«Рассмотрено»
на заседании Методического совета
ОГБУ «БРЦ ПМСС»
Протокол № __
от «___» _____2017г.

«Утверждаю»
Директор ОГБУ «БРЦ ПМСС»
_____ Викторова Е.А.
«___» _____2017г.

Областное государственное бюджетное учреждение для детей, нуждающихся в психолого-педагогической и медико-социальной помощи «Белгородский региональный центр психолого-медико-социального сопровождения»

Программа элективного курса

«АЗБУКА ИНТЕРНЕТ-БЕЗОПАСНОСТИ»

Авторы составители:
Викторова Екатерина Александровна,
Директор ОГБУ «БРЦ ПМСС»

Скляренко Наталья Ивановна,
Заместитель директора ОГБУ «БРЦ ПМСС»

Рецензент:

Белгород, 2017

Актуальность и перспективность.

Современная реальность сложна и многогранна, она предъявляет к человеку все новые и новые требования. Это связано:

- с темпом и ритмом технического прогресса.
- с насыщенным характером информации, которая накрывает нас огромной информационной волной подобно цунами. Глубоко воздействует на психику подростка, у которого еще не выработано четкой жизненной позиции.
- с экологическими и экономическими кризисами, поразившими наше общество, что вызывает у детей и подростков чувство безнадежности и сильной эмоциональной напряженности.

Тенденции социализации подростка определяет активная информационная среда, в том числе и Интернет. Интернет сегодня для подростка не просто интересная сфера, это часть их жизни, такая же, как и все остальные. Сегодня для подрастающего поколения уже нет разделения реального и виртуального мира, просто один является продолжением другого.

Как показывают исследования Г. Солдатовой и Фонда Развития Интернета в России, количество детей, ежедневно пользующихся Интернетом выросло до 89%. Но при этом лишь 53% родителей посещают Интернет ежедневно, а 17% опрошенных родителей не посещают его вообще.

Также исследования показывают нам реальное несоответствие между грамотностью в отношении информационных средств между детьми и взрослыми: большинство взрослых имеют недостаточные сведения о том, что делают их дети в Интернете, как они это делают и с чем при этом сталкиваются.

Интернет-среда, слабо контролируемая или не контролируемая взрослыми является зоной повышенного риска для подростка. Взрослым надо понимать, что Виртуальный мир может предложить ребенку как широкие возможности познания, образования, развития, так и расставить ловушки: нанести вред их жизни и здоровью, моральному и духовному развитию.

В связи с вышесказанным проблемы Интернет-безопасности становятся крайне актуальными и привлекают особое внимание общественности.

Реализация программы элективного курса «Азбука Интернет-безопасности» может выступать условием решения обозначенной проблемы.

Научные, методологические, нормативно-правовые и методические основы программы.

- ✓ ***Нормативно-правовой основой программы выступает:***

Федеральный закон Российской Федерации № 124-ФЗ от 24 июля 1998 г. «Об основных гарантиях прав ребенка в Российской Федерации» (с изменениями и дополнениями)

Федеральный закон Российской Федерации № 149-ФЗ от 27 июля 2006 г. «Об информации, информационных технологиях и о защите информации» (с изменениями и дополнениями).

Федеральный закон Российской Федерации № 436-ФЗ от 29 декабря 2010 года "О защите детей от информации, причиняющей вред их здоровью и развитию"

Федеральный закон Российской Федерации от 21 июля 2011 г. № 252-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона "О защите детей от информации, причиняющей вред их здоровью и развитию

«Концепция информационной безопасности детей», утвержденная Распоряжением Правительства 2 декабря 2015 года РФ № 2471-р. Концепция разработана для защиты детей от дестабилизирующего воздействия информационной продукции и создания условий информационной среды для позитивной социализации и индивидуализации, оптимального социального, личностного, познавательного и физического развития, сохранения психического и психологического здоровья и благополучия, а также формирования позитивного мировосприятия молодого поколения.

✓ ***Методологическими основами данной программы явились:***

Концепция культурно-исторического развития психики Л.С. Выготского, заключающаяся в понимании непрерывности процесса количественных и качественных, структурных и функциональных изменений психики;

Исследования Г.У. Солдатовой, изучающие особенности использования подростками сети Интернет, а также вопросы безопасности подрастающего поколения в рамках Интернет-пространства. «Одним из важнейших результатов данных исследований явилась констатация того факта, что российские дети и подростки стремительно овладевают Интернетом в ситуации значительного и медленно сокращающегося цифрового разрыва между взрослыми и детьми. Российские родители и педагоги пока еще недостаточно осведомлены как о колоссальных возможностях Интернета, так и о новых рисках и угрозах в Сети. В результате дети стихийно приобретают знания и остаются в цифровом мире без активной и грамотной поддержки со стороны взрослых» (1).

В связи с вышеизложенным ***практическая направленность*** программы элективного курса «Азбука Интернет-безопасности» заключается в повышении цифровой грамотности подростков, а также в формировании компетенций по безопасному использованию информационных ресурсов.

Программа ориентирована на формирование ответственного поведения при использовании информационных ресурсов, а также сети Интернет.

При отборе содержания и его организации мы опирались на следующие принципы:

- принцип научности;
- принцип системности;
- принцип последовательности;
- принцип единства диагностики и коррекции;
- принцип «ближайшей зоны развития».

Адресат, целевая аудитория

Программа предназначена для подростков 8-11-х классов. Поскольку они в большинстве своем являются самостоятельными пользователями Интернет, их интересы становятся шире, поисковая активность активизируется, а знания остаются стихийными. Такое «полевое поведение» увеличивает возможности столкновения с интернет-угрозами и рисками, может привести к приобретению негативного опыта. Поэтому обучение алгоритмам использования информационных ресурсов становится необходимым для сохранения их безопасности.

Количество участников в группе от 15 до 25 человек (списочный состав класса).

Основная ***цель нашего курса*** заключается в формировании набора ключевых компетенций («Безопасное детство») по безопасному использованию информационных ресурсов среди участников образовательного процесса.

Основные задачи:

- повысить уровень информационной компетентности подростков;
- сформировать набор ключевых компетенций: информационную и медиакомпетентность, коммуникативную компетентность, потребительскую и техническую компетентность;
- разработать правила поведения подростков в сети Интернет;
- сформировать навыки ответственного поведения с целью обеспечения информационной безопасности в сети Интернет;

Продолжительность элективного курса

Программа элективного курса включает в себя 34 часа. Реализуется с периодичностью 1 раз неделю.

Программа элективного курса состоит из нескольких последовательных этапов:

1. Вводный блок: постановка основных целей и задач курса, первичная диагностика.
2. Блок занятий, направленный на формирование технической компетентности подростков.
3. Блок занятий, направленный на формирование информационной и медиакомпетентности подростков.
4. Блок занятий, направленный на формирование коммуникативной компетентности в Сети.
5. Блок занятий, направленный на формирование потребительской компетентности в Сети.
6. Заключительный блок: подведение итогов курса, итоговая диагностика.

Методы и формы работы:

- лекционные занятия;

- диагностические процедуры;
- групповые беседы, дискуссии, «мозговой штурм»;
- групповые развивающие и тренинговые упражнения;
- игровое моделирование поведения в значимых ситуациях.

Основные права и обязанности участников элективного курса

Ведущий специалист обязан: проводить занятия согласно расписания, соблюдать этические нормы педагога, обеспечить участников необходимым раздаточным материалом и средствами.

Участники обязаны посещать занятия, имеют право выражать свое мнение о занятиях и пожелания относительно будущих занятий.

***Оснащение и методическое обеспечение курса*:** компьютер, подключенный к сети Интернет, мультимедийный проектор, экран, доска, листы бумаги, бланки методик, цветные карандаши, фломастеры, ручки и другой инструментарий, необходимый для проведения конкретного занятия.

Требования к результату усвоения программы

Учащиеся должны знать:

- требования безопасного использования информационных ресурсов, в том числе и информационных ресурсов сети Интернет;
- основные правила соблюдения Интернет-безопасности;
- основные линии получения профессиональной помощи, при столкновении с Интернет-угрозами;

Учащиеся должны уметь:

- получать, обрабатывать, анализировать и прогнозировать полученную информацию;
- определять источник интернет-угроз и избегать их;
- грамотно использовать программное обеспечение, снижающее риски столкновения с интернет-угрозами.
- соблюдать морально-этические нормы в Сети
- ответственно и безопасно использовать различные способы подключения к Интернету и возможности их настройки в соответствии с текущими задачами, а также осваивать новые средства связи.

Комплект учебников и учебно-методических пособий, обеспечивающих процесс обучения по программе курса:

1. Солдатова Г., Зотова Е., Лебешева М., Шляпников В. Интернет: возможности, компетенции, безопасность. Методическое пособие для работников системы общего образования. Часть 1. Лекции. – М.: Google, 2013.- 165 с.
2. Солдатова Г., Зотова Е., Лебешева М., Шляпников В. Интернет: возможности, компетенции, безопасность. Методическое пособие для

работников системы общего образования. Часть 2. Практикум. – М.: Google, 2013.- 137 с.

***Связь курса с другими учебными дисциплинами*:** курс «Азбука интернет-безопасности» носит дисциплинарный характер. Приобретенные компетенции могут быть использованы учащимися при освоении курсов таких дисциплин как: основы безопасности жизнедеятельности, информатика, обществознание, а также других дисциплин, поскольку поиск, анализ и работа с различного рода информацией это умение, которое востребовано во всех областях знаний.

Курс «Азбука Интернет-безопасности» предназначен для учащихся 9-11-х классов. Курс занятий рассчитан на 34 часа. Курс представлен как теоретической, так и практической частью. Курс занятий может вести педагог-психолог, социальный педагог, педагог.

УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН

№	Название темы	Количество часов	В том числе	
			теория	практика
1	Вводное занятие. «Что такое Интернет?»	1	0,5	0,5
2	Я и Интернет (диагностическое обследование)	1	0,5	0,5
Техническая компетентность при использовании сети Интернет				
3	Техническая онлайн компетентность	1	1	-
4	Безопасность подключений	1	0,5	0,5
5	Осторожно – вирус!	1	0,5	0,5
6	Защита персональных данных. Надежные пароли.	1	0,5	0,5
7	Осторожно! Искусственный интеллект.	1	0,5	0,5
8	Алгоритм соблюдения технической безопасности при использовании Интернет. Проектная работа.	1	-	1
Информационная и медиакомпетентность при использовании сети Интернет				
9	Интернет как источник информации: польза или вред?	1	0,5	0,5
10	Информационная и медиакомпетентность.	1	1	-
11	Информация как оружие массового поражения (риски и угрозы)	1	0,5	0,5
12	Возможности поиска в Интернете	1	0,5	0,5
13	Достоверность информации	1	0,5	0,5

14	Авторское право	1	0,5	0,5
15	Алгоритм защиты от негативной информации	1	-	1
16	Творчество и Интернет. Проектная работа	1	-	1
Коммуникативная компетентность в Интернет среде				
17	Особенности коммуникации в Интернете.	1	0,5	0,5
18	Коммуникативная компетентность и общение в Сети.	1	0,5	0,5
19	Какой Я в Интернете?	1	0,5	0,5
20	Репутация в Сети.	1	0,5	0,5
21	Интернет: группы и сообщества.	1	0,5	0,5
22	Скажи мне кто твой друг	1	0,5	0,5
23	Правила общения в Интернете	1	-	1
24	Агрессия в Интернете.	1	0,5	0,5
25	Служба помощи в Сети	1	0,5	0,5
26	Алгоритм соблюдения безопасности коммуникаций в интернет-пространстве. Проектная работа.	1	-	1
Потребительская компетентность в Интернет среде				
27	Интернет-среда и средство потребления	1	1	-
28	Потребительская компетентность пользователей Интернет	1	1	-
29	Цифровое потребление: возможности и риски	1	0,5	0,5
30	Реклама в Интернете: доверять или нет?	1	0,5	0,5
31	Мошенничество в Сети	1	0,5	0,5
32	Проектная работа «Научи хорошему»	1	-	1
33	Я и Интернет (итоговое диагностическое обследование)	1	-	1
34	Заключительное занятие. Правила ответственного и безопасного поведения в современной информационной среде.	1	0,5	0,5
Итого количество часов по курсу:		34	15,5	18,5

Календарно-тематическое планирование для обучающихся 9-11-х классов по курсу «Азбука интернет-безопасности»

№	Тема занятия	Цель занятия	Содержание занятия	Кол-во часов		Дата проведения
				теория	Практика	
1	Вводное занятие. «Что такое Интернет?»	Знакомство с целями и задачами курса.	Знакомство. Исторический экскурс. Определение основных целей и этапов работы. Определение места и роли Интернета в жизни современного человека. Игра «Мир без Интернета». Определение понятий цифровая грамотность и цифровая компетентность. Основные компоненты цифровой компетентности. Мозговой штурм «Достоинства и недостатки Интернета». Выводы и рефлексия.	0,5	0,5	
2	Я и Интернет (диагностическое обследование)	Изучение особенностей взаимодействия подростков с сетью Интернет.	Приветствие. Диагностическое обследование «Я и Интернет». Рефлексия.		1	
Техническая компетентность при использовании сети Интернет						
3	Техническая онлайн компетентность	Изучение основных компонентов технической онлайн компетентности	Приветствие. Анализ современной ситуации развития Интернет в России. Знакомство с	0,5	0,5	

			понятием «Техническая онлайн компетентность» Три основные составляющие нормальной работы Интернет. Три основных группы технических рисков. Упражнение «Окно в Интернет». Безопасность беспроводных подключений. Выводы. Рефлексия.			
4	Осторожно – вирус!	Знакомство с основными правилами безопасного поведения при столкновении с вредоносными программами в Интернете	Приветствие. Актуализация знаний обучающихся о вирусах и другом вредоносном ПО. Упражнение «Разрушители мифов», Обсуждение морально-этической стороны создания вредоносного ПО.	0,5	0,5	
5	Персональные данные. Личное или публичное?	Знакомство участников с понятием «персональные данные», с основными видами персональных данных.	Приветствие. Введение в проблематику. Упражнения: «Мой профиль», «Информационный светофор», «Детективное агентство». Выводы. Рефлексия занятия.	-	1	
6	Почему нужно управлять персональными данными.	Знакомство участников с основными рисками, которые связаны с распространением персональных данных в сети (спам, фишинг, репутационные риски, кибербуллинг и т.д.)	Приветствие. Введение в проблематику. Упражнение: По секрету всему свету», «Скорая помощь онлайн» «Свой ключ всегда носи с собой» Обсуждение, выводы, рефлексия.	-	1	

7	Осторожно! Искусственный интеллект.	Обсуждение вопросов, связанных с проблемой быстрого развития компьютерных технологий и понятием «искусственный интеллект»	Приветствие. История вопроса. Зачем нам нужен искусственный интеллект, для чего мы его создаем. Упражнение «тест на искусственный интеллект». Выводы, обсуждение, рефлексия.	0,5	0,5	
8	Алгоритм соблюдения технической безопасности при использовании Интернет. Проектная работа.	Разработка алгоритма технической безопасности при использовании Интернет.	Приветствие. Презентация проектных работ обучающихся (конкурс проектных работ). Обсуждение. Рефлексия.		1	
Информационная и медиакомпетентность при использовании сети Интернет						
9	Интернет как источник информации: польза или вред?	Знакомство обучающихся с видами и формами информации, представленными в Интернете, видами позитивного и негативного контента в Сети.	Приветствие. Обсуждение вопроса «Интернет: польза или вред?» Упражнение «Убеди меня», «Киберфанаты против кибескептиков». Обсуждение, рефлексия.	0,5	0,5	
10	Информационная и медиакомпетентность.	Изучение основных компонентов информационной и медиакомпетентности	Приветствие. Анализ вопросов: информационная компетентность и информационная культура. Основные компоненты информационной компетентности, выводы. Заключение.	1		
11	Информация как оружие массового поражения (риски и угрозы)	Изучение особенностей использования информации.	Приветствие. Проблемная беседа на тему «Что такое негативный контент?», контентные риски и угрозы. Способы защиты от негативной	0,5	0,5	

			информации. Выводы, рефлексия.			
12	Возможности поиска в Интернете	Обучение эффективному поиску информации, усвоение критерием достоверности информации в Интернете, обучение возможностям поиска Google, работа с настройками безопасности в поисковых сервисах.	Приветствие. История и будущее поиска в Интернете. Мастер поиска Google: надежные инструменты. Упражнения: «Астрономическая конференция», «Найди код от сейфа». Выводы. Рефлексия.	0,5	0,5	
13	Достоверность информации	Знакомство учащихся с проблемой достоверности информации в Интернете, критериями оценки информации и надежности сайтов.	Приветствие. Обсуждение проблемы достоверности информации, представленной в Интернете Упражнения: «Как отличить фэйк от правды?», «От правды к вымыслу», «Как обнаружить ложь и остаться правдивым в Интернете?». Обсуждение, подведение итогов.	0,5	0,5	
14	Авторское право	Знакомство с понятием «авторское право» и порядком использования материалов других людей в Интернете.	Приветствие. Знакомство с понятием «авторское право», его защита законом РФ. Обсуждение проблемы пиратства в Интернете. Упражнения «Я – пират!» «Копирайт». Обсуждение, выводы, рефлексия.	0,5	0,5	
15	Алгоритм защиты от негативной информации	Разработка алгоритма информационной и медиабезопасности при использовании Интернет.	Приветствие. Мозговой штурм «Разработка алгоритма информационной и медиабезопасности». Обсуждение, выводы, рефлексия.		1	

