Автономная некоммерческая организация
«Центр опережающей профессиональной подготовки»

Утверждено
Директор АНО «Центр опережающей профессиональной подготовки»
_____ А.В. Потрясаев
приказ № ____ от 10.01 2022 года

Программа дополнительного профессионального образования
повышения квалификации

Информационная безопасность обучающихся

Объем программы: 24 часа

Белгород, 2022

Составители (разработчики) программы:

Внукова Наталья Владимировна, преподаватель ОГАПОУ «Белгородский индустриальный колледж»

ОГЛАВЛЕНИЕ

1. Пояснительная записка

Дополнительная профессиональная программа повышения квалификации «Информационная безопасность обучающихся» (24 часа) разработана с учётом требований и положений:

– Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации»;

– Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам (утв. приказом Министерства образования и науки РФ от 1 июля 2013 г. № 499);

– Порядка разработки дополнительных профессиональных программ, содержащих сведения, составляющие государственную тайну, и дополнительных профессиональных программ в области информационной безопасности (утв. приказом Министерства образования и науки РФ от 05 декабря 2013 г. № 1310);

– Порядка организации и осуществления образовательной деятельности по основным программам профессионального обучения, утвержденным приказом Министерства образования и науки РФ от 18 апреля 2013 года № 292.

Реализация Программы предусмотрена на базе ОГАПОУ «Белгородский индустриальный колледж» на основе Устава.

Организация-разработчик: ОГАПОУ «Белгородский индустриальный колледж».

Дополнительная профессиональная программа повышения квалификации направлена на совершенствование и (или) получение новой компетенции, необходимой для профессиональной деятельности, и (или) повышение профессионального уровня в рамках имеющейся квалификации.

Цели программы:

– повышения профессионального уровня педагогических работников в области информационной безопасности в образовательных организациях

Задачи программы:

формирование знаний, навыков, профессиональных компетенций, необходимых для:

– разработки пакета локальных нормативных документов, обязательное наличие которых в образовательной организации предписано федеральным законодательством в области информационной безопасности;

– составления плана мероприятий, направленных на создание инфобезопасной образовательной среды;

– формирования и развития педагогической ИКТ-компетентности в соответствии с требованиями ФГОС;

– формирования навыков медиаграмотности и «информационной гигиены»;

– формирования навыков работы с современным программным обеспечением;

– применения методов профилактики интернет-зависимости у обучающихся.

Категория слушателей, на обучение которых рассчитана программа дополнительного профессионального образования (далее – программа): преподаватели (мастера производственного обучения) профессиональных образовательных организаций, реализующих программы среднего профессионального образования.

Полученные в ходе повышения квалификации профессиональные компетенции, умения и знания предназначены для применения при планировании реализации основных образовательных программ, программ профессионального обучения и дополнительного профессионального образования, решающих задачи подготовки специалистов среднего звена.

Слушатель, приступающий к освоению программы, должен владеть основами работы на персональном компьютере, уметь работать с программным обеспечением Microsoft Office или его аналогами.

Обучение по программе ведется на русском языке.

Трудоемкость обучения: нормативная трудоемкость обучения по данной программе составляет 24 академических часа.

Форма обучения: очная.

1.1. Планируемые результаты освоения программы:

знать:

- сущность, цели и принципы информационной безопасности в образовательной организации, направления их практической реализации;
- концепцию информационной безопасности в образовательной организации, конституционные и законодательные основы ее реализации;
- информационно-правовые аспекты безопасности информационных ресурсов, основные проблемы информационного права, информационно-правовых отношений, принципы и способы охраны интеллектуальной собственности;
- задачи информационной безопасности, основные тенденции и направления формирования и функционирования комплексной системы защиты информации в образовательной организации;
- направления и методы обеспечения безопасности информационных ресурсов, ведения аналитической работы по выявлению угроз несанкционированного доступа к информации, ее утраты;
- функциональные возможности и предпосылки эффективного использования различных типов технологических систем и способов обработки, и хранения традиционных и электронных конфиденциальных документов;
- методы охраны зданий, помещений, оборудования, документации и персонала в обычных и экстремальных ситуациях, проведения охранных мероприятий в том числе с использованием соответствующих технических средств;

- организационно-правовое обеспечение функционирования и совершенствование систем защиты информации, служб безопасности, конфиденциальной документации и персонала в образовательной организации.

