

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
«НАУЧНЫЙ ЦЕНТР ПРАВОВОЙ ИНФОРМАЦИИ»
(ФБУ НЦПИ ПРИ МИНЮСТЕ РОССИИ)

«Утверждаю»
Директор ФБУ НЦПИ
при Минюсте России



Е.Н. Честнов

Е.Н. Честнов 2024 г.

**«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
НЕСОВЕРШЕННОЛЕТНИХ:
ЗАЩИТА ОТ КИБЕРБУЛЛИНГА»**

Программа курса
дополнительного профессионального образования
повышения квалификации

МОСКВА
2024

Составители:

Шикула И.Р., профессор департамента права Института экономики, управления и права Московского городского педагогического университета, доктор юридических наук, доцент; член экспертного совета комитета Государственной Думы Российской Федерации по защите семьи, вопросам отцовства, материнства и детства, член-корреспондент РАЕН;

Сергин М.Ю., начальник отдела научно-исследовательской и образовательной деятельности ФБУ НЦПИ при Минюсте России, доктор технических наук, профессор.

Содержание

1.	Общие положения	4
2.	Требования к результатам освоения программы	7
3.	Объем учебного времени на освоение программы.....	9
4.	Содержание тем программы	10
5.	Перечень, трудоемкость, последовательность и распределение учебного материала по разделам и темам	11
6.	Методические рекомендации по реализации программы.....	16
7.	Материально-техническое обеспечение программы.....	18
8.	Учебно-методическое и информационное обеспечение программы	19
9.	Оценка качества освоения программы	24

1. Общие положения

Постоянное развитие и повсеместное внедрение в повседневную жизнь информационно-телекоммуникационных технологий дает возможность доступа практически к любой информации, которая удовлетворяет образовательные, коммуникативные, познавательные и иные потребности. «Интернет-пространство как совокупность компьютерных сетей и информации в первую очередь представляет собой множество людей, активно взаимодействующих между собой в виртуальном пространстве, в котором создаются собственная культура, иерархия ценностей и особый язык»¹.

Сегодня практически в каждой семье есть доступ в глобальную сеть. В результате подключения к Интернету общеобразовательных и профессиональных учебных заведений в рамках национального проекта пользовательская активность российских школьников резко возросла. Интернет стал неотъемлемой частью жизни, который призван помогать в получении актуальных и полезных знаний, что возможно только при правильном его применении. Однако все чаще несовершеннолетние используют информационные ресурсы не только и не столько в учебных целях (коллективные сетевые игры, создание разного рода сообщества в социальных сетях и т.д.).

Несмотря на действующие в Российской Федерации нормативные правовые акты², регулирующие вопросы защиты психофизиологического здоровья детей от вредоносной информации, наблюдается повсеместное распространение в интернет-пространстве материалов, содержащих насилие, агрессию, эротику и порнографию, пропаганду суицида, азартных игр и наркотических веществ, кибербуллинг (интернет-травля)³, груминг, троллинг, оказывающих негативное влияние на нравственно-психическое состояние детей и подростков, что вызывает необходимость в разработке организационно-правовых мер по защите несовершеннолетних от вредоносного контента в сети Интернет⁴ посредством блокировки сайтов, пропагандирующих суициды, введения уголовной ответственности за травлю в интернет-сети (преследование, stalking, буллинг и

¹ Домбровский В., Ломтев И., Городбин А. Проект «Мы в интернет-безопасности» // Молодой ученый. 2016. № 8-1. С. 21—29.

² Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» // Российская газета. 2010. № 297; Концепция информационной безопасности детей в Российской Федерации (утв. распоряжением Правительства Российской Федерации от 28.04.2023 № 1105-р); О Стратегии развития информационного общества в Российской Федерации на 2017—2030 годы: Указ Президента Российской Федерации от 09.05.2017 № 203 // Собрание законодательства РФ. 2017. № 20. Ст. 2901; Госдума приняла в I чтении законопроект Яровой, защищающий детей от вовлечения в преступное сообщество и опасные группы. URL: <https://яровая.рф/news/zashchita-detey/gosduma-prinyala-v-i-chtenii-zakonoproekt-yarovoy-zashchishchayushchiy-detey-ot-vo vlecheniya-v-prest>

³ 49% российских подростков от 8 до 17 лет становились жертвой этих деяний, при этом виртуальное преследование часто дополняет реальное насилие.

