Государственное бюджетное учреждение
дополнительного профессионального образования
«Санкт-Петербургский центр оценки качества образования
и информационных технологий»

ПРИНЯТА
Научно-методическим советом
Протокол от 28.08.24 № 7

УТВЕРЖДАЮ
Директор
_____ О.В. Дуброва
___.___.2024

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«Цифровая гигиена и кибербезопасность в электронной информационно-образовательной среде»

Разработчик: И.А. Туманов,
методист

Санкт-Петербург
2024 год

Раздел 1. Характеристика программы

1.1 Цель реализации программы – совершенствование профессиональных компетенций слушателей в области цифровой гигиены и кибербезопасности в ЭИОС.

Актуальность и практическая значимость

Современное образование невозможно представить без сети Интернет, которая является как обширным источником и хранилищем разнородной информации, так и коммуникационной средой, и привносит с собой цифровые угрозы, несущие реальные риски как для физического, так и психологического здоровья. Программа направлена на развитие цифровой компетентности педагогов образовательных организаций в области цифровой гигиены и кибербезопасности, формирования профессиональных компетенций, необходимых для противодействия и профилактики деструктивного онлайн-поведения несовершеннолетних в электронной информационной образовательной среде.

1.2 Категория слушателей: педагогические работники образовательных организаций.

Программа рекомендована для слушателей, прошедших подготовку в области ИКТ на уровне общепользовательской ИКТ-компетентности.

1.3 Объем программы 18 часов.

1.4 Форма обучения: очная

1.5 Особенности реализации программы

Программа реализуется с использованием электронного обучения.

Программа реализуется ГБУ ДПО «СПбЦОКОиИТ» самостоятельно

1.6 Планируемые результаты обучения:

Программа направлена на развитие следующих профессиональных компетенций:

Модуль ДПП	**Профессиональные компетенции (ПК), подлежащие развитию**
Модуль 1 «Цифровая гигиена и кибербезопасность в ЭИОС»	ПК2. Способность использовать возможности информационно-образовательной среды. ПК3. Способность работать с информацией в компьютерных сетях.

Содержание образовательной программы учитывает требования профессионального стандарта «Педагог (педагогическая деятельность в сфере дошкольного, начального общего, основного общего, среднего общего образования) (воспитатель, учитель)», «Педагог дополнительного образования детей и взрослых», «Педагог-психолог (психолог в сфере образования)», «Специалист в области воспитания», «Специалист, участвующий в организации деятельности детского коллектива (вожатый)».

Планируемые результаты обучения направлены на выполнение слушателем следующих трудовых функций:

Категория слушателей	**Профстандарт**	**Трудовая функция**	**Трудовые действия**
Педагогические работники	Педагог (педагогическая деятельность в сфере дошкольного,	Общепедагогическая функция. Обучение	Формирование навыков, связанных с информационно-коммуникационными технологиями

	начального общего, основного общего, среднего общего образования) (воспитатель, учитель)	Воспитательная деятельность	Формирование правил безопасного поведения в информационной среде в соответствии с возрастными особенностями обучающихся Регулирование поведения обучающихся для обеспечения безопасной образовательной среды
Педагогические работники	Педагог дополнительного образования детей и взрослых	Организация и проведение массовых досуговых мероприятий	Планирование массовых досуговых мероприятий
Вожатый	Специалист, участвующий в организации деятельности детского коллектива (вожатый)	Сопровождение деятельности временного детского коллектива (группы, подразделения, объединения) в организациях отдыха детей и их оздоровления под руководством педагогического работника	Проведение под руководством педагогического работника игр, сборов и иных мероприятий во временном детском коллективе (группе, подразделении, объединении), направленных на формирование коллектива, его развитие, поддержание комфортного эмоционального состояния
Психолог Педагог-психолог Психолог образовательной организации	Педагог-психолог (психолог в сфере образования)	Психологическая экспертиза (оценка) комфортности и безопасности образовательной среды образовательных организаций Психологическая профилактика	Психологическая экспертиза программ развития образовательной организации с целью определения степени безопасности и комфортности образовательной среды Разработка психологических рекомендаций по проектированию образовательной среды, комфортной и безопасной для личностного развития обучающегося на каждом возрастном этапе, для своевременного предупреждения нарушений в развитии и становлении

