

Муниципальное бюджетное общеобразовательное учреждение
основная общеобразовательная школа с.Юнны
муниципального района Илишевский район Республики Башкортостан

«Согласовано»

Заместитель директора по УВР

Г.Х. Рахматуллина /Рахматуллина Г.Х./

17.08.2022 г.

«Утверждаю»

Директор Ф.А. Миннигулова /Миннигулова Ф.А./

Приказ №125

от 17.08.2022



Рабочая программа внеурочной деятельности
“Медиабезопасность в сети Интернет”
для 7 класса

Составитель : Насруллина Зиля Аскатовна
учитель информатики

Пояснительная записка

Программа межпредметного курса внеурочной деятельности «Безопасность в сети Интернет» адресована учащимся 7 классов. Она разработана на основе учебного плана внеурочной деятельности МБОУ ООШ с.Юнны. Программа разработана с учетом требований законов Российской Федерации: «Об образовании в Российской Федерации», «О защите детей от информации, причиняющей вред их здоровью и развитию» и «Санитарно-эпидемиологических требований к условиям и организации обучения в общеобразовательных учреждениях». Программа учитывает требования, выдвигаемые федеральным государственным образовательным стандартом основного общего образования.

Основными целями изучения курса «Безопасность в сети Интернет» являются:

- обеспечение условий для профилактики негативных тенденций в информационной культуре учащихся, повышения защищенности детей от информационных рисков и угроз;
- формирование навыков своевременного распознавания онлайн-рисков (технического, контентного, коммуникационного, потребительского характера и риска интернет-зависимости).

Задачи программы:

Образовательные:

1. способствовать формированию знаний о безопасном поведении при работе с компьютерными программами, информацией в сети Интернет;
2. формировать умения соблюдать нормы информационной этики;
3. формировать умения безопасной работы с информацией, анализировать и обобщать полученную информацию.

Развивающие:

1. развивать компьютерную грамотность информационную культуру личности в использовании информационных и коммуникационных технологий;
2. развивать умение анализировать и систематизировать имеющуюся информацию;
3. развивать познавательную и творческую активность в безопасном использовании информационных и коммуникационных технологий;

Воспитательные:

1. способствовать выработке сознательного и бережного отношения к вопросам собственной информационной безопасности;
2. способствовать формированию и развитию нравственных, этических, патриотических качеств личности.
3. стимулировать поведение и деятельность, направленные на соблюдение информационной безопасности.

Актуальность программы «Безопасность в сети Интернет» заключается в исследовании проблем безопасности детей и подростков в сети Интернет, в связи с бурным развитием IT-технологий и со свободным использованием детьми и подростками современных информационно - коммуникационных технологий (Интернет, сотовая (мобильная) связь).

Отличительной особенностью программы является то, что она способствует разностороннему раскрытию индивидуальных способностей учащихся, развитию у них интереса к различным видам деятельности, желанию активно участвовать в практической деятельности, используя различные сетевые формы общения (социальные сети, игры, пр.), мотивации ответственного отношения к обеспечению своей личной безопасности, безопасности своей семьи и своих друзей.

Программа учебного курса внеурочной деятельности «Безопасность в сети Интернет» рассчитана на 34 часа, 1 час в неделю.

В процессе реализации программы используются следующие формы работы:

- групповая,
- индивидуальная,
- индивидуально - групповая (3-5 человек).

Занятия проводятся в комбинированной, теоретической и практической форме:

- теоретические занятия: основы безопасного поведения при работе с компьютерными программами, информацией в сети интернет, изучение терминов, беседы, лекции;
- практические занятия: работа с мобильными устройствами; закупки в интернет магазине; квесты; создание буклетов и мультимедийных презентаций.

Содержание программного материала, как в теории, так и на практических занятиях составлено с учётом возрастных особенностей обучающихся, весь материал построен по принципу от простого к сложному.

Практические работы в содержании программы, возможно, использовать в качестве вариативных, индивидуальных практических заданий разного уровня углубленности, доступности и степени сложности исходя из диагностики и стартовых возможностей каждого из участников рассматриваемой программы.