уметь:

- организовать направления работы по реализации информационной безопасности;
- применять методы профилактики интернет-зависимости обучающихся.

владеть:

- информацией о правовой защите обучающихся от влияния негативной информации;
- методами и формами защиты информации в образовательной организации;
- педагогической компетентностью в сфере информационной безопасности.

обладать:

профессиональными компетенциями, включающими в себя способность:

- разработки пакета локальных нормативных документов, обязательное наличие которых в образовательной организации предписано федеральным законодательством в области информационной безопасности;
- составления плана мероприятий, направленных на создание инфобезопасной образовательной среды;
- формирования и развития педагогической ИКТ-компетентности в соответствии с требованиями ФГОС;
- формирования навыков медиаграмотности и «информационной гигиены»;
- формирования навыков работы с современным программным обеспечением;
- применения методов профилактики интернет-зависимости у обучающихся.

2. Содержание программы

2.1. Учебный план дополнительной профессиональной программы повышения квалификации «Информационная безопасность обучающихся»

Категория слушателей – административные и педагогические работники профессиональных образовательных организаций.

(*область профессиональной деятельности)*

Срок обучения – 24 часа.

Форма обучения – очно-заочная.

№ п/п	Наименование дисциплин, модулей	Всего, ак.час.	В том числе:			
			Лекции	Практические занятия	Самостоятельная работа	Форма контроля
1	2	3	4	5	6	7
1.	Раздел 1. Правовые аспекты безопасности информационного пространства в образовательной среде	6	4	2		Тест, практическое задание
2.	Раздел 2. Безопасность образовательной среды: психолого-педагогическое сопровождение	8	2	6		Тест, практическое задание
3.	Раздел 3. Информационная безопасность образовательной организации	6	2	4		Тест, практическое задание
Итоговая аттестация		4				Тест, практическое задание
Итого		24	8	12		

2.2. Учебно-тематический план дополнительной профессиональной программы повышения квалификации «Информационная безопасность обучающихся»

Категория слушателей – административные и педагогические работники профессиональных образовательных организаций.

Срок обучения – 24 часа.

Форма обучения – очно-заочная.

№ п/п	Наименование дисциплин, модулей	Всего, ак.час.	В том числе:			
			Лекции	Практические занятия	Самостоятельная работа	Форма контроля
1	2	3	4	5	6	7
1.	**Раздел 1. Правовые аспекты безопасности информационного пространства в образовательной среде**	**6**	**4**	**2**		**Тест, практическое задание**
1.1.	Тема 1. Правовое обеспечение информационной безопасности в образовательной организации	2	2			
1.2.	Тема 2. Правовое регулирование открытых информационных ресурсов образовательной организации	2	2			
1.3	Тема 3. Правовая защита обучающихся от влияния негативной информации	2		2		
2.	**Раздел 2. Безопасность образовательной среды: психолого-педагогическое сопровождение**	**8**	**2**	**6**		**Тест, практическое задание**
2.1.	Тема 1. Психолого-педагогическая подготовка педагогов в области информационной безопасности	2	2			
2.2.	Тема 2. Организация педагогической работы по реализации информационной безопасности	2		2		

2.3.	Тема 3. Влияние интернет-пространства на психологическое состояние и поведение обучающегося	2		2		
2.4.	Тема 4. Интернет-зависимость, ее диагностика и профилактика	2		2		
3.	**Раздел 3. Информационная безопасность образовательной организации**	**6**	**2**	**4**		**Тест, практическое задание**
3.1.	Тема 1. Основы информационной безопасности образовательной организации	2	2			
3.2.	Тема 2. Программное обеспечение информационной безопасности	4	2	2		
Итоговая аттестация		**4**				Тест, практическое задание
	Итого	**24**	**4**	**10**		

2.3. Календарный учебный график

График обучения / **Форма обучения**	**Ауд. часов в день**	**Дней в неделю**	**Общая продолжительность программы, месяцев (дней, недель)**
очно-заочная	8	3	24 часа, 3 дня, 1 неделя

2.4. Рабочая программа дополнительной профессиональной программы повышения квалификации «Информационная безопасность обучающихся»

