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

«Утверждаю»
Первый заместитель директора
ФБУ НЦПИ
при Минюсте России

_____ В.В. Прытков
«27» февраля 2025 г.

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ НЕСОВЕРШЕННОЛЕТНИХ: ЗАЩИТА ОТ КИБЕРБУЛЛИНГА»

Программа курса
дополнительного профессионального образования
повышения квалификации

МОСКВА
2025

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, действительный член РАЕН по секции геополитики и безопасности (по согласованию);

Сергин М.Ю., начальник отделения повышения квалификации ФБУ НЦПИ при Минюсте России, доктор технических наук, профессор.

Содержание

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 акты[2], 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 Интернет[4] посредством блокировки сайтов, пропагандирующих суициды, введения уголовной ответственности за травлю в интернет-сети (преследование, сталкинг, 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-vovlecheniya-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 «кибербезопасность», «киберпространство», «киберкультура», «киберугрозы»;

– о различных формах ответственности за правонарушения 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 кибербулингу;

– 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		
Тема 2.1 Информационная безопасность несовершеннолетних: психолого-педагогические критерии	2	Лекция 2.1 Информационная безопасность несовершеннолетних с позиций психолого-педагогического подхода. Критерии оценки состояния информационной безопасности подростков (рекомендации для родителей, педагогов)
Тема 2.2 Экстремистская и террористическая деятельность с использованием электронных или информационно-телекоммуникационных сетей: алгоритм вовлечения несовершеннолетних	1	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
Тема 2.3 Профилактика вовлечения несовершеннолетних в преступную деятельность посредством информационных технологий	1	Лекция 2.3 Основы профилактики вовлечения несовершеннолетних в преступную деятельность посредством информационных технологий. Интернет-технологии как способ вовлечения несовершеннолетних в преступную деятельность: проблемы профилактики

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		
Тема 2.1 Информационная безопасность несовершеннолетних: психолого-педагогические критерии	2	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)
Тема 2.2 Экстремистская и террористическая деятельность с использованием электронных или информационно-телекоммуникационных сетей: алгоритм вовлечения несовершеннолетних	2	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

1	2	3
Тема 2.3 Профилактика вовлечения несовершеннолетних в преступную деятельность посредством информационных технологий	2	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
Промежуточный контроль		Проведение дискуссии по итогам обучения по Разделу 2.

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.inioni.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 Российской Федерации «Об образовании в Российской Федерации» № 273 от 29.12.2012.

3. Федеральный закон Российской Федерации от 27.07.2006 № 149-ФЗ (ред. от 12.12.2023) «Об информации, информационных технологиях и о защите информации» // «Собрание законодательства РФ», 31.07.2006, № 31 (1 ч.), ст. 3448.

4. 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: 25.11.2024).

5. Приказ Роскомнадзора № 84, МВД РФ № 292, Роспотребнадзора № 351, ФНС РФ № ММВ-7-2/461@ от 18.05.2017 «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», а также сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие запрещенную информацию, в единую автоматизированную информационную систему «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» (Зарегистрировано в Минюсте России 27.06.2017 № 47207) https://mvd.consultant.ru/documents/1056300 (дата обращения: 10.12.2024).

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: 25.01.2025).

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 26.10.2012 № 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. Письмо Минобрнауки России от 28.04.2014 № ДЛ-115/03 «О направлении методических материалов для обеспечения информационной безопасности детей при использовании ресурсов сети Интернет».

11. Распоряжение Правительства Российской Федерации от 28.04.2023 № 1105-р «Об утверждении Концепции информационной безопасности детей в РФ и признании утратившим силу распоряжения Правительства Российской Федерации от 02.12.2015 № 2471-р» https://www.garant.ru/products/ipo/prime/doc/406740607/?ysclid=m4hc8yjftb574221910.

Учебная и научная литература
Основная:

1. Васильева Т. Ю., Куприянов А. И., Мельников В. П. Информационная безопасность. Учебник. М.: КноРус. 2023. 372 с.