			личности, ее аффективной, интеллектуальной и волевой сфер
Советник директора по воспитанию и взаимодействию с детскими общественными объединениями Социальный педагог Педагог-организатор Педагог-библиотекарь	Специалист в области воспитания	Организация воспитательной деятельности в образовательной организации Организация социально-педагогической поддержки обучающихся в процессе социализации Организация работы по направлениям внеурочной деятельности Организационно-методическое обеспечение воспитательной деятельности Проведение мероприятий по воспитанию у обучающихся информационной культуры	Консультирование участников образовательных отношений по вопросам воспитания с использованием современных информационных технологий Обеспечение досуговой занятости обучающихся Разработка программ внеурочной деятельности по направлениям развития личности: спортивно-оздоровительному, духовно-нравственному, социальному, общеинтеллектуальному, общекультурному Разработка информационно-методических материалов по основным направлениям воспитательной работы Организационно-методическое сопровождение досуговых мероприятий Реализация мероприятий по обеспечению информационной безопасности обучающихся в образовательной организации

В результате обучения по программе слушатель должен

знать:

- нормативные документы по ограничению в образовательных организациях доступа обучающихся к неправомерной информации;
- нормативные документы по обеспечению безопасности персональных данных;
- виды киберугроз;
- классификацию видов цифровой компетентности в области онлайн-безопасности.

уметь:

- использовать нормативные документы в области кибербезопасности и цифровой гигиены в профессиональной деятельности;

- настраивать уровень приватности в социальных сетях и мессенджерах;
- оценивать необходимость получения согласий на публикацию фотографий и персональных данных;
- настраивать безопасный поиск в интернет-браузере.

Раздел 2. Содержание программы

2.1 Учебно-тематический план

Тема	Всего часов	В том числе		Форма аттестации
		Аудиторные занятия с ЭО		
		Лекции	Практические занятия	
Тема 1. Основы кибербезопасности и цифровой гигиены	**3**	**3**	**-**	
1.1 Государственное регулирование в области ограничения распространения и защиты информации	1	1	-	
1.2 Понятия кибербезопасности и цифровой гигиены в ЭИОС	1	1	-	
1.3 Классификация онлайн-рисков	1	1	-	
Тема 2. Защита обучающихся от неправомерной информации	**4**	**3**	**1**	
2.1 Законодательство в области ограничения доступа к ресурсам сети Интернет	1	1	-	
2.2 Организация доступа к ресурсам сети Интернет	2	1	1	
2.3 Меры профилактики деструктивного поведения несовершеннолетних	1	1	-	
Тема 3. Формирование и развитие навыков цифровой гигиены у обучающихся	**5**	**4**	**1**	
3.1 Виды цифровых компетентностей	4	3	1	
3.2 Формирование безопасного	1	1	-	

поведения в цифровой среде				
Тема 4. Обеспечение безопасности персональных данных	**4**	**3**	**1**	
4.1 Законодательство и основные понятия в области персональных данных	1	1	-	
4.2 Требования к организации защиты персональных данных	1	1	-	
4.3 Особенности согласий на публикацию изображений и обработку персональных данных	2	1	1	
Итоговая аттестация	2	-	2	Зачет
ИТОГО	**18**	**13**	**5**	

2.2 Рабочая программа

***Тема 1.*Основы кибербезопасности и цифровой гигиены (3 часа).**

1.1. Государственное регулирование в области ограничения распространения и защиты информации (1 час).

Лекция (1 час): Государственное регулирование в области ограничения распространения и защиты информации. Понятия информационной безопасности детей, государства и защиты информации.

1.2. Понятия кибербезопасности и цифровой гигиены в ЭИОС(1 час).

Лекция (1 час): Определение и взаимосвязь понятий кибербезопасность и цифровая гигиена, их место в ЭИОС.

1.3. Классификация онлайн-рисков (1 час).

Лекция (1 час): Классификация и обзор онлайн-рисков (контентные, коммуникационные, потребительские, технические) и форм деструктивного онлайн-поведения у несовершеннолетних.

***Тема 2.* Защита обучающихся от неправомерной информации (4 часа).**

2.1. Законодательство в области ограничения доступа к сети Интернет (1 час).

Лекция (1 час): Законы и иные нормативные акты, регламентирующие ограничения информации, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования.

2.2. Организация доступа к ресурсам сети Интернет (2 часа).

Лекция (1 час): Варианты организации системы контентной фильтрации в образовательном учреждении и для домашнего использования. Сложности фильтрации.

Практическая работа 1 (текущий контроль, 1 час): «Настройка безопасного поиска в интернет-браузере». Слушатели должны настроить в интернет-браузере использование безопасного поиска вместо встроенной поисковой системы.

2.3. Меры профилактики деструктивного поведения несовершеннолетних (1 час).