№ п/п	Наименование темы	Содержание обучения (по темам в дидактических единицах), наименование и тематика лабораторных работ, практических занятий (семинаров), самостоятельной работы, используемых образовательных технологий и рекомендуемой литературы
1.	2.	3.
Раздел 1. Правовые аспекты безопасности информационного пространства в образовательной среде		
1.	Тема 1. Правовое обеспечение информационной безопасности в образовательной организации	Лекция. Понятие информационной безопасности. Национальная безопасность. Доктрина безопасности Российской Федерации. Концепция информационной безопасности России. Международные договоры, доктрины в области информационной безопасности. Информационные права граждан. Информационная безопасность как институт информационного права. Законодательство в области интеллектуальной собственности, информационных ресурсов, информационных продуктов и информационных услуг в образовательной организации. Законодательство о безопасности и защите информации, его структура и содержание. Законодательство о защите государственной и коммерческой тайны, персональных данных, его структура и содержание. Безопасность функционирования образовательной организации. Основные задачи и уровни реализации информационной безопасности. Правовые механизмы защиты в нормах законов, регулирующих отношения по поводу создания и распространения информации. Правовые механизмы защиты в нормах законов, регулирующих отношения в области формирования информационных ресурсов, продуктов и услуг. Правовые механизмы защиты в нормах законов, регулирующих отношения по поводу права на потребление информации. Правовые механизмы защиты в нормах законов, регулирующих отношения в области создания и применения информационных систем, информационных технологий и средств их обеспечения в образовательной организации (2 часа)
2.	Тема 2. Правовое регулирование открытых информационных ресурсов образовательной организации	Лекция. Защита информации институтом интеллектуальной собственности. Информационный характер интеллектуальной и материальной собственности. Охрана результатов творческой деятельности. Российский и зарубежный опыт охраны интеллектуальной собственности. Международные правовые акты. Реализация интеллектуальной собственности на документированную информацию. Характеристика норм

		патентного права. Характеристика норм авторского права и смежных прав. Законодательные акты, охраняющие вещную собственность на документированную информацию в образовательной организации. Правовая защита субъектов в области массовой информации, обеспечение гарантий свободы массовой информации. Организация деятельности средств массовой информации. Отношения средств массовой информации с гражданами и организациями. (2 часа) Практическое занятие. Ответственность за нарушение законодательства в средствах массовой информации (2 часа)
3.	Тема 3. Правовая защита обучающихся от влияния негативной информации	Практическое занятие. Правовая защита информационных ресурсов ограниченного доступа. Понятие тайны, секрета, конфиденциальности. Направления и методы защиты тайны в России и зарубежных странах. Институт тайн в законодательстве Российской Федерации. Защита информации институтом государственной тайны. Субъекты и объекты информационных правоотношений в области образовательной организации. Правовая форма защиты ценной деловой и производственной информации в образовательной организации. Служебная тайна. Профессиональная тайна. Банковская тайна. Документированная информация (документы) секретная и несекретная. Понятие конфиденциальности как определение сферы несекретной информации ограниченного доступа. Правовые и технологические аспекты присвоения информации в образовательной организации категории конфиденциальной. Конфиденциальная информация и ее виды. Персональные данные. Ограничения на отнесение информации к категории конфиденциальной. Понятие конфиденциального документа, его особенности. Общая классификация конфиденциальных документов. Сроки (период) конфиденциальности. Деление документов на документы кратковременного и долговременного периода конфиденциальности. (2 часа)
Раздел 2. Безопасность образовательной среды: психолого-педагогическое сопровождение		
1.	Тема 1. Психолого-педагогическая подготовка педагогов в области информационной безопасности	Лекция. Психолого-педагогическая подготовка педагогов в области информационной безопасности. Педагогическое проектирование безопасной информационной образовательной среды в условиях развития нашей страны в соответствии со Стратегией развития информационного общества Российской Федерации и реализации современного комплекса информационных угроз и опасностей. Понятие информационной культуры. Развитие информационной культуры личности педагога. Информационная подготовка педагога как обязательная

