ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ УЧРЕЖДЕНИЕ
ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
ИНСТИТУТ РАЗВИТИЯ ОБРАЗОВАНИЯ РЕСПУБЛИКИ БАШКОРТОСТАН

КАФЕДРА ФИЗИКИ, МАТЕМАТИКИ И ИНФОРМАТИКИ

Программно-экспертный совет
ГАУ ДПО ИРО РБ
_____ Л.Ф.Шакурова

Протокол заседания
№ 11 от 10 марта 2017 г.

«УТВЕРЖДАЮ»
Ректор ГАУ ДПО ИРО РБ
_____ Р.Г.Мазитов
10 марта 2017 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

БЕЗОПАСНОСТЬ ДЕТЕЙ В СЕТИ ИНТЕРНЕТ

Авторы-составители программы:
Ткачев В.И., к.ф.-м.н., и.о.зав. кафедрой физики, математики и информатики
Тагиров И.Х., ст. преподаватель
Ишемгулова И.Г., ст. методист
Тимерьянова Л.Н., к.п.н. доцент каф. психологии

Принята на заседании кафедры ФМИ

Протокол № 6 от 3 марта 2017 г.

Уфа – 2017

Общая характеристика программы
Нормативно-методические основы разработки программы:

Федеральный закон от 29.12.2012 г. №273-ФЗ «Об образовании в Российской Федерации»; закон Республики Башкортостан «Об образовании в Республике Башкортостан»; Приказ Министерства образования и науки Российской Федерации от 1 июля 2013 г. №499 «Об утверждении порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам»; Трудовой кодекс Российской Федерации от 30 декабря 2001 г. №197-ФЗ; Приказ Минсоцразвития РФ от 11 января 2011 г. №1н «Об утверждении единого квалификационного справочника должностей руководителей, специалистов и служащих, раздел «Квалификационная характеристика должностей руководителей и специалистов высшего профессионального и дополнительного профессионального образования»; Методические рекомендации-разъяснения по разработке дополнительных профессиональных программ на основе профессиональных стандартов Министерства образования и науки РФ от 22 апреля 2015 г.; Распоряжение Правительства РФ от 02.12.2015 N 2471-р "Об утверждении Концепции информационной безопасности детей"; Государственная программа Российской Федерации «Развитие образования на 2013-2020 годы»; Стратегия развития отрасли ИТ в РФ и на 2014 - 2020 годы и на перспективу до 2025 года; Концепция развития электронного образования в Республике Башкортостан на период 2015-2020 годов; Постановление Главного государственного санитарного врача РФ от 29.12.2010 г. N 189 «Об утверждении СанПиН 2.4.2.2821-10 «Санитарно - эпидемиологические требования» (зарегистрировано в Минюсте РФ 3.03. 2011 г. Регистрационный N 19993), Устав ГАУ ДПО ИРО РБ.

Реализация программы по совершенствованию деятельности в сфере профилактики негативного влияния современных информационных технологий на психику детей и подростков предусматривает обязательное обучение педагогов по данной проблеме через систему повышения квалификации.

Интернет — всемирная система объединённых компьютерных сетей для хранения и передачи информации. Интернет стал достоянием всего человечества. Его услугами регулярно пользуется более трети населения земного шара. Практически неограниченное и труднорегулируемое распространение сети постоянно рождает новые проблемы. Одной из главных является безопасность.

Стремительное развитие информационных и коммуникационных ресурсов, возрастающая доступность медиасредств (в первую очередь, смартфонов и планшетных компьютеров) открывают практически безграничные возможности для доступа к информации самого разного уровня, в том числе и к запрещенному контенту порнографического, экстремистского, дезинформирующего характера. Контролировать этот процесс крайне трудно. Кропотливая работа по запрету доступа к ресурсам сети Интернет, содержащим вредоносный контент, не может полностью обеспечить информационную безопасность нам и нашим детям, поскольку, когда блокируешь одни каналы, открываются другие. В условиях демократического общества невозможно полностью ограничить доступ к нелицензируемым и нелегитимным веб-ресурсам, сохранив право посещения только проверенных источников.

Поэтому данная программа нацелена на:

- продуктивную организация в образовательной организации работы по профилактике медиааддикций среди детей и подростков;
- просвещение педагогических работников по вопросам безопасного поведения в современном информационно-коммуникативном пространстве;
- формирование у обучающихся навыков безопасного пользования информационно-коммуникативными сетями и интернетом, а также профилактика

негативного влияния современных информационных технологий на психику современных школьников.

Комплексная дидактическая цель и планируемые результаты обучения: совершенствование профессиональной компетентности педагогических работников в области информационной безопасности в образовательных организациях			
Профессиональные компетенции	**Практический опыт**	**Умения**	**Знания**
Проектировать психологически безопасную и комфортную образовательную среду, проводить профилактику различных форм насилия в школе	Содействие обеспечению информационной безопасности детей	- реализовать комплекс мер по обеспечению безопасности детей использующих Интернет; -применять методы диагностики и профилактики Интернет-зависимости обучающихся; - применять программные и технические средства обеспечения информационной безопасности	-основное содержание нормативно-правового обеспечения информационной безопасности детей; - основные принципы обеспечения информационной безопасности детей; -форм и методов педагогического сопровождения информационной безопасности школьников

Учебные материалы размещены в системе дистанционного обучения (далее СДО). Предусмотрено взаимодействие обучающихся с ППС и административно-управленческим персоналом в форме электронной переписки, видеоконференцсвязи с плановой периодичностью согласно расписанию занятий КПК.

Итоговый контроль знаний обучающихся проводится преподавателем в форме электронного тестирования в СДО. Также промежуточный контроль знаний проводится по модульно, так как каждый модуль разработан по деятельностной методике, то есть предусматривает получение от обучающегося готового продукта – выполненного практического задания.

С помощью СДО, осуществляется полноценный процесс дистанционного обучения и независимой проверки знаний. Данная система рассчитана на большие потоки слушателей. Она состоит из компонентов организации и управления учебным процессом.