Лекция (1 час): Рекомендации по выявлению и профилактике деструктивного поведения несовершеннолетних. Обзор возможностей средств родительского контроля.

***Тема 3.* Формирование и развитие навыков цифровой гигиены у обучающихся (5 часов).**

3.1. Виды цифровых компетентностей (4 часа).

Лекция (3 часа): Классификация видов цифровых компетентностей в области цифровой гигиены и кибербезопасности.

Практическая работа №2 (текущий контроль, 1 час): "Создание словаря сетевого сленга". Слушатели должны разработать текстовой документ, содержащий таблицу из 2-х столбцов: сленговое слово и его пояснение. В таблице должно быть представлено не менее трех пунктов.

3.2. Формирование безопасного поведения в цифровой среде (1 час).

Лекция (1 час): Рекомендации по формированию навыков цифровой гигиены.

***Тема 4.* Обеспечение безопасности персональных данных (4 часа).**

4.1. Законодательство и основные понятия в области персональных данных (1 час).

Лекция (1 час): Понятие персональных данных (ПДн), категории ПДн, оператора ПДн. Правила обработки персональных данных и ответственность.

4.2. Требования к организации защиты персональных данных (1 час).

Лекция (1 час): Обзор требований к мерам по обеспечению безопасности обработки персональных данных, осуществляемой без использования средств автоматизации и в информационных системах персональных данных.

4.3. Особенности согласий на публикацию изображений и обработку персональных данных (2 часа).

Лекция (1 час): Общие требования к содержанию согласий на обработку персональных данных. Особенности согласий на распространение ПДн. Электронная форма согласия. Согласие на использование изображения гражданина.

Практическая работа №3 (текущий контроль, 1 час): "Анализ персональных данных на сайте образовательной организации". Слушатели исследуют информацию, размещенную на сайте своей ОО, и определяют, на какие публикации требуются согласие на обнародование фотографий и распространение персональных данных.

Итоговая аттестация (устный зачет). 2 часа.

2.3 Календарный учебный график

Общая продолжительность обучения составляет: одна – четыре недели в зависимости от расписания занятий.

Режим аудиторных занятий: 1 – 8 академических часов в день, 1 – 6 дней в неделю.

Дата начала обучения определяется по мере комплектования групп, и на каждую группу составляется календарный учебный график.

Раздел 3. Условия реализации программы

3.1 Материально-технические условия реализации программы

Техническое обеспечение

- аудитория для проведения лекционных занятий, снабженная компьютером и мультимедийным оборудованием для презентаций;
- рабочие станции слушателей и преподавателя, объединенные в локальную компьютерную сеть, с возможностью работы с мультимедиа, доступом к учебному серверу и выходом в Интернет.

Программное обеспечение:

1. Интернет-браузеры.
2. ПО для просмотра файлов в формате pdf
3. Мультимедийный проигрыватель.

3.2 Организационно-педагогические условия реализации программы

3.2.1 Общие требования к организации образовательного процесса

Процесс обучения осуществляется с позиций андрагогики, т.к. одной из важных особенностей обучения взрослых является получение дополнительных знаний и

совершенствование профессиональных умений на основе осмысления ими собственной деятельности. Одним из важнейших условий реализации данной программы является активная позиция каждого слушателя, его инициатива, осмысление собственного опыта. При проведении занятий используются следующие педагогические технологии: технологии развития критического мышления, технологии коллективного обучения, технологии реализации системно-деятельностного подхода.

При изучении курса предполагается активное участие слушателей в практических занятиях, обеспечивающих получение опыта в решении профессиональных задач по обеспечению кибербезопасности.

По завершении курса слушателям предлагается заполнить рефлексивную анкету по итогам обучения по данной ДПП.

3.2.2 Квалификация педагогических кадров

Обучение по данной программе осуществляется старшими преподавателями, имеющим опыт методической или практической деятельности по тематике курса и опыт работы с техническими и программными средствами, использующимися при реализации программы.

3.3 Учебно-методическое обеспечение программы

3.3.1 Основная литература

1. Туманов И.А., Методические рекомендации по обеспечению информационной безопасности обучающихся при работе в сети Интернет. [Текст] / Сост.: Туманов И.А., Дорофеева Т.В.- СПб: ГБУ ДПО «СПбЦОКОиИТ», 2018. – 39 с.

2. Вангородский, С. Н. Основы кибербезопасности [Текст] : учебно-методическое пособие. 5—11 классы / С. Н. Вангородский. – М. : Дрофа, 2019. –238 с. URL: https://rosuchebnik.ru/upload/iblock/096/096c62d56dba3800eb92b649eb54388b.pdf (дата обращения : 16.04.2024).