⁴ Из доклада Генерального прокурора Ю.Чайки на заседании Совета Федерации Федерального собрания Российской Федерации в 2018 г. URL: <https://genproc.gov.ru/smi/news-1366820>

т. д.). Дети в силу возраста, отсутствия жизненного опыта и знаний в области информационной безопасности не обладают способностью фильтровать качество информации и наиболее подвержены влиянию запрещенной информации. Развитие и использование информационных технологий нередко оказывает на детей негативное влияние, побуждает их к противоправному, деструктивному поведению.

Цели и задачи программы

Целями преподавания программы является:

- формирование у слушателей основ теоретических знаний, практических умений и навыков профессиональной деятельности в области информационной безопасности детей;
- развитие способностей слушателей к самостоятельной работе по углублению знаний в данной области;
- выработка у слушателей мотивационной установки и формирование их морально-психологической готовности к выполнению задач, связанных с противодействием преступности в интернет-пространстве.

Категории слушателей: руководители, заместители руководителей образовательных организаций, учителя, реализующие программы общего образования, преподаватели общеобразовательных организаций высшего образования, обучающиеся образовательных организаций.

Цель изучения программы:

овладение слушателями знаний:

- о социально-правовом негативном явлении кибербуллинга и современных особенностях его проявлений;
- о правовой регламентации проявлений кибербуллинга;
- о причинном комплексе, детерминирующем проявления кибербуллинга;
- о формировании отрицательного отношения ко всем проявлениям жестокости, насилия, агрессии в сети Интернет;
- об особенностях, характеризующих личность преступника-террориста;
- о принципах, правовых основах, организационных формах противодействия кибербуллингу;
- овладение первичными умениями и навыками решения практических задач по противодействию кибербуллингу.

Основными задачами преподавания программы являются:

- формирование у слушателей устойчивых знаний о сущности информационной безопасности;
- формирование у слушателей знаний об уголовной ответственности за совершение преступлений в сфере информационной безопасности;

- формирование у слушателей знаний о причинах совершения и условиях, способствующих совершению кибербуллинга;
- формирование у слушателей знаний о системе, структуре и правовых основах противодействия кибербуллингу в отношении несовершеннолетних.

Освоение слушателями программы предполагает формирование и укрепление у них следующих профессионально значимых качеств:

- общей и правовой культуры;
- патриотизма и чувства гражданской ответственности;
- профессиональной коммуникативной компетентности;
- морально-психологической устойчивости, выдержки, инициативности, решительности;
- понимания роли и места субъектов системы противодействия кибербуллингу.

2. Требования к результатам освоения программы

В результате изучения учебной программы слушатели должны:

иметь представление:

- о безопасном поведении при работе с компьютерными программами, информацией в сети Интернет;
- о понятии «компьютерная грамотность и информационная культура личности в использовании информационных и коммуникационных технологий»;
- о понятиях «киберпространство», «киберкультура», «киберугрозы»;
- о различных формах ответственности за поступки в области информационной безопасности;
- о современном состоянии проблем теории и практики по противодействию кибербуллингу;
- о зарубежном опыте противодействия кибербуллингу,

знать:

- сущность и содержание социально-правового явления кибербуллинга;
- нормативную правовую базу, регламентирующую информационную безопасность несовершеннолетних;
- пути совершенствования института информационной безопасности;
- комплекс причин и условий, детерминирующих проявление кибербуллинга;
- сущность и содержание основных организационно-правовых мер противодействия кибербуллингу;
- основы общей, специально-криминологической и частной превенции проявлений кибербуллинга,

уметь:

- соблюдать нормы информационной этики;
- безопасно работать с информацией, анализировать и обобщать полученную информацию;
- анализировать и систематизировать имеющуюся информацию;
- выстраивать безопасное общение в сети Интернет;
- распознавать киберугрозы разного вида,

владеть:

- навыками составления учебных программ, учебных комплексов по профилактике кибербуллинга;
- навыками составления плана мероприятий по противодействию кибербуллингу в сфере своей профессиональной деятельности.