Система позволяет проводить обучение и проверку знаний в сети Интернет.

В системе реализованы следующие автоматизированные функции:

управление учебным процессом;

распределение прав доступа к образовательным ресурсам и средствам управления системой;

разграничение взаимодействия участников образовательного процесса;

ведение журналов активности пользователей учебного комплекса;

обучение и оценка знаний в среде Интернет, в корпоративных и локальных сетях.

Системные требования.

К серверу СДО и клиентским компьютерам предъявляются системные требования.

Сервер СДО работает на независимой компьютерной системе, подключенной к Интернету, корпоративной или локальной сети.

Клиентским называется компьютер, с которого участники учебного процесса (администраторы, организаторы, тьюторы и слушатели) получают доступ к функциям системы, то есть взаимодействуют с учебным комплексом СДО.

Сервер СДО

Ресурс	*Минимальные*	*Рекомендуется*
Процессор	Pentium 1500 МГц	Pentium IV 2,8 МГц и выше
ОЗУ	1000 Мб	4000 Мб и выше
Диск	200 Гб	500 Гб, SCSI
CD-ROM	4x	40x и выше
Операционная система	MS Windows 2000/2003 Server	
СУБД	Microsoft SQL Server 2000	
Интернет	от 512 кбит/с	от 1Мбит/с

Клиентский компьютер

Ресурс	*Минимальные*	*Рекомендуется*
Процессор	Pentium 500 МГц	Pentium IV 2,8 МГц и выше
ОЗУ	512 МБ	2024 Мб и выше
Видео	SVGA, 1МБ	36 Гб, SCSI
CD-ROM	4x	40x и выше
Веб-браузер	MS Internet Explorer 5.0	MS Internet Explorer 6.0 и выше
Канал Интернета, корпоративной или локальной сети	от 512 кбит/с	1Мбит/с и выше

Категория обучающихся: руководители и педагогические работники образовательных организаций, учителя, воспитатели, социальные педагоги, методисты, психологи.
Форма обучения: заочная
Срок освоения программы: 72 часа
Режим занятий: 8 учебных часов в день
Виды учебных занятий: лекции, практические занятия
Формы итоговой аттестации обучающихся: проектная работа
Документ, выдаваемый после завершения обучения: удостоверение о повышении квалификации установленного образца

Учебный план

дополнительной профессиональной программы повышения квалификации

БЕЗОПАСНОСТЬ ДЕТЕЙ В СЕТИ ИНТЕРНЕТ

№	Наименование модулей и учебных элементов	Всего часов	В том числе		Форма контроля
			Лекции	Практические занятия	
Базовая часть					
Раздел 1. Основы законодательства Российской Федерации в области образования					
Инвариантные модули					
	Входной контроль	**1**		**1**	**Тест**
1.	**Модуль 1. Нормативно правовые аспекты безопасности информационного пространства в образовательной среде**	**16**	**6**	**9**	
1.1	Правовое обеспечение информационной безопасности в образовательной организации	2	2		
1.2	Правовое регулирование открытых информационных ресурсов образовательной организации	4	2	2	
1.3	Правовая защита информационных ресурсов ограниченного доступа	2	1	1	
1.4	Правовая защита детей от влияния негативной информации	7	2	5	
1.5	Промежуточный контроль	1		1	Тест
Профильная часть					
Раздел 2. Предметно-методическая деятельность					
Инвариантные модули					
2.	**Модуль 2. Безопасность образовательной среды: психолого-педагогическое сопровождение**	**16**	**5**	**11**	
2.1	Влияние интернет - пространства на психологическое состояние и поведение современного школьника	5	2	3	
2.2	Интернет-зависимость, ее диагностика и профилактика	5	2	3	
2.3	Психологическая компетентность педагога, как фактор безопасности образовательной среды	5	1	4	

2.4	Промежуточный контроль	1		1	Реферат
Вариативные модули					
3.	**Модуль 3. Информационная безопасность образовательной организации**	**16**	**3**	**8**	
3.1	Основы информационной безопасности образовательной организации	4	2	2	
3.2	Программное обеспечение информационной безопасности	11	3	8	
3.3	Промежуточный контроль	1		1	Контрольная работа
4.	**Модуль 4. Методические основы организации мероприятий Безопасности детей в сети Интернет**	**20**	**3**	**17**	
4.1	Методика организации мероприятий по безопасности школьников в сети Интернет	6	2	4	
4.2	Организация мероприятий для родительской аудитории	6	1	5	
4.3	Методические материалы для организации и проведения мероприятий с учащимися по безопасности в сети Интернет	6		6	Контрольная работа
4.4	Промежуточный контроль	2		2	Контрольная работа
5.	**Выходной контроль**	**1**		**1**	**Тест**
6.	**Итоговая аттестация**	**2**		**2**	**зачет**
	Итого	**72**	**17**	**48**	

2.2. Календарный учебный план

модульной программы курсов повышения квалификации
БЕЗОПАСНОСТЬ ДЕТЕЙ В СЕТИ ИНТЕРНЕТ
(наименование программы)

Категория обучаемых: руководители и педагогические работники образовательных организаций, учителя, воспитатели, социальные педагоги, методисты, психологи.

График обучения Форма обучения	Аудиторных часов в день	Дней, недель	Общая продолжительность программы, месяцев (дней, недель)
заочная	8 часов	9 дней	1,5 недели

УЧЕБНАЯ ПРОГРАММА

«БЕЗОПАСНОСТЬ ДЕТЕЙ В СЕТИ ИНТЕРНЕТ»

Входной контроль. Тест (1 ч. ПЗ)

Модуль 1. Нормативно правовые аспекты безопасности информационного пространства в образовательной среде (16 ч.: 6 ч. ЛЗ, 9 ч. ПЗ)

Интегрированные дидактические цели: Знакомство с федеральными документами, регламентирующими нормативно-правовые аспекты безопасности информационного пространства в образовательной среде, в том числе в сети Интернет

Учебный элемент 1.1. Правовое обеспечение информационной безопасности в образовательной организации (2 ч.: 2 ч. ЛЗ).