Планируемые результаты:

Предметные:

- 1 Сформированы знания о безопасном поведении при работе с компьютерными программами, информацией в сети интернет;
- 2 Сформированы умения соблюдать нормы информационной этики;
- 3 Сформированы умения безопасно работать с информацией, анализировать и обобщать полученную информацию.

Метапредметные:

1. Развиваются компьютерная грамотность и информационная культура личности в использовании информационных и коммуникационных

технологий;

2. Развиваются умения анализировать и систематизировать имеющуюся информацию;

3. Развиваются познавательная и творческая активность в безопасном использовании информационных и коммуникационных технологий.

Личностные:

1. Вырабатывается сознательное и бережное отношение к вопросам собственной информационной безопасности;

2. Формируются и развиваются нравственные, этические, патриотические качества личности;

3. Стимулируется поведение и деятельность, направленные на соблюдение информационной безопасности.

Формы подведения итогов реализации программы - выставки буклетов, выполненных обучающимися; проведение квестов; выступления обучающихся по актуальным вопросам информационной безопасности с собственными мультимедийными презентациями на ученических мероприятиях; демонстрация созданных видеороликов и др.

Содержание курса

Тема 1. Общение в сети Интернет и сетевой этикет. (6 часов)

Основные вопросы: Почему соцсети стали настолько популярными? Механизмы Интернет – общения. Графическая модель типов пользователей социальных сетей. Механизмы Интернет – общения.

Анонимность (человек в сети может проявлять и проявляет большую свободу высказываний и поступков (вплоть до нецензурных выражений), так как риск разоблачения минимален)

Своеобразие протекания процессов межличностного восприятия в условиях отсутствия невербальной информации (сильное влияние на представление о собеседнике имеют механизмы стереотипизации и идентификации, а также установка желаемых качеств в партнере)

Добровольность и желательность контактов (пользователь Интернета добровольно завязывает всевозможные контакты или уходит от них, а также может прервать их в любой момент)

Затрудненность эмоционального компонента общения (стойкое стремление к эмоциональному наполнению текста, которое выражается в создании смайликов для обозначения эмоций)

Стремление к ненормативному поведению (пользователи проигрывают нереализуемые в деятельности вне сети роли, сценарии ненормативного поведения.

Требования к знаниям и умениям:

Обучающиеся должны знать: популяризация интернета. Почему соцсети стали настолько популярными? Механизмы Интернет –

общения. Обучающиеся должны уметь различать графическая модель типов пользователей социальных сетей. Обучающиеся должны уметь использовать этические

и правовые нормы информационной деятельности человека, информационный этикет и право, информационную безопасность

Тематика практических работ:

Практическая работа. Составить информационный буклет «Моя безопасная сеть», создать групповую газету «Безопасность в Интернет», «Упражнение Интернет общение глазами ребят».

Тема № 2. (5 часов) Риски в сети Интернет.

Основные вопросы: риски в сети Интернет.

Обучающиеся должны знать: Контентные риски. Различные информационные ресурсы (тексты, картинки, аудио, видеофайлы, ссылки на сторонние ресурсы), содержащие противозаконную, неэтичную и вредоносную информацию. Коммуникационные риски связаны с общением и межличностными отношениями Интернет-пользователей. Электронные риски – это вероятность столкнуться с хищением персональной информации или подвергнуться атаке вредоносных программ. Потребительский риск заключается в потере денег без приобретения товара или приобретения товара низкого

качества. Психологические риски интернет-зависимости.

Требования к знаниям и умениям:

Обучающиеся должны уметь различать риски в сети Интернет.

Тематика практических работ:

Практическая работа. Групповая работа «Риски в сети Интернет»

Создание буклета «Риски в сети Интернет».