Режим занятий: 20 аудиторных часов (10 часов — лекционные занятия, 4 часа — практические занятия; 4 часа — самостоятельная работа; 2 часа — контрольные занятия).

Форма обучения: очно-заочная.

Календарный учебный график: режим занятий и расписание занятий составляются по согласованию с заказчиком.

Форма входной аттестации: анкетирование.

Форма промежуточной (текущей) аттестации: дискуссия.

Форма и виды итоговой аттестации: экзамен в форме тестирования.

3. Объем учебного времени на освоение программы

№ п/п	Наименование дисциплины	Объем (час)			Форма контроля знаний
		Всего часов	в том числе:		
			Лекции	Практические и прочие виды занятий (в т. ч. самост. работа слушателя в заочной форме)	
1	2	3	4	5	6
1.	Раздел I. Теоретические аспекты информационной безопасности несовершеннолетних: проблемы правового регулирования	8	4	4 (2)	Промежуточный контроль: дискуссия
1.1.	Государственная политика в сфере регулирования информационной безопасности несовершеннолетних	4	2	2	Промежуточный контроль: дискуссия
1.2.	Основные направления профилактики кибербуллинга в отношении несовершеннолетних	4	2	2 (2)	Промежуточный контроль: дискуссия
2.	Раздел II. Уголовно-правовые и криминологические аспекты обеспечения информационной безопасности несовершеннолетних: современное состояние и меры по дальнейшему совершенствованию	10	4	6 (2)	Промежуточный контроль: дискуссия
2.1.	Информационная безопасность несовершеннолетних: психолого-педагогические критерии	4	2	2	Промежуточный контроль: дискуссия
2.2.	Экстремистская и террористическая деятельность с использованием электронных или информационно-телекоммуникационных сетей: алгоритм вовлечения несовершеннолетних	3	1	2	Промежуточный контроль: дискуссия
2.3.	Профилактика вовлечения несовершеннолетних в преступную деятельность посредством информационных технологий	3	1	2 (2)	Промежуточный контроль: дискуссия
3.	Итоговая аттестация	2		2	Экзамен в форме тестирования
ВСЕГО:		20	8	12 (4)	

4. Содержание тем программы

По разделу 1 «Теоретические аспекты информационной безопасности несовершеннолетних: проблемы правового регулирования» обучающиеся изучат:

Государственная политика в сфере общего образования Российской Федерации. Проблемы нормативно-правового регулирования информационной безопасности несовершеннолетних. Информационная защита несовершеннолетних в образовательном процессе. Основы противодействия угрозам здоровью и жизни, исходящих из электронных или информационно-телекоммуникационных сетей, в том числе сети Интернет. Организация работы по профилактике кибербуллинга, скулшутинга («колумбайн»), суицидального поведения несовершеннолетних.

По разделу 2 «Уголовно-правовые и криминологические аспекты обеспечения информационной безопасности несовершеннолетних: современное состояние и меры по дальнейшему совершенствованию» обучающиеся изучат:

Информационная безопасность несовершеннолетних с позиций психолого-педагогического подхода. Критерии оценки состояния информационной безопасности подростков (рекомендации для родителей, педагогов). Основы противодействия вовлечению подростков в экстремистскую и террористическую деятельность с использованием электронных или информационно-телекоммуникационных сетей, в том числе сети Интернет: проблемы профилактики.

5. Перечень, трудоемкость, последовательность и распределение учебного материала по разделам и темам

Планы лекций

Разделы и темы дисциплины	Аудиторные часы	Краткое содержание
1	2	3
Раздел 1. Теоретические аспекты информационной безопасности несовершеннолетних: проблемы правового регулирования		
Тема 1.1. Государственная политика в сфере регулирования информационной безопасности несовершеннолетних	2	Лекция 1.1 Государственная политика в сфере общего образования Российской Федерации. Проблемы нормативно-правового регулирования информационной безопасности несовершеннолетних. Информационная защита несовершеннолетних в образовательном процессе
Тема 1.2. Основные направления профилактики кибербуллинга в отношении несовершеннолетних	2	Лекция 1.2 Основы противодействия угрозам здоровью и жизни, исходящих из электронных или информационно-телекоммуникационных сетей, в том числе сети Интернет. Организация работы по профилактике кибербуллинга, скулшутинга («колумбайн»), суицидального поведения несовершеннолетних