3. Мы в ответе за цифровой мир: Профилактика деструктивного поведения подростков и молодежи в Интернете : учебно-методическое пособие / Г. У. Солдатова, С. В. Чигарькова, А. А. Дренёва, С. Н. Илюхина. – М. : Когито-Центр, 2019. – 176 с. URL: http://detionline.com/assets/files/research/my_v_otvete_za_cifrovoy_mir.pdf (дата обращения : 16.04.2024)

4. Солдатова Г.У., Рассказова Е.И., Вишнева А.Е., Теславская О.И., Чигарькова С.В. Рожденные цифровыми: семейный контекст и когнитивное развитие. — Акрополь Москва, 2022. — 356 с. URL: http://detionline.com/assets/files/research/digital_generation_2022.pdf (дата обращения : 16.04.2024)

5. Солдатова Г. У., Рассказова Е. И., Чигарькова С. В. Киберагрессия и цифровая культура: представления подростков, молодежи и родителей. — Издательство Московского института психоанализа Москва, 2023. — 288 с. URL: http://detionline.com/assets/files/research/kiberagressiya_2023.pdf (дата обращения : 16.04.2024)

3.3.2 Рекомендуемая литература

1. Механизмы противодействия органов внутренних дел (полиции) государств – участников СНГ вовлечению несовершеннолетних в деструктивные группы в сети Интернет : аналитический обзор с предложениями / И. Ю. Сундиев, А. Б. Коноплин, М. А. Никитина, Е. Е. Феоктистова, А. Г. Кузнецов, О. И. Новосельцев, О. В. Демковец, Д. А. Брехов, Ю. Н. Карайман. – М. : ФГКУ «ВНИИ МВД России», 2021. – 72 с.

2. Ашманов, И. С. Цифровая гигиена / Игорь Ашманов, Наталья Касперская. - Санкт-Петербург : Питер, 2022. - 398 с.

3.3.3 Интернет-ресурсы

1. Российская Федерация. Президент (2012 – 2018 ; В. В. Путин). Об утверждении Доктрины информационной безопасности Российской Федерации : указ Президента Российской

Федерации от 5 декабря 2016 г. № 646 / Российская Федерация. Президент (2012 – 2018 ; В. В. Путин). – Текст : электронный // Электронный фонд нормативно-технической и нормативно-правовой информации Консорциума «Кодекс». – URL: https://docs.cntd.ru/document/420384668 (дата обращения : 16.04.2024).

2. Российская Федерация. Президент (2012 – 2018 ; В. В. Путин). О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы [Электронный документ] : указ Президента Российской Федерации от 9.05.2017 г. № 203 / Российская Федерация. Президент (2012 – 2018 ; В. В. Путин). – Текст : электронный // Электронный фонд нормативно-технической и нормативно-правовой информации Консорциума «Кодекс». – URL: https://docs.cntd.ru/document/420397755 (дата обращения: 16.04.2024).

3. Российская Федерация. Законы. Об информации, информационных технологиях и защите персональных информации : Федеральный закон от 27.07.2006 г. N 149-ФЗ / Российская Федерация. Законы. – Текст : электронный // Электронный фонд нормативно-технической и нормативно-правовой информации Консорциума «Кодекс». – URL: https://docs.cntd.ru/document/901990051 (дата обращения: 16.04.2024).

4. Российская Федерация. Законы. О персональных данных : Федеральный закон от 27 июля 2006 г. N 152-ФЗ / Российская Федерация. Законы. – Текст : электронный // Электронный фонд нормативно-технической и нормативно-правовой информации Консорциума «Кодекс». – URL: https://docs.cntd.ru/document/901990046 (дата обращения: 16.04.2024).

5. Российская Федерация. Законы. О защите детей от информации, причиняющей вред их здоровью и развитию : Федеральный закон от 29 декабря 2010 года N 436-ФЗ / Российская Федерация. Законы. – Текст : электронный // Электронный фонд нормативно-технической и нормативно-правовой информации Консорциума «Кодекс». – URL: https://docs.cntd.ru/document/902254151 (дата обращения: 16.04.2024).

6. Российская Федерация. Законы. О противодействии экстремистской деятельности : Федеральный закон от 25 июля 2002 года N 114-ФЗ / Российская Федерация. Законы. – Текст : электронный // Электронный фонд нормативно-технической и нормативно-правовой информации Консорциума «Кодекс». – URL: https://docs.cntd.ru/document/901823502 (дата обращения: 16.04.2024).