Тема № 3. (3 часов)

Новостная грамотность в киберпространстве

Основные вопросы: Новостная грамотность. *Новость* - не жанр журналистского произведения, а новый фрагмент реальности, меняющий привычный ход вещей и потому требующий в той или иной степени общественного внимания. Виды новостей: «Жесткая» новость, «Мягкая» новость, инфотейнмент, финишинг. Главное, чтобы поднятая проблема была доведена до конца, закрыта в плане ее практического решения. Причем при использовании этого приема допускается повтор какой-то ситуации, факта, картинки, вопроса и т. д. Как оценить достоверность новостной информации? Как проверять информацию и не оказаться жертвой fake news? Принципы распознавания fake news. *Принцип первый:* проверьте площадку. *Принцип второй:* проверьте источники. *Принцип третий:* пускайте в свою голову только настоящих экспертов. *Принцип четвертый:* чем больше труда, тем лучше. *Принцип пятый:* ищите и распространяйте добавленную стоимость.

Требования к знаниям и умениям:

Обучающиеся должны знать новостную грамотность, виды новостей, как оценить достоверность новостной информации? Принципы распознавания fake news.

Тематика практических работ:

Практическая работа. «Создание мультимедийной презентации «Осторожно фейк!».

Тема № 4. (5 часов)

Интернет зависимость

Основные вопросы: Термин "Интернет-зависимость" Термин "Интернет-зависимость" еще в 1996 году предложил доктор Айвен Голдберг для описания неоправданно долгого, возможно патологического, пребывания в Интернете. Виды интернет-зависимостей. Киберотношения. Зависимость от дружеских отношений, завязанных в комнатах общения, интерактивных играх и

конференциях, которая заменяет реальных друзей и семью. Чрезмерная сетевая вовлеченность. Включает в себя вовлечение в азартные сетевые игры, зависимость от интерактивных аукционов и навязчивое состояние продавать и покупать через сеть. Информационная перегрузка и как ее опознать. Компьютерная зависимость. На сегодняшний день игровая зависимость официально признана врачами всего мира психическим заболеванием и включена в Международную классификацию болезней. Последствия компьютерной зависимости. *Физиологические проблемы:* Нарушение осанки; Рассеивается внимание; Снижаются умственные способности; Ухудшается память и зрение; Бессонница и потеря аппетита.

Требования к знаниям и умениям:

Обучающиеся должны знать виды интернет-зависимостей.

Киберотношения. Информационная перегрузка и как ее опознать. Компьютерная зависимость и ее последствия.

Тематика практических работ:

Практическая работа. Создание презентации на тему: «Информационная перегрузка». Эссе «Я и Интернет»

Тема № 5. (5 часов) Мошеннические действия в Интернете. Киберпреступления.

Основные вопросы: Виды интернет - мошенничества (письма, реклама, охота за личными данными и т.п.). Фишинг (фарминг). Мошеннические действия в сети .Предложения о разблокировании программ (блокировщики windows). Ложные антивирусы. Сбор «пожертвований» на благотворительность. «Легкий заработок» в Интернете. Пирамиды. Мошенничество при распространении «бесплатного» ПО. Продажа «обучающих курсов» для бизнеса. Опасности мобильной связи. Предложения по

установке вредоносных приложений. Мошеннические СМС. Прослушивание разговоров. Определение местоположения телефона. Азартные игры. Онлайн - казино. Букмекерские конторы. Предложения для «инвестирования» денег. Выигрыш в лотерею.

Технологии манипулирования в Интернете. Техника безопасности при интернет-общении.

Требования к знаниям и умениям:

Обучающиеся должны знать: виды интернет-мошенничества, опасности мобильной сети, технику безопасности при регистрации на веб-сайтах, сайтах знакомств, понятия компьютерное пиратство, плагиат, кибернаемники и кибердетективы.

Обучающиеся должны уметь обезопасить себя при интернет-общении.

Тематика практических работ:

Практическая работа. Круглый стол «Как не стать жертвой сетевых шуток и розыгрышей».

Тема № 6. (3 часа)

Агрессия в сети и ее виды

Основные вопросы: Термины «Агрессия и агрессивность»

Если вы стали жертвой компьютерной агрессии: службы помощи личное общение и общение в группе – чем они отличаются (чаты, форумы, службы мгновенных сообщений). Киберагрессия (оскорбление, унижение, манипуляция, буллинг в интернет-среде) — ситуация, в которую, по статистике, в России регулярно вовлекается каждый пятый подросток. С размытием границ реального и виртуального киберагрессия оказывает не менее пагубное влияние на эмоциональное и психологическое здоровье детей, чем реальная травля в школе (и одно нередко перетекает в другое). Кибербуллинг. Признаки кибербуллинга – осознанное и длительное причинение человеку вреда в сети. При этом агрессоров может быть несколько, они выступают как от своего лица, так и анонимно.

