

Общество с ограниченной ответственностью  
«ПРОФСТАНДАРТ»

УТВЕРЖДАЮ  
Генеральный директор ООО «ПрофСтандарт»  
А.И. Данько  
2020 г.



**Дополнительная профессиональная программа  
(повышение квалификации)**

**Организация защиты детей от информации,  
причиняющей вред здоровью, развитию детей,  
не соответствующей задачам образования**

Рег. номер 005

Разработчики курса:  
Сорокин П.А.  
Самсонюк А.С.  
Новиков К.А.

**Направление: ИТ и средовые компетенции**  
**Уровень: базовый**

Москва - 2020

## Раздел 1. «Характеристика программы»

### 1.1. Цель реализации программы

Совершенствование профессиональных компетенций слушателей в области организация защиты детей от информации, причиняющей вред здоровью, развитию детей, не соответствующей задачам образования.

### Совершенствуемые/новые компетенции

№ п/п	Компетенции	Направление подготовки 44.03.01 Педагогическое образование (Бакалавр)
		Код компетенции
1.	Способен осуществлять профессиональную деятельность в соответствии с нормативными правовыми актами в сфере образования и нормами профессиональной этики	ОПК-1

### 1.2. Планируемые результаты обучения

№ п/п	Знать - уметь	Направление подготовки 44.03.01 Педагогическое образование (Бакалавр)
		Код компетенции
1.	<b>Знать:</b> алгоритм безопасного использования сети Интернет в повседневной жизни и в образовательных организациях. <b>Уметь:</b> организовывать безопасное использование сети Интернет в повседневной жизни и в образовательных организациях.	ОПК-1
2.	<b>Знать:</b> алгоритм проектирования образовательного мероприятия по защите детей от причиняющей вред здоровью, развитию детей, не соответствующей задачам образования. <b>Уметь:</b> проектировать образовательное мероприятие по защите детей от причиняющей вред здоровью, развитию детей, не соответствующей задачам образования.	ОПК-1

**1.3. Категория обучающихся:** уровень образования - высшее образование, область профессиональной деятельности – основное общее, среднее общее образование.

**1.4. Форма обучения:** программа реализуется с применением дистанционных образовательных технологий.

**1.5. Режим обучения:** доступ к образовательной платформе организации круглосуточно при соблюдении установленных сроков обучения.

**1.5. Срок обучения:** 16 часов.

## Раздел 2. «Содержание программы»

### 2.1. Учебный (тематический) план

№ п/п	Наименование разделов (модулей) и тем	Виды учебных занятий, учебных работ		Форма контроля	Трудоемкость
		Лекции	Интерактивные занятия		
1.	Нормативные основания обеспечения безопасности детей в Интернет-пространстве и при работе с компьютерной техникой	1	2	Входное тестирование	3
2	Алгоритм обеспечения безопасного использования сети Интернет	1	2	Практическая работа № 1	3
3.	Виды информационных угроз	1	2	Практическая работа № 2	3
4.	Образовательные программы по безопасному использованию ресурсов в сети Интернет	1	2		3
5.	Проектирование образовательного мероприятия по защите от	1	2	Практическая работа № 3	3

	информации, причиняющей вред здоровью, развитию детей, не соответствующей задачам образования				
6.	Итоговая аттестация		1	Зачет Итоговое тестирование	1
	<b>Итого</b>	<b>5</b>	<b>11</b>		<b>16</b>

## 2.2. Учебная программа

Наименование темы	Виды учебных занятий, учебных работ	Основное содержание
Тема 1. Нормативные основания обеспечения безопасности детей в Интернет-пространстве и при работе с компьютерной техникой	<i>Лекция, 1 час</i>	<p>Мировые и российские тенденции в вопросах безопасности детей в Интернет-пространстве. Обзор нормативных документов, регламентирующих вопросы информационной и компьютерной безопасности:</p> <p>ФЗ РФ "Об образовании в Российской Федерации, ФЗ РФ "О защите детей от информации, причиняющей вред их здоровью и развитию", Концепция информационной безопасности детей, утвержденной распоряжением Правительства РФ.</p> <p>Санитарно-эпидемиологические требования к условиям и организации обучения в общеобразовательных учреждениях.</p> <p>Деятельность организаций, занимающиеся обеспечению безопасности детей в сети Интернет:</p> <p>Федеральная служба безопасности РФ Роскомнадзор Общественная палата РФ Комиссия по безопасности Московской городской думы ООПН «Безопасная столица» Координационный совет негосударственной сферы безопасности Гильдия НСБ Московской торгово-промышленной палаты Лига безопасного интернета РОЦИТ Фонд развития Интернет</p>