16	Творчество и Интернет. Проектная работа	Создание позитивного информационного контента для сверстников.	Приветствие. Презентация проектных работ. Обсуждение, выводы, рефлексия.		1	
Коммуникативная компетентность в Интернет среде						
17	Особенности коммуникации в Интернете.	Изучение особенностей коммуникации в Интернете.	Приветствие. Коммуникация без границ. Виды и возможности интернет-коммуникации: электронная почта, социальные сервисы, форумы, онлайн-игры и виртуальные миры, мобильная связь: смс и ммс, мессенджеры и IP – телефония, чаты. Мини-опрос обучающихся: наиболее востребованные средства коммуникации с Сети. Выводы. Рефлексия.	0,5	0,5	
18	Коммуникативная компетентность и общение в Сети.	Определение понятия «коммуникативная компетентность», особенностей онлайн общения.	Приветствие. Что такое коммуникативная компетентность? Важность коммуникативных навыков в жизни человека. Насколько вы коммуникативный человек? Коммуникации в реальной жизни и в жизни онлайн. Выводы. Рефлексия.	0,5	0,5	
19	Какой Я в Интернете?	Изучение способов самопрезентации в Интернете, расширение представлений о правилах личной безопасности в Интернете.	Приветствие. Проблемная беседа: «Какой я в Интернете?», «Реальное, идеальное, вымышленное». Упражнения «Моя автарка», «Я	0,5	0,5	

			реальный, я виртуальный». Подведение итогов, рефлексия.			
20	Репутация в Сети.	Знакомство с понятием онлайн-репутация.	Приветствие. Проблемная беседа: что такое репутация? Насколько она важна, почему о ней нужно заботиться и формировать с детства? Упражнения «Цифровой след», «Управление репутацией». Подведение итогов, рефлексия.	0,5	0,5	
21	Интернет: группы и сообщества.	Обсуждение особенностей интернет-сообществ и их возможностей для общения, сотрудничества, поиска нужных людей.	Приветствие. Упражнение «Опутанные паутиной». Проблемная беседа: в чем плюсы и минусы социальных сетей? Легко ли освободиться из «паутины». Упражнение «Мы в Интернете». Подведение итогов. Рефлексия.	0,5	0,5	
22	Скажи мне кто твой друг	Изучение возможностей Интернета для поиска новых знакомых по интересам, актуализация вопроса о возможностях риска при встречах с незнакомцами из Интернета.	Приветствие. Проблемная беседа на тему «Чем отличается реальный друг, от виртуального?». Упражнение «Кто твой друг?». Как оградить себя от посторонних посягательств. Обсуждение. Подведение итогов. Рефлексия.	0,5	0,5	
23	Правила общения в Интернете	Определение основных правил общения и взаимодействия в сети.	Приветствие. Проблемная беседа: нужны ли правила в Сети? Должно ли интернет		1	

			пространство регулироваться законом? Упражнение: «Кодекс цифрового мира», «Утверждаю законопроект». Обсуждение. Подведение итогов. Рефлексия.			
24	Агрессия в Интернете.	Рассмотрение особенностей агрессивного поведения в Интернете, поиск стратегий для решения проблем, возникающих в процессе взаимодействия в Сети,	Приветствие. Знакомство с понятиями буллинга и кибербуллинга в Сети, обсуждение последствий кибербуллинга. Упражнение «Не корми тролля». Обсуждение. Подведение итогов. Рефлексия.	0,5	0,5	
25	Служба помощи в Сети	Определение механизмов помощи человеку, подвергающемуся насилию.	Приветствие. Проблемная беседа: обсуждение вариантов и стратегии поведения при столкновении с кибербуллингом. Упражнение «Линия поммощи», Определение стратегий поведения в Интернете и в реальной жизни для решения проблем. Упражнение «Скажем агрессии нет». Подведение итогов, бсуждение. Рефлексия.	0,5	0,5	
26	Алгоритм соблюдения безопасности коммуникаций в интернет-пространстве. Проектная работа.	Определение алгоритма безопасных интернет-коммуникаций.	Приветствие. Представление проектных работ обучающихся. Обсуждение. Подведение итогов. Рефлексия.		1	
Потребительская компетентность в Интернет среде						
27	Интернет-среда и средство потребления	Осознание учащимися	Приветствие. Интернет как	1		

		собственных потребностей в приобретении товаров и услуг, а также возможностей их удовлетворения с помощью различных онлайн-технологий.	торговая площадка. Что продают через интернет? Кто продает через Интернет? Как покупать через интернет? Подведение итогов. Рефлексия.			
28	Потребительская компетентность пользователей Интернет	Определение понятия «потребительская компетентность», особенностей потребления в Сети.	Приветствие. Знакомство с понятием «потребительская компетентность». Определение ключевых компетенций потребительской компетентности. Потребитель и его права. Потребительские риски. Обсуждение. Подведение итогов. Рефлексия.	1		
29	Цифровое потребление: возможности и риски	Осознание учащимися себя в качестве потребителя товаров и услуг в Интернете.	Приветствие. Обсуждение проблемной темы: «Я как интернет-потребитель». Упражнения «Интернет-шоппинг» и его риски, «Охота за подарками». Обсуждение. Подведение итогов. Рефлексия.	0,5	0,5	
30	Реклама в Интернете: доверять или нет?	Формирование у учащихся способности и готовности к оценке рисков, связанных с распространением рекламы в Интернете.	Приветствие. Обсуждение проблемной темы: реклама в Интернете: доверять или нет? Упражнение «Нажми на кнопку», «реклама или информация». Рекламные риски. Обсуждение. Подведение итогов. Рефлексия.	0,5	0,5	

31	Мошенничество в Сети	Формирование у обучающихся готовности к оценке рисков, связанных с мошенничеством в Сети.	Приветствие. Обсуждение темы: интернет-мошенничество, что мы знаем, с чем сталкивались. Упражнение «Кто пишет «нигирийские» письма», «Роман в письмах». Обсуждение. Подведение итогов. Рефлексия.	0,5	0,5	
32	Проектная работа «Научи хорошему»	Мотивация подростков на создание позитивного контента.	Приветствие. Представление проектных работ. Обсуждение. Рефлексия.		1	
33	Я и Интернет (итоговое диагностическое обследование)	Изучение изменения особенностей взаимодействия подростков с сетью Интернет.	Приветствие. Диагностическое обследование. Беседа на тему «Я и Интернет, что изменилось?» Выводы и рефлексия.		1	
34	Заключительное занятие. Правила ответственного и безопасного поведения в современной информационной среде.	Определение правил ответственного и безопасного использования Интернет-технологий.	Приветствие. Работа в группах. Разработка правил безопа сного использования Интернет-технологий. Защита своих проектов. Обсуждение. Подведение итогов занятия и курса в целом. Рефлексия. Прощание.	0,5	0,5	
Итого количество часов по курсу:				**15,5**	**18,5**	

1. Интернет: возможности, компетенции, безопасность. Методическое пособие для работников системы общего образования. Часть 1. Лекции / Солдатова Г., Зотова Е., Лебешева М., Шляпников В.,– М.: Google, 2013. – 137 с.
2. Интернет: возможности, компетенции, безопасность. Методическое пособие для работников системы общего образования. Часть 2.

Практикум / Солдатова Г., Зотова Е., Лебешева М., Шляпников В.,– М.: Google, 2013. – 137 с.

3. Практическая психология безопасности: управление персональными данными в Интернете: учебно-методическое пособие для работников системы общего образования / Г.У. Солдатова, А.А. Приезжаева, О.И. Олькина, В.Н. Шляпников. – М.: Генезис, 2017. – 224 с.
4. Цифровая компетентность подростков и родителей. Результаты всероссийского исследования / Г.У. Солдатова, Т.А. Нестик, Е.И. Рассказова, Е.Ю. Зотова. — М.: Фонд Развития Интернет, 2013. — 144 с.

СОДЕРЖАНИЕ ЗАНЯТИЙ

Занятие 1.
Тема занятия: «Что такое интернет?»

Цель: введение обучающихся в проблематику курса, знакомство с целями и задачами курса.

Задачи:

- познакомиться с историей возникновения Интернета;
- осознать особенности влияния Интернета на общество в целом и образ жизни отдельного человека;
- понимание позитивных и негативных сторон Интернета;

Оснащение и методическое обеспечение урока: класс, доска, компьютер, видеопроектор для вывода презентации, ручки, листы А4 для работы в группах.

Ход урока.

Приветствие.

Добрый день, дорогие друзья! Рада вас приветствовать на наших занятиях. они будут не совсем похожи на классические уроки, к которым вы привыкли. И первое, чем они будут отличаться, это приветствием.

Предлагаю вам определить новую традицию приветствия, которая сохранится у нас с вами и на дальнейших занятиях, называется она «Передача электронного импульса» (поскольку тема у нас электронно-техническая, то и приветствие должно ей подстать. Заключается оно в передаче хлопка ладонями правой руки от соседа к соседу по кругу).

Вот мы и поприветствовали друг друга. Перейдем теперь непосредственно к нашей основной теме.

Вводная часть. Исторический экскурс (сопровождается материалами презентации на доске).

Сегодня мы начинаем курс занятий под названием «Азбука Интернет-безопасности». Как вы думаете, чему он будет посвящен?

- Ответы обучающихся.

Совершенно верно, он посвящен формированию ответственного и безопасного поведения в Сети.

Актуальна ли для вас сегодня эта проблема? Почему?

- Ответы обучающихся.

Конечно, информационные технологии развиваются небывалыми темпами, постоянно идут научные разработки, появляются технические новинки, накопление информационного материала в Сети увеличивается в геометрической прогрессии. Но давайте задумаемся: давно ли это началось, как все начиналось?

Только вдумайтесь в следующие цифры и даты:

В 1943 году был запущен первый электронный компьютер ENIACENIAC. Он был построен в университете штата Пенсильвания. Это

сооружение было более 30 м. в длину, площадью 170 метров квадратных и весом 30 т. В аналогии компьютерные технологии развивались и в СССР: машины «Минск-32», «Урал-16». Затем компьютеры становились меньше. И в 1976 г. на свет появился первый серийный ПК Apple – 1, а в 1977 г. - Apple2. Так началась эпоха компьютеризации населения во всем мире.

За сорок лет компьютер стал неотъемлемой вещью в жизни практически каждого человека. На смену стационарным ПК пришли ноутбуки, планшетные компьютеры.

В 1960-х годах появился проект американского Министерства обороны под названием «Агентство по перспективным научным проектам и исследованиям» (англ. Advanced Research Projects Agency), сокращённо ARPA. Этой организации было поручено разработать компьютерную сеть, с помощью которой могла бы осуществляться передача секретных данных. Первым учёным, высказавшимся о возможности создания такой сети, был Дж. Ликлайдер из Массачусетского технологического института, писавший ещё в 1962 году о проекте, который он называл «Галактическая сеть» (Galactic Network). Эта идея учёного была очень близка к тому, что в настоящее время понимается как Интернет. Впереди были важнейшие шаги: поиск технических возможностей и алгоритмов для её осуществления, а также годы экспериментов в попытке добиться положительного результата.

Первое успешное подключение было совершено 29 октября 1969 года время 22.30. Этот день принято считать Днем рождения Интернета. Тогда в Калифорнийском университете Лос-Анджелеса был расположен сервер сети ARPANET, и начались попытки установить соединение между двумя городами: Лос-Анджелесом и Стэнфордом, расстояние между которыми составляло 640 км. Необходимо было удалённым способом подключиться к другому компьютеру в сети и отправить письменное сообщение, а для подтверждения передачи использовался телефон. Эксперимент проводили университетские учёные Чарли Клайн и его коллега Билл Дювалль. Именно тогда удалось полностью передать по сети из двух компьютеров короткое слово log (сокращённо от login, как в дальнейшем стал называться пароль для входа в систему). Так началась история создания и развития Интернета, которая продолжается и по сей день.

К 1971 г. была разработана первая программа для отправки электронной почты по сети.

В 1973 г. к сети были подключены через трансатлантический телефонный кабель первые иностранные организации из Великобритании и Норвегии, сеть стала международной.

В 1989 г. в Европе, в стенах Европейского совета по ядерным исследованиям родилась концепция всемирной паутины.

19 сентября 1990 г. зарегистрирован домен su для вебсайтов Советского Союза.

В 1991г. Всемирная паутина стала общедоступна в Интернете. Всемирная паутина набирала популярность.

Уже к 1997 году история создания Интернета была практически завершена, и Глобальная сеть стала примерно такой, какой мы её знаем в наши дни. Но разница в том, что тогда к Интернету было подключено всего 10 млн компьютеров, а сейчас цифра достигла 1,2 млрд. Ни одно из прежних средств коммуникации не достигало таких ошеломительных результатов за столь короткие сроки.

Что же Интернет сегодня для нас?

- ответы детей.

Да, Интернет, конечно же величайшее изобретение человечества, которое кардинальным образом изменило наш мир.

Давайте задумаемся, как именно Интернет повлиял на нашу с вами жизнь?

Упражнение «Мир без Интернета». Представьте, что Интернет так и не изобрели. Какой бы была наша жизнь сегодня? Что исчезло бы из нашей жизни? Что появилось бы в нашей жизни?

(класс делится на две проблемные группы. Одна прорабатывает задание «Что появилось бы в нашей жизни, если бы в ней не было Интернета?» другая – «Что исчезло бы из нашей жизни, если бы не было Интернета»)

- ответы детей представляют защиту работы своей группы.

Обсуждение:

Стала бы наша жизнь лучше или хуже без Интернета?

Как влияет Интернет на ваш образ жизни и образ жизни других людей?

Подводим итоги.

Интернет сегодня позволяет нам:

1. Осуществлять быстрый поиск информации
2. Предоставляет нам широту общения
3. Расширяет территориальные границы (стирает границы и пространства)
4. Позволяет получать дополнительное образование и культурное развитие
5. Обеспечивает нам досуг
6. Формирует нашу с вами цифровую грамотность
7. Повышает информационную или цифровую компетентность.

Что же такое информационная грамотность, как вы это понимаете?

- ответы обучающихся.

Итак, информационная грамотность это - совокупность умений и навыков, позволяющие человеку запрашивать, искать, отбирать, оценивать и перерабатывать нужную информацию, создавать и обмениваться новой информацией.

Очень важное и необходимое в современной жизни умение.

Цифровая компетентность – заключается не только в сумме общепользовательских и профессиональных знаний и умений, которые представлены в различных моделях ИКТ-компетентности, но и установка на эффективную деятельность и личное отношение к ней, основанное на чувстве ответственности (Г.У. Солдатова).

Цифровая компетентность базируется на четырех основных столпах:

- знания
- умения и навыки
- мотивация,
- ответственность (включающая в том числе безопасность).

Каждый из компонентов может реализовываться в различных сферах деятельности в Интернете: работа с компьютером, коммуникация, техносфера, потребление – в разной степени.

1. **Информационная и медиакомпетентность** – знания, умения и навыки, мотивация, ответственность, связанные с поиском, пониманием, организацией, архивированием цифровой информации и ее критическим осмыслением, а также с созданием информационных объектов с использованием цифровых ресурсов (текстовых, изобразительных, аудио и видео и т.д.);
2. **Коммуникативная компетентность** - знания, умения и навыки, мотивация, ответственность, необходимые для различных форм коммуникации (электронная почта, чаты, блоги, форумы, социальные сети и пр.) и с различными целями;
3. **Техническая компетентность** - знания, умения и навыки, мотивация, ответственность, позволяющие эффективно и безопасно использовать технические и программные средства для решения различных задач, в том числе использования компьютерных сетей, облачных сервисов и т.п.;
4. **Потребительская компетентность** - знания, умения и навыки, мотивация, ответственность, позволяющие решить различные повседневные задачи, связанные с конкретными жизненными ситуациями, предполагающими удовлетворение различных потребностей.

Но, дорогие, ребята, знания, умения и навыки использования компьютера, Интернет мы с вами получаем на уроках информатики. Мы же с вами уделим больше внимания мотивации, ответственности и безопасности в Сети.

Мы с вами очень быстро и с большим желанием видим плюсы Интерната. Но, как и у всех медалей есть две стороны, так и у Интернета, есть свои достоинства и свои недостатки. Давайте проведем с вами небольшой **«мозговой штурм»** и подумаем: что входит в перечень достоинств, а что в перечень недостатков или рисков, связанных с работой в Интернете (организуется групповая работа двух команд. Одна составляет список достоинств, другая – недостатков или рисков).

Представление командами своих результатов «мозгового штурма». Обсуждение.

Выводы: для того чтобы минимизировать угрозы столкновения с интернет-рисками, определить стратегии поведения в проблемных ситуациях и разработан наш курс. На наших занятиях мы постараемся ответить на самые злободневные и острые вопросы, которые возникают у вас, как юных пользователей в повседневной жизни.

Рефлексия занятия:

1. Что нового для себя сегодня узнали, что заинтересовало?
2. Над чем задумались, возможно, впервые?
3. Что понравилось?

Занятие 2.

Тема занятия: «Я и Интернет (диагностическое обследование)»

Цель: Изучение особенностей взаимодействия подростков с сетью Интернет.

Задачи:

- определить актуальный уровень взаимодействия подростков с сетью Интернет;
- определить «проблемные зоны» подростков при использовании Интернет;
- актуализировать необходимость получения дополнительных систематизированных знаний в вопросах работы и взаимодействия со Всемирной паутиной.

Оснащение и методическое обеспечение урока: класс, доска, раздаточный материал с бланками методик на каждого ученика, ручки.

Ход урока.

Приветствие.

Добрый день, рада видеть вас сегодня на занятии. Предлагаю поприветствовать друг друга перед началом работы.

Упражнение «Приветствие». (см. конспект занятия №1).

Вводная часть.

На прошлом занятии мы с вами говорили о том, что такое Интернет, как он появился, о перспективах его развития. Сегодня нам предстоит определить какое же место Интернет занимает именно в вашей жизни. Для этого вам предлагается ответить на следующую анкету.

Пожалуйста, уделите внимание перечисленным вопросам, отвечайте искренне и помните, что правильных или неправильных вопросов не существует, существует объективная реальность, которую вы отражаете в своих ответах.