7. Российская Федерация. Правительство. Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации : постановление Правительства РФ от 15 сентября 2008 г. N 687 / Российская Федерация. Правительство. – Текст : электронный // Электронный фонд нормативно-технической и нормативно-правовой информации Консорциума «Кодекс». – URL.: https://docs.cntd.ru/document/902119128 (дата обращения: 16.04.2024).

8. Российская Федерация. Правительство. Об утверждении требований к защите

9. персональных данных при их обработке в информационных системах персональных данных : постановление Правительства РФ от 1 ноября 2012 г. N 1119 / Российская Федерация. Правительство. – Текст : электронный // Электронный фонд нормативно-технической и нормативно-правовой информации Консорциума «Кодекс». – URL.: https://docs.cntd.ru/document/902377706 (дата обращения: 16.04.2024).

Раздел 4. Формы аттестации и оценочные материалы

Контроль достижения планируемых результатов обучающихся по программе осуществляется следующим образом:

- итоговая аттестация в форме устного зачета.

4.1 Оценочные материалы

4.1.1 Текущий контроль

Текущий контроль знаний слушателей проводится посредством выполнения практических работ. Практические работы считаются выполненными, если слушатель самостоятельно (или в основном самостоятельно) выполнил задания с незначительными замечаниями, при этом оценка не выставляется.

Тематика практических работ:

Практическая работа 1 (текущий контроль, 1 час): «Настройка безопасного поиска в интернет-браузере»

Слушатели должны настроить в интернет-браузере использование безопасного поиска вместо встроенной поисковой системы.

Практическая работа №2 (текущий контроль, 1 час): "Создание словаря сетевого сленга".

Слушатели должны разработать текстовой документ, содержащий таблицу из 2-х столбцов: сленговое слово и его пояснение. В таблице должно быть представлено не менее трех пунктов.

Практическая работа №3 (текущий контроль, 1 час): "Анализ персональных данных на сайте образовательной организации".

Слушатели исследуют информацию, размещенную на сайте своей ОО, и определяют, на какие публикации требуются согласие на обнародование фотографий и распространение персональных данных.

4.1.2 Промежуточная аттестация

Не предусмотрена.

4.1.3 Итоговая аттестация

Итоговая аттестация проводится в форме устного зачёта.

Продолжительность устного зачета 2 часа.

Каждый слушатель отвечает на 1 вопрос по выбору преподавателя.

Вопросы устного зачета:

1. Какими федеральными законами регулируются основные направления в области ограничения распространения и защиты информации?
2. Объясните связь понятий информационная безопасность, кибербезопасность и цифровая гигиена.
3. Укажите официальные реестры запрещенных материалов и сайтов и организации, ответственные за их исполнение.
4. Приведите варианты организации доступа к ресурсам сети Интернет в образовательной организации.
5. Укажите виды онлайн-рисков и цифровых компетенций.
6. Приведите примеры слов из современного молодежного интернет-сленга с объяснением значения.
7. Укажите примеры и меры профилактики деструктивного онлайн-поведения несовершеннолетних.
8. Назовите категории персональных данных и основные правила их обработки в соответствии с ФЗ-152.
9. Укажите особенности согласий на распространение персональных данных.
10. В каких случаях не требуются согласия на публикацию фотографий несовершеннолетних?

Критерии оценки устного ответа:

"Зачтено" выставляется слушателю в том случае, если:

- ответы на поставленные вопросы излагаются логично, последовательно и не требуют дополнительных пояснений;
- полно раскрываются причинно-следственные связи между требованиями федерального законодательства, регулирующего рассматриваемые в программе вопросы, и мерами, которые необходимо принять в образовательной организации для приведения системы работы в соответствие установленным требованиям;
- делаются обоснованные выводы, демонстрируются глубокие знания базовых нормативно-правовых актов, особенностей организации работы по обеспечению информационной безопасности образовательной организации.

“Не зачтено” выставляется слушателю в том случае, если:

- ответы на поставленные вопросы излагаются с нарушением последовательности и логики изложения, требуют дополнительных пояснений;
- не раскрыты причинно-следственные связи между требованиями федерального законодательства, регулирующего организацию информационной безопасности в образовательной организации и мерами, которые необходимо принять в образовательной организации для приведения системы работы в соответствие установленным требованиям;
- не сделаны обоснованные выводы, слушатель демонстрирует поверхностные знания базовых нормативно-правовых актов, особенностей организации работы по обеспечению информационной безопасности образовательной организации.