1	2	3
Раздел 2. Уголовно-правовые и криминологические аспекты обеспечения информационной безопасности несовершеннолетних: современное состояние и меры по дальнейшему совершенствованию		
<p>Тема 2.1 Информационная безопасность несовершеннолетних: психолого-педагогические критерии</p>	2	<p>Лекция 2.1 Информационная безопасность несовершеннолетних с позиций психолого-педагогического подхода. Критерии оценки состояния информационной безопасности подростков (рекомендации для родителей, педагогов)</p>
<p>Тема 2.2 Экстремистская и террористическая деятельность с использованием электронных или информационно-телекоммуникационных сетей: алгоритм вовлечения несовершеннолетних</p>	1	<p>Лекция 2.2 Сущность экстремистской и террористической деятельности с использованием электронных или информационно-телекоммуникационных сетей. Основы противодействия вовлечению подростков в экстремистскую и террористическую деятельность с использованием электронных или информационно-телекоммуникационных сетей, в том числе сети Интернет. Раннее реагирование на девиантное поведение. Меры защиты, восстановления, ресоциализации и психологической помощи</p>
<p>Тема 2.3 Профилактика вовлечения несовершеннолетних в преступную деятельность посредством информационных технологий</p>	1	<p>Лекция 2.3 Основы профилактики вовлечения несовершеннолетних в преступную деятельность посредством информационных технологий. Интернет-технологии как способ вовлечения несовершеннолетних в преступную деятельность: проблемы профилактики</p>

Планы практических (самостоятельных) занятий

Разделы и темы дисциплины	Аудиторные часы	Краткое содержание
1	2	3
Раздел 1. Теоретические аспекты информационной безопасности несовершеннолетних: проблемы правового регулирования		
Тема 1.1. Государственная политика в сфере регулирования информационной безопасности несовершеннолетних	2	Семинар 1.1. Обсуждение, ответы на вопросы по теме. Государственная политика в сфере общего образования Российской Федерации. Проблемы нормативно-правового регулирования информационной безопасности несовершеннолетних. Информационная защита несовершеннолетних в образовательном процессе
Тема 1.2. Основные направления профилактики кибербуллинга в отношении несовершеннолетних	2	Самостоятельное занятие 1.2 Основы противодействия угрозам здоровью и жизни, исходящих из электронных или информационно-телекоммуникационных сетей, в том числе сети Интернет. Организация работы по профилактике кибербуллинга, скулшутинга («колумбайн»), суицидального поведения несовершеннолетних
Промежуточный контроль		Проведение дискуссии по итогам обучения по Разделу 1

1	2	3
Раздел 2. Уголовно-правовые и криминологические аспекты обеспечения информационной безопасности несовершеннолетних: современное состояние и меры по дальнейшему совершенствованию		
<p>Тема 2.1 Информационная безопасность несовершеннолетних: психолого-педагогические критерии</p>	2	<p>Семинар 2.1. Обсуждение, ответы на вопросы по теме. Информационная безопасность несовершеннолетних с позиций психолого-педагогического подхода. Критерии оценки состояния информационной безопасности подростков (рекомендации для родителей, педагогов)</p>
<p>Тема 2.2 Экстремистская и террористическая деятельность с использованием электронных или информационно-телекоммуникационных сетей: алгоритм вовлечения несовершеннолетних</p>	2	<p>Семинар 2.2. Обсуждение, ответы на вопросы по теме. Сущность экстремистской и террористической деятельности с использованием электронных или информационно-телекоммуникационных сетей. Основы противодействия вовлечению подростков в экстремистскую и террористическую деятельность с использованием электронных или информационно-телекоммуникационных сетей, в том числе сети Интернет. Раннее реагирование на девиантное поведение. Меры защиты, восстановления, ресоциализации и психологической помощи</p>