(Вопросы анкеты составлены на основе анкеты Фонда Развития Интернет, Ассоциации RELARN и факультете психологии МГУ им. Ломоносова)

Анкета для обучающихся

Уважаемые ученики! Пожалуйста, ответьте на представленные ниже вопросы. Ваше мнение для нас очень важно и интересно.

ФИО _____ класс _____

Дата _____ полных лет_____

1. Есть ли у Вас дома компьютер?

№	Утверждение	Ответ
1	да, подключен к сети Интернет	
2	да, не подключен к сети Интернет	
3	нет	

2. С какого возраста пользуетесь компьютером?

_____

3. Являетесь ли Вы пользователем:

Интернет-ресурсов

№	Утверждение	Ответ
1	Да	
2	Нет	

социальных сетей?

№	Утверждение	Ответ
1	Да	
2	Нет	

4. С какого возраста пользуетесь сетью Интернет?

5. С какого устройства вы обычно выходите в Сеть?

№	Утверждение	Ответ
1	Домашний компьютер	
2	Школьный компьютер	
3	Компьютер в общественном месте	
4	Планшет/планшетный компьютер	
5	Ноутбук/нетбук	
6	Телефон	
7	Смартфон	
8	Айпад	
9	Айфон	

6. В каких социальных сетях зарегистрированы?

_____

_____

7. Есть ли у Вас в школе Интернет?

№	Утверждение	Ответ
1	Да	
2	Нет	

8. Доступен ли в Вашей школе Интернет для школьников во внеурочное время?

№	Утверждение	Ответ

1	Да	
2	Нет	

9. Пользуетесь ли Вы Интернетом в школе (на переменах, после уроков)?

№	Утверждение	Ответ
1	Да	
2	Нет	

10. Установлены ли в Вашей школе программы, ограничивающие доступ на какие-либо сайты?

№	Утверждение	Ответ
1	Да	
2	Нет	
3	Не знаю	

11. Установлены ли у вас на домашний компьютер программы, защитного характера:

№	Утверждение	Ответ
1	Да	
2	Нет	
3	Не знаю	

12. Если да, то какие:

№	Утверждение	Ответ
1	Антивирусная защита	
2	Программы-фильтры типа «родительский контроль»	
3	Подключен ли «детский интернет»	
4	Не знаю	

13. Как часто Вы сами пользуетесь Интернетом?

№	Утверждение	Ответ
1	каждый день	
2	один-два раза в неделю	
3	один раз в месяц	
4	в Интернете моя вторая жизнь	
5	не пользуюсь Интернетом	

14. Если Вы пользуетесь Интернетом, сколько времени Вы в нем проводите за один сеанс?

№	Утверждение	Ответ
1	10-20 мин	
2	до 1 часа	
3	1-3 часов	
4	5-10 часов	
5	Другое	

15. Получаешь ли ты удовольствие от своей работы в Интернете?

№	Утверждение	Ответ
1	никогда	

2	иногда	
3	всегда	

16. Кто учил вас пользоваться интернетом?

№	Утверждение	Ответ
1	Родители	
2	Учитель информатики	
3	Классный руководитель	
4	Друзья	
5	Одноклассники	
6	Старшие товарищи	
7	Никто, обучался сам	

17. В Интернете я обычно (отметьте галочкой):

№	утверждение	отметка
1	пользуюсь электронной почтой	
2	общаюсь с друзьями посредством голосовой связи через Интернет (ICQ, Skype, MSN)	
3	веду виртуальный дневник	
4	ищу информацию для учебы	
5	ищу информацию для культурного и духовного развития	
6	общаюсь и принимаю участие в социальных сетях (Одноклассники, Вконтакте, Facebook, Reta, Orkut)	
7	качаю программы, музыку, фото, видео	
8	слушаю Интернет-радио	
9	смотрю Интернет-телевидение	
10	узнаю о последних событиях и новостях в стране и мире	
11	играю в онлайн игры	
12	принимаю участие в Интернет-акциях, голосованиях и пр.	
13	просматриваю сайты, которые мои родители запретили бы мне смотреть	
14	развлекаюсь	

18. Чем еще можно заниматься в Интернете и что не попало в перечисленный перечень?

Ваш ответ: _____
_____

19. Как Вы считаете, находиться в Интернете опасно?

№	Утверждение	Ответ
1	Да	
2	Нет	
3	Иногда	
4	Затрудняюсь ответить	

20. Как часто вы сталкиваетесь:

№	Утверждение	никогда	редко	часто
1	с вирусами в Интернете?			
2	с мошенничеством и кражами в Интернете?			
3	С предложениями предоставить свои персональные данные (логин и пароль от своей страницы в соц. сетях, эл. почты, телефон, адрес, номер и пароль банковской карты и т.д.)			
4	с оскорблением и унижением со стороны других пользователей в Интернете?			
5	с сексуальными домогательствами со стороны других пользователей в Интернете?			
6	с вымогательством, угрозами со стороны других пользователей в Интернете?			
7	с неэтичной и навязчивой рекламой со стороны других пользователей в Интернете?			
8	с порнографией в Интернете?			
9	с психологическим давлением со стороны других пользователей в Интернете?			
10	с терроризмом в Интернете?			
11	с экстремизмом в Интернете?			
12	с призывами причинить вред себе и/или окружающим в Интернете?			
13	с предложением запрещенной продукции (алкоголь, наркотики)			

21. Назовите, с чем еще Вы сталкивались в Интернете, но это не вошло в перечень?

Ваш ответ: _____

_____

22. Часто ли Вы сталкиваетесь в Интернете с информацией, которая раздражает или вызывает неприятные эмоции?

№	Утверждение	Ответ
1	никогда	
2	иногда	
3	часто	

23. Если Вы пользуетесь Интернетом, как часто в Интернете:

№	Утверждение	никогда	редко	часто

1	Вы даете малознакомым (едва знакомым) людям адрес своей электронной почты?			
2	Вы даете малознакомым (едва знакомым) людям номер своего мобильного телефона?			
3	Вы даете малознакомым (едва знакомым) людям Ваш домашний адрес?			
4	Вы даете малознакомым (едва знакомым) людям номер своей школы или класса?			
5	Вы публикуете или даете малознакомым (едва знакомым) людям свои фотографии и фотографии своих одноклассников или родственников?			

24. Вы хотите встретиться с людьми, с которыми познакомились в Интернете?

№	Утверждение	Ответ
1	Да	
2	Нет	
3	Может быть	

25. Если Ваши друзья, пользуясь Интернетом, часто дают свои контактные данные малознакомым людям или встречаются с ними. Как Вы к этому относитесь?

№	утверждение	отметка
1	Считаю это естественным и безопасным	
2	Считаю, что из-за этого могут быть иногда неприятности	
3	Считаю, что это опасно	
4	Другое	

26. Если вы пользуетесь Интернетом, какие сайты Вы посещаете чаще всего? (выберите 3 варианта ответа)

№	утверждение	отметка
1	Игровые	
2	С музыкой и фильмами	
3	Сайты Интернет-знакомств	
4	Сайты для детей	
5	Сайты для взрослых	
6	С учебной информацией	
7	Другое (укажи)	

27. Назови 3 причины, почему стоит заходить в Интернет.

1. _____
2. _____
3._____

28. Назови 3 причины, почему стоит покинуть Интернет.

1. _____
2. _____
3._____

29. Как Вы считаете, в большей степени Интернет:

№	утверждение	Приносит пользу	вредит
1	Вашему физическому здоровью		
2	Вашему психическому здоровью		
3	Вашей морали/нравственности		
4	Вашему культурному уровню		
5	Вашей успеваемости		

30. Как твои родители относятся к твоей деятельности в Интернете?

№	утверждение	отметка
1	Разрешают свободно пользоваться и не ограничивают во времени	
2	Устанавливают временной режим и следят за тем, какие сайты я посещаю	
3	Разрешают заходить в интернет только в своем присутствии	
4	Запрещают пользоваться Интернетом вообще	
5	Другое (указать)	
6		
7		

31. Рассказываете ли Вы родителям о том, чем занимаетесь в Интернете?

№	Утверждение	Ответ
1	Никогда	
2	Иногда	
3	Всегда	

32. Интересуются ли Ваши родители тем, чем Вы занимаетесь в Интернете?

№	Утверждение	Ответ
1	Никогда	
2	Иногда	
3	Всегда	

33. Установлены ли на твоем домашнем компьютере программы, ограничивающие вход на какие-либо сайты?

№	Утверждение	Ответ
1	Да	
2	Нет	
3	Не знаю	

34. Существует мнение, что виртуальное пространство Интернета в настоящее время сравнялось по степени опасности с реальной средой?

№	Утверждение	Ответ
1	Согласен(на)	
2	Считаю это большим преувеличением	
3	Виртуальное пространство в чем-то опасно, в чем-то безопасно	
4	Считаю Интернет абсолютно безопасной средой	
5	Не знаю	

35. Считаете ли Вы, что Интернет – это свободное пространство, в котором по своему усмотрению можно делать все, что пожелаешь?

№	Утверждение	Ответ
1	Да	
2	Нет	
3	Считаю, что должны быть правила, регулирующие пользование Интернетом	
4	Не знаю	

36. Если Вы пользуетесь Интернетом, какие эмоции и чувства Вы чаще всего испытываете, находясь в Интернете? (укажите не более пяти):

№	Утверждение	Ответ
1	Радость	
2	Страх	
3	Удивление	
4	Печаль	
5	Восторг	
6	Стыд	
7	Доверие	
8	Вина	
9	Интерес	
10	Разочарование	
11	Любопытство	
12	Уверенность	
13	Унижение	
14	Счастье	
15	Отвращение	
16	Удовольствие	
17	Обида	
18	Надежда	
19	Тревога	
20	Гнев	
21	Восхищение	

37. Насколько безопасно Вы чувствуете себя:

№	Утверждение	Очень опасно	Скорее опасно	Не знаю	Скорее безопасно	Очень безопасно

1	На улице					
2	В школе					
3	В Интернете					
4	Дома					

38. Если Вы согласны с суждением, ответьте «да», если не согласны, ответьте «нет»:

№	Утверждение	Да	Нет
1	Вы используете Интернет, чтобы уйти от проблем или избавиться от плохого настроения		
2	Каждый раз Вы проводите в Интернете больше времени, чем планировали		
3	Вы чувствуете беспокойство или раздражение, когда Вас отрывают от Интернета		
4	Вы думаете об Интернете, когда находитесь вне сети		
5	Находясь вне сети, Вы испытываете подавленность или беспокойство		
6	Вы можете лишиться отношений с кем-либо, перестать ходить в школу из-за Интернета.		

39. По Вашему мнению Интернет это _____

_____
_____
_____
_____

40. Каких знаний по вопросам работы в Интернете вам не хватает?

_____
_____
_____
_____
_____

Спасибо за работу!

Рефлексия занятия:

1. Над чем задумались особенно, отвечая на вопросы?
2. Над чем задумались впервые?

Занятие 3.

Тема занятия: «Техническая онлайн компетентность»

Цель: Изучение основных компонентов технической онлайн компетентности.

Задачи:

- познакомиться с понятием технической онлайн компетентности
- обсудить функций браузера и способов его настройки на примере Google Chrome.
- обсудить риски, связанные с использованием тех или иных функций браузера.

Оснащение и методическое обеспечение урока: класс, оснащенный компьютерами с выходом в Интернет, доска, карточки с заданиями для групповой работы, ручки, тетради.

Ход урока.

Приветствие.

Добрый день, рада видеть вас сегодня на занятии. Предлагаю поприветствовать друг друга перед началом работы.

Упражнение «Приветствие». (см. конспект занятия №1).

Жизнь современного человека постоянно связана с использованием инфокоммуникационных технологий. Компьютерная техника окружает нас повсюду. Увеличивается разнообразие технических средств, имеющих выход в интернет.

Уже в 2012 году количество мобильных устройств с выходом в Интернет превышало количество жителей на планете. Сейчас эта цифра приближается к 10 млрд.

Численность пользователей Интернет в России от 18 и старше составляет 82,4 млн человек, что составляет 70% от всего населения страны.

Проникновение Интернет среди молодых россиян (16-29) лет достигает 97%.

Сегодня 56 млн россиян в возрасте от 16 лет пользуются интернетом на мобильных устройствах – смартфонах и планшетах (46,6% от всей аудитории Рунета).

Более 50% онлайн-транзакций были совершены в 2016 г. с мобильных устройств.

Поэтому современный человек для успешной деятельности должен быть технически компетентным, то есть знать и уметь использовать компьютерную технику эффективно и безопасно.

Техническая компетентность как вид цифровой компетентности – это способность и готовность эффективно и безопасно использовать компьютер, соответствующее программное обеспечение и Интернет для решения различных задач. Быть мотивированным на дальнейшее развитие своих технических знаний и умений. Нести ответственность за безопасное применение знаний не только в повседневной жизни, но и в образовательном процессе.

Использование интернета невозможно без обеспечения нормальной работы трех составляющих:

- «железа» (устройств, позволяющих нормально работать компьютеру и выходить в Интернет);

- программное обеспечение работы компьютера и использования Интернет;

- непосредственное подключение к Сети.

На основе этих составляющих выделяют и три группы технических рисков при работе в сети Интернет:

- риски, связанные с «железом». Компьютер представляет собой сложное электронное устройство, вследствие чего его работа неизбежно подвержена сбоям. Последствия большинства мелких сбоев остаются незамеченными для пользователя, так как программное обеспечение справляется с ними. Однако некоторые ошибки в работе «железа» могут привести к утрате работоспособности отдельных подсистем или даже всего устройства. Аппаратный ремонт персональных устройств, как правило, требует вмешательства профессионалов.

- риски, связанные с программным обеспечением. Программное обеспечение также подвержено ошибкам, которые могут привести к непредвиденному поведению программы, потере или порче данных, уязвимостям в безопасности. Эти риски связаны как с вредоносными программами, так и с проблемами при использовании прикладного программного обеспечения и ошибками в работе ПО.

- риски, связанные с Сетью. Нарушения в работе Сети не влияют на работоспособность «железа» и ПО, однако могут нарушить привычный процесс использования Интернета: пользователь может потерять доступ к данным, хранящимся в «облаке», информации в Интернете, общению с коллегами и друзьями. Отдельный класс рисков, связанных с работой в Сети, представляют риски кражи конфиденциальных данных и заражения устройства вредоносным ПО, которое в основном распространяется через интернет.

Итак, первая группа рисков устраняется профессионалами.

Как мы можем минимизировать риски, связанные с работой программного обеспечения?

- Ответы детей (установление антивирусных программ, их систематическое обновление, установление лицензионного программного обеспечения).

- Чем характеризуются риски, связанные с Сетью? Как мы можем защититься? Что такое безопасное подключение?

- Ответы детей (это также установление антивирусных программ, не предоставлять свои личные данные при непонятных запросах, не идти по ссылкам всплывающих окон и т.д.).

Предлагаю вам практическим способом изучить вопросы безопасного подключения к Интернет.

Упражнение «Окно в Интернет».

Сейчас, используя Интернет вам необходимо уточнить предназначение браузера – программного обеспечения для просмотра веб-страниц.

Определить: какие основные настройки браузеров существуют, в чем заключаются их основные функции и преимущества.

Участники делятся на 8 команд. Каждая группа получает карточку с одной из функций браузера для ее анализа:

Функции браузера Google Chrome			
Сохранение паролей	Функция автоматического запоминания введенных данных	Управление всплывающими окнами	Режим «Инкогнито»
Сохранение истории посещенных страниц	Функция защиты от фишинга и вредоносного ПО	Управление информации о моем местоположении	Управление загрузкой файлов

В течение 5 минут участники каждой группы должны найти в Интернете:

- информацию о конкретной функции браузера и определить, для чего она нужна;
- понять в каком случае ее следует использования;
- что произойдет, если отключить данную функцию.

По истечении пяти минут каждая группа представляет найденную информацию, а остальные участники обсуждают, хотят ли они пользоваться этой функцией браузера и в каких случаях.