Лекционное занятие. Правовое обеспечение информационной безопасности в образовательной организации. Понятие информационной безопасности. Доктрина безопасности Российской Федерации. Концепция информационной безопасности России. Информационные права граждан. Законодательство в области интеллектуальной собственности, информационных ресурсов, информационных продуктов и информационных услуг в образовательной организации. Законодательство о защите персональных данных. Безопасность функционирования образовательной организации. Правовые механизмы защиты в нормах законов, регулирующих отношения по поводу создания и распространения информации. Правовые механизмы защиты в нормах законов, регулирующих отношения в области создания и применения информационных систем, информационных технологий и средств их обеспечения в образовательной организации.

Практическое занятие. Изучение нормативно-правовых документов правового обеспечения информационной безопасности в образовательной организации.

Учебный элемент 1.2. Правовое регулирование открытых информационных ресурсов образовательной организации. (4 ч.: 2 ч. ЛЗ, 2 ч. ПЗ).

Лекционное занятие. Правовое регулирование открытых информационных ресурсов образовательной организации. Информационный характер интеллектуальной и материальной собственности. Охрана результатов творческой деятельности. Реализация интеллектуальной собственности на документированную информацию. Характеристика норм патентного права. Характеристика норм авторского права и смежных прав.

Практическое занятие. Изучение законодательных актов, охраняющие вещную собственность на документированную информацию в образовательной организации

Учебный элемент 1.3. Правовая защита информационных ресурсов ограниченного доступа. (2 ч.: 1 ч. ЛЗ, 1 ч ПЗ).

Лекционное занятие. Правовая защита информационных ресурсов ограниченного доступа. Понятие тайны, секрета, конфиденциальности. Правовая форма защиты ценной деловой и производственной информации в образовательной организации. Конфиденциальная информация и ее виды. Персональные данные. Ограничения на отнесение информации к категории конфиденциальной. Понятие конфиденциального документа, его особенности.

Практическое занятие. Составление глоссария по правовой защите информационных ресурсов ограниченного доступа.

Учебный элемент 1.4 Правовая защита детей от влияния негативной информации. (7ч.: 2 ч. ЛЗ, 5 ч. ПЗ).

Лекционное занятие. Правовая защита детей от влияния негативной информации. Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию». Цели правовой защиты детей. Правовые аспекты проблемы защиты несовершеннолетних от негативного воздействия средств массовой информации и информации, распространяемой в сети Интернет. Возможности ограничений детей от негативной и вредной для них информации в образовательной организации. Правовая защита детей от разрушительного, травмирующего их психику информационного воздействия, а также от информации, способной развить в ребенке порочные наклонности, в том числе и через сеть Интернет. Законодательный запрет на информацию, вызывающую у детей страх, ужас и панику, а также оправдывающую насилие и противоправное поведение. Законодательный запрет на бесконтрольное распространение информации, способной вызвать у детей желание употреблять наркотики, алкоголь или побуждающую к причинению вреда своей жизни и здоровью. Меры по повышению эффективности защиты в образовательной организации.

Практическое занятие. Изучение нормативно-правовой базы защиты детей от влияния негативной информации.

Учебный элемент 1.5. Промежуточный контроль. (1 ч. ПЗ). Тест.

Учебно-методическое обеспечение программы

Рекомендуемая литература.

Основная:

1) Гендина Н.И., Косолапова Е.В. Основы информационной культуры школьника – М.: РШБА, 2012 – 200с.
2) Справочно-поисковые системы информационно-правового обеспечения ГАРАНТ-Максимум и КОНСУЛЬТАНТ +

Дополнительная:

1) Новое образовательное пространство: выигрывают учащиеся: Д. Лоэртшер и др. [ред. В.В.Зверевич].- М.: РШБА, 2015. – 304 с.
2) Цифровая компетентность подростков и родителей. Результаты всероссийского исследования /Г.У. Солдатова и др. – М.: Фонд развития Интернет, 2013
3) Центр проблем информационного права - http://www.medialaw.ru/
4) Институт развития информационного общества в России http://www.iis.ru/index.html

Электронные издания, ЦОРы:

1) Фонд развития Интернет: сделаем интернет безопаснее вместеhttp://detionline.com
2) Методические рекомендации по информированию родителей об услуге «Родительский контроль», позволяющий устанавливать ограничения к информационно-коммуникационной сети «Интернет» http://www.kriroipk.com/index/bezopasnaja_rabota_v_seti_internet/0-341 -
3) Национальная стратегия действий в интересах детей на 2012 - 2017 годы [Электронный ресурс]http://www.soprotivlenie.org.
4) Центр безопасного Интернета в России www.saferunet.ru
5) Детский правовой сайт www.mir.pravo.by/library/edu

Нормативно-правовые акты:

1) Конституция Российской Федерации (с учётом поправок, внесенных законами РФ от 30.12.2008 №6-ФКЗ; от 30.12.2008 №7-ФКЗ; от 5.02.2014 №2-ФКЗ; от 21.07.2014 №11-ФКЗ)

2) Федеральный закон № 273-ФЗ от 29.12.2012 «Об образовании в Российской Федерации»
3) Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 09.09.2000 N Пр-1895) // http://base.garant.ru/182535/
4) Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» http://www.consultant.ru/document/cons_doc_LAW_108808/
5) Концепция информационной безопасности детейhttp://government.ru/media/files/mPbAMyJ29uSPhL3p20168GA6hv3CtBxD.pdf
6) Республиканский закон «Об образовании» от 01.07.2013 г. №696-з
7) Стратегия развития отрасли ИТ в РФ и на 2014 - 2020 годы и на перспективу до 2025 года
8) Государственная программа «Информационное общество (2011 - 2020 годы)»http://www.consultant.ru/document/cons_doc_LAW_162184/4b6b1ec3d9a61a8204d8fdc520469db8e0daa367/
9) Постановление Главного государственного санитарного врача РФ от 29.12.2010 г. N 189 «Об утверждении СанПиН 2.4.2.2821-10 «Санитарно - эпидемиологические требования»

Материально-техническое обеспечение:

Компьютерный кабинет с локальной сетью и выходом в Интернет, интерактивная доска, документ-камера.