1	2	3
<p>Тема 2.3 Профилактика вовлечения несовершеннолетних в преступную деятельность посредством информационных технологий</p>	<p>2</p>	<p>Самостоятельное занятие 2.3 Основы профилактики вовлечения несовершеннолетних в преступную деятельность посредством информационных технологий. Интернет-технологии как способ вовлечения несовершеннолетних в преступную деятельность: проблемы профилактики</p>
<p>Промежуточный контроль</p>		<p>Проведение дискуссии по итогам обучения по Разделу 2</p>

6. Методические рекомендации по реализации программы

Методические рекомендации отражают принципы формирования соответствующих компетенций у целевой группы слушателей в рамках своих полномочий в реализации мероприятий и программ по противодействию кибербуллингу.

Программа предполагает разбивку занятий на теоретические и практические. Вместе с тем рекомендуется сохранить за преподавателями право самостоятельно определять наиболее эффективную форму реализации Программы для каждой из групп слушателей в зависимости от формы обучения. При этом преподаватели должны опираться на свой личный опыт, индивидуальную методику и потребности слушателей.

Эффективной реализации Программы способствует соблюдение ряда условий;

- ориентация содержания программы на потребности и запросы слушателей;
- высокая квалификация преподавательского состава и используемые ими образовательные технологии;
- наличие необходимого и достаточного комплекта учебно-методического комплекта курса;
- превалирование деятельностного аспекта обучения над информационной составляющей.

В ходе освоения содержания Программы рекомендуется использовать образовательные технологии, предусматривающие различные методы и формы изучения материала (активные и интерактивные формы занятий, лекции, видеоматериалы и др.):

1. Во время проведения занятий следует активно использовать лекции в форме диалога или проблемные лекции.

2. На семинарских занятиях рекомендуется обсуждать проблемы с целью изучения наиболее важных вопросов темы. Рекомендуется также использовать форму проведения семинаров в виде интервью или пресс-конференций.

3. В качестве активных форм занятий можно использовать игровое моделирование (деловые и ролевые игры).

Кроме того, в процессе обучения рекомендуется использовать такие формы и методы, как коллективное решение проблемных ситуаций, групповая дискуссия, проектная деятельность, метод мозгового штурма, тренинги, разбор кейсов, работа с программными продуктами и обучающими комплексами.

Самостоятельная работа слушателей подразумевает работу под руководством преподавателя и индивидуальную работу, выполняемую с использованием электронных информационно-образовательных ресурсов.

При реализации образовательных технологий используются следующие виды самостоятельной работы:

- работа с конспектом лекций;
- работа с учебниками, учебными пособиями и рекомендованной литературой;
- самостоятельная проработка тем и вопросов, предусмотренных программой, но не раскрытых полностью на лекциях;
- выполнение тестовых заданий;
- подготовка к практической работе;
- подготовка творческого задания;
- подготовка к аттестации.

7. Материально-техническое обеспечение программы

Наименование специализированных аудиторий, кабинетов, лабораторий	Вид занятий	Наименование оборудования, программного обеспечения
аудитория	лекции	Компьютер, мультимедийный проектор, экран, флипчарт. Набор электронных презентаций для использования в аудиторных занятиях
аудитория	практические (семинарские) занятия	Компьютер, мультимедийный проектор, экран, флипчарт, доступ в Интернет

8. Учебно-методическое и информационное обеспечение программы

Информационные ресурсы

1. Портал «Нормативные правовые акты в Российской Федерации». URL: <http://pravo-minjust.ru>
2. Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru>
3. СПС «КонсультантПлюс». URL: <http://www.consultant.ru>
4. СПС «Гарант». URL: <http://www.garant.ru>
5. Федеральный правовой портал «Юридическая Россия». URL: <http://www.law.edu.ru>
6. Методы и средства защиты информации. URL: <http://asu.gubkin.ru>
7. Федеральный образовательный портал «Информационно-коммуникационные технологии в образовании». URL: <http://window.edu.ru>
8. Федеральный портал «Российское образование». URL: <https://www.edu.ru/>
9. Федеральный центр информационно-образовательных ресурсов. URL: <http://fcior.edu.ru>
10. Федеральный портал «Российская электронная школа». URL: <https://www.resh.edu.ru>
11. Федеральный портал «Федеральные государственные образовательные стандарты и примерные основные общеобразовательные программы». URL: <https://fgosreestr.ru>
12. Жертвы кибербуллинга: как защитить детей от травли в интернете. URL: <https://www.m24.ru/articles/deti/27062019/155723>. Текст: электронный.
13. По дороге домой тебе не поздоровится: что такое кибербуллинг? URL: <https://ria.ru/20180804/1525897862.html?inj=1>. Текст: электронный.