(Ведущий может дополнять ответы участников на основе Таблицы, в которой дана информация о функциях настроек и рисках, связанных с их использованием)

Функции браузера	**Основные возможности**	**Будьте внимательны**
Сохранение паролей	Данная настройка позволяет упростить доступ к регулярно посещаемым сайтам. Достаточно один раз ввести логин и пароль, применить функцию «Запомнить пароль», и в дальнейшем браузер будет вводить данную информацию автоматически.	Не используйте эту функцию на общественных компьютерах или в случае, если кто-то другой имеет доступ к вашему устройству.
История посещенных страниц	В Google Chrome история посещенных страниц сохраняется автоматически. Журнал посещения сохраняет все адреса веб-страниц, которые вы	При использовании общественного компьютера желательно очищать исорию посещенных страниц или использовать режим «Инкогнито», при

	посетили за определенное время. Это удобно, если нужно вернуться к какому-либо сайту.	котором история не сохраняется.
Функция автозаполнения форм	Когда вы в первый раз вводите данные в форму, Google Chrome автоматически сохраняет ваше имя, адрес, номер телефона, адрес электронной почты и другую контактную информацию для автозаполнения. Вы можете сохранить несколько адресов в качестве отдельных записей. Также Google Chrome запоминает текст, введенный в определенные поля формы. При повторном заполнении одного поля формы уже введенный ранее текст отобразится в появившемся меню автозаполнения.	При совершении покупки в интернет-магазине или заполнении анкеты на сайте пользователь, как правило, оставляет конфиденциальную информацию (домашний адрес, телефон, паспортные данные). При включенной функции автозаполнения личная информация может стать доступна злоумышленникам, поэтому используйте эту функцию только при заполнении не конфиденциальной информации.
Функция защиты от фишинга и вредоносного ПО	Этот параметр в разделе «Конфиденциальность» включен по умолчанию в Google Chrome: браузер показывает предупреждение, если сайт подозревается в фишинге или распространении вредоносного ПО.	Не включайте эту функцию, иначе возрастает риск стать жертвой злоумышленников.
Управление всплывающими окнами	Всплывающие окна чаще всего используются для размещения рекламных сообщений в Сети. Google Chrome автоматически блокирует всплывающие окна, чтобы они не загромождали экран. При этом в адресной строке появляется значок.	При включенной опции блокировки всплывающих окон в отдельных случаях может быть заблокирована не только реклама, но и нужная информация. В отдельных случаях может быть полезно отключить «блокировщика».
Управление информацией о моем местоположении	Браузер может использовать данные о вашем местоположении для вывода персонализированной информации, например о ближайших к вам магазинах, кафе и т.д.	Будьте внимательны при использовании автоматических сервисов геолокации: Google Chrome не передает данные без вашего разрешения. Автоматическую

	Google Chrome никогда не передает сведения о вашем местоположении без разрешения. Когда вы заходите на сайт, который запрашивает такую информацию, в верхней части страницы Google Chrome по умолчанию появляется предупреждение. Данные передадутся, только если в строке запроса вы нажимаете кнопку «Разрешить»	геолокацию можно отключить.
Управление загрузкой файлов	Браузеры позволяют сохранять файлы из Интернета на локальном диске вашего компьютера, чтобы воспользоваться ими позднее, например, когда будет отсутствовать подключение к интернету. При загрузке исполняемого файла (например, с расширением EXE, DLL или BAT) сначала над подтвердить операцию, нажав кнопку «сохранить», которая появляется на панели загрузок. Это подтверждение позволяет предотвратить автоматическую загрузку вредоносного ПО на ваш компьютер. Если URL загружаемого файла находится в актуальном списке вредоносных веб-сйтов, опубликованном в API безопасного просмоотра, браузер выдаст предупреждение.	К файлам, полученным из интернета, даже от знакомых вам людей, нужно относиться с осторожностью. Не открывайте подозрительные файлы.
Функция «Инкогнито»	Функция особенно полезна на общедоступных компьютерах. Используя ее вы можете быть уверены, что при закрытии последнего окна все данные (в том числе cookie) будут удалены. Единственное	

	исключение составляют загруженные файлы.	

Обсуждение:

- Как вы считаете, какие функции браузера делают использование Интернета более безопасным?

- С какими рисками можно столкнуться, если не пользоваться этими функциями?

- Какие функции браузера полезны при использовании Интернета на персональном компьютере на компьютере, находящемся в общем доступе?

Особое внимание мы с вами заострим на **использовании общественного доступа к Wi-Fi.**

Как обеспечить безопасность беспроводной сети?

В силу того, что в беспроводных сетях данные передаются с помощью электромагнитных волн и среда распространения не ограничена (как в случае передачи данных через кабель), содержание передачи может быть доступно посторонним. Передавать незашифрованные данные в открытой беспроводной сети – как разговаривать вслух в общественном месте: любой может подслушать ваш диалог.

Давайте подумаем, как мы с вами можем защитить свои данные?

- Ответы детей.

Итак, вывод:

- необходимо стараться осуществлять подключение к сетям, использующим шифрование.

- если вы подключаетесь к незащищенной сети, не передавайте данные по незащищенным протоколам. Используйте протоколы, поддерживающие шифрование, например HTTPS. В особенности это касается данных, содержащих приватную информацию: пароли к веб-ресурсам и платежным системам, онлайн-банки.

Выводы:

1. Для того, чтобы грамотно пользоваться такой сложной интеллектуальной техникой как компьютер, необходимо не просто иметь знания по ее использованию, но и ставить перед собой задачи постоянного обучения, так как технический прогресс не стоит на месте, а новые разработки и их внедрение предъявляют к человеку все новые и новые требования.
2. Использование компьютерных технологий, интернет технологий должно быть безопасным. За свое поведение в сети мы несем такую же ответственность как и за поведение в повседневной «реальной» жизни.

Рефлексия занятия:

4. Что нового для себя сегодня узнали, что заинтересовало?
5. Над чем задумались, возможно, впервые?
6. Что понравилось?

Занятие 4.

Тема занятия: «Осторожно – вирус!»

Цель: знакомство с основными правилами безопасного поведения при столкновении с вредоносными программами в Интернете.

Задачи:

- актуализировать знания обучающихся о вредоносном программном обеспечении
- определить основные линии поведения по защите от воздействия вредоносного ПО
- определить основные линии поведения при столкновении с воздействием вредоносного ПО
- обсудить морально-этическую сторону создания вредоносного ПО

Оснащение и методическое обеспечение урока: класс, оснащенный компьютерами и с выходом в Интернет, мультимедийный проектор, доска, карточки с заданиями для групповой работы, ручки, тетради.

Ход урока.

Приветствие.

Добрый день, рада видеть вас сегодня на занятии. Предлагаю поприветствовать друг друга перед началом работы.

Упражнение «Приветствие». (см. конспект занятия №1).

Сегодня наше занятие будет посвящено проблемам вирусного воздействия, заражения компьютера или другой электронной техники.

Что же такое вирус?

- ответы обучающихся. Подытожим:

Компьютерный вирус – это вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также способного распространять свои копии по разнообразным каналам связи.

Какие виды вирусов вы знаете или, может быть, с какими вы сталкивались?

- ответы обучающихся.

Основные виды компьютерных вирусов:

Червь – программа, которая делает копии самой себя. Ее вред заключается в захламлении компьютера, из-за чего он начинает работать медленнее. Отличительной особенностью червя является то, что он не может стать частью другой безвредной программы.

Троянская программа (троянский конь, троян)

Троянская программа маскируется в других безвредных программах. До того момента как пользователь не запустит эту самую безвредную программу, троян не несет никакой опасности. Тронская программа может нанести различный ущерб для компьютера. В основном трояны используются

для кражи, изменения или удаления данных. Отличительной особенностью трояна является то, что он не может самостоятельно размножаться.

Программы – шпионы

Шпионы собирают информацию о действиях и поведении пользователя. В основном их интересует информация (адреса, пароли).

Зомби

Зомби позволяют злоумышленнику управлять компьютером пользователя. Компьютеры – зомби могут быть объединены в сеть и использоваться для массовой атаки на сайты или рассылки спама. Пользователь может не догадываться, что его компьютер зомбирован и используется злоумышленником

Программы – блокировщики (баннеры)

Это программа, которая блокирует пользователю доступ к операционной системе. При загрузке компьютера появляется окно, в котором пользователя обвиняют в скачивание нелицензионного контента или нарушение авторских прав. И под угрозой полного удаления всех данных с компьютера требуют отослать смс на номер телефона или просто пополнить его счет. Естественно после того как пользователь выполнит эти требования банер никуда не исчезнет.

Вредоносная программа (Malware) – это любое программное обеспечение, созданное для получения несанкционированного доступа к компьютеру и его данным, с целью хищения информации или нанесению вреда.

Существует много мифов и легенд о вредоносных программах и иногда бывает сложно понять, что на самом деле является правдой, а то вымыслом.

Упражнение «Разрушители мифов». Предлагаю вам побывать в роли экспертов и попробовать отличить распространенные мифы от истины.

Разделимся на 5 групп. Каждая группа получит определенное утверждение. Нужно определить миф это или реальность и аргументировать свой ответ после коллегиального обсуждения.

Карточки для участников.

Мифы
Карточка 1. На большинстве персональных компьютеров нет никаких важных данных, используя которые злоумышленник может заработать деньги или нанести пользователю какой-либо ущерб.
Карточка 2. Если на компьютер попадает вредоносная программа, то компьютер ломается

Карточка 3.

Если просто просматривать веб-страницы и ничего не скачивать, невозможно «поймать» вредоносную программу.

Карточка 4.

Невозможно поймать вредоносную программу на сайтах крупных и уважаемых компаний (например: Яндекса, Википедии и пр.).

Карточка 5.

Если установить антивирус и регулярно его обновлять, ни один вирус компьютеру не страшен.

Карточка-подсказка для педагога.

Аргументы мифов.

Карточка 1.

- Если вы пользуетесь какими-либо системами оплаты через интернет, то воспользовавшись вашим логином и паролем, злоумышленник может украсть ваши деньги.

- Злоумышленник может получать деньги за рассылку спама, организовать с вашего компьютера DDoS- атаку. Вы же вынуждены будете оплачивать лишний трафик, мириться с медленной работой компьютера и даже, возможно, общаться со службой безопасности организации, атакованной с использованием вашего взломанного компьютера.

- злоумышленник может использовать персональный компьютер или почтовый сервис для распространения вируса на компьютеры ваших друзей и знакомых, среди которых наверняка найдется кто-то, на ком можно заработать.

Вывод. Если вам кажется, что на вашем компьютере нет ценных данных, которые нужно защищать, подумайте об оплате трафика, скорости работы ПО и реакции друзей, когда они получат от вас письмо с вирусом или спамом.

Карточка 2.

- создатель программ, ломающий компьютер, не получил бы никакой выгоды. Современные вредоносные программы остаются незаметными для хозяина компьютера и в это время собирают личную информацию, рассылают спам и т.п.

- Если же работа компьютера нарушается, то часто это связано с вымогательством и мошенничеством, например в случаях, когда за разблокировку компьютера просят отправить платную смс.

Вывод: если вы не замечаете никаких нарушений в работе вашего компьютера и ПО, это еще не значит, что компьютер не заражен.

Карточка 3.

- есть два способа заражения при просмотре страниц в Интернете: через уязвимость самих браузеров и через активные элементы страниц.

Вывод: даже если вы просто просматриваете веб-страницы, вам необходимо позаботиться о безопасности компьютера. Следует не только своевременно обновлять уязвимые программы, но и ограничивать выполнение различных активных элементов (ActiveX, Java-апплеты, VBS/Java-скрипты и т.п.) при просмотре документов с ненадежных сайтов.

Карточка 4.

- конечно, крупные и уважаемые компании не будут заниматься распространением вредоносного ПО на своих сайтах. Однако, необходимо помнить, что странички даже таких компаний могут быть взломаны и изменены злоумышленниками. Хотя степень защиты таких страниц высока, в истории были примеры, когда взламывались компьютеры Пентагона и сервисы NASA.

Вывод: даже если вы просматриваете веб-страницы надежных компаний, необходимо помнить о безопасности.

Карточка 5.

- Обновления антивирусных баз выходят после первых заражений новыми вирусами, а не до их создания.

Вывод: при работе в Сети, помимо технических инструментов защиты, всегда необходима личная бдительность. Если на компьютере хранятся важные для вас данные, позаботьтесь о резервных копиях и предусмотрите план действий, необходимый в случае попадания этих данных в руки злоумышленника.

На основе наших размышлений и умозаключений давайте выделим основные правила безопасности и защиты от вредоносного ПО

1. **Следует внимательно относиться к файлам, пришедшим к Вам по почте**

Если Вы без предупреждения получили письмо, которое в строке «отправитель» содержит имя Вашего знакомого, не торопитесь его открывать. Сначала постарайтесь связаться с человеком, с чьего адреса было отправлено

это письмо (связаться можно по телефону, ICQ или электронной почте), и уточните, действительно ли это он отправлял? Если выяснится, что не отправлял, посоветуйте ему срочно проверить свой компьютер на вирусы. А письмо это обязательно удалите (и из корзины тоже).

Если же отправитель недоступен, а Вам необходимо срочно узнать, что Вам прислали, то лучше обратиться к специалисту, но можно и попытаться справиться самому. Для этого сначала нужно вложенный файл сохранить в компьютере в отдельную папочку, но ни в коем случае не открывать. Далее нужно проверить расширение. Существуют так называемые опасные расширения (например: exe, com, pif, vbs, vsh, lnk, bat, cmd), которые при открытии могут Вам навредить. Если файл имеет именно такое расширение, лучше его не открывать до выяснения обстоятельств.

2. Будьте бдительны при получении писем рекламного характера

Если Вы получили рекламное письмо, не следует на него отвечать. Если Вы на него отреагируете, то покажете, что Ваш ящик еще «жив» и всегда готов принять новый СПАМ. Кроме того, если Вам предлагается отказаться от рассылки, перейдя по ниже указанной ссылке, не надо этого делать. И вообще, нельзя открывать ссылки, содержащиеся в рекламных письмах. Перейдя по такой ссылке, Вы опять же можете подтвердить, что Ваш почтовый ящик «жив».

3. Придумайте сложное имя для своего почтового ящика

Регистрируясь на почтовом сервере, Вы, как правило, стараетесь выбирать себе имя попроще (например: vasia, katia, sasha и другие). Оно и понятно: такое имя проще запомнить, да и смотрится красиво! Но дело в том, что СПАМер, составляя свою базу для рассылок, использует самые простые и популярные имена. И Ваше имя тоже легко может оказаться в этом списке. Поэтому рекомендуется выбирать себе имя посложнее («не словарное»), состоящее из комбинаций букв (заглавных и строчных, русских и латинских и т.п.), цифр и символов

4. Используйте сложные пароли

Ваш пароль не должен:

- Совпадать с логином;
- Быть слишком коротким;
- Состоять из одних цифр;
- Состоять из символов, которые находятся на клавиатуре на одном ряду;
- Быть словом «пароль».

Распространена практика, набирать русские слова в английской раскладке. Вариант неплохой, но слово стоит выбирать не словарное, к тому же, у вас могут возникнуть проблемы при наборе такого пароля при отсутствии руссифицированной клавиатуры. Старайтесь аккуратно хранить пароли (не стоит записывать пароль на бумажку или в черновики смс-сообщений в телефоне).

5. Не оставляйте адрес своей электронной почты где попало

Очень часто при регистрации Вас просят указать e-mail. Но прежде чем делать это, хорошенько подумайте. Если Вы уверены в надежности данного

сервера (например, это может быть старый проверенный форум или крупный Интернет-сервис), и список зарегистрированных пользователей не попадет в руки СПАМерам, тогда можете оставлять свой настоящий адрес.

Бывают случаи, когда зарегистрироваться необходимо, а адрес оставлять не хочется. В этом случае целесообразно завести себе дополнительный почтовый ящик, специально для подобных регистраций, или воспользоваться сервисом mailinater.com (при регистрации на подозрительном сайте вы указываете почтовый адрес user_name@mailinater.com, регистрируетесь, потом идёте на сайт mailinater.com, вводите логин, который Вы выбрали (пароль не нужен) и можете просмотреть там письмо, отправленное Вам при регистрации). Плюс ко всему убедитесь, что на всех форумах, которые Вы посещаете в настройках аккаунта установлен флажок «не показывать мой e-mail» другим пользователям.

6. **Игнорируйте (закрывайте) на незнакомых сайтах в диалоговых окнах кнопку «ОК»**

Прежде чем что-то нажимать на незнакомом сайте, нужно внимательно прочитать, что Вам предлагают сделать. Если предлагают установить какую-либо программу или обновление, не соглашайтесь. Если Вам приходит сообщение от браузера о том, что содержимое на странице не безопасно, то выбирайте вариант, который обеспечит Вашу безопасность. Не стоит игнорировать подобные предупреждения.

7. **Устанавливайте лицензионное программное обеспечение.**

Путешествуя по Сети и скачивая различные «мини-программы», Вы рискуете скачать вместе с программой какой-нибудь вирус. Многие «мини-программы» и «программы-приколы» именно для этого и создаются.

8. **Своевременно устанавливайте обновления**

Многие программы умеют закачивать обновления (не нужно путать обновления с новыми версиями программ). И это очень важно. Предположим (а, скорее всего, так и есть), у Вас установлена некая антивирусная программа. И каждый день в Сети появляются все новые и новые вирусы, а она о них ничего не знает, поэтому и не может успешно бороться, а для этого ей необходимы обновления базы определений вирусов. Такие обновления обычно выполняются автоматически, либо программа через определенный промежуток времени предлагает осуществить проверку. Очень важно обновлять Ваш антивирус, операционную систему (параметры обновления: Windows XP — Пуск / настройка / панель управления / Система / Автоматическое обновление). Не забывайте, что самое главное при пользовании Интернетом – это внимание (особенно к мелочам) и здравый смысл.

9. **Создавай и копируй.**

Для сохранения своих файлов предусмотрительно создавайте их копии на внешних носителях. Так будет проще восстановить утерянные файлы.

10. **Если ПК - тормозит**, исчезают документы, почта сама начала отправлять кучу писем - первым делом отключите от сети (выдернув сетевой кабель или отключив соединение),а еще лучше вовсе выключить ПК и

разбираться с проблемой загружаясь со съемного носителя (флешка, диск) - а потом приступаем к лечению. или уже к переустановке (как повезет).

Если самостоятельно справиться не получилось: звонок в службу поддержки по России бесплатно: «Дети онлайн» 8-800-250-00-15.

Давайте рассмотрим с вами морально-нормативную сторону вопроса создания и распространения вредоносного ПО.

Зачастую мы с вами являемся потерпевшими, на нас осуществляются атаки, за нами следят, пользуются нашими данными. Но ведь это тоже делают люди. Почему они это делают? Хорошо это или плохо? Правомерно ли здесь говорить только о понятиях хорошо-плохо или здесь актуальна тема законно-незаконно? Ведь эти люди по сути являются кибер-мошенниками. Распространяется ли на них закон? Возможно вы, как будущее поколение будете выходить на предложение законопроектов, регулирующих поведение, работу и общение в Интернете? Что бы вы предложили внести в этот законопроект?

-ответы обучающихся.

Выводы.

Рефлексия занятия:

1. Что нового для себя сегодня узнали, что заинтересовало?
2. Какие выводы вы сделали?

Занятие 5.

Тема занятия: «Персональные данные. Личное или публичное?»

Цель: знакомство с понятием «персональные данные»

Задачи:

- объяснить учащимся, что такое персональные данные, и показать, как безличная информация становится персональной
- определить основные виды персональных данных, осознать уровень их значимости
- научить участников определять, какую персональную информацию могут содержать различные материалы, размещаемые в сети.