Организационные условия.

Модуль выступает как инвариантная часть модульной программы. Каждый обучающийся в течение всего периода обучения должен быть обеспечен неограниченным доступом к электронно-библиотечным системам, содержащим издания основной и дополнительной литературы.

Электронно-библиотечная система должна обеспечивать возможность индивидуального доступа к сети Интернет.

Описание системы оценки качества освоения модуля.

Вид контроля: промежуточный.

Форма контроля: тест.

Вопросы для промежуточного контроля:

1. Стратегической целью государственной политики в области информационной безопасности детей является
   1) повышение интерактивности и индивидуализации обучения;
   2) обеспечение гармоничного развития молодого поколения при условии минимизации всех негативных факторов, связанных с формированием гиперинформационного общества в России;
   3) обеспечения сферы образования методологией и практикой разработки и оптимального использования современных информационных технологий;
   4) предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию;

2. Обеспечение информационной безопасности детей возможно исключительно при условии
   1) эффективного сочетания государственных и общественных усилий при определяющей роли семьи;
   2) эффективного сочетания государственных и экономических усилий;

3) организации образовательной деятельности, с применением содержащейся в базах данных и используемой при реализации образовательных программ информации и обеспечивающих ее обработку информационных технологий;
4) применения информационно-телекоммуникационных сетей при опосредованном (на расстоянии) взаимодействии обучающихся и педагогических работников;

3. Федеральный закон от 29.12.2010 N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию" распространяется на
   1) отношения в сфере оборота информационной продукции, содержащей научную, научно-техническую, статистическую информацию;
   2) отношения в сфере оборота информационной продукции, имеющей значительную историческую, художественную или иную культурную ценность для общества;
   3) отношения в сфере рекламы;
   4) регулирование отношений связанной с защитой детей от информации, причиняющей вред их здоровью и (или) развитию, в том числе от такой информации, содержащейся в информационной продукции;

4. Информационная безопасность детей – это…
   1) возможность получения и использования детьми свободно распространяемой информации;
   2) состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию;
   3) состояние сохранности информационных ресурсов государства и защищённости законных прав личности и общества в информационной сфере;
   4) процесс обеспечения сферы образования методологией и практикой разработки и оптимального использования современных информационных технологий, ориентированных на реализацию целей обучения, воспитания и развития;

5. Информационная продукция для детей – это …
   1) информационная продукция, соответствующая по тематике, содержанию и художественному оформлению физическому, психическому, духовному и нравственному развитию детей;
   2) информация (в том числе содержащаяся в информационной продукции для детей), распространение которой среди детей запрещено или ограничено в соответствии с настоящим Федеральным законом;
   3) информации об окружающем мире в виде наскальных рисунков, а позднее в виде картин, фотографий, схем, чертежей на бумаге, холсте, мраморе и др. материалах, изображающих картины реального мира;
   4) информация имеющая следующие общие качественные свойства: объективность, достоверность, полнота, точность, актуальность, полезность.

Вопросы входного контроля:

1. Когда можно полностью доверять новым онлайн-друзьям?

   a) Ничто не может дать 100%-ную гарантию того, что онлайн-другу можно доверять
   b) Поговорив по телефону
   c) После обмена фотографиями
   d) Когда есть общие друзья
   e) После длительного онлайн-знакомства (переписки)

2. Что делать, если ты столкнулся с троллем в Сети?

a) Сообщить модераторам сайта
b) Рассказать взрослым
c) Игнорировать выпады тролля
d) Заблокировать тролля
e) Проучить или доказать свою правоту

3. Что является признаком фишинг-сообщения?

a) В сообщении много ошибок, неточностей и противоречий
b) Сообщение содержит обещание большой выгоды с минимальными усилиями
c) В сообщении требуется срочно сменить пароль от электронной почты по причине вероятной попытки взлома электронного ящика, при этом сообщение не отправлено с официального адреса почтовой службы
d) В сообщении запрашиваются твои личные данные, финансовая информация, пароли
e) Сообщение содержит угрозу для жизни и здоровья близких людей

4. Как обезопасить себя при первой встрече с онлайн-другом?

a) Заранее пообщаться с "незнакомцем" по телефону, попросить прислать фотографии, таким образом убедиться, что он тот, за кого себя выдает
b) Встречаться с интернет-незнакомцами очень опасно, лучше не назначать встречу, если не знакомы с человеком лично
c) Попросить присутствовать взрослых
d) Сообщить о встрече родителям/взрослым, спросить их совета
e) Взять на встречу друзей и выбрать людное место в светлое время суток

5. Какую информацию о себе опасно выкладывать в Интернете в открытом доступе?

a) Дату рождения
b) О своих интересах
c) Информацию о доходах родителей
d) Домашний адрес и телефон
e) Место работы родителей

6. Как нужно себя вести, если вы стали жертвой кибербуллинга?

a) Обратиться за поддержкой к модераторам сайта
b) Пытаться бороться с обидчиками в одиночку
c) Заблокировать обидчиков
d) Сообщить родителям/взрослым
e) Обратиться на Линию помощи «Дети онлайн»

7. Как защититься от негативного контента?

a) Установить программы родительского контроля
b) Сообщить модераторам сайта, пожаловаться на неприемлемый контент с помощью специальных инструментов, доступных на сайте
c) Обратиться к автору негативного контента
d) Не обращать на него внимания
e) Использовать безопасный поиск Google и безопасный режим на YouTube

8. Как защитить компьютер от атак вредоносных программ?