		составляющая образовательного процесса, направленная на подготовку специалистов, способных эффективно применять средства информационных и коммуникационных технологий в процессе осуществления своей профессиональной деятельности. (2 часа)
2.	Тема 2. Организация педагогической работы по реализации информационной безопасности	Практическое занятие. Критерии оценки состояния информационной безопасности в образовательной организации (на основе Концепции РФ). Информационное представление образовательной среды, ее преобразование в систематизированное информационное пространство, организованное, многомерное, упорядоченное. Особенности внедрения компьютерной техники и использовании сети Интернет в образовательных учреждениях. Модель информационно-образовательной среды. Личная информационно-образовательная среда конкретной личности (школьника, учителя). Угрозы информационной безопасности молодежи, средства их предотвращения. Контроль, анализ ситуации и соответствующая коррекция информационной безопасности образовательной организации. Методы и способы повышения эффективности обеспечения безопасности информационной среды образовательного учреждения и личной информационной среды каждого учащегося. Организация педагогической работы по реализации информационной безопасности. (2 часа)
3.	Тема 3. Влияние интернет-пространства на психологическое состояние и поведение обучающегося	Практическое занятие. Понятие интернет–пространства. Информационно-психологическая безопасность личности обучающегося. Основы законодательства РФ о защите детей от информации, причиняющей вред их здоровью и развитию. Позитивные информационные возможности интернета для интеллектуального и личностного развития обучающихся. Основные угрозы для личностной безопасности обучающихся, деструктивные информационные влияния интернет-пространства. Информационно-психологическое воздействие интернет – пространства, его негативные последствия. Факторы негативного влияния на личность интернет - пространства, развитие интернет-зависимости. Нарушение системы отношений личности в отношении государства, нарушение поведения и состояния обучающихся, разрушение целостности самой личности. Характеристики личности, провоцирующие повышенную склонность к виртуальной активности и использованию интернет-технологий (мотивационные, коммуникативные, эмоционально-ценностные, нравственно-духовные), выступающие внутриличностными причинами психологической зависимости и интернет-технологий. Формы и методы педагогического сопровождения информационной безопасности обучающихся. Интернет-зависимость, ее диагностика и профилактика (2 часа)

4.	Тема 4. Интернет-зависимость, ее диагностика и профилактика	Практическое занятие. Интернет-зависимость, ее диагностика и профилактика. Основные критерии Интернет-зависимости. Классификация типов интернет-зависимости, её причин и симптомов. Навязчивый веб-серфинг (информационная перегрузка) — бесконечные путешествия по Всемирной паутине, поиск информации. Пристрастие к виртуальному общению и виртуальным знакомствам — большие объёмы переписки, постоянное участие в чатах, веб-форумах, избыточность знакомых и друзей в Сети. Игровая зависимость — навязчивое увлечение компьютерными играми по сети. Навязчивая финансовая потребность — игра по сети в азартные игры, ненужные покупки в интернет-магазинах. Пристрастие к просмотру фильмов через Интернет. Интернет-аддикция, психологические особенности "киберрасстройства" личности ребенка. Угроза психическому здоровью аддиктивной личности. Социальная дезадаптация аддиктивной личности. Пути решения проблемы, методы психолого-педагогической коррекции. (2 часа)
Раздел 3. Информационная безопасность образовательной организации		
1.	Тема 1. Основы информационной безопасности образовательной организации	Лекция. Основы информационной безопасности образовательной организации. Основные аспекты информационной безопасности образовательной среды. Обеспеченность оптимизации действия всех значимых информационных факторов; посильность создания субъектами образовательного процесса действительных условий среды безопасной информационной модальности; реальность обеспечения согласования, комплементарной основы контактов личности и образовательного пространства; осуществимость построения специализированного культурологического базиса преобразования образовательной среды; перспективная направленность на развитие не только представлений об информации как ресурсе, но также отношения, технологий взаимодействия личности и информационной среды в состоянии защищенности от негативного воздействия опасных факторов внутреннего и внешнего характера; определенность уровней индивидуальных аксиологических фильтров личности и социальных установок на формирование безопасной информационной образовательной среды; неограниченность масштабных характеристик безопасности планируемого образовательного процесса. Меры по обеспечению информационной безопасности в образовательной организации: правовое обеспечение информационной безопасности; нравственный и этический контроль; защита психики и здоровья ребенка; организационная защита; воспитательные меры по