Оснащение и методическое обеспечение урока: класс, оснащенный компьютерами и с выходом в Интернет, мультимедийный проектор, доска, карточки с заданиями для групповой работы, ручки, тетради.

Ход урока.

Приветствие.

Добрый день, рада видеть вас сегодня на занятии. Предлагаю поприветствовать друг друга перед началом работы.

Упражнение «Приветствие». (см. конспект занятия №1).

Сегодня, мы посвятим нашу встречу обсуждению вопроса о персональных данных, их безопасности и защите.

Что вы знаете о персональных данных? Что это такое?

- ответы обучающихся?

Итак, **персональные данные** – это любая информация, которая имеет отношение к конкретному человеку.

Где вы зачастую предоставляете свои персональные данные? Что из персональных данных вы представляете в Интернете и в каких случаях?

- ответы обучающихся.

Конечно, процедура регистрации на каком-либо сайте вам знакома всем. Но, чтобы разобраться в этом вопросе более глубоко, предлагаю выполнить следующее упражнение **«Мой профиль»**

«Представьте, что в Интернете появился новый популярный ресурс. Он объединяет возможности уже существующих ресурсов: социальных сетей, видеохостингов, викисред, онлайн-каналов, а также содержит новые уникальные возможности для учебы и отдыха. Большинство ваших друзей уже зарегистрированы на новом ресурсе, поэтому вам не терпится тоже туда поскорее попасть. Для этого вам всего лишь нужно заполнить простую регистрационную форму.»

Участникам раздаются формы регистрации для заполнения (вып. 5 мин)

Создание учетной записи

Логин* _____

Пол* Мужской ◯ Женский ◯

Возраст* _____

Электронная почта* _____

Номер мобильного телефона _____

Пароль* _____

Подтверждение пароля* _____

Страна _____

Город _____

Skype _____

Семейное положение _____

Образование _____

Место работы/учебы _____

Интересы _____

Любимая музыка _____

Любимые книги _____

Любимые кинофильмы _____

Любимые телепередачи _____

Создать учетную запись

После заполнения, ведущий собирает регистрационные формы и говорит участникам группы о том, что после регистрации на ресурсе вся информация

из профиля, кроме пароля, становится доступной для всех пользователей, зарегистрированных на сайте, а если профиль открыт, то и для посторонних.

Что же говорит о нас информация, размещенная в профиле? Давайте проанализируем. Сейчас я в случайном порядке раздам заполненные профили участникам группы, вы подумаете 3-4 мин и постараетесь угадать, чей это профиль. Напишите свою догадку на листочке с профилем. (Важно, чтобы участники не подсказывали друг другу)

Когда все участники выполнят задание, каждый по очереди озвучивает логин хозяина профиля, а затем высказывает предположение о личности. Только после того, как все догадки были высказан, ведущий предлагает подтвердить или опровергнуть правильность ответов.

Обсуждение результатов:

- Какой профиль было угадать проще/труднее всего?
- Что помогло/помешало угадать личность хозяина профиля?
- Какими соображениями мы руководствуемся, заполняя профили?

Выводы:

Как можно убедиться в ходе выполнения упражнения, персональные данные позволяют нам установить или идентифицировать личность человека. Чем больше информации о себе человек размещает в Интернете, тем проще другим пользователям установить его личность.

Информация, размещенная нами в Интернете, влияет на нашу репутацию в сети и помогает находить новых друзей со сходными увлечениями и интересами.

Каждый из нас имеет право самостоятельно принимать решения о том, какую информацию о себе размещать в Интернете.

Упражнение «Информационный светофор»

Итак, каждый принимает самостоятельно решение о том, какие персональные данные представлять в Интернет, а какие нет. Сейчас я раздам каждому участнику группы три вида стикеров, каждых по 5 штук: красные, зеленые и желтые. Подумайте: какую информацию о себе вы готовы выложить в Интернет, а какую – нет (каждую идею вы фиксируете на отдельном стикере).

Информацией, которой вы готовы поделиться – вы пишите на зеленых листочках.

Информацией, которой вы не готовы поделиться - на красных листочках.

Информацией, которой вы готовы поделиться только с друзьями – на желтых листочках.

После того, как все участники прописали свои мысли, ведущий предлагает пометить как-то все свои стикеры и разделиться на 3 команды. Работая в микрогруппах участники должны объединить все стикеры и рассортировать их на группы и каждой группе дать название. На выполнение задания отводится 5 мин. Затем участники представляют результаты своей работы. Названия выделенных групп выписываются на доске.

Затем ведущий с помощью проектора выводит на доску виды персональных данных и обсуждает их с полученными результатами.

Виды персональных данных

3. Регистрационные идентификационные данные (паспортные данные, пароли, пин-коды)
4. Физические характеристики (внешние данные, биометрические данные, состояние здоровья и т.п.)
5. Пространственная локализация (фиксация местоположения и перемещения)
6. Материально-экономическое положение (движимое, недвижимое имущество, зарплата, накопления и др.).
7. Официальные статусы (семейное положение, достижения, награды, наличие судимостей и т.д.)
8. Профессиональная занятость (включая образование)
9. Социальные связи (информация о родственниках, друзьях, знакомых, принадлежность к различным формальным и неформальным группам)
10. Образ жизни и поведенческие установки (мировоззрение, ценности, интересы и хобби, социальные привычки и действия, настроения, вкусы, особенности)
11. Психологические особенности (черты характера, способности, знания, умения, навыки, личностные черты)
12. Хроника личных событий

Обсуждение

1. Какой вид данных набрал больше всего красных/зеленых стикеров? Почему?
2. Какой вид информации набрал меньше голосов? Почему мы о нем забыли?
3. Какой информацией мы делимся более/менее охотно? Почему?

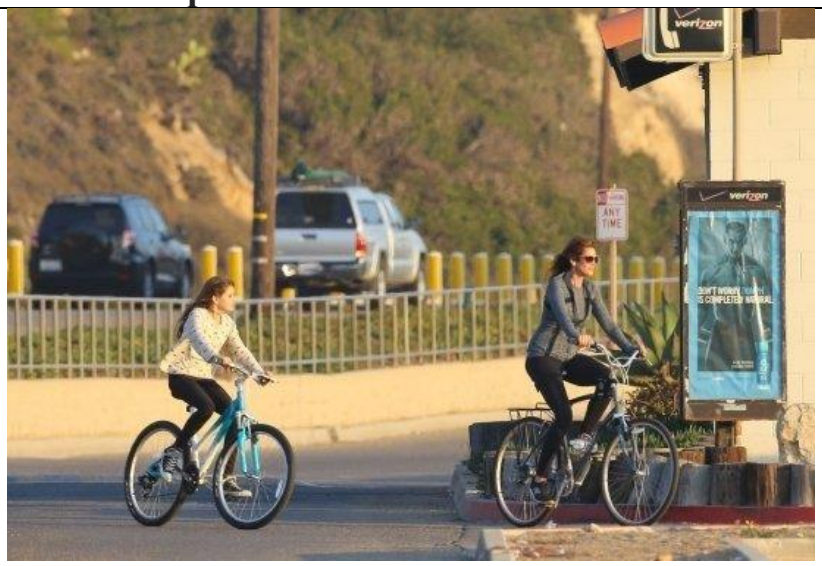
Мы с вами узнали, что существуют разные виды персональных данных. Сообщение, выложенное в Интернет, может содержать сразу несколько видов персональных данных. Например, фотография или видеозапись может рассказать другим пользователям не только о нашей внешности, но и о нашем местоположении, наших друзьях и т.д. важно научиться аккуратно обращаться с личными данными и по ошибке не выложить в сеть информацию, которую хотелось бы сохранить в тайне.

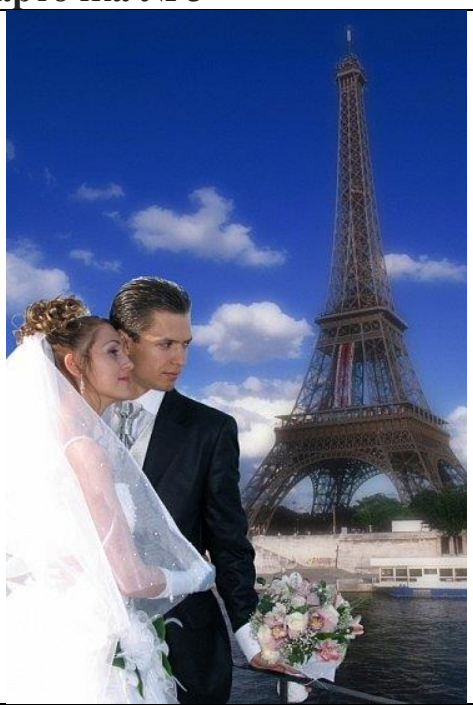
Предлагаю вам побывать немножко в роли детективов. Разделимся на 5 команд.

Упражнение «Детективное агентство». Каждая команда будет проводить расследование по одной улике. Вы получите карточку с постом из социальной сети. Ваша задача – провести расследование и узнать, как можно больше информации об авторе этого поста. На выполнение задания отводится 3 минуты.

Карточки с заданиями

Карточка № 1	
Арина Как же я люблю это время года	
	Маша: Аринка, отлично выглядишь! Ты это где?)

Карточка № 2	
Анжела Гусева Наконец-то вытащила Машку на прогулку!!!)))	
	Линочка Смирнова: молодец!!! Так и надо!!! Маму от дочки не отличишь!!!

Карточка № 3	
Денис Бобров Принимаю поздравления!	
	Злой фотограф: Отличный кадр! Ждем продолжения!

Карточка № 4	
ЛеноК Хорошо погуляли!	
	Дашутка: Точно)))

Карточка № 5	
Каринка Еще вопросы будут?	
	Тимур: а еще СНИЛС и ИНН)))

Затем каждая группа кратко представляет результаты своего расследования. Участники других групп могут задавать вопросы и давать свои комментарии. Ведущий в процессе обсуждения сверяется с комментариями.

Комментарии для ведущего.

При обсуждении результатов упражнения ведущий обращает внимание учеников на то, что информация, размещенная в Интернете, никогда не может быть однозначно интерпретирована на 100%. Всегда существует вероятность того, что мы имеем дело с подставным профилем или информацией, намеренно искаженной автором. Еще более неоднозначную информацию содержат отдельные посты, вырванные из ленты. Во всех случаях по комментариям мы можем проследить социальные связи постов.

Пример № 1. В данном случае мы можем предположить, что автор поста – молодая девушка или женщина. Мы можем сделать вывод о некоторых особенностях ее внешности, однако идентифицировать ее практически невозможно, так как на фото она стоит в каплях воды.

Пример № 2. Мы можем предположить, что на фотографии изображены мать и дочь. Фотография содержит информацию об их внешности, семейных отношениях, образе жизни, привычках. Комментарий к фотографии предоставляет нам информацию о родственной связи изображенных на ней людей. Исходя из подписи под фото, можно предположить, что, скорее всего, автором поста является сама мама.

Пример № 3. На фотографии, по всей видимости, изображен автор поста и его невеста. В этом случае мы располагаем информацией об их внешнем виде, семейном положении, образе жизни, интересах, материальном положении. Изображение Эйфелевой башни на заднем плане дает возможность установить местоположение пары.

Примет № 4. Скорее всего, на фото изображен автор поста. По-видимому, фотография сделана на память о значимом событии. Изображение Кремлевской стены дает возможность установить, что фото сделано на Красной площади в Москве.

Пример № 5. Автор поста выложил собственную фотографию и паспорт: мы видим все паспортные данные (ФИО, дата и место рождения, номер, серия, место и дата выдачи паспорта). Также мы совершенно точно знаем, как она выглядит.

В конце занятия общим голосованием определяется группа, которая провела самое тщательное и точное расследование и собрала максимальное количество персональных данных.

Вопросы для обсуждения:

- Какие материалы содержат в себе больше информации: текст или изображение? Почему?

-Какие виды персональной информации, размещенной в сети, более/менее однозначны? Почему?

- Всегда ли информация, которую мы размещаем в Интернете, говорит онас то, что мы хотим?

Выводы и итоги занятия:

Итак, существуют разные виды персональной информации. Некоторыми видами данных большинство из нас делится охотно, иные мы предпочитаем хранить при себе, а о некоторых вообще не задумываемся. В любом случае, каждый из нас имеет право принимать решение, какой информацией о себе делиться с другими пользователями, а какой – нет.

Тем не менее необходимо помнить, что неосторожное обращение с персональными данными может привести к «утечке» важной и значимой для нас информации, которой мы не хотели бы делиться с другими. Прежде чем выкладывать в Интернет какой-либо материал (иначе говоря, оставлять «цифровые следы»), следует хорошо подумать, какая персональная информация в нем содержится и как она может быть использована другими пользователями (в том числе и против вас), а также какое значение она будет иметь для вас спустя несколько лет.

Рефлексия занятия:

1. Что нового для себя сегодня узнали, что заинтересовало?
2. Какие выводы вы сделали?
3. Что понравилось/не понравилось на занятии?

Занятие 6.
Тема занятия: «Почему нужно управлять персональными данными?»

Цель: знакомство участников с основными рисками, которые связаны с распространением персональных данных в сети (спам, фишинг, репутационные риски, кибербуллинг и т.д.)

Задачи:

- помочь обучающимся осознать особенности и последствия утраты контроля над информацией после того, как она выложена в сеть, а также сложности контроля за персональными данными в Интернете.

- научить обучающихся прогнозировать возможные риски и последствия размещения личной информации в сети.

Оснащение и методическое обеспечение урока: класс, оснащенный компьютерами, мультимедийный проектор, доска, карточки с заданиями для групповой работы, листочки из отрывных блоков ручки, тетради.

Ход урока.

Приветствие.

Добрый день, рада видеть вас сегодня на занятии. Предлагаю поприветствовать друг друга перед началом работы.

Сегодня мы продолжаем наш разговор о персональных данных, их защите и нашей с вами безопасности.

Для разминки я предлагаю вам взять сейчас небольшие листочки бумаги и написать на них какой-либо секрет про себя.

(Ведущий должен отметить, что секреты не будут зачитываться в слух, но тем не менее они не должны быть слишком личными и значимыми для участников).

Затем листочки складываются несколько раз. Их можно также запечатать или заклеить клеевым карандашом. Затем участники должны разбиться на пары по своему желанию.

По команде ведущего правой рукой каждый участник передал свой секрет партнеру, а левой – принял секрет партнера. В таком положении они остаются на 1-2 минутки. Затем также меняются секретами обратно.

(Упражнение можно провести и другим способом в зависимости от уровня доверия среди участников группы. Если уровень доверия высок – то можно всем сесть в круг, а передачу секретов пустить по кругу и завершить упражнение, когда секретики вернулись к хозяевам).

При возвращении секретов участники должны проверить: сохранна ли печать, запечатан ли секрет. На этом игра заканчивается и переходим к обсуждению.

(В помощь ведущему: когда мы делимся информацией с другими людьми – не важно, лично или выкладывая в сеть – мы теряем над ней контроль. Как правило, в реальной жизни потеря контроля вызывает у людей чувство дискомфорта и тревоги. В интернете потеря контроля над персональной информацией, которая, по сути является секретом, часто не замечается и не ощущается. Это упражнение помогает ученикам осознать чувство дискомфорта, связанное с потерей контроля над информацией, и осознать, что аналогичная ситуация происходит в интернете.

Следует отметить, что выполнение этого упражнения предполагает достаточно высокий уровень сплоченности и доверия внутри группы. Если ведущий не уверен в этом, он может предложить участникам выписать на

листочки шутливые, безобидные секреты. Напротив, если ведущий чувствует, что уровень доверия в группе высок, секреты могут быть более значимыми, что усилит эффект упражнения.

Обсуждение:

- Что вы чувствовали, когда ваш секрет находился в чужих руках? Почему?
- Что вы чувствовали, когда чужой секрет находился в ваших руках? Почему?
- Хотелось ли вам узнать чужой секрет? Почему?
- Если кто-то вскрыл чужой секрет. Обсуждается почему он это сделал, что получил взамен?
- Случалось ли вам выкладывать личную или секретную информацию о другом человеке в сеть? Зачем вы это делали? Что вы при этом чувствовали?
- Этично ли так поступать? Какие последствия будут иметь такие поступки?

Чувство дискомфорта – это самое меньшее, что может возникнуть в результате потери контроля над персональными данными. А на самом деле, ваши сверстники сталкиваются с куда более серьезными последствиями неаккуратного обращения с персональными данными. В таких ситуациях многие из них обращаются на Линию помощи «Дети онлайн».

ИНФОРМАЦИЯ О ВСЕРОССИЙСКОЙ ЛИНИИ ПОМОЩИ «ДЕТИ ОНЛАЙН»

В 2009 г. в рамках Года Безопасного Интернета в России была создана линия помощи «Дети онлайн» для оказания психологической и информационной поддержки детям и подросткам.

Линия помощи «Дети онлайн» - это служба телефонного и онлайн-консультирования по вопросам безопасного использования интернета и мобильной связи для детей, подростков, родителей и работников образовательных учреждений.

На Линии помощи работают профессиональные психологи-эксперты Фонда Развития Интернет и факультета психологии МГУ имени М.В. Ломоносова.

Обратиться на линию помощи можно как по телефону, так и по электронной почте или в онлайн-чате.

Часы работы: с 9 до 18 часов в будние дни (перерыв с 13 до 14 часов), звонок по России бесплатный.

Телефон: 8-800-25-000-15

Электронная почта: helpline@detionline.com

Онлайн-чат: http://detionline.com

Все обращения на Линию полностью анонимны и конфиденциальны.

Предлагаю вам побывать в роли экспертов и помочь «потерпевшим» разрешить сложны ситуации.