		Фонд содействия развитию сети Интернет «Дружественный рунет» Центр безопасного интернета в России Федеральная служба по техническому и экспортному контролю РФ.
	<i>Интерактивное занятие, 2 часа</i>	Круглый стол. Дискуссия «Что является более действенным в борьбе с вредоносным контентом: создание ограничительных мер технического характера или просветительская деятельность социального характера?» <sup>1</sup> . Входное тестирование на платформе <a href="https://kurs.profstandart24.ru/course/view.php?id=7">https://kurs.profstandart24.ru/course/view.php?id=7</a>
Тема 2. Алгоритм обеспечения безопасного использования сети Интернет	<i>Лекция, 1 час</i>	Алгоритм безопасного использования сети Интернет в повседневной жизни и в образовательных организациях. Государственный контроль за обеспечением информационной и компьютерной безопасности. Контроль и надзор в сфере информационной безопасности детства и ответственность в сфере информационной безопасности детства. Ответственность образовательной организации и провайдеров в сфере доступа обучающихся к видам информации распространяемой посредством сети Интернет, причиняющей вред здоровью и развитию детей и не соответствующей задачам образования.
	<i>Интерактивное занятие, 2 часа</i>	<i>Практическая работа №1.</i> «Определение сферы ответственности различных организаций в области безопасного использования сети Интернет». Используйте перечень организаций из лекции или другие известные вам. Дайте краткое описание деятельности этих организаций в области безопасного использования ресурсов в сети Интернет.

<sup>1</sup> Дискуссии реализуются с фиксацией мнений на Форуме курса повышения квалификации.

<p>Тема 3. Виды информационных угроз</p>	<p><i>Лекция, 1 час</i></p>	<p>Виды информационных угроз: социальный блок (внутренние и внешние по отношению к образовательному коллективу коммуникационные угрозы). Понятия и существующие явления: социальные сети, кибербуллинг, Интернет-зависимость, информационные (гибридные) войны, компьютерные игры (геймификация) Технологический блок: возможные угрозы сбора и использования персональных данных, банковской и иной конфиденциальной информации компьютерные вирусы, уязвимость ПО физическое воздействие на аппаратуру ("железо", доступ к видео и аудио каналам компьютеров и устройств). Понятия и существующие тренды: хакеры, антивирусы, дополнительное ПО (родительский контроль), dark-net ("темный" сегмент Всемирной сети Интернет).</p>
	<p><i>Интерактивное занятие, 2 часа</i></p>	<p><i>Практическая работа № 2.</i> «Определение проблемы безопасного использования сети Интернет, описанной в кейсе и его решение». Групповая работа: обучающиеся анализируют ситуацию, описанную в кейсах и предлагают пути решения возникшей проблемы.</p>
<p>Тема 4. Образовательные программы по безопасному использованию ресурсов в сети Интернет</p>	<p><i>Лекция, 1 час</i></p>	<p>Образовательные программы ведущих ИТ-компаний по безопасному использованию ресурсов в сети Интернет в повседневной жизни и в образовательных организациях.</p>
	<p><i>Интерактивное занятие, 2 часа</i></p>	<p>Круглый стол. Дискуссия «Мы в ответе за тех, кого приручили» (А. Сент-Экзюпери «Маленький принц»). Можно ли переложить всю ответственность за безопасность действий детей в сети Интернет на поставщиков Интернета (Интернет провайдеров), на сотрудников образовательной организации? Какова роль законных представителей несовершеннолетних детей и самих детей в безопасном использовании сети Интернет?</p>

Тема 5. Проектирование образовательного мероприятия по защите от информации, причиняющей вред здоровью, развитию детей, не соответствующей задачам образования	<i>Лекция, 1 час</i>	Примеры образовательных мероприятий по защите от информации, причиняющей вред здоровью, развитию детей, не соответствующей задачам образования. Факторы, которые необходимо учитывать при проектировании образовательного мероприятия для обучающихся.
	<i>Интерактивное занятие, 2 часа</i>	<i>Практическая работа № 3.</i> «Проектирование сценария образовательного мероприятия, направленного на профилактические меры по защите детей от видов информации, распространяемой посредством сети Интернет, причиняющей вред здоровью, развитию детей, а также не соответствующей задачам образования, в образовательных организациях»
6. Итоговая аттестация	<i>Интерактивное занятие, 1 час</i>	Зачет: совокупность успешно выполненных практических работ, участие в дискуссиях Круглых столов. Итоговое тестирование: <a href="https://moodle.mioo.ru/">https://moodle.mioo.ru/</a>

### **Раздел 3. «Формы аттестации и оценочные материалы»**

Оценка качества освоения программы осуществляется в форме текущей и итоговой аттестации.