a) Никогда не переходить по ссылкам из всплывающих окон

b) Перед запуском проверять все файлы, скачанные из Интернета, с помощью антивируса
c) Регулярно обновлять браузер, операционную систему, антивирусную программу и прикладное программное обеспечение
d) Установить антивирусную программу с официального сайта
e) Не открывать вложения в письмах, присланных с неизвестных электронных адресов, а также с осторожностью относиться к письмам, которые пришли с известного вам адреса, но чье содержание кажется подозрительным: аккаунт ваших знакомых может быть взломан и содержать вирусы

9. Как защитить свою электронную почту от взлома и махинаций?

a) Регулярно менять пароли
b) Активировать систему двухэтапной верификации на сервисах, которые позволяют это сделать
c) Никому не сообщать свой пароль
d) Периодически менять адрес электронной почты, менять провайдеров
e) Не открывать сообщения с незнакомых и подозрительных адресов
f) Создавать разные пароли от разных аккаунтов, включая электронную почту, систему электронного банкинга и пр.

10. Что делать, если ты столкнулся с троллем в Сети?

a) Игнорировать выпады тролля
b) Проучить или доказать свою правоту
c) Заблокировать тролля
d) Рассказать взрослым
e) Сообщить модераторам сайта

11. При каких условиях можно доверять письму от неизвестного отправителя?

a) Никогда нельзя доверять письму от неизвестного отправителя
b) К вам обращаются по имени
c) Отправитель использует логотип авторитетной компании
d) Письмо содержит важную информацию о ваших близких
e) Отправитель ссылается на ваших друзей

12. Что делать, если вам пришло письмо о том, что вы выиграли в лотерее?

a) Отметить сообщение как спам
b) Перейти по ссылке в письме, ведь в редких случаях информация может оказаться правдой
c) Удалить его
d) Заблокировать отправителя
e) Написать в ответ разоблачающее письмо мошенникам

Модуль 2. Безопасность образовательной среды: психолого-педагогическое сопровождение (16 ч.: 5 ч. ЛЗ, 11 ч. ПЗ)

Интегрированные дидактические цели: знать направления и методы обеспечения безопасности информационных ресурсов, ведения аналитической работы по выявлению угроз несанкционированного доступа к информации и уметь организовать направления своей педагогической работы по реализации информационной безопасности.

Учебный элемент 2.1. Влияние интернет - пространства на психологическое состояние и поведение современного школьника (5ч.: 2 ч. ЛЗ, 3 ч. ПЗ).

Лекционное занятие. Организация педагогической работы по реализации информационной безопасности. Информационное представление образовательной среды, ее преобразование в систематизированное информационное пространство, организованное, многомерное, упорядоченное. Особенности внедрения компьютерной техники и использовании сети Интернет в образовательных учреждениях. Модель информационно-образовательной среды. Угрозы информационной безопасности обучающихся, средства их предотвращения. Методы и способы повышения эффективности обеспечения безопасности информационной среды образовательного учреждения и личной информационной среды каждого обучающегося.

Практическое занятие. Организация педагогической работы по реализации информационной безопасности.

Учебный элемент 2.2. Интернет-зависимость, ее диагностика и профилактика (5 ч.: 2 ч. ЛЗ, 3 ч. ПЗ).

Лекционное занятие. Влияние интернет - пространства на психологическое состояние и поведение современного школьника. Понятие интернет – пространства. Информационно-психологическая безопасность личности ребенка. Позитивные информационные возможности Интернета для интеллектуального и личностного развития детей. Основные угрозы для личностной безопасности школьника, деструктивные информационные влияния интернет - пространства. Информационно-психологическое воздействие интернет – пространства, его негативные последствия. Факторы негативного влияния на личность интернет - пространства, развитие интернет-зависимости. Характеристики личности, провоцирующие повышенную склонность к виртуальной активности и использованию интернет-технологий (мотивационные, коммуникативные, эмоционально-ценностные, нравственно-духовные), выступающие внутриличностными причинами психологической зависимости и интернет-технологий. Формы и методы педагогического сопровождения информационной безопасности школьников.
Практическое занятие. Интернет-зависимость, ее диагностика и профилактика. Парольная защита с помощью стандартных системных средств

Учебный элемент 2.3. Психологическая компетентность педагога, как фактор безопасности образовательной среды (5ч.: 1 ч. ЛЗ, 4 ч. ПЗ).
Лекционное занятие. Интернет-зависимость, ее диагностика и профилактика. Основные критерии Интернет-зависимости. Классификация типов интернет-зависимости, её причин и симптомов. Навязчивый веб-серфинг (информационная перегрузка) — бесконечные путешествия по Всемирной паутине, поиск информации. Пристрастие к виртуальному общению и виртуальным знакомствам — большие объёмы переписки, постоянное участие в чатах, веб-форумах, избыточность знакомых и друзей в Сети. Игровая зависимость — навязчивое увлечение компьютерными играми по сети. Навязчивая финансовая потребность — игра по сети в азартные игры, ненужные покупки в интернет-магазинах. Государственный, общественный, педагогический и родительский контроль доступности для школьников интернет-ресурсов.
Практическое занятие. Компьютерная практика: изучение сайтов и их анализ

Учебный элемент 2.4. Промежуточный контроль. (1 ч. ПЗ). Реферат

Учебно-методическое обеспечение программы

Рекомендуемая литература.