Библиотеки

1. Библиотека РАН. URL: <http://www.benran.ru>
2. Российская государственная библиотека. URL: <http://www.rsl.ru>
3. Сервер правовой информации. URL: <http://www.pravopoliten.ru>
4. ИНИОН РАН. URL: <http://www.inion.ru>
5. Российская государственная библиотека. URL: <http://www.rsl.ru>
6. Национальная электронная библиотека. URL: <http://www.net.nns.ru>
7. Научная электронная библиотека. URL: <http://elibrary.ru>

Нормативные правовые акты

1. Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 28.04.2023) «О защите детей от информации, причиняющей вред их здоровью и развитию».
2. Федеральный закон «Об образовании в Российской Федерации» от 29.12.2012 № 273-ФЗ. URL: http://www.consultant.ru/document/cons_doc_LAW_140174 (дата обращения: 25.01.2024).
3. Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам: приказ Минобрнауки России от 01.07.2013 № 499. URL: http://www.consultant.ru/document/cons_doc_LAW_151143 (дата обращения: 25.01.2024).
4. Об утверждении Порядка применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ: приказ Минобрнауки России от 23.08.2017 № 816. URL: http://www.consultant.ru/document/cons_doc_LAW_278297 (дата обращения: 25.03.2022).
5. Об утверждении критериев оценки материалов и (или) информации, необходимых для принятия решений Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций, Министерством внутренних дел Российской Федерации, Федеральной службой по надзору в сфере защиты прав потребителей и благополучия человека, Федеральной налоговой службой о включении доменных имен и (или) указателей страниц сайтов в информационно-телекоммуникационной сети Интернет: межведомственный приказ Роскомнадзора, МВД России, Роспотребнадзора, ФНС России от 18 мая 2017 г. № 84/292/351/ММВ-7-2/461С // МВД РФ : официальный сайт. 2017. 18 мая. URL: <https://мвд.рф/mvd/documents/межведомственные-нпа/item/12304217> (дата обращения: 27.01.2024).
6. О Стратегии развития информационного общества в Российской Федерации на 2017—2030 годы: Указ Президента Российской Федерации от 09.05.2017 № 203 // Собрание законодательства РФ. 2017. № 20. Ст. 2901.
7. Федеральные государственные образовательные стандарты и примерные основные общеобразовательные программы. URL: <https://fgosreestr.ru> (дата обращения: 25.01.2024).
8. Концепция информационной безопасности детей в Российской Федерации (утв. распоряжением Правительства Российской Федерации от 28.04.2023 № 1105-р).
9. Постановление Правительства Российской Федерации от 26 октября 2012 года № 1101 «О единой автоматизированной информационной системе «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети "Интернет" и сетевых адресов, позволяющих

идентифицировать сайты в информационно-телекоммуникационной сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено» // Российская газета. 29.10.2012.

10. Рекомендации парламентских слушаний «Актуальные вопросы обеспечения безопасности и развития детей в информационной безопасности», прошедшие в Совете Федерации 17.04.2017.

11. Письмо Минобрнауки России от 28.04.2014 № ДЛ-115/03 «О направлении методических материалов для обеспечения информационной безопасности детей при использовании ресурсов сети Интернет».

Учебная и научная литература

1. Авдулова Т.П. Подростки в информационном пространстве / Т.П. Авдулова // Психология обучения. 2010. № 4. С. 28—38.

2. Авдулова Т.П. Тенденции социализации подростков в контексте информационных предпочтений // Психологические исследования: электрон. науч. журн. 2011. № 6 (20). С. 8.