#### **Текущая аттестация:**

- участие в дискуссиях Круглых столов. Дискуссия реализуется с фиксацией мнений на Форуме курса повышения квалификации. Оценивание зачет / незачет. Зачет ставится, если обучающийся принял участие в работе Круглого стола и высказал свое мнение по обсуждаемому вопросу.
- выполнение Практических работ № 1-3. Зачет ставится, если критерии оценивания выполнены. Описание практических работ и их критерии оценивания в **Приложении 1**.

**Итоговая аттестация** – осуществляется на основании совокупности успешно выполненных практических работ, оцененных «зачет» и результата

итогового тестирования (примеры вопросов итогового тестирования в **Приложении 2**).

Обучающийся считается сдавшим зачет (аттестованным), если:

- получил положительные оценки и(или) отзывы не менее чем на 70% практических работ, выполненных в процессе обучения.
- результат итогового тестирования – 60% и более процентов правильных ответов.

Практические работы при качественном выполнении могут быть использованы обучающимися в качестве материала (образовательного продукта), применяемого в педагогической практике. Основным продуктом планируемым в результате обучения на курсе – сценарий образовательного мероприятия, направленный на профилактические меры по защите детей от видов информации, распространяемой посредством сети Интернет, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, в образовательных организациях.

Все практические задания обучающихся выполняют и сдают в удобное время в рамках учебной программы через модули дистанционной поддержки курса на платформе moodle.mioo.ru.

### **Перечень практических заданий**

<b>Проверяемые практические работы</b>	
Практическая работа № 1	Определение сфер деятельности различных организаций в области безопасного использования сети Интернет
Практическая работа № 2	Определение проблемы безопасного использования сети Интернет, описанной в кейсе и его решение
Практическая работа № 3	Проектирование сценария образовательного мероприятия, направленного на профилактические меры по защите детей от видов информации, распространяемой посредством сети Интернет, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, в образовательных организациях

## Соответствие практических заданий заявленным компетенциям

№ п/п	Знать	Направление подготовки 44.04.01 Педагогическое образование (магистратура) Код компетенции	Контроль
1.	Алгоритм безопасного использования сети Интернет в повседневной жизни и в образовательных организациях	ОПК-1	<i>Круглый стол Практическая работа № 1, 2 Выходной контроль</i>
2.	Алгоритм проектирования образовательного мероприятия по мерам профилактики защиты детей от видов информации, распространяемой посредством сети Интернет, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования	ОПК-1	<i>Круглый стол Практическая работа № 3 Выходной контроль</i>
№ п/п	Уметь	Направление подготовки 44.04.01 Педагогическое образование (магистратура) Код компетенции	Контроль
1.	Организовывать безопасное использование сети Интернет в повседневной жизни и в образовательных организациях	ОПК-1	<i>Практическая работа № 1, 2</i>
2.	Применять общепедагогические ИКТ-компетентности в проектировании образовательного мероприятия по мерам профилактики защиты детей от видов информации, распространяемой посредством сети Интернет, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования	ОПК-1	<i>Практическая работа № 3</i>

## Раздел 4. «Организационно-педагогические условия реализации программы»

### 4.1. Учебно-методическое обеспечение и информационное обеспечение программы

**Нормативные документы:**

1. Федеральный закон от 29.12.2012 N 273-ФЗ (ред. от 17.06.2019) "Об образовании в Российской Федерации", <http://www.consultant.ru/cons/cgi/online.cgi?from=140174-0&rnd=710A3E4F040E5C54764AABD85EB1E35D&req=doc&base=LAW&n=326937&REFDOC=140174&REFBASE=LAW#18c4n3x280h> (дата обращения 08.07.2019)
2. Федеральный закон от 29.12.2010 N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию" <https://mosmetod.ru/metodicheskoe-prostranstvo/documenti/436-fz-o-zaschite-detei-ot-informmatcii.html> (дата обращения 08.07.2019)
3. Концепция информационной безопасности детей, утвержденной распоряжением Правительства РФ от 02.12.2015 N 2471
4. Профессиональный стандарт «Педагог (педагогическая деятельность в дошкольном, начальном общем, основном общем, среднем общем образовании) (воспитатель, учитель)», приложение к приказу Минтруда РФ № 544н от 18.10.2013г., URL [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_155553/сса\\_в\\_системе\\_Департамента\\_образования\\_города\\_Москвы.\\_Москва,\\_2008](http://www.consultant.ru/document/cons_doc_LAW_155553/сса_в_системе_Департамента_образования_города_Москвы._Москва,_2008) (дата обращения 08.07.2019)
5. Постановление Главного государственного санитарного врача РФ от 29 декабря 2010 г. N 189 "Об утверждении СанПиН 2.4.2.2821-10 "Санитарно-эпидемиологические требования к условиям и организации обучения в общеобразовательных учреждениях" (с изменениями и дополнениями). Система ГАРАНТ: <http://base.garant.ru/12183577/#ixzz5r69ysA2h> (дата обращения 08.07.2019).