Основная:

1) Цифровая компетентность подростков и родителей. Результаты всероссийского исследования /Г.У. Солдатова и др. – М.: Фонд развития Интернет, 2013
2) Полезный и безопасный Интернет. Правила безопасного использования интернета для детей младшего школьного возраста: методическое руководство /под ред. Г.У. Солдатовой. – М.: ФИРО, 2012

Электронные издания, ЦОРы:

3) Фонд развития Интернет: сделаем интернет безопаснее вместе http://detionline.com
4) Методические рекомендации по информированию родителей об услуге «Родительский контроль», позволяющий устанавливать ограничения к информационно-коммуникационной сети «Интернет» http://www.kriroipk.com/index/bezopasnaja_rabota_v_seti_internet/0-341 -
5) Безопасность детей в Интернете www.ifap.ru/library/book099.pdf
6) Информационный портал школьных библиотек России www.rusla.ru/rsba/technology/safety
7) Игра для детей про безопасность в Интернете www.wildwebwoods.org/popup.php?lang=ru
8) Разбираем интернет (новый ресурс Фонда Развития Интернет) http://www.razbiraeminternet.ru/teacher
9) Лига безопасного интернета http://www.ligainternet.ru/
10) Основы детской безопасности от Googlehttps://www.google.ru/safetycenter/families/start/basics/
11) Руководство для родителей по безопасности детей в Интернете http://m.nsportal.ru/shkola/materialy-dlya-roditelei/library/2014/10/20/rukovodstvo-dlya-roditeley-po-bezopasnosti-detey

Описание системы оценки качества освоения модуля.

Вид контроля: промежуточный.

Форма контроля: реферат.

Краткие критериальные требования к качеству выполнения реферата. Объем – от 6 до 10 страниц машинописного текста, напечатанного в формате Word; шрифт TimesNewRoman, размер шрифта - 12. Степень раскрытия темы предполагает: соответствие плана теме реферата; соответствие содержания теме и плану реферата; полноту и глубину раскрытия основных понятий; обоснованность способов и методов работы с материалом; умение работать с литературой, систематизировать и структурировать материал; умение обобщать, делать выводы, сопоставлять различные точки зрения по рассматриваемому вопросу. Обоснованность выбора литературы и источников оценивается: полнотой использования источников по исследуемой проблеме; привлечением наиболее известных и новейших работ по проблеме (научные публикации (монографии, научные статьи из реферируемых журналов и т.д.). Соблюдение требований к оформлению определяется: правильным оформлением ссылок на используемую литературу; оценкой грамотности и культуры изложения; владением терминологией и понятийным аппаратом проблемы; соблюдением требований к объему реферата; культурой оформления. Рефераты представляются на заключительном этапе изучения модуля как результат промежуточной самостоятельной работы слушателя.

Примерные темы рефератов:

1) Основы информационной безопасности педагогической деятельности.
2) Анализ законодательных актов об охране информационных ресурсов открытого

доступа.

3) Анализ законодательных актов о защите информационных ресурсов ограниченного доступа.

4) Соотношение понятий: информационные ресурсы, информационные системы и информационная безопасность.

5) Информационная безопасность образовательной среды.

6) Правовые основы защиты конфиденциальной информации в образовательной организации.

7) Структура, содержание и методика составления перечня сведений, относящихся к тайне в образовательной организации.

8) Назначение, виды, структура и технология функционирования системы защиты информации в образовательной организации.

9) Анализ функций секретаря-референта в образовательной организации в области защиты информации.

10) Направления и методы защиты персональных данных об учащихся в образовательной организации.

11) Организация педагогической работы по реализации информационной безопасности.

12) Психологическая компетентность педагога, как фактор безопасности образовательной среды.

13) Влияние интернет - пространства на психологическое состояние и поведение современного школьника.

14) Методика инструктирования и обучения педагогических работников правилами защиты информации.

Модуль 3. Информационная безопасность образовательной организации (16 ч.: 3 ч. ЛЗ, 8 ч. ПЗ)

Интегрированные дидактические цели: овладение методами и формами защиты информации в образовательной организации, совершенствование педагогической компетентности в сфере информационной безопасности

Учебный элемент 3.1. Основы информационной безопасности образовательной организации (4 ч.: 2 ч. ЛЗ, 2 ч. ПЗ).

Лекционное занятие. Основы информационной безопасности образовательной организации. Основные аспекты информационной безопасности образовательной среды. Меры по обеспечению информационной безопасности в образовательной организации: правовое обеспечение информационной безопасности; нравственный и этический контроль; защита психики и здоровья ребенка; организационная защита; воспитательные меры по обеспечению информационной безопасности; техническое и программное обеспечение информационной безопасности.

Практическое занятие. Программно-технические методы обеспечения информационной безопасности.

Учебный элемент 3.2. Программное обеспечение информационной безопасности (11 ч.: 3 ч. ЛЗ, 8 ч. ПЗ).

Лекционное занятие. Программное обеспечение информационной безопасности. Классификация и характеристика классификационных групп технических средств охраны. Программно-технические методы обеспечения информационной безопасности. Парольная защита с помощью стандартных системных средств. Идентификация и аутентификация. Разграничение доступа. Межсетевые экраны как средство защиты от

несанкционированного доступа. Профилактика вирусного заражения. Антивирусные программы.
Практическое занятие. Компьютерная практика: изучение программ информационной безопасности. Установка программ на компьютер, настройка.

Учебный элемент 3.3. Промежуточный контроль. (1 ч. ПЗ). Реферат.

Учебно-методическое обеспечение программы
Рекомендуемая литература.
Основная:

1) Коротенков Ю.Г. Информационная образовательная среда основной школы М.: Академия АйТи, 2011. 152 с.

Электронные ресурсы:

1) Справочно-поисковые системы информационно-правового обеспечения ГАРАНТ-Максимум и КОНСУЛЬТАНТ +
2) Центр проблем информационного права - http://www.medialaw.ru/
3) Институт развития информационного общества в России http://www.iis.ru/index.html
4) Портал Российского Оргкомитета по проведению Года Безопасного Интернета https://www.betterinternetforkids.eu
5) Компьютерные угрозы. Интернет и дети www.kaspersky.ru/keeping_children_safe
6) Молодежь и чистый Интернет. http://www.honestnet.ru/internet-i-deti/chasto-zadavaemye-voprosy.html

Описание системы оценки качества освоения модуля.
Вид контроля: промежуточный.
Форма контроля: реферат.
Примерные темы рефератов:

1) Информационное право и информационная безопасность в образовательной организации.
2) Концепция информационной безопасности.
3) Составление инструкции по обработке и хранению конфиденциальных документов.
4) Направления и методы защиты аудио- и визуальных документов.
5) Организационное обеспечение защиты информации, обрабатываемой средствами вычислительной и организационной техники.
6) Правовая защита детей от влияния негативной информации.
7) Интернет-зависимость, ее диагностика и профилактика.