3. Бабаева Ю.Д. Интернет: воздействие на личность / Ю.Д. Бабаева, А.Е. Войскунский, О.В. Смылова // Гуманитарные исследования в Интернете / Ред. А.Е. Войскунский. М., 2000. С. 11—39.

4. Белинская Е.П. Взаимосвязь Интернет-зависимости и стратегий совладания с трудными жизненными ситуациями // Интернет-зависимость: психологическая природа и динамика развития / Сост. и ред. А. Е. Войскунский. М. : Акрополь, 2009.

5. Белинская Е.П. Информационная социализация подростков: опыт пользования социальными сетями и психологическое благополучие // Психологические исследования. 2013. Т. 6. № 30. С. 5.

6. Бородин К.В. Объекты и субъекты правового регулирования борьбы с распространением вредной информации в сети Интернет // Информационное право. 2016. № 2. С. 13—17.

7. Бочавер А.А. Кибербуллинг: травля в пространстве современных технологий // Журнал Высшей школы экономики. Т. 11. Психология. 2014. № 3. С. 177—191.

8. Войскунский А.Е. Психология и Интернет. М. : Акрополь, 2010.

9. Гавриченко О.В., Смолякова Т.В. Особенности саморепрезентации в Интернет-дневниках подростков и молодежи // Психологические исследования: электронный научный журнал. 2008. № 1 (1). URL: <http://psystudy.ru>

10. Голубева Н.А. Эндогенные факторы информационных предпочтений современных подростков // Психологические исследования. 2012. № 1 (21). С. 7. URL: <http://psystudy.ru>

11. Домбровский В., Ломтев И., Городбин А. Проект «Мы в интернет-безопасности» // Молодой ученый. 2016. № 8-1. С. 21—29.
12. Зиновьева Н.О. Психология и психотерапия насилия. Ребенок в кризисной ситуации : учеб. пособие / Н.О. Зиновьева, Н.Ф. Михайлова. СПб. : Речь, 2005. 248 с.
13. Зинцова А.С. Социальная профилактика кибербуллинга // Вестник Нижегородского университета им. Н.И. Лобачевского. Серия: Социальные науки. 2014. № 3 (35). С. 122—128.
14. Ивашура В. Интернет-троллинг и кибербуллинг. URL: <http://fb.ru/article/167695/что-такое-kiberbulling-internet-trolling-i-kiberbulling>
15. Игнатьева Э.А. Выявление уровня сформированности коммуникативных умений виртуального общения // Психологическая наука и образование. 2011. № 4.
16. Изотова Е.И. Инструменты эмоциональной насыщенности интернет-сообщения: эмоциональный интеллект и способы кодирования эмоций // Психологические исследования. 2014. Т. 7. № 37. С. 5.
17. Изотова Е.И. Особенности виртуального общения современного подростка // Мир психологии. 2010. № 3. С. 102—112.
18. Кобец П.Н. Противодействие угрозам киберсталкинга — важнейшей проблеме, исследуемой в рамках совершенствования аспектов информационной безопасности регионов в условиях глобализации информационного пространства // Вестник Прикамского социального института. 2017. № 1 (76). С. 29—32.
19. Ковалева С.Е. О некоторых актуальных социально-психологических проблемах виртуальной коммуникации в информационную эпоху // XXI век: итоги прошлого и проблемы настоящего плюс. 2017. № 5-6 (39-40). С. 122—127.
20. Колодей К. Моббинг. Психотеррор на рабочем месте и методы его преодоления. Пер. с нем. Харьков : Гуманитарный Центр, 2007. 324 с.
21. Мальцева В.А. Защита детей от кибербуллинга. Вопросы уголовно-правового регулирования // Закон и право. 2019. № 10. С. 95—99. DOI: 10.24411/2073-3313-2019-10463.
22. Марцинковская Т.Д. Информационная социализация в изменяющемся информационном пространстве // Психологические исследования. 2012. Т. 5. № 26. С. 7.
23. Меновщиков В.Ю. Психологическое консультирование: работа с кризисными и проблемными ситуациями. М. : Смысл, 2002. 182 с.
24. Моббинг, буллинг, хейзинг — чем они опасны для школьников. URL: <http://eduinspector.ru/2016/12/29/mobbing-bulling-hejzing-chem-oni-opasny-dlyashkolnikov>