		обеспечению информационной безопасности; техническое и программное обеспечение информационной безопасности. (2 час)
2.	Тема 2. Программное обеспечение информационной безопасности	Лекция. Классификация и характеристика классификационных групп технических средств охраны. Охранные системы. Программно-технические методы обеспечения информационной безопасности. Парольная защита с помощью стандартных системных средств. Идентификация и аутентификация. Разграничение доступа. Протоколирование и аудит. Межсетевые экраны как средство защиты от несанкционированного доступа. Персональные и корпоративные межсетевые экраны. Критерии оценки защищённости систем информационной безопасности. Международные критерии. Основные принципы категорирования защищаемых ресурсов, принятые в Российской Федерации. Основные виды компьютерных вирусов: загрузочные вирусы, вирусы в исполняемых компьютерных файлах, макро-вирусы, скрипт-вирусы, вирусы-мистификации. Профилактика вирусного заражения. Антивирусные программы. Методика применения антивирусных программ. Криптографические средства защиты. Криптографическое преобразование данных. Симметричные и асимметричные методы шифрования. Общая технология шифрования. Технология шифрования речи. (2 часа) Практическое занятие. Программное обеспечение информационной безопасности (Программно-технические методы обеспечения информационной безопасности. Парольная защита с помощью стандартных системных средств). (2 часа)

3. Формы итоговой аттестации

По дополнительной профессиональной программе повышения квалификации «Информационная безопасность обучающихся» проводится контроль знаний слушателей: входной, текущей, итоговый контроль.

Текущий контроль проводится по каждой теме в виде теста и/или практического занятия с целью определения уровня самостоятельной работы слушателей по учебным материалам. Контроль текущих знаний проводится на занятиях в форме устного или письменного опроса, теста. Объектами текущего контроля при изучении дисциплин являются: посещение лекций; подготовка и качество выполнения практических работ.

Промежуточная аттестация слушателей данного курса повышения квалификации осуществляется в форме теста.

Промежуточная аттестация оценивается положительно оценками: «зачтено», либо отрицательно – «не зачтено».

Итоговая аттестация проводится в форме теста и практической работы. Оценивается положительно оценками: «отлично», «хорошо», «удовлетворительно», либо отрицательно – «неудовлетворительно». Пересдача неудовлетворительной оценки допускается не более двух раз. Требования к уровню освоения программы владение знаниями учебных дисциплин в объеме не менее 75%.

3.1. Оценочные материалы (Приложение 1).

Итоговая аттестация слушателей

Для итоговой аттестации используется тест. По результатам освоения программы дополнительного профессионального обучения выдается удостоверение о повышении квалификации.

Материалы для итоговой аттестации

1. Определить место информационной безопасности в обеспечении системы безопасности образовательной среды.
2. Дать определение информационной безопасности.
3. Назвать основные направления и задачи обеспечения информационной безопасности образовательной организации.
4. Назвать основные компоненты информационной безопасности автоматизированных информационных систем.
5. Охарактеризовать уровни реализации информационной безопасности в образовательной организации.
6. Дать определение и классификацию информационных ресурсов.
7. Определить основные виды угроз информационным ресурсам в образовательной организации.
8. Охарактеризовать особенности угроз конфиденциальной информации.
9. Проанализировать причины возникновения угроз утраты или утечки конфиденциальной информации.
10. Описать причины возникновения каналов несанкционированного доступа к информации.
11. Классифицировать виды каналов несанкционированного доступа к информации.
12. Описать характер действия организационных каналов несанкционированного доступа к информации.
13. Проанализировать основные направления правовой защиты информации в образовательной организации.
14. Раскрыть содержание нормативных актов, защищающих право учащихся образовательной организации на своевременное получение достоверной информации.

15. Показать порядок защиты прав учащихся на личную тайну и неприкосновенность частной жизни законодательством Российской Федерации.

16. Определить объекты защиты прав детей от влияния негативной информации.

17. Перечислить сведения, составляющие государственную тайну и сведения, которые не могут относиться к государственной тайне.

18. Назвать основные виды служебной тайны, определенные законодательством Российской Федерации.

19. Изложить принципы и направления комплексного подхода к обеспечению информационной безопасности образовательной среды.

20. Назвать основные положения концепции информационной безопасности образовательной организации.

21. Изложить содержание регламента обеспечения информационной безопасности образовательной организации.