Модуль 4. Методические основы организации мероприятий Безопасности детей в сети Интернет. (20 ч.: 3 ч. ЛЗ, 17 ч. ПЗ)

Интегрированные дидактические цели: овладение методами и формами по организации педагогической работы в сфере безопасности детей в сети Интернет.

Учебный элемент 4.1. Методика организации мероприятий по безопасности школьников в сети Интернет (6 ч.: 2 ч. ЛЗ, 4 ч. ПЗ).

Лекционное занятие. Особенности внедрения компьютерной техники и использовании сети Интернет в образовательных учреждениях. Модель информационно-образовательной среды. Личная информационно-образовательная среда конкретной личности (школьника, учителя). Угрозы информационной безопасности молодежи, средства их предотвращения. Контроль, анализ ситуации и соответствующая

коррекция информационной безопасности образовательной организации. Методы и способы повышения эффективности обеспечения безопасности информационной среды образовательного учреждения и личной информационной среды каждого учащегося.

Практическое занятие. Организация педагогической работы по реализации информационной безопасности. Критерии оценки состояния информационной безопасности в образовательной организации (на основе Концепции РФ). Информационное представление образовательной среды, ее преобразование в систематизированное информационное пространство, организованное, многомерное, упорядоченное.

Учебный элемент 4.2. Организация мероприятий для родительской аудитории. (6 ч.: 1 ч. ЛЗ, 5 ч. ПЗ).

Лекционное занятие. Профилактическая работа родителей как важнейшую составную часть психолого-педагогической проблемы обеспечения информационной безопасности ребенка, от успешного решения которой зависит духовное, физическое и нравственное благополучие детей.

Практическое занятие. Сценарий мероприятия с родителями.

Учебный элемент 4.3. Методические материалы для организации и проведения мероприятий с учащимися по безопасности в сети Интернет. (6 ч.: 6 ч. ПЗ).

Практическое занятие. Изучение всех методических материалов. Разработка сценария мероприятия – классный час, урок, внеклассное мероприятие по безопасности в сети Интернет.

Учебный элемент 4.4.. Промежуточный контроль (2 ч.: 2 ч. ПЗ).

Учебно-методическое обеспечение программы

Рекомендуемая литература.

Основная:

1. Коротенков Ю.Г. Информационная образовательная среда основной школы М.: Академия АйТи, 2011. 152 с.

Электронные ресурсы:

1. Справочно-поисковые системы информационно-правового обеспечения ГАРАНТ-Максимум и КОНСУЛЬТАНТ +
2. Центр проблем информационного права - http://www.medialaw.ru/
3. Институт развития информационного общества в России http://www.iis.ru/index.html
4. Портал Российского Оргкомитета по проведению Года Безопасного Интернета https://www.betterinternetforkids.eu
5. Компьютерные угрозы. Интернет и дети www.kaspersky.ru/keeping_children_safe
6. Молодежь и чистый Интернет. http://www.honestnet.ru/internet-i-deti/chasto-zadavaemye-voprosy.html

Описание системы оценки качества освоения модуля.

Вид контроля: промежуточный.

Форма контроля: Контрольная работа.

Контрольная работа. оформить контрольную работу по безопасности в сети Интернет на выбор:

1. Конспект урока
2. Сценарий классного часа
3. Сценарий внеклассного мероприятия
4. Сценарий родительского собрания
5. Сценарий семинара

6. План работы дистанционных мероприятий

Выходной контроль: 1 ч. ПЗ. Тест

Итоговая аттестация: 1 ч. ПЗ. Зачет

Вопросы выходного контроля.

1. Где можно найти информацию для реферата в Интернете?
   a) На сайтах средств массовой информации
   b) В электронной библиотеке
   c) В поисковой системе
   d) В Википедии
2. Как пожаловаться на неприемлемый контент на YouTube?
   a) Отметить видео “флажком”, который находится под ним
   b) Такого функционала нет
   c) Выразить свое недовольство в комментариях к видео
   d) Найти электронный адрес автора видео и написать ему сообщение
3. Что делать, если вы стали жертвой интернет-мошенничества?
   a) Сообщить взрослым
   b) Сменить все пароли
   c) Попробовать решить проблему самостоятельно
   d) Позвонить на Линию помощи «Дети онлайн»
4. Что следует делать, если на сайте вас просят отправить бесплатное сообщение на короткий номер?
   a) Как можно быстрее отправить СМС
   b) Постараться найти стоимость СМС на сайте, после этого поискать в интернете, какова стоимость отправки СМС на этот номер, и перепроверить эту информацию. До перепроверки информации не отправлять СМС
   c) Использовать телефон друга или знакомого чтобы, отправить СМС
5. Что делать, если вам приходит сообщение по электронной почте или во всплывающих окнах о том, что ваш компьютер заражён?
   a) Пройти по предлагаемым ссылкам и скачать антивирусную систему
   b) Закрыть всплывающее окно и не нажимать на ссылки в нём
   c) Просканировать компьютер на возможные вирусы, при этом не переходить по незнакомым ссылкам
6. Какие функции браузера не следует использовать на общественном компьютере?
   a) Безопасный поиск
   b) Автозаполнение форм
   c) Автосохранение паролей
   d) Режим инкогнито
7. В каком случае нарушается авторское право?
   a) При размещении на YouTube собственного видеоролика с концерта любимой группы
   b) При размещении нелицензионного контента в социальных сетях
   c) При просмотре нелицензионного контента в социальных сетях
   d) При чтении романа Л.Н. Толстого «Война и мир» в Интернете
8. Что в Интернете запрещено законом?
   a) Размещать информацию о себе
   b) Размещать информацию других без их согласия
   c) Копировать файлы для личного использования
9. Действуют ли правила этикета в Интернете?
   a) Интернет - пространство свободное от правил

b) В особых случаях
c) Да, как и в реальной жизни

10. Чем опасны социальные сети?
    a) Личная информация может быть использована кем угодно в разных целях
    b) При просмотре неопознанных ссылок компьютер может быть взломан
    c) Все вышеперечисленное верно
11. Что не дает хакерам проникать в компьютер и просматривать файлы и документы:
    a) Применение брандмауэра
    b) Обновления операционной системы
    c) Антивирусная программа
12. Какое незаконное действие преследуется в России согласно Уголовному Кодексу РФ?
    a) Уничтожение компьютерных вирусов
    b) Создание и распространение компьютерных вирусов и вредоносных программ
    c) Установка программного обеспечения для защиты компьютера