Упражнение «Скорая помощь онлайн».

Формируем команды по 5 человек.

Инструкция: Вы являетесь операторами Линии помощи и находитесь на дежурстве. К вам поступает обращение ребенка или подростка, который попал в затруднительную ситуацию в результате неаккуратного обращения с персональными данными. Ваша задача – внимательно изучить пример и сформулировать ответы на следующие вопросы:

- почему произошла эта ситуация? Что стало причиной возникновения проблемы?

- что можно посоветовать подростку, обратившемуся за помощью, чтобы решить возникшую проблему?

- что нужно делать, чтобы подобные ситуации впредь не возникали? Какие действия впредь нужно избегать?

На выполнение этого задания отводится 5-10 минут. Когда все готовы представитель от каждой группы описывает проблему, представленную в карточке, называет причины, которые по мнению группы, привели к ее возникновению, а затем предлагает пути решения проблемы и способы, позволяющие ее избегать. Каждой группе на выступление отводится 2-3 минуты. Остальные участники могут задавать вопросы выступающему и высказывать свои комментарии, например, выразить несогласие и предложить свое решение проблемы.

В ходе дискуссии ведущий выписывает на доску все рекомендации по решению и профилактике проблем, сформулированные участниками группы, а также дополняет их, используя комментарии для ведущего. В результате получается набор рекомендаций по решению и профилактике проблем, возникших в результате неаккуратного обращения с персональными данными в интернете.

Обсуждение:

- Приходилось ли вам или вашим знакомым сталкиваться с подобными проблемами?

- Как вы думаете, какова основная причина возникновения подобных ситуаций?

Что можно посоветовать человеку, оказавшемуся в таких обстоятельствах?

Примеры обращений на линию помощи «Дети онлайн»

Пример №1.

Добрый день! Меня зовут Марина, мне 14 лет. Недавно кто-то взломал мой аккаунт в ВКонтакте и стал размещать на моей странице неприличные изображения. А еще оскорблять от моего имени друзей в комментариях и в личке. Обо всем я узнала от подруги, так как на даче, где я была, не было Интернета. Я восстановила доступ к аккаунту и поменяла пароль, но было уже поздно. Многие удалили меня из друзей и добавили в «черный список», а кое-кто даже перестал со мной разговаривать. Я несколько лет вела эту страницу, у меня была почти тысяча подписчиков, а теперь все пропало. Подскажите, как мне поступить? Как вернуть доверие подписчиков?

Пример №2.
Доброго времени суток! Я Артем, учусь в 9-м классе. Однажды на уроке информатики я зашел в свой аккаунт в социальной сети и забыл выйти. Через неделю один из моих одноклассников создал паблик, в которой он выкладывает скриншоты моей личной переписки с друзьями и гадкие комментарии к ним. Там нет ничего такого, но это все равно неприятно. Надо мной все смеются. Я и раньше не был популярным в классе, а теперь стал настоящим изгоем. Что мне делать? Можно ли удалить этот паблик? Как наказать одноклассника?

Пример №3.
Здравствуйте! Меня зовут Настя, мне 15 лет. Недавно я познакомилась с парнем в социальной сети. Он был знакомым моей подруги и показался мне интересным. Мы стали общаться, оказалось, что у нас много общего. Мы рассказывали друг другу о себе, о том, где учимся, путешествуем. Вообще-то я скрытная, и профиль у меня только для друзей, но с ним, я кажется, позволила себе лишнего. Однажды он предложил встретиться. Я немного испугалась и отказала ему. Он сказал, что знает, где я учусь и где живу, обещал подстеречь по дороге из школы домой. Я не знаю, правда это, или он меня просто запугивает. Мне действительно страшно. Теперь одна, без подруги, я в школу не хожу. Подскажите, как мне быть?

Пример №4.
Добрый день! Меня зовут Егор, мне 12 лет. Я тут видел в Интернете рекламу новой игры Dragons &Unicorns. Для этого чтобы в нее поиграть, нужно было зарегистрироваться на сайте и указать номер мобильного, что я и сделал. В результате игра мне совсем не понравилась, и я быстро забыл про нее. А через несколько дней мне на телефон стали приходить СМС-ки с рекламой с разных номеров. Я удалил свой аккаунт на сайте игры, но это не помогло, СМС-ки продолжают приходить. Подскажите, как от них избавиться?

Пример №5.
Добрый день! Меня зовут Лена, мне 15 лет. Меня обманула моя «подруга» из социальной сети. Мы общались больше года. Познакомились в паблике про ролевые игры. Я говорила ей, что мечтаю приобрести последний сет игры Dungeons &Dragons, но у нас он не продается. Заказать по интернету я не могу. У меня нет банковской карты, а родители свою не дают. Подруга предложила мне помочь купить сет. Она уже студентка и у нее есть карта. Она предложила мне перевести ей деньги на Яндекс-Кошелек и обещала сделать заказ с доставкой на мой адрес. Я с радостью согласилась и перевела ей деньги. Прошел месяц, а посылка не приходила. Когда я спрашивала ее об этом, она отвечала, что нужно подождать. Потом она стала появляться в сети все реже и реже, пока совсем не пропала. Совершенно случайно я узнала, что она обманула еще несколько человек аналогичным способом. Подскажите, можно ли что-то сделать? Вернуть деньги или наказать эту мошенницу?

Комментарии для ведущего

Пример №1.

в данном случае мы имеем дело со взломом аккаунта школьницы с целью нанесения вреда ее репутации. Это довольно распространенная проблема. По статистике Фонда Развития Интернет, более четверти российских школьников (28%) сталкивались со взломом аккаунта в социальных сетях.

Из письма довольно сложно установить причину произошедшего. Наиболее распространенные причины взлома аккаунта: использование простых паролей; неправильное хранение паролей; вход в аккаунт с чужого устройства; ввод пароля на поддельной страничке; действие вредоносных программ; передача пароля третьим лицам.

В этой ситуации для восстановления репутации школьнице **можно порекомендовать следующие действия:**

- сменить пароли к аккаунтам на других онлайн-ресурсах;
- удалить все неприятные сообщения со своей страницы;
- разместить на странице пост, разъясняющий причины произошедшего, извиниться перед читателями;
- постараться лично поговорить с самыми близкими друзьями и объяснить им ситуацию;

Чтобы избежать подобной проблемы, следует предпринять следующие шаги:

- использовать сложные пароли и двухэтапную систему аутентификации;
- установить антивирусные программы на все устройства, с которых осуществляется выход в интернет;
- соблюдать правила предосторожности при входе в аккаунт с чужого компьютера;
- соблюдать правила поведения при столкновении с поддельными страницами.

Пример №2.

В данном случае мы имеем дело с кибербуллингом – травлей, организованной с помощью электронных средств связи. По статистике Фонда Развития Интернет, каждый четвертый российский школьник (24%) сталкивался с оскорблениями, унижениями, преследованиями и обидами в сети. Из письма становится ясно, что одной из причин буллинга стала кража аккаунта и персональных данных, которые произошли из-за неосторожного входа в социальную сеть на чужом компьютере. В этой ситуации школьнику можно **порекомендовать следующие действия:**

- сменить пароль от аккаунта и временно его закрыть;

Написать в службу поддержки социальной сети письмо с просьбой удалить паблик, приложив скриншоты из самого паблика и из личной

переписки, подтвердив тем самым неправомерное использование личных данных одноклассником;

- если ситуация повторится, и после удаления будет создан новый паблик, написать в службу поддержки социальной сети письмо с просьбой удалить аккаунт пользователя, нарушившего правила пользования ресурсом;

- рассказать о ситуации взрослым (родителям или учителям) и попросить их вмешаться в ситуацию в школе.

Для того, чтобы избежать подобной проблемы в будущем, следует предпринять следующие шаги:

- использовать двухэтапную систему аутентификации;

- соблюдать правила предосторожности при входе в аккаунт с чужого компьютера;

- соблюдать осторожность в личной переписке в социальных сетях.

Пример №3.

В данном случае мы имеем дело с преследованием и шантажом, которые могут быть частью как буллинга, так и сексуальных домогательств. Из письма можно заключить, что причиной проблемы стала некоторая личная информация, которую автор письма сообщил шантажисту. В этой ситуации школьнице можно **порекомендовать следующие действия**:

- внимательно прочитать историю переписки и понять, какая персональная информация попала к шантажисту;

- внимательно изучить общие контакты и понять, какую информацию о школьнице шантажист мог узнать косвенно от третьих лиц, например прочитать на странице и в профилях друзей;

- рассказать или показать историю переписки взрослым (родителям, учителям), чтобы они могли предпринять действия по защите школьницы, вплоть до обращения в правоохранительные органы;

- в случае, если шантажист выйдет на связь, сообщить ему обо всех предпринятых действиях и добавить его в «черный список».

Чтобы избежать подобной проблемы, следует предпринять следующие шаги:

- с большой осторожностью добавлять незнакомцев в друзья и вступать с ними в переписку, даже если они являются друзьями друзей;

- не сообщать личную информацию незнакомцам. Даже если она кажется безобидной, она может быть легко использована против жертыв.

Пример №4.

В данном случае мы имеем дело со спамом – рассылкой коммерческой и иной рекламы или подобных коммерческих видов сообщений лицам, не выражавшим желания их получать. Как видно из письма, проблема, скорее всего, возникла после того, как школьник ввел свой номер телефона на сайте игры.

В этом случае необходимо обратиться к оператору, предоставляющему услуги сотовой связи, и подключить опцию «блокировка отправлений с

коротких номеров». Также это можно сделать самостоятельно в личном кабинете на сайте оператора.

Для того, чтобы подобные проблемы не повторялись вновь, важно не оставлять номер мобильного телефона на незнакомых сайтах и непроверенных онлайн-ресурсах.

Пример №5.

Мы имеем дело с «мошенничеством на доверии». По статистике ФРИ, каждый десятый российский школьник сталкивался с кражей денег в сети. Судя по письму, мошеннице удалось втереться в доверие к школьнице благодаря той личной информации, которую она могла узнать как от нее самой, так и из ее профиля в социальной сети. Как правило, «мошенники на доверии» действуют очень осторожно и ждут удобного случая, чтобы обмануть жертву. В данном случае школьница сама спровоцировала событие, рассказав «подруге» о своем желании приобрести игровой сет.

В такой ситуации помочь школьнице очень трудно. Доказать факт мошенничества и вернуть похищенное практически не возможно, так как деньги были переданы по собственному желанию и без давления со стороны. Единственный способ решения проблемы – это коллективное заявление в прокуратуру. В этом случае все пострадавшие лица должны собрать доказательства противоправных действий мошенницы (личная переписка, реквизиты платежей и т.д.). Можно поискать других жертв мошенницы в социальных сетях. Чем больше пострадавших подадут заявление, тем больше шансов призвать мошенника к ответственности.

Для того, чтобы подобные проблемы не возникали вновь, нужно:

- с большой осторожностью добавлять незнакомцев в друзья и вести с ними переписку;
- никогда не обсуждать с незнакомцами финансовые вопросы, например, касающиеся дорогих покупок или путешествий.

Выводы

Кода мы делимся информацией с окружающими нас людьми, то теряем над ней контроль, что может вызвать у нас чувство тревоги и дискомфорта. Выкладывая персональные данные в интернет, довольно часто мы не замечаем потери контроля – в этом и состоит основной риск неаккуратного обращения с личной информацией.

Любая персональная информация, выложенная в сеть, может стать причиной серьезных проблем. Наши фамилия, имя, номер телефона помогают хакеру подобрать пароль к нашему аккаунту, наши хобби, интересы и увлечения позволяют многое о нас узнать и использовать эти знания в своих целях. Поскольку мы не думаем об этом заранее, такая ситуация становится для нас досадной неожиданностью. Именно поэтому необходимо бережно относиться к персональным данным, попадающим в интернет.

Можно назвать три главные составляющие, обеспечивающие более или менее надежную защиту персональных данных:

- надежный пароль

- управление уровнями доступа к персональным данным (настройки приватности)

- сознательное отношение к информации, размещаемой в интернете.

Как вы видите, практически все рекомендации связаны с установкой надежных паролей. Поэтому предлагаю вам актуализировать и систематизировать свои знания по их созданию.

Оказывались ли вы в такой ситуации, когда у вас взламывали аккаунт в социальной сети ли электронный почтовый ящик? Что вы делали в таком случае?

- ответы обучающихся.

Предлагаю выслушать мнение профессионалов и посмотреть видеоролик «Правила безопасности от команды YouTube. Выбираем пароль» (htpp://www.YouTube.com/watch?v=QvOlgob5njQ/), в котором объясняются правила создания паролей.

После просмотра ролика акцентирует внимание участников на основных рекомендациях и используя «Правила составления надежных паролей».

Упражнение «Свой ключ всегда носи с собой».

Делимся на 5 команд. Каждая команда получает задание придумать – придумать свой уникальный алгоритм для создания и запоминания пароля.

Алгоритм должен отвечать трем требованиям:

- быть быстрым в использовании, создание пароля с его помощью должно быть быстрым и легким;

- позволять придумать не только надежный, но и легкий для запоминания пароль: чтобы его помнить, достаточно запомнить легко применимый для конкретного ресурса алгоритм;

- позволять легко придумывать уникальные (различные) пароли для разных сайтов (например, использовать части названия сайта или сервиса в самом пароле).

Командам раздается следующая опорная информация:

Алгоритм 1.

1. Выбираем любое прилагательное. Например, «зажаренный».
2. Выбираем любое существительное. Главное, чтобы это существительное логически не сочеталось с выбранным прилагательным. Например, «снежок».
3. Берем любую цифру, которую легко запомнить (любимую цифру, дату рождения, последние четыре цифры мобильного телефона и т.д.). Например, «1984»
4. Берем любой знак препинания. Например, «!»
5. Запишем выбранные слова, цифры и символы в одну строку без пробелов. Получится: «зажаренныйснежок1984!».

6. Поменяем в этой строке какую-нибудь строчную букву на прописную. Например, так: «Зажаренныйснежок1984!»

Алгоритм 2

Для того, чтобы пароль было легче запомнить, сделайте начало, середину или конец всех ваших паролей одинаковым. Например, «18H!p1n».

К этим символам добавьте части, которые ассоциируются с конкретным сервисом, дл которого этот пароль предназначен, например для почты – «mail». В результате получим: «18H!p1n mail».

Алгоритмы 3

В качестве пароля можно использовать словосочетание, которое известно только вам и имеет отношение к соответствующему сайту. Например, выбирая пароль для электронной почты, вы можете составить такую фразу: «Мой друг Вася 1 раз в день присылает мне смешные письма». Затем нужно ее транслитерировать и взять первую букву каждого слова. В результате получиться: «MdV1rvdpmsp». Угадать такую комбинацию невозможно. Поступайте так же, когда выбираете пароли для других сайтов.

Обсуждение

- Что труднее – придумать сложный пароль или запомнить его?
- Помогут ли представленные алгоритмы запомнить пароль и далее сохранять его в безопасности?
- Знаете ли вы какие-либо приемы, которые помогают защитить аккаунт от взлома помимо паролей?
- что вы будете делать, если ваш аккаунт взломают?

Итоги и выводы

Ключ от дома защищает наши ценности в реальном мире, а пароль защищает в мире виртуальном. Всегда используйте надежные пароли для всех своих аккаунтов в интернете и в мобильных приложениях. Один плохо защищенный аккаунт может стать причиной взлома остальных аккаунтов.

Особенно надежным должен быть пароль от электронной почты, который используется для регистрации на других ресурсах. Лучше всего его защитить с помощью процедуры двухэтапной аутентификации. В этом случае всегда можно будет использовать мобильный телефон для восстановления пароля и контроля за несанкционированным доступом к аккаунту.

Хороший пароль – это не только тот пароль, который трудно взломать, это еще и тот пароль, который легко запомнить. Использование различных приемов для шифрования и запоминания поможет вам создать хороший пароль. Аккаунты взламываются либо методом логического угадывания, либо методом простого перебора. Использование длинных паролей, включающих в себя бессмысленный для других людей набор букв, цифр и специальных символов значительно усложнит задачу злоумышленникам.

Берегите свои пароли: не храните их записанными на рабочем месте, не передавайте другим людям, не сохраняйте на чужих компьютерах, не вводите их на подставных страницах. Будьте бдительны, оберегая свои персональные данные.

Рефлексия занятия:

1. Что нового для себя сегодня узнали, что заинтересовало?
2. Какие выводы вы сделали?
3. Что понравилось/не понравилось на занятии?

Занятие 7.

Тема занятия: «Осторожно! Искусственный интеллект»

Цель: обсуждение вопросов, связанных с проблемой быстрого развития компьютерных технологий и понятием «искусственный интеллект»

Задачи:

-

Оснащение и методическое обеспечение урока: класс, оснащенный компьютерами, мультимедийный проектор, доска, карточки с заданиями для групповой работы, четыре маски с прорезями для глаз, ручки, тетради.

Ход урока.

Приветствие.

Добрый день, рада видеть вас сегодня на занятии. Предлагаю поприветствовать друг друга перед началом работы.

Упражнение «Приветствие» (см. конспект урока № 1).

Сегодня я предлагаю вам порассуждать над вопросами создания и развития искусственного интеллекта. Как вы думаете, актуальна ли эта тема сегодня? О чем беспокоятся ученые? О каких разработках в этом направлении вы слышали?

- ответы обучающихся.

На самом деле история искусственного интеллекта как нового научного направления начинается в середине XX века. К этому времени уже было сформулировано множество предпосылок его зарождения: среди философов давно шли споры о природе человека и процессе познания мира, нейрофизиологи и психологи разработали ряд теорий относительно работы человеческого мозга и мышления, экономисты и математики задавались вопросами оптимальных расчетов и представления знаний о мире в формализованном виде; наконец зародился фундамент математической теории вычислений – теории алгоритмов – и были созданы первые компьютеры.