Требования к знаниям и умениям:

Обучающиеся должны знать термины «Агрессия и агрессивность». Кибербуллинг. Признаки кибербуллинга. Обучающиеся должны уметь использовать этические и правовые нормы информационной деятельности человека.

Тематика практических работ:

Практическая работа. Рисунок «Моя киберагрессия»

Тема №7. (3 часов)

Троллинг в киберпространстве

Основные вопросы: *Троллинг* — форма социальной провокации или издевательства в сетевом общении, использующаяся как персонифицированными участниками, заинтересованными в большей узнаваемости, публичности, эпатаже, так и анонимными пользователями. Виды троллинга: обычная провокация;

преднамеренная провокация; целенаправленная провокация; троллинг по заказу. Типы троллей: эмоциональный тролль; тролль-оффтопикт; тролль-борец за справедливость; тролль — любитель спойлеров; тролли-всезнайки; «Бесмысленные» тролли.; «Актуальные» тролли; жестокие тролли.

Требования к знаниям и умениям:

Обучающиеся должны знать термит «Троллинг», его виды и типы. Обучающиеся должны уметь распознать троллинг и его виды в сети Интернет.

Тематика практических работ:

Практическая работа Буклет «Не кормите Провокатора. Тролли в Интернете»
Тема №8. (3 часов)

Хейтинг: способы нейтрализации

Основные вопросы: Хейтинг — это такой вид социальной активности. Хейтерами обычно называют людей, которые по злому насмеваются или поливают грязью в интернете. Злые комменты, едкие выражения в адрес кого-либо. На этом многие даже себе сделали имя. Некоторые хейтеры причисляют себя к критикам, но критика по крайней мере имеет какой-то конструктив. Виды хейтеров: «Правдурб»; «Белое пальто»; «Тролль обыкновенный»; «Эффект Шарикова». Если вы понимаете мотивы поведения хейтера, то вы можете защищаться и атаковать его.

Требования к знаниям и умениям:

Обучающиеся должны знать термит «Хейтинг», его виды. Обучающиеся должны уметь распознать хейтинг и его виды в сети Интернет.

Тематика практических работ:

Практическая работа. Создание презентации на тему: «Хейтинг: способы нейтрализации».

Тематическое планирование

П/п	Наименование раздела, тем	Количество часов	Из них	
			теория	практика
1	Общение в сети Интернет и сетевой этикет	6	3	3
2	Риски в сети Интернет	5	2	3
3	Новостная грамотность в киберпространстве.	3	2	1
4	Интернет – зависимость	5	3	2
5	Мошеннические действия	5	4	1

	в Интернете. Киберпреступления			
6	Агрессия в сети и ее виды	3	2	1
7.	Троллинг в киберпространстве	3	2	1
8.	Хейтинг: способы нейтрализации	3	2	1
9.	Итоговое занятие.	1	1	
Итого:		34	21	13

Календарно-тематический план

№ п/п	Название темы	Кол-во часов		Формы организации познавательной деятельности учащихся	Виды/ формы контроля
		Теор.	Прак.		
1	Социальные сети	1		Лекция.	Текущий. Устный опрос.
2	Механизмы Интернет - общения	1		Лекция.	Текущий. Устный опрос.
3	Практическая работа «Информационный буклет «Моя безопасная сеть»		1	Рассказ-беседа.	Текущий. Индивидуальная работа.
4	Графическая модель типов пользователей социальных сетей	1		Беседа.	Текущий. Фронтальный опрос.
5	Практическая работа «Информационная газета Безопасность в Интернет»		1	Практическая работа	Текущий. Групповая работа.
6	Упражнение «Интернет общение глазами ребят». Тест «Сетевой этикет»		1	Лекция.	Текущий. Устный опрос.
7,8	Контентные и коммуникационные риски в сети Интернет. Практическая работа.	1	1	Практическая работа	Текущий. Устный опрос.
9,10	Электронные и потребительские риски в сети Интернет. Практическая работа.	1	1	Практическая работа	Текущий. Устный опрос.
11	Психологические риски интернет- зависимости. Блиц-опрос «Я и моя		1	Практическая работа	Текущий. Уплотнённый опрос.