2. Гродзенский Я. С. Информационная безопасность. Учебное пособие. М.: РГ-Пресс. 2024. 144 с.

3. Дугенец А.С., Павлова Л.В. Государственное регулирование обеспечения информационной безопасности несовершеннолетних как составляющая национальной безопасности России // Административное право и процесс. 2023. № 5. С. 22 — 25.

4. Зенков А. В. Информационная безопасность и защита информации. М.: Юрайт. 2023. 108 с.

5. Корабельников С. М. Преступления в сфере информационной безопасности. М.: Юрайт. 2024. 112 с.

6. Куприянов А. И., Мельников В. П. Информационная безопасность. Учебник. М.: КноРус. 2022. 268 с.

7. Максуров А. А. Обеспечение информационной безопасности в сети Интернет. Монография. М.: Инфра-М. 2023. 226 с.

8. Нестеров С. А. Основы информационной безопасности. М.: Лань. 2023. 324 с.

9. Никитина Е.Е. Информационная безопасность как элемент конституционного статуса личности // Журнал российского права. 2024. № 1. С. 81 — 94.

Дополнительная:

1. Андреенкова В.Л., Мельничук В.А., Калашник О.А. Противодействие буллингу в учебном заведении: системный подход: методическое пособие. – Киев: ООО «Агентство Украина», 2019 – 132 с.

2. Ануфриева Е.В., Набойченко Е.С., Ковтун О.П. Буллинг и кибербуллинг: проблема современного подростка // Педиатрическая фармакология. – 2021 – Т. 18 – № 5 – С. 423-429.

3. Бородина В.Н., Петимко А.И. Кибербуллинг среди подростков в образовательной среде как предмет исследования // Мир науки, культуры, образования. – 2021 – № 6 (91). – С. 154-1

4. Бочкарева Е.В., Стренин Д.А. Теоретико-правовые аспекты кибербуллинга // Всероссийский криминологический журнал. 2021 Т. 15, № 1 С. 91–97

5. Ефремова Г.Инновационные технологии в современном образовательном пространстве: коллективная монография / Под общ.редакцией Г.Л. Ефремовой. – Сумы: Изд-во СумГПУ имени А. С.Макаренко, 2020 – 444 с.

6. Назаров В.Л., Авербух Н.В. Проблемы кибербуллинга в российской школе // Образование и наука 2022 – Том 24, № 2 – С.169-205

Интернет-ресурсы:

1. Официальный интернет-портал правовой информации – [Электронный ресурс]. Режим доступа: http://pravo.gov.ru/ (дата обращения: 25.01.2025)

2. СПС Консультант Плюс [Электронный ресурс]. Режим доступа: Поиск по сайту \ Консультант Плюс (consultant.ru) (дата обращения: 25.01.2025)

3. СПС Гарант – [Электронный ресурс]. Режим доступа: http://www.garant.ru/ (дата обращения: 25.01.2025)

4. Федеральный портал [Электронный ресурс]: Российское образование – Режим доступа: https://www.edu.ru/ . (дата обращения: 25.01.2025)

5. Федеральный портал [Электронный ресурс]: Российская электронная школа – Режим доступа: https://www.resh.edu.ru/. (дата обращения: 25.01.2025) Федеральный портал [Электронный ресурс]: Федеральные государственные образовательные стандарты и примерные основные общеобразовательные программы – Режим доступа: https://fgosreestr.ru/. (дата обращения: 25.01.2025)

6. Жертвы кибербуллинга: как защитить детей от травли в интернете. URL: https://www.m24.ru/articles/deti/27062019/155723. Текст: электронный (дата обращения: 25.01.2025)

7. Федеральные государственные образовательные стандарты и примерные основные общеобразовательные программы: сайт [Электронный ресурс]. URL: https://fgosreestr.ru/ (дата обращения: 25.01.2025).

8. По дороге домой тебе не поздоровится: что такое кибербуллинг? URL: https://ria.ru/20180804/1525897862.html . Текст: электронный (дата обращения: 25.01.2025)

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, скулшутинга («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.