Мы с вами помним, что первый компьютер был запущен в 1943 году. И уже через 13 лет Джон Маккартни (в 1956 году) на конференции в Дартмутском университете дал определение «Искусственного интеллекта». Он указывал, что проблема «искусственного интеллекта» состоит в том, что пока мы не можем в целом определить, какие вычислительные процедуры мы

хотим называть интеллектуальными. Мы понимаем некоторые механизмы интеллекта и не понимаем остальные. Поэтому под интеллектом в пределах этой науки понимается только вычислительная составляющая, способность достигать целей в мире.

Сегодня «Искусственный интеллект» это – с одной стороны, раздел науки и технологии создания интеллектуальных машин, особенно интеллектуальных компьютерных программ. С другой – это свойство интеллектуальных систем выполнять творческие функции, которые традиционно считаются прерогативой человека.

Возможности новых вычислительных машин в плане скорости вычислений оказались гораздо больше человеческих, поэтому вопрос: каковы границы возможностей компьютеров и достигнут ли машины уровня развития человека – не теряет своей актуальности уже много лет.

В 1950 году один из пионеров в области вычислительной техники, английский ученый Алан Тьюринг, пишет статью под названием «Может ли машина мыслить?», в которой описывает процедуру, с помощью которой можно будет определить момент, когда машина сравняется в плане разумности с человеком, получившую название Тест Тьюринга.

В чем заключается Тест Тьюринга?

Стандартная интерпретация этого теста звучит следующим образом: «Человек взаимодействует с одним компьютером и одним человеком. На основании ответов на вопросы он должен определить, с кем он разговаривает: с человеком или с компьютерной программой. Задача компьютерной программы ввести человека в заблуждение, заставив сделать неверный выбор».

Все участники теста не видят друг друга. Если судья не может сказать определенно, кто из собеседников является человеком, то считается, что машина прошла тест. Чтобы протестировать именно интеллект машины, а не ее возможность распознавать устную речь, беседа ведется в режиме «только текст», например с помощью клавиатуры и экрана (компьютера-посредника). Переписка должна производиться через контролируемые промежутки времени, чтобы судья не мог дать заключения, исходя из скорости ответов. Во времена Тьюринга компьютеры реагировали медленнее человека. Сейчас это правило тоже необходимо, потому что они реагируют гораздо быстрее, чем человек.

Предлагаю вам воссоздать этот эксперимент и посмотреть, сложно ли нам будет отгадать кто перед нами, с кем мы общаемся: с человеком или компьютером.

Упражнение «Тест на искусственный интеллект»

Для начала мне нужны четверо добровольцев.

Добровольцы ненадолго выходят из класса вместе с ведущим. Ведущий распределяет роли: двое будут выступать в роли «человека», двое – в роли «компьютера» (участники просто тянут жребий или карточки с уже прописанными инструкциями для «человека» и для «компьютера»). Все одевают маски. Ведущий оставляет их готовиться.

Карточка 1

(инструкция для первого добровольца, выполняющего роль «компьютера»)

Через несколько минут вам нужно будет надеть маску, войти в класс, сесть за компьютер, аккуратно положить инструкцию перед монитором и ответить письменно на пять вопросов аудитории. отвечайте на вопросы репликами из предложенного списка. подбирайте ответы, максимально совпадающие с вопросами. ответы вы будете печатать, их все увидят на доске. Ни в коем случае не разговаривайте и постарайтесь вести себя бесстрастно!

Ответы компьютера:

Затрудняюсь ответить.
Бесспорно, вы правы.
Работаю с утра до вечера.
Живу я долго и счастливо.
Не знаю, что ответить.
Это не главное.
Все потом объясню.
Да, я все умею.
Зовут меня Катя.
Где бы то ни было.
Спроси эксперта.
Время покажет.
Я бы хотел, чтобы вы сами ответили на этот вопрос.

Карточка 2

(инструкция для второго и третьего добровольцев, выполняющих роль «человека». Необходимо подготовить два экземпляра инструкции. Инструкции для «человека» и для «компьютера», желательно, должны быть на листах одного формата и размера)

Через несколько минут вам нужно будет надеть маску, войти в класс, сесть за компьютер, аккуратно положить инструкцию перед монитором и ответить письменно на пять вопросов аудитории. Отвечайте как пожелаете, ответы вы будете печатать, их все увидят на доске. Ни в коем случае не разговаривайте и постарайтесь вести себя бесстрастно!

Карточка 3

(инструкция для четвертого добровольца, выполняющего роль «компьютера»)

Через несколько минут вам нужно будет надеть маску, войти в класс, сесть за компьютер, аккуратно положить инструкцию перед монитором и ответить письменно на пять вопросов аудитории. отвечайте на вопросы репликами из предложенного списка. подбирайте ответы, максимально совпадающие с вопросами. ответы вы будете печатать, их все увидят на доске. Ни в коем случае не разговаривайте и постарайтесь вести себя бесстрастно!

Ответы компьютера:

Это для меня трудный вопрос.
Конечно, я с вами согласен.
А ты что делаешь?
Сколько ни есть – все мои.
Это несущественно.
Да не волнуйся, все будет хорошо.
Как часто вы бываете непонятливы?
А ты что юзаешь?
Меня зовут просто – Костя.
Где бы то ни было.
Думаю, Эйнштейн бы тебе с удовольствием на это ответил.
Поживем – увидим.
А ты?

Ведущий возвращается к остальным участникам и рассказывает, что им предстоит угадать, с кем они будут разговаривать – с человеком или с компьютером.

Добровольцы по одному заходят в комнату и садятся за компьютер. Участники могут задать каждому добровольцу по пять любых вопросов, на которые доброволец отвечает, набирая ответ на компьютере. Ответ должен выводиться на экран. Для круга вопросов есть ограничения: нельзя задавать прямые вопросы, например: «Ты – компьютер?» или «Ты – человек?». Вопросы должны имитировать обычную беседу. Задача участников – определить, когда на вопросы отвечает «человек», а когда «компьютер».

В случае отсутствия возможности вывода набираемого текста на экран для всех участников, упражнение проводится в устной форме. В этом случае добровольца лучше сажать за ширму.

Добровольцы заходят по одному в комнату, отвечают на вопросы участников и уходят. После того, как все добровольцы ответили на вопросы, остальные участники путем голосования решают, в каком случае они общались с «компьютером», а когда, по их мнению, на вопросы отвечал «человек» (каждый участник высказывает свое мнение о подсчитывается процент голосов в пользу «человека» и в пользу «компьютера», если «компьютер» набирает большее количество голосов как «человек», то он победил). Ведущий записывает результаты голосования на доске и приглашает добровольцев, которые сообщают участникам, какую роль они исполняли: «компьютера» или «человека».

Обсуждение:

- Трудно ли было отличить «человека» от «компьютера»?
- По каким признакам вы отличали ответы «компьютера» от «человека»?
- Как вы думаете, можно ли создать искусственный интеллект, который заменит интеллект человека?
- Вы в своей жизни в сети сталкивались с искусственным интеллектом? (Боты)
- Догадывались ли вы, что общаетесь с компьютером?

- Как вы думаете зачем и почему это делают?

- Будет ли искусственный интеллект способен к полноценному мышлению и творчеству? Кем предстоит ему стать – помощником или соперником человеческого разума?

Следует также отметить, что сегодня ученые и разработчики компьютерных программ неоднозначно относятся к Тесту Тьюринга. Дело в том, что искусственный интеллект в большей своей степени относится к системе «правильной логики», человеческий же интеллект он алогичен, непредсказуем в некоторых случаях (в некоторых случаях человек поступает заведомо неправильно исходя из каких-то причин и обстоятельств). Поэтому, если развивать искусственный интеллект с целью улучшения выполнения отдельных функций, то он будет превосходить человеческий интеллект в решении вопросов и выполнении задач. Если же работать над тем, чтобы компьютер смог «обмануть» человека и продемонстрировать «человеческий интеллект», то его нужно учить обманывать. И сам по себе результат не удовлетворит исследователей, потому что компьютер работал снова по программе, созданной человеком, он не чувствовал, не переживал. Отдельным вопросом в поведении человека стоит «интуиция» и как этому научить компьютер, если люди сами еще досконально не разобрались что это такое.

На сегодняшний день ни одна машина не может даже близко подойти к тому, чтобы пройти тест Тьюринга, хотя некоторые из них весьма неплохо работают в узких областях. Предположим, тем не менее, что в один прекрасный день машина все-таки сможет пройти тест Тьюринга. Будет ли это означать что она разумна и обладает интеллектом?

Джон Сирл, преподаватель философии Калифорнийского университета в Беркли, разработал воображаемую систему, которая показывает, что машина не сможет считаться разумной. Эта система по названием «Китайская комната» работает следующим образом. Вы сидите в комнате. В стен этой комнаты есть две щели. Через первую щель вам передают вопросы, написанные по-китайски (предполагается, что участники не знают китайского языка, если это не так, то необходимо выбрать другой язык). Затем вы просматриваете книги с инструкциями типа: «Если вы получили такой-то

набор символов, напишите на листке бумаги такой-то (отличный от исходного) набор символов и передайте его обратно через другую щель».

Ясно, что, если книги с инструкциями исчерпывающи, «машина», состоящая из вас и комнаты, сможет пройти тест Тьюринга. При этом очевидно, что вам совсем не обязательно понимать, что вы делаете. По мнению Сирла, это показывает, что даже если машина прошла тест Тьюринга, это еще не значит, что она разумна и обладает интеллектом.

В последнее время многие ученые отмечают, что темп технологического развития человечества ускоряется. В перспективе это можетпривести к возникновению так называемой «технологической сингулярности» - момента, после которого научно-технический прогресс станет настолько сложным и быстрым, что станет недоступен для осмысления силами одного человеческого интеллекта. В качестве предпосылок достижения этого момента ученые указывают:

- появление вычислительных машин, превосходящих интеллектом человека;
- развитие глобальных компьютерных сетей, в результате чего все пользователи этих сетей станут частью единого «сверхинтеллекта»;
- развитие связи человека и компьютера до такой степени, когда они образуют единое существо.

Сторонники данной концепции утверждают, что предсказать последствия наступления технологической сингулярности современными методами мышления невозможно. Можно лишь сказать, что личностная и социальная идентичность человека может измениться до неузнаваемости.

Выводы.

Рефлексия занятия:

1. Что нового для себя сегодня узнали, что заинтересовало?
2. Какие выводы вы сделали?
3. Что понравилось/не понравилось на занятии?

Занятие 8.
Тема занятия: «Алгоритм соблюдения технической безопасности при использовании Интернет»

Цель: разработка алгоритма технической безопасности при использовании Интернет.

Задачи:

- определение и закрепление алгоритмов безопасного использования сети Интернет.

Оснащение и методическое обеспечение урока: класс, оснащенный компьютерами, мультимедийный проектор, доска, ручки, тетради.

Ход урока.

Приветствие.

Добрый день, рада видеть вас сегодня на занятии. Предлагаю поприветствовать друг друга перед началом работы.

Упражнение «Приветствие» (см. конспект урока №1).

Сегодня наше занятие посвящено закреплению алгоритмов безопасного использования Интернет.

Вам было дано задание разработать свои проекты по безопасному использованию Интернет. Сегодня каждая группа защищает свои проекты. Все остальные участники могут внимательно слушать, дополнять, задавать вопросы.

Защита проектов обучающимися.

Обсуждение, выводы.

Рефлексия занятия:

1. Что нового для себя сегодня узнали, что заинтересовало?
2. Какие выводы вы сделали?
3. Что понравилось/не понравилось на занятии?

Занятие 9.

Тема занятия: «Интернет как источник информации: польза или вред?»

Цель: знакомство обучающихся с видами и формами информации, представленными в Интернете, видами позитивного и негативного контента, а также способами борьбы с вредоносным контентом.

Задачи:

- определение и закрепление алгоритмов безопасного использования сети Интернет.

Оснащение и методическое обеспечение урока: класс, оснащенный компьютерами, мультимедийный проектор, доска, ручки, тетради.

Ход урока.

Приветствие.

Добрый день, рада видеть вас сегодня на занятии. Предлагаю поприветствовать друг друга перед началом работы.

Упражнение «Приветствие» (см. конспект урока №1).

Мы с вами уже обсуждали много разных вопросов, касающихся Интернета, а сегодня я хотела бы с вами обсудить такую проблему как «Что же такое интернет: польза или вред?»

Упражнение «Убеди меня».

Давайте представим с вами ненадолго, что я человек, который никогда не пользовался Интернетом. Я много про него слышала, но сомневаюсь, что в Интернете есть что-либо интересное и полезное. А ваша задача – меня в этом переубедить. Но аргументы не должны повторяться и должны начинаться с фразы: «В Интернете вы можете найти…».

Итак, я отправляю вам мяч с фразой: «Мне кажется, в Интернете нет ничего интересного и полезного!».

(Далее ведущий бросает мяч кому-либо из участников. Поймавший игрушку приводит аргумент в пользу Интернета, начиная со словами: «В Интернете вы можете найти…», и перекидывает мяч ведущему. Ведущий бросает мяч следующему участнику и т.д. Игра заканчивается, когда все участники привели свои аргументы.)

При желании ведущий может записывать аргументы обучающихся на доске для дальнейшего обсуждения. Подводя итоги, ведущий резюмирует, удалось его убедить в пользе Интернета или нет, и объясняет почему.

Обсуждение.

Легко ли было придумать аргументы, чтобы переубедить меня?

Часто ли вы сами ищите и пользуетесь той информацией, о которой говорилось в ходе упражнения?

Вы знакомы со всеми названными возможностями? Что из перечисленного вы любите больше всего?

Как вы думаете, можно ли обойтись без интернета в Повседневной жизни?

В XXI веке знания и информация становятся все более значимыми факторами, определяющими вектор развития современного общества. многие ученые, политические деятели, экономисты, педагоги и все, кто задумывался о вопросах общественного устройства мира, сходятся во мнении, что на смену постиндустриальному идет информационное общество. Его отличительные черты:

- увеличение роли информации и знаний в технологической, социальной, политической, экономической и культурной сферах жизни;
- интенсивное развитие средств для хранения, распределения и использования информации;
- создание глобального информационного пространства, определяющего доступ к мировым информационным ресурсам и обеспечивающего интенсивный обмен информацией;
- усиление влияния средств массовой информации.

Объем информации, которую обычный человек в XVIII веке воспринимал за целую жизнь, сегодня соответствует информации в ленте крупного новостного портала всего за 2-3 дня. Для записи информации, которая появляется в сети каждый час, потребуется около 7 млн DVD -дисков. На популярном видеохостинге в YouTube ежеминутно появляется более 100 часов видео – это, как если бы Голливуд выпускал около 260000 новых полнометражных фильмов каждую неделю. За один только 2012 год было создано и передано количество информации, равное 2800000000000000000000 байт. Это огромное число соответствует 2,8 млрд гигабайт или 2,8 зеттабайт. Для того, чтобы попытаться как-то осмыслить эти масштабы, представим, что каждый байт – это одна песчинка. Так вот, 2,8 зеттабайт – это в 57 раз больше, чем песчинок на всех пляжах мира. Вся эта информация хранится в

Глобальной Сети более чем на 650 млн сайтах, каждый из которых представляет структурированный набор файлов, размещенных на специальном языке. В Рунете к концу 2012 года было уже более 5 млн сайтов.

Представители индустрии информационных технологий считают, что человечество производит информацию в цифровом виде такими быстрыми темпами, что скоро ее негде будет хранить. По ожиданиям аналитиков в области информационных технологий, в 2014 году придется работать с таким объемом данных, что уже сейчас следует вводить новые единицы измерения – человечество собирается вступать в Йоттабайтную эру.

По данным Фонда Развития Интернет, для российских подростков Глобальная сеть – главный источник информации, и в этом смысле Интернет серьезно конкурирует с учителями, друзьями и даже родителями.

При попытке классифицировать информацию в Интернете возникают большие сложности в силу ее многогранности и разнообразия. Специалисты в области информационных технологий, анализируя контент в Интернете, пытаются найти ответы на три основных вопроса.

- Какая информация есть в интернете?
- В какой форме она подается и хранится?
- Кто предлагает эту информацию?

Информационные ресурсы в Интернете можно разделить на четыре категории.

1. **Информационные сайты**. Интернет изначально создавался как среда для обмена информацией, поэтому данная категория основная и является наиболее крупной. Среди информационных сайтов по характеру представляемого контента можно выделить информационно-тематические, новостные, развлекательные сайты, сайты библиотеки, сайты-базы, например, базы рефератов, разнообразные сайты-справочники, онлайн-энциклопедии и словари, сайты-каталоги, обобщающие информацию о других сайтах и т.п. по тематике информационные сайты хорошо каталогизированы, например, в «Яндекс-каталоге». В нем представлены следующие категории информационных ресурсов: развлечения, СМИ, дом, Hi-Tech, отдых, справки, работа, производство, спорт, общество, учеба, авто, игровая, порталы, культура, бизнес. В специальном каталоге «Яндекса» для школьников существуют следующие категории: учеба, музыка, технологии, спорт, развлечения, каникулы, игры, культура.
2. **Онлайн-сервисы**. К данной категории относятся поисковые системы, почтовые сервисы, хостинги, файлообменники, а также сайты для общения: форумы, блоги, чаты, доски объявлений, социальные сети, сервисы «вопрос-ответ», сайты знакомств, биржи фрилансеров и др.
3. **Сайты электронной коммерции**. Сюда входят в первую очередь интернет-магазины, сайты электронных платежных систем, сайты банков и системы онлайн-банкинга.

4. **Интернет-представительства**. Сюда входят как личные странички отдельных пользователей, так и официальные сайты органов государственной власти и различных организаций

По форме, способам представления, способам кодирования и хранения информацию в Сети можно разделить на текстовую, визуальную (фото, графики) аудиальную (звук) и аудиовизуальную (видео). Некоторые ресурсы в Интернете в большей степени ориентированы на тот или иной тип контента (музыкальные порталы, видеохостинги, текстовые хранилища). Но современные технологии, построенные на принципе интерактивности, позволяют задействовать при передаче информации все ее доступные формы.