Оценочные материалы

для проведения итоговой аттестации в форме зачета по дополнительной профессиональной программе курса повышения квалификации

«БЕЗОПАСНОСТЬ ДЕТЕЙ В СЕТИ ИНТЕРНЕТ»

I. ПАСПОРТ КОМПЛЕКТА ОЦЕНОЧНЫХ СРЕДСТВ

Предмет(ы) оценивания	Объект(ы) оценивания	Показатели оценки
Проектировать психологически безопасную и комфортную образовательную среду, проводить профилактику различных форм насилия в школе	зачет	- реализовать комплекс мер по обеспечению безопасности детей использующих Интернет;
		- умение применять методы диагностики и профилактики Интернет-зависимости учащихся;
		-умение применять программные и технические средства обеспечения информационной безопасности

Предмет(ы) оценивания	Объект(ы) оценивания	Показатели оценки	Критерии
Проектировать психологически безопасную и комфортную образовательную среду, проводить профилактику различных форм насилия в школе	зачет	- реализовать комплекс мер по обеспечению безопасности детей использующих Интернет	-умение ориентироваться в нормативно-правовом обеспечении Интернет-безопасности; -владение навыками безопасного использования интернет-ресурсов; -умение применять специализированные интернет-ресурсы по обучению Интернет-Безопасности; -умение грамотно организовывать мероприятия по основам Интернет-безопасности. С привлечением, большого количества фактов, результатов социологических исследований и т.п. подчеркивающих важность проблемы; - умение обучать детей и подростков критической оценке Интернет-контента;
		- умение применять методы диагностики и профилактики Интернет-зависимости учащихся	- владение методиками диагностики Интернет-зависимости обучающихся; - умение анализировать результаты диагностики - владение методиками проведения мероприятий по профилактике Интернет-зависимости обучающихся; - применение методик по избавлению от Интернет-зависимости

		-умение применять программные и технические средства обеспечения информационной безопасности	- владение навыками установки и обслуживания программных средств обеспечения информационной безопасности; - владение навыками установки и настройки технических средств обеспечения информационной безопасности; - владение навыками работы с программными и техническими средствами обеспечения безопасности.

II. КОМПЛЕКТ ОЦЕНОЧНЫХ СРЕДСТВ

Оценка качества освоения программы обучающимся включает итоговую аттестацию в форме зачета.

Вопросы для зачета:

1. Определить место информационной безопасности в обеспечении системы безопасности образовательной среды.
2. Дать определение информационной безопасности.
3. Назвать основные направления и задачи обеспечения информационной безопасности образовательной организации.
4. Назвать основные компоненты информационной безопасности автоматизированных информационных систем.
5. Охарактеризовать уровни реализации информационной безопасности в образовательной организации.
6. Дать определение и классификацию информационных ресурсов.
7. Определить основные виды угроз информационным ресурсам в образовательной организации.
8. Охарактеризовать особенности угроз конфиденциальной информации.
9. Проанализировать причины возникновения угроз утраты или утечки конфиденциальной информации.
10. Описать причины возникновения каналов несанкционированного доступа к информации.
11. Классифицировать виды каналов несанкционированного доступа к информации.
12. Описать характер действия организационных каналов несанкционированного доступа к информации.
13. Проанализировать основные направления правовой защиты информации в образовательной организации.
14. Раскрыть содержание нормативных актов, защищающих право учащихся образовательной организации на своевременное получение достоверной информации.
15. Показать порядок защиты прав учащихся на личную тайну и неприкосновенность частной жизни законодательством Российской Федерации.
16. Определить объекты защиты прав детей от влияния негативной информации.
17. Перечислить сведения, составляющие государственную тайну и сведения, которые не могут относиться к государственной тайне.
18. Назвать основные виды служебной тайны, определенные законодательством

Российской Федерации.
19. Изложить принципы и направления комплексного подхода к обеспечению информационной безопасности образовательной среды.
20. Назвать основные положения концепции информационной безопасности образовательной организации.
21. Изложить содержание регламента обеспечения информационной безопасности образовательной организации.
22. Определить основные методы и способы работы службы безопасности предприятия по защите конфиденциальной информации.
23. Определить критерии ценности информационных ресурсов и длительности сохранения ими этой характеристики.
24. Проанализировать содержание понятия разрешительной системы доступа персонала к конфиденциальным сведениям образовательной организации.
25. Обосновать критерии выделения конфиденциальных документов из общего потока поступающих документов.
26. Классифицировать состав бумажных и технических носителей информации, применяемых для составления деловой (управленческой) и технической конфиденциальной документации в образовательной организации.
27. Сформулировать возможности, трудности и направления организации педагогической работы по реализации информационной безопасности.
28. Психологическая компетентность педагога, как фактор безопасности образовательной среды.
29. Проанализировать задачи защиты информации, которые должны быть решены при формировании и оформлении дел с конфиденциальными документами учащихся.
30. Проанализировать виды угроз информационной безопасности в образовательной организации.
31. Назвать основные элементы защиты территории и помещений образовательной организации.
32. Интернет-зависимость учащихся, ее диагностика и профилактика.