключ к ПО или файл, который Вы можете прочесть, только повысив свои привилегии. В заданиях на криптографию и стеганографию флагом является раскодированная строка, секретный ключ шифрования или скрытая стеганографией информация.

В результате работы на рабочем столе должен быть предоставлен файл с отчетом для системных администраторов с именем report_1, содержащий следующую информацию:

• Номер и ФИО участника.

• Таблица с отчетом по найденным уязвимостям, содержащую следующую информацию:

• № задачи (виртуальной машины);

• вид уязвимости;

• флаг;

• место расположение (позволяет точно идентифицировать нахождение уязвимости);

• краткое описание уязвимости.

Примеры тестовых заданий

Время выполнения тестирования – 1 час.

1. Какой документ определяет требования к защите персональных данных при их обработке в информационных системах персональных данных:

a. Постановление от 1 ноября 2012 г. N 1119;

b. Приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. N 21;

c. ФЗ -152 «О персональных данных».

2. Информационная система обрабатывающая персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных является:

a. информационной системой, обрабатывающей специальные категории персональных данных;

b. информационной системой, обрабатывающей биометрические персональные данные;

c. информационной системой, обрабатывающей общедоступные персональные данные;

d. информационной системой, обрабатывающей иные категории персональных данных.

3. В каком случае фотографию можно отнести к биометрическим персональным данным?

a. В случае если эта фотография находится в личном деле;

b. В случае если фотография зарегистрирована в СКУД (система контроля управления доступом);

c. В случае если эта фотография сделана в публичном месте.

4. Среда переноса от субъекта к объекту атаки (а, возможно, и от объекта к субъекту атаки) действий, осуществляемых при проведении атаки – это...

a. канал атаки;

b. атака;

c. контролируемая зона.

5. Угрозы безопасности могут быть реализованы двумя путями:

a. через технические каналы утечки;

b. путем несанкционированного доступа

6. Информационная система обрабатывающая персональные данные субъектов персональных данных, полученные только из общедоступных источников персональных данных является:

a. информационной системой, обрабатывающей специальные категории персональных данных;

b. информационной системой, обрабатывающей биометрические персональные данные;

c. информационной системой, обрабатывающей общедоступные персональные данные;

d. информационной системой, обрабатывающей иные категории персональных данных.

7. Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных определяет документ:

a. Постановление от 1 ноября 2012 г. 119;

b. Приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21;

c. ФЗ -152 «О персональных данных».

8. Технический канал утечки информации – это..

a. совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация;

b. совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных

несанкционированных действий при их обработке в информационной системе персональных данных;

c. совокупность программных и техническую элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

9. Угрозы безопасности персональных данных – это...

a. совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация;

b. совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных;

c. совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

10. Сведения, которые характеризуют физиологические особенности человека, и на основе которых можно установить его личность, включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию – это...

a. Биометрические персональные данные;

b. Специальные персональные данные;

c. Общедоступные персональные данные.

11. Какие действия можно производить с персональными данными?

a. чтение и рассылка;

b. хранение, уничтожение;

c. обезличивание, блокирование;

d. фасовка и упаковка.

12. Сопоставьте персональные данные с их видами

1. общедоступные	a) медицинская карта
2. биометрические	b) фамилия, имя, отчество
3. особая категория	c) сведения, полученные на полиграфе
4. не относятся ни к одному из видов	d) нечеткое изображение

13. Может ли являться оператором персональных данных физическое лицо?

a. да

b. нет

6. Составители программы

Щедрина Елена Геннадьевна, преподаватель ГАПОУ ТО «Тюменский колледж производственных и социальных технологий»

Савченко Айрат Алексеевич, методист ГАПОУ ТО «Тюменский колледж производственных и социальных технологий»

Чайкина Ольга Юрьевна, старший методист ГАПОУ ТО «Тюменский колледж производственных и социальных технологий»