22. Определить основные методы и способы работы службы безопасности предприятия по защите конфиденциальной информации.

23. Определить критерии ценности информационных ресурсов и длительности сохранения ими этой характеристики.

24. Проанализировать содержание понятия разрешительной системы доступа персонала к конфиденциальным сведениям образовательной организации.

25. Обосновать критерии выделения конфиденциальных документов из общего потока поступающих документов.

26. Обосновать состав показателей учетной карточки (по выбору преподавателя) и правила их заполнения.

27. Проанализировать особенности контроля за исполнением конфиденциальных документов, его организационное и технологическое отличие от контроля открытых документов в образовательной организации.

28. Классифицировать состав бумажных и технических носителей информации, применяемых для составления деловой (управленческой) и технической конфиденциальной документации в образовательной организации.

29. Сформулировать возможности, трудности и направления организации педагогической работы по реализации информационной безопасности.

30. Психологическая компетентность педагога, как фактор безопасности образовательной среды.

31. Проанализировать задачи защиты информации, которые должны быть решены при формировании и оформлении дел с конфиденциальными документами учащихся.

32. Составить и проанализировать технологическую схему (цепочку) приема (перевода) лиц на работу в образовательную организацию, связанную с владением конфиденциальной информацией.

33. Проанализировать виды угроз информационной безопасности в образовательной организации.

34. Назвать основные элементы защиты территории и помещений образовательной организации.

35. Интернет-зависимость обучающихся, ее диагностика и профилактика.

4. Организационно-педагогические условия

4.1. Материально-техническое обеспечение программы

Реализация программы предполагает наличие материально-технической базы, соответствующей действующим санитарно-техническим нормам и обеспечивающим проведение всех видов подготовки слушателей, предусмотренных учебным планом. Материально-техническое обеспечение учебного процесса соответствует требования к современной организации образовательного процесса, включает наличие учебных аудиторий, мультимедийных проекторов, компьютеров.

Оборудование учебного кабинета:

1. Компьютерный класс и мультимедиа;
2. Мастерская «Анализ защищенности информационных систем от внешних угроз»;
3. Доступ к информационно-коммуникационной сети интернет.

Программное обеспечение:

- операционная система Windows (версия 2010 и выше);
- интернет-браузеры MS Internet Explorer, Opera и др.

4.2. Учебно-информационное обеспечение программы

Основная литература:

1. Афанасьев, Алексей Алексеевич Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов. Гриф УМО МО РФ / Афанасьев Алексей Алексеевич. - М.: Горячая линия - Телеком, 2020. - 438 с.

2. Безопасная образовательная среда: моделирование и развитие: учеб. пособие / под науч. ред. И.А. Баевой, С.В. Тарасова. – СПб. : ЛОИРО, 2019 – 265 с.

3. Богатырева Ю.И., Основные угрозы информационной безопасности субъектов образовательного процесса // Известия ТулГУ. Гуманитарные науки. Тула, 2019. Вып. 3. С. 427-431.

4. Ефимова, Л. Л. Информационная безопасность детей. Российский и зарубежный опыт / Л.Л. Ефимова, А С. А, Кочерга. - М.: Юнити-Дана, 2020. - 240 с.

5. Пимонов В.А., Основные проблемы обеспечения информационной безопасности субъектов образовательного процесса // журнал Психология и право, 2019.

6. Указ Президента РФ от 02.07.2021 N 400 "О Стратегии национальной безопасности Российской Федерации" [Электронный ресурс] URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LA

W&n=389271#McSI2xSEW32zwL1O

Дополнительная литература:

1. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам: моногр. . - Москва: Мир, 2020. - 552 с.
2. Безопасность России. Правовые, социально-экономические и научно-технические аспекты. Основы информационно-психологической безопасности. - М.: Международный гуманитарный фонд "Знание", 2019. - 416 с.
3. Статей, Сборник Информационная безопасность и вопросы профилактики киберэкстремизма среди молодежи / Сборник статей. - М.: Флинта, 2021. - 587 с.

4.3. Кадровое обеспечение программы

Реализация программы должна обеспечиваться высококвалифицированными преподавателями, привлеченными специалистами, экспертами WS ведущих образовательных организаций и учреждений дополнительного профессионального образования, профессиональных образовательных организаций и иных организаций.