В зависимости от того, кто является источником информации, сетевой контент условно делят на два типа:

- **профессиональный контент** – данный тип создается СМИ и другими профессиональными производителями контента.

- **любительский контент** – к данному типу контента относятся записи в блогах, форумах, комментариях к сообщениям на сайтах СМИ, записи на персональных страницах в социальных сетях, созданный потребителем фото-, видео- и аудиоконтент, Интернет-ресурсы, созданные самими пользователями.

Предлагаю вам несколько обобщить ваши знания об информации, представленной в интернете и выполнить упражнение **«Киберфанаты против киберскептиков».**

Ведущий раздает участникам листочки с клейким краем: по три – одного цвета и по три – другого (например, красного и зеленого). Затем он просит участников написать на зеленых листочках, какая информация в Интернете, по их мнению, является полезной и нужной, а на красных – какая информация может быть вредной, негативной или опасной. На выполнение этого задания дается 5 минут. Затем ведущий проводит на доске вертикальную линию, которая делит пространство пополам. Левая половина доски сверху обозначается знаком «+» (позитивный контент), а правая – знаком «-» (негативный контент). Участники должны подойти к доске и приклеить свои листочки, на которых обозначена полезная информация в Интернете, на половину доски. Отмеченную «+», а листочки, на которых обозначена негативная информация, - на половину доски, отмеченную «-«. После этого все садятся на места, и ведущий предлагает обсудить полученный результат. Как правило, школьники легче и активнее обсуждают позитивную информацию, которую они находят в Интернете.

Обсуждение.

- Что было легче вспомнить: полезные или вредные виды информации в Интернете?

- Чем «позитивная» сторона доски отличается от «негативной»? Почему?

- хотели бы вы что-то еще добавить на доску или изменить что-то на ней? Почему?

Затем ведущий озаглавливает левую половинку доски со знаком «+» - «Киберфанаты», а правую, со знаком «-« - «Киберскептики». Он объясняет, что киберфанаты – это большие поклонники и защитники Интернета, считающие, что он дает много возможностей пользователям, а киберскептики – те, кто могут покритиковать Интернет и считают, что в Сети много негативной информации, которая легкодоступна и оказывает плохое влияние на людей. Он просит каждого из участников выбрать для себя наиболее подходящую группу и подойти к соответствующей половине доски. (Если случится так, что фанатов будет больше или будут только фанаты, то применить жребий и сформировать таким образом и вторую группу).

Обсуждение.

- Почему киберфанатов получилось больше, чем киберскептиков (или наоборот)?

- Как вы думаете, кого в мире больше: киберфанатов или кибескептиков? Почему?

Далее, собравшиеся в группы участники получают задания: киберфанаты – проанализировать все листочки с позитивной информацией, киберскептики – с негативной.

Задача каждой группы состоит в том, чтобы проанализировать информацию на своей стороне доски и сформулировать пять основных аргументов в пользу своей позиции. Ведущий предлагает участникам в группах:

- подсчитать количество повторяющихся ответов;

- классифицировать все ответы и выдать 5-7 категорий;

- дополнить результаты на доске, если, по мнению группы, на ней не хватает каких-то важных категорий. На выполнение этих заданий группам дается около 10 мин.

Затем группам предоставляется возможность защитить свою позицию в дискуссии, которая проводится в форме дебатов. Каждая группа по очереди приводит свои аргументы. От каждой группы в дебатах участвует по одному представителю, остальные помогают ему и подсказывают. Ведущий выступает модератором дебатов и следит за тем, чтобы аргументы были конструктивными и не повторялись. Выступления представителей групп и получившиеся классификации позитивной и негативной информации обсуждаются классом.

Затем ведущий выводит на доску таблицы результатов Всероссийского исследования «Оценка школьниками позитивных и негативных сторон Интернета» (проведенного ФРИ в 2013г.) и предлагает участникам сопоставить результаты.

«Оценка школьниками позитивных и негативных сторон Интернета»

Обсуждение:

- На основании каких критериев можно оценить информацию в Интернете как полезную и как вредную?
- Какие существуют способы защиты от негативной информации в Сети?
- Какая позитивная информация может помочь в борьбе с негативной?
- Совпадают ли полученные категории с данными Всероссийского исследования «Дети онлайн» ?

Рефлексия занятия:

- Узнали ли вы что-то новое о видах информации, представленной в Интернете?

- Узнали ли вы что-то новое о возможностях получения информации в Интернете?

Занятие 10.

Тема занятия: «Информационная и медиакомпетентность»

Цель: изучение основных компонентов информационной и медиакомпетентности.

Задачи:

- проанализировать потребность человека в получении информации;
- проанализировать важность управления информацией и информационными потоками;
- получить представление о информационной и медиакомпетентности, ее основныхкомпонентах.

Оснащение и методическое обеспечение урока: класс, оснащенный компьютерами, мультимедийный проектор, доска, ручки, тетради.

Ход урока.

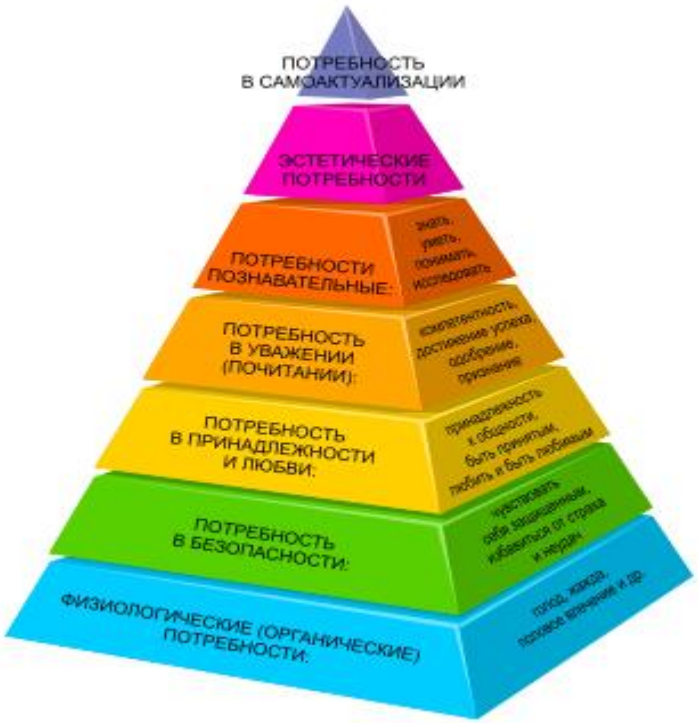
Приветствие.

Добрый день, рада видеть вас сегодня на занятии. Предлагаю поприветствовать друг друга перед началом работы.

Упражнение «Приветствие» (см. конспект урока №1).

Всю первую четверть мы посвятили изучению технической компетенции в рамках информационной компетентности. Теперь мы переходим к изучению новой веточки нашего дерева компетенций - информационной и медиакомпетентности.

Обратим наше внимание на то, что потребность человека в информации – одна из базовых потребностей человека. Пирамида потребностей, представленная Абрахамом Маслоу демонстрирует нам следующее:



Познавательные потребности находятся в верхней половине пирамиды, приближающейся к верхушке, и обозначаются уже не как потребности «нужды», а как потребности «роста».

Современный человек, у которого удовлетворены базовые потребности в еде, тепле, комфорте и безопасности, стремится к удовлетворению более высоких потребностей – в любви, внимании, признании, в самореализации и личностном росте. Зачастую, перечисленные потребности мы стремимся реализовать в Интернете. Если общение в Интернете нередко создает лишь иллюзию удовлетворения потребности в любви и принятии, то в реализации познавательной потребности – жажды знаний и желания воспринимать как можно больше информации – Интернет играет сегодня ключевую роль.

В процессе информационной социализации реализуется два основных типа информационных потребностей: конкретные, состоящие в стремлении получить определенную информацию по какой-либо заданной теме, и общего плана, обусловленные присущей человеку любознательностью и заключающиеся в его стремлении быть в курсе всего, что происходит в мире. В ситуации активной вовлеченности в интернет-среду, информация, которую получают подростки в процессе обучения в школе, нередко перебивается мощным информационным онлайн-потоком, удовлетворяющим их любознательность в самом широком диапазоне. Таким образом, эти два типа потребностей пересекаются, сталкиваются и конфликтуют.

Необходим значимый взрослый (родитель, педагог, наставник), который сможет нас вести в этом информационном потоке, который сможет научить воспринимать, анализировать информацию и продуктивно работать в информационном поле.

Почему важно учиться управлять информацией и информационными потоками?

Сегодня даже взрослые люди, не говоря уже о подростках, с трудом справляются с тем, чтобы воспринять, осмыслить и как-то оценить всю ту информацию, которая непрерывно обрушивается на современного человека. Колоссальный поток данных заставляет пользователей потреблять контент на бегу, урывками, в надежде узнать все новости и события. Естественным следствием подобного хаотичного и беспрерывного «поглощения» информации становится информационная перегрузка. Проблема сложности принятия решения в условиях переизбытка информации возникла уже во второй половине прошлого века. В своей книге «Шок будущего», мгновенно ставшей бестселлером в 1970-х годах, социолог и футуролог Элвин Тоффлер, подчеркивая ускоряющийся темп изменений в обществе, впервые обратил внимание широкой общественности на проблему информационной перегрузки. Он описал симптомы вызванного ею информационного стресса, который по мнению Тоффлера, является естественной человеческой реакцией на чрезмерную стимуляцию. На когнитивном уровне чрезмерная стимуляция приводит к снижению способности отбирать, оценивать и запоминать информацию.

Обратим внимание, что вопрос был поднят задолго до возникновения Интернета. Ученых уже тогда беспокоили темпы роста количества информации. Но если до XX века ее объемы удваивались каждые 50 лет, то с середины XX века удвоение информации начало происходить каждые десять лет. Темпы со временем стали только нарастать: 1970-х годов удвоение происходило каждые пять лет, а с 1990-х – уже ежегодно. Наиболее значительный скачок в ускорении роста количества информации произошел с появлением Интернета. Ученые считают, что информационные перегрузки ослабляют способность людей думать, приводят к снижению творческого потенциала, появлению острого дефицита времени. Как это ни парадоксально, но, в ситуации перенасыщения информацией человек может даже испытывать информационный голод. Избыток информации приводит к невозможности ее охватить, выделить нечто важное, потребление информации становится все более фрагментарным и обрывочным.

В 1960-х годах Джеймс Миллер провел серию исследований о влиянии информационной перегрузки на человека, сообщества и социальные институты. Результаты показали, что с возрастающим объемом информации возможно справляться лишь до определенного предела, после которого ресурсы человека исчерпываются. Чтобы справиться с перегрузкой человек прибегает, осознанно или не осознанно, к различным защитным механизмам. Миллер выделил семь стратегий преодоления информационной перегрузки:

1. Бездействие – произвольная временная остановка обработки информации.
2. Ошибочная обработка информации.
3. Выбор очередности – откладывание обработки некоторых видов информации в надежде вернуться к ним позднее.
4. Фильтрация – пренебрежение некоторыми видами информации во время обработки других, более приоритетных.

5. Приблизительная точность – за счет снижения точности обработки информации увеличивается скорость.
6. Множественная обработка – распределение процессов обработки информации , если это представляется возможным.
7. Избегание – уход от решения задач, связанных с обработкой информации.

В наши дни важным становится не только вопрос о сохранении личности под влиянием нарастающего информационного потока, но и формирование индивидуальной культуры потребления информации. Ученые пытаются изучить эти процессы. Так, например, в самом начале XXI века появился термин «эгокастинг» (от англ. Egocasting), суть которого состоит в формировании каждым человеком индивидуальной матрицы потребления информации. Кристен Розен, автор этого термина, использовала его, чтобы отразить стремление человека потреблять медийный контент по запросу, отражающему индивидуальный, а не массовый вкус.

Проведем с вами маленький эксперимент. У каждого из вас есть компьютер с выходом в Сеть, вам необходимо найти информацию и подготовить доклад на тему: «Жизнь и творчество Леонардо да Винчи». Воспользуйтесь выходом в Интернет и осуществите поиск информации, но дайте свой запрос самостоятельно, без совета с соседями.

Далее необходимо сверить ту информацию, которую нашли дети, какие сайты открылись, с какой информацией и т.д. (как правило они не будут одинаковыми, доклад писать конечно же на уроке не будем).

Это упражнение нам продемонстрировало фрагмент построения персональной информационной вселенной.

На построение персональной информационной вселенной нацелены многие социальные сервисы Интернета. Помимо задач доставки пользователю релевантной информации, в первую очередь – коммерческой, решается также задача ограничения его от избыточного информационного потока. Этот феномен достаточно подробно описан в книге Эли Паризера "За стеной фильтров. Что Интернет скрывает от нас?». По мнению автора, Интернет анализирует всю совокупность личных данных пользователей, например время, которое тратиться на выбор того или иного результата, место подключения к Сети, степень внимательности при прочтении той или иной книги, людей, которым уделяется больше внимания. На этой основе строится «стена» фильтров и создается персональный информационный мир для каждого пользователя. На первый взгляд, это выглядит заманчиво, но есть опасность пропустить что-то действительно важное, остаться в определенных рамках, ведь мы не знаем, за кого нас принимает тот или иной сервис и какую информацию он решает нам показать, а какую – нет. Тем не менее, колоссальные темпы роста информационной продукции не оставляют нам выбора: Интернет движется в сторону персонализации и становится личным информационным агентом, не только для взрослых, но и для детей.

В связи с чем очень важно грамотно сформировать свои информационные приоритеты: необходимые в современном мире навыки

поиска, хранения, обработки, распределения информационных потоков и передачи информации.

Особое значение приобретает информационная культура пользователя, основу для ее формирования составляет информационная компетентность, не обладая которой невозможно стать полноценным цифровым гражданином.

Довольно часто, когда речь идет об умении эффективно и безопасно использовать современные интернет-технологии, используются понятия «информационная грамотность» и «медиаграмотность». Эти два вида грамотности – важнейшие составляющие цифровой компетентности.

Впервые понятие «информационная грамотность» было использовано в 1977 году в США. Ведущая роль в разработке и популяризации этого понятия принадлежит библиотекарям. Так, наиболее часто цитируется и используется определение Американской библиотечной ассоциации: «Быть информационно грамотным означает, что человек способен понять востребованность информации и может ее найти, оценить и эффективно использовать».

В Александрийской декларации 2005 года «Об информационной грамотности и образовании на протяжении всей жизни» информационная грамотность рассматривается как важный элемент конкурентной способности в современном обществе. Она включает умение осознавать информационные потребности, находить, оценивать, применять и создавать информацию в культурном и социальном контексте, а также критически воспринимать ее и интерпретировать.

Появившееся позже понятие медийной грамотности связано прежде всего с огромным влиянием средств массовой информации на человека и с теми специальными знаниями и навыками, которые необходимы для адекватного использования любого вида СМИ. По мнению специалистов, в области медиапедагогики, понятие «медийная грамотность» включает:

- умение критично воспринимать медиатексты и «читать» их язык;
- постоянно совершенствующие умения использовать зрительную память, воображение;
- различные виды мышления (логическое, критическое, образное, творческое, интуитивное);
- умение понимать идеи (нравственные, философские, политические и т.д.) и образы.

Таким образом, информационная грамотность подчеркивает важность доступа к информации, важность ее оценки и этичного использования, а медийная грамотность делает акцент на способности понимать функции медиа, оценивать качество их выполнения и эффективно использовать медиа в интересах самовыражения.

Компетентность в области информационной и медиакомпетентности позволяет людям более широко использовать свои фундаментальные права, в частности право, предусмотренное ст. 19 «Всеобщей декларации прав человека», которая гласит: «Каждый человек имеет право на свободу убеждений и свободное выражение их; это право включает свободу

беспрепятственно придерживаться своих убеждений и свободу искать их, получать и распространять информацию и идеи любыми средствами и независимо от государственных границ». Соответствующая статья есть и в Конституции Российской Федерации, согласно которой «Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом» (гл. 2, ст. 29).

Исходя из вышесказанного, мы будем понимать следующее:

Информационная и медиакомпетентность это – знания, умения и навыки, мотивация, ответственность, связанные с поиском, пониманием, организацией, архивированием цифровой информации и ее критическим осмыслением, а также с созданием информационных объектов с использованием цифровых ресурсов (текстовых, изобразительных, аудио и видео и т.д.).

Информационную и медиакомпетентность можно определить, как способность и готовность:

- осознавать личные информационные потребности;
- проводить эффективный поиск информации в Интернете и работать с информационными потоками;
- объективно оценивать точность и надежность информации, представленной в Интернете;
- интерпретировать и анализировать найденную в Интернете информацию;
- ответственно и безопасно использовать информацию в Интернете для достижения необходимого результата;
- использовать информацию в Интернете этично, в соответствии с правами ее авторов, а также осознавать собственные права, связанные с созданием и распространением контента в Сети.

Предлагаю вам обсудить вышеперечисленные пункты (обсуждение с классом)

- Как вы понимаете эти утверждения?
- Что это для вас они значат?

Информационная компетентность – это часть информационной культуры. В рамках этого понятия особенный упор делается на творческом и критическом подходе к использованию информации личностью в целях решения задач, возникающих в учебной, профессиональной или иной деятельности. Суть новой информационной культуры четко выразил Элвин Тоффлер «В XXI веке безграмотным считается уже не тот, кто не умеет писать и читать, а тот, кто не умеет учиться, доучиваться и переучиваться».

Выводы.

Рефлексия занятия:

- Что нового сегодня узнали?
- Что показалось интересным
- О чем ранее не знали, не слышали?