### **Основная литература:**

1. Малюк А.А. Глобальная культура кибербезопасности // Горячая линия - Телеком. М., 2017. С. 308.
2. Информационная безопасность: учебное пособие. / С.В.Петров, И.П.Слинькова, В.В.Гафнер, П.А.Кисляков. – Новосибирск: АРТА, 2012. – 296 с. – (серия «Безопасность и жизнедеятельность»).

3. Джули Дирксен. Искусство обучать. Как сделать любое обучение нескучным и эффективным; пер. с англ. Москва: Манн, Иванов и Фербер, 2015.

4. Международная информационная безопасность: Теория и практика: В трех томах: Учебник для вузов / Под общ. ред. А.В.Крутских. — М.: Издательство «Аспект Пресс», 2019.

5. Хломов К.Д., Давыдов Д.Г., Бочавер А.А. Кибербуллинг в опыте российских подростков. [Электронный ресурс] // Психология и право. 2019(9). No 2. С. 276-295. doi: 10.17759/psylaw.2019090219.

### **Интернет ресурсы:**

1. Курс «Безопасность в интернете» от Яндекса [https://academy.yandex.ru/events/online-courses/internet\\_security/](https://academy.yandex.ru/events/online-courses/internet_security/) (дата обращения 08.07.2019).

2. Журнал для педагогов, психологов и родителей «Дети в информационном обществе». <http://detionline.com/journal> (дата обращения 08.07.2019).

3. Методическое пособие «Интернет: возможности, компетенции, безопасность». Солдатова Г., Зотова Е., Лебешева М., Шляпников В. <http://detionline.com/internet-project/training-aids> (дата обращения 08.07.2019).

4. «Урок полезного и безопасного Интернета» от компании МТС. <http://detionline.com/mts/lessons> (дата обращения 08.07.2019).

5. «Защита детей в интернете» от компании Касперского <https://kids.kaspersky.ru/>

6. Видеоурок «Безопасность в Интернете» от компании Касперского <https://урокцифры.рф/teachers.html> (дата обращения 08.07.2019)

7. Проект «Разбираем Интернет вместе с Google» <http://www.razbiraeminternet.ru/> (дата обращения 08.07.2019).

8. Интернет и безопасность. Онлайн курс для детей и взрослых. <https://sites.google.com/site/kyrsbez/home> (дата обращения 08.07.2019).

9. Think with Google. Новое поколение интернет-пользователей: исследование привычек и поведения российской молодежи онлайн. URL:

<https://www.thinkwithgoogle.com/intl/ru-ru/insights-trends/user-insights/novoe-pokolenie-internet-polzovatelei-issledovanie-privyчек-i-povedeniia-rossiiskoi-molodezhi-onlain/> (дата обращения 08.07.2019).

10. Солдатова Г.У., Нестик Т.А., Рассказова Е.И., Зотова Е.Ю. Цифровая компетентность подростков и родителей результаты всероссийского исследования [Электронный ресурс]. М., Фонд Развития Интернет, 2013. 144 с. URL: <http://detionline.com/assets/files/research/DigitalLiteracy.pdf> (дата обращения 08.07.2019).

11. PricewaterhouseCoopers: аналитический обзор по теме информационной безопасности (2018) <https://www.pwc.ru/ru/publications/global-information-security-survey-2018.html> (дата обращения 08.07.2019).

12. «Исследования» от Mail.ru Group <https://corp.mail.ru/ru/press/infograph/>

#### 4.2. Материально-технические условия реализации программы

Персональный компьютер обучающегося; колонки или наушники, микрофон (в том числе вмонтированный в моноблок или в ноутбук).

## Приложение 1

### Описание практических работ

*Практическая работа №1.* «Определение сфер деятельности различных организаций в области безопасного использования сети Интернет».