25. Нечаева Е.А. Психологические особенности общения пользователей в сети INTERNET : курсовая работа. Ростов н/Д, 2015. URL: <http://www.studfiles.ru/preview/6022578>
26. Никольская И.М. Психологическая защита у детей / И.М. Никольская, Р.М. Грановская. СПб. : Речь, 2000. 507 с.
27. Прихожан А.М. Информационная безопасность и развитие информационной культуры личности // Мир психологии. 2010. № 3. С. 135—141.
28. Психология Интернет-коммуникации : учеб. пособие / М. : МПСУ : Воронеж : МОДЭК, 2013. 192 с.
29. Орлов Г.А. Интернет как средство формирования преступности среди несовершеннолетних // Международный студенческий научный вестник. 2018. № 4. С. 1007—1009.
30. Собкин В.С. Виртуальная атака. Компьютер в подростковой субкультуре / В.С. Собкин, Ю.М. Евстигнеева // Первое сентября. 2002. № 8. С. 2—7.
31. Склямина М.Ю. Обеспечение информационной безопасности учащихся в системе общего образования // Молодой ученый. 2018. С. 52—55.
32. Тимофеева Л.Л. Методические рекомендации по обеспечению информационной безопасности в образовательной организации. Орел : БУДПО «ИРД», 2020. 58 с.
33. Тхостов А.Ш. Влияние современных технологий на развитие личности и формирование патологических форм адаптации: обратная сторона социализации / Тхостов А.Ш., Сурнов К.Г. // Психологический журнал. 2005. № 26 (6). С. 16—24.
34. Ураева Г.Е. Опыт переживания онлайн-агрессии у молодых взрослых: современное состояние и перспективы исследования проблемы / Г.Е. Ураева, О.Н. Боголюбова // Психологические исследования. 2013. Т. 6. № 27. С. 12.
35. Федунина Н.Ю. Представления о триаде «преследователь — жертва — наблюдатель» в кибербуллинге в англоязычной литературе // Психологические исследования. 2015. Т. 8. № 41. С. 11.
36. Чудова Н.В. Особенности образа «Я» жителя Интернета // Психологический журнал. 2002.

9. Оценка качества освоения программы

Формой текущего контроля (промежуточной аттестации) является проведение дискуссии по результатам изучения каждого раздела.

Оценка качества освоения программы осуществляется в виде экзамена в форме тестирования. По итогам экзамена принимается решение о сдаче итоговой аттестации.

Примерный перечень вопросов для подготовки к экзамену в форме тестирования

1. Необходимость обеспечения безопасности в информационных системах.
2. Нормативно-правовые аспекты информационной безопасности.
3. Классификация угроз безопасности информационных объектов.
4. Умышленные и неумышленные угрозы информационной безопасности.
5. Государственное регулирование информационной безопасности в России.
6. Теоретические аспекты информационной безопасности несовершеннолетних: проблемы правового регулирования.
7. Государственная политика в сфере общего образования Российской Федерации.
8. Проблемы нормативно-правового регулирования информационной безопасности несовершеннолетних.
9. Информационная защита несовершеннолетних в образовательном процессе.
10. Основы противодействия угрозам здоровью и жизни, исходящих из электронных или информационно-телекоммуникационных сетей, в том числе сети Интернет.
11. Организация работы по профилактике кибербуллинга, суицидологии («колумбайн»), суицидального поведения несовершеннолетних.
12. Уголовно-правовые и криминологические аспекты обеспечения информационной безопасности несовершеннолетних: современное состояние и меры по дальнейшему совершенствованию.
13. Информационная безопасность несовершеннолетних с позиций психолого-педагогического подхода.
14. Критерии оценки состояния информационной безопасности подростков.
15. Основы противодействия вовлечению подростков в экстремистскую и террористическую деятельность с использованием электронных или информационно-телекоммуникационных сетей, в том числе сети Интернет.
16. Интернет-технологии как способ вовлечения несовершеннолетних в преступную деятельность: проблемы профилактики.