Алгоритм выполнения	<ul style="list-style-type: none"> <li>• Просмотрите предложенные преподавателем сайты организаций, у которых есть контент по безопасному использованию сети Интернет, в повседневной жизни и в образовательных организациях.</li> <li>• С помощью текстового процессора сделайте памятку для участников образовательного процесса, описав на каком ресурсе, какую полезную информацию по безопасному использованию сети Интернет можно найти. Памятку можно сделать для обучающихся / воспитанников, их родителей или для своих коллег учителей-предметников.</li> <li>• Файл с выполненным заданием опубликовать в соответствующей ветке форума.</li> </ul>
Критерии оценивания	<ul style="list-style-type: none"> <li>• Памятка содержит информацию, направленную на одну категорию участников образовательного процесса.</li> </ul>

	<ul style="list-style-type: none"> <li>• Выявлен и описан полноценный объем из первоисточника о безопасности в сети Интернет.</li> <li>• Файл с выполненным заданием опубликован в учебном курсе.</li> </ul>
Оценка	Зачет / Незачет

**Практическая работа №2.** «Определение проблемы безопасного использования сети Интернет, описанной в кейсе и его решение».

Алгоритм выполнения	<ul style="list-style-type: none"> <li>• Изучить предложенные преподавателем кейсы с описанием проблем, которые могут возникнуть у пользователей сети Интернет.</li> <li>• Руководствуясь алгоритмом безопасного использования сети Интернет в повседневной жизни определить, описанную в кейсе проблему.</li> <li>• Сделать краткие рекомендации по решению / мерам предотвращения возникшей ситуации в будущем.</li> <li>• Текст отчета по заданию опубликовать в соответствующей ветке форума.</li> </ul>
Критерии оценивания	<ul style="list-style-type: none"> <li>• Выявлены все проблемы, описанные в кейсе.</li> <li>• Применен полный алгоритм безопасного использования сети Интернет в повседневной жизни.</li> <li>• Текст отчета опубликован в учебном курсе.</li> </ul>
Оценка	Зачет / Незачет

**Практическая работа №3.** «Проектирование сценария образовательного мероприятия, направленного на профилактические меры по защите детей от видов информации, распространяемой посредством сети Интернет, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, в образовательных организациях»

Алгоритм выполнения	<ul style="list-style-type: none"> <li>• Проанализируйте, предложенные преподавателем схемы и идеи для организации мероприятий. Выберите одну из них или сформируйте собственную идею.</li> <li>• Используя известные вам офисные приложения, сервисы по созданию интерактивных заданий, спроектируйте краткий сценарий образовательного мероприятия по мерам профилактики защиты детей от видов информации, распространяемой посредством сети Интернет, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования.</li> <li>• Файл или URL-адрес с выполненным заданием опубликовать в соответствующей ветке форума</li> </ul>
Критерии оценивания	<ul style="list-style-type: none"> <li>• Сценарий соответствует описанному заданию.</li> <li>• Файл или URL-адрес с выполненным заданием опубликован в учебном курсе.</li> </ul>

	<ul style="list-style-type: none"> <li>• Сценарий мероприятия носит образовательный характер и может быть использован в образовательном учреждении, как профилактика защиты детей от видов информации, распространяемой посредством сети Интернет, причиняющей вред здоровью и (или) развитию детей</li> </ul>
Оценка	Зачет / Незачет

## Приложение 2

### Примеры вопросов входного и итогового тестирования

Какую информацию нельзя разглашать в Интернете?

1. Мир увлечений
2. Ваш адрес проживания
3. Рассказ о встречах с знакомыми и друзьями
4. Рассказ о вашей мечте

На страничке социальной сети Вас оскорбили, обозвали нецензурными словами, прислали порнографические картинки. Что сделаете Вы в таком случае?

1. Ответите тоже грубо и с бранью
2. Игнорируете своего обидчика
3. Посмеетесь над невоспитанностью своего знакомого

Какой пароль стоит ставить на Интернет-ресурсе?

1. Одинаковый с логином
2. Основанный на словарном запасе Длиной менее 8-ми символов
3. В котором используются не только буквы, но и цифры или специальные символы

При проектировании образовательного мероприятия для обучающихся необходимо учитывать:

1. Возраст обучающихся
2. Уровень владения компьютерной грамотностью родителей

### 3. Результаты опросов участников образовательного процесса

На личную почту пришло письмо с официальным запросом от Вашего интернет-провайдера - в результате сбоя системы потеряны данные, позволяющие обеспечивать работу в Интернете. Запрашивается ваш личный логин и пароль для повторного внесения в систему. Как действовать?

1. Предоставить данные по запросу
2. Предоставить только пароль (логин и дополнительная информация есть у провайдера по умолчанию)
3. Отметить письмо как спам