	информационная безопасность»				
12	Новостная грамотность. Виды новостей	1		Лекция.	Текущий. Устный опрос
13	Принципы распознавания fake news. Как оценить достоверность новостной информации?	1		Рассказ-беседа.	Текущий. Устный опрос
14	Практическая работа. Создание презентации «Осторожно fake news»		1	Практическая работа	Текущий. Групповая работа.
15	Виды Интернет – зависимостей. Киберотношения.	1		Лекция.	Текущий. Устный опрос.
16	Информационная перегрузка. Как опознать информационную перегрузку.	1		Беседа.	Текущий. Устный опрос.
17	Практическая работа. Создание презентации «Информационная перегрузка»		1	Практическая работа	Текущий. Работа в парах.
18	Компьютерная зависимость. Её последствия.	1		Лекция.	Текущий. Устный опрос.
19	Практическая работа. Эссе «Я и Интернет»		1	Практическая работа	Тематический. Индивидуальная работа.
20	Виды интернет – мошенничества. Опасность мобильной сети	1		Лекция.	Текущий. Работа в парах.
21	Техника безопасности при Регистрации на веб-сайтах	1		Лекция.	Текущий. Устный опрос.
22	Понятие компьютерное пиратство, плагиат.	1		Лекция.	Текущий. Устный опрос.
23	Кибернаемники, кибердетективы.	1		Дискуссия.	Текущий. Устный опрос.
24	Практическая работа. Круглый стол «Как не стать жертвой сетевых шуток и розыгрышей»		1	Практическая работа	Тематический. Групповая работа.
25	Агрессия и агрессивность. Кибербуллинг.	1		Беседа.	Текущий.
26	Виды кибербуллинга.	1		Лекция.	Текущий. Устный опрос.
27	Практическая работа.		1	Практическая работа	Тематический.

	Рисунок «Моя киберагрессия»				Индивидуальная работа.
28, 29	Троллинг. Виды и типы троллинга.	2		Беседа.	Текущий. Устный опрос.
30	Практическая работа. Информационный буклет «Не корми провокатора. Троллинг в интернете».		1	Практическая работа	Текущий. Индивидуальная работа.
31	Хейтинг. Виды хейтеров.	1		Лекция.	Текущий. Устный опрос.
32	Что делать, если вас хейтят?	1		Дискуссия.	Текущий. Устный опрос.
33	Практическая работа. Создание презентации «Хейтинг: способы нейтрализации?»		1	Практическая работа	Тематический. Индивидуальная работа.
34	Итоговое занятие.	1		Беседа.	Итоговое. Коллективная работа.

Раздел 5. Методическое обеспечение

Материально-техническое обеспечение курса внеурочной деятельности «Кибербезопасность подростков в сети Интернет» включает следующий перечень необходимого оборудования:

№	Наименование объектов и средств материально-технического обеспечения	Дидактическое описание	Обеспеченность, %
СРЕДСТВА ИКТ			
	ПК	Используется учителем и учащимися	100
	Мультимедийный проектор.	Используется учителем	100
	Доступ к сети Интернет.	Используется учителем и учащимися	100

Список литературы.

- Бирюков А.А. Информационная безопасность защита и нападение 2 е издание: Издательство: ДМК-Пресс., 2017, 434 с.
- Бирюков А.А. Информационная безопасность защита и нападение.: Издательство: ДМК-Пресс., 2018, 474 с.
- Колесниченко Денис. Анонимность и безопасность в интернете. От чайника к пользователю. Самоучитель Издательство: БХВ-Петербург, 2018, 240с.

- Мазаник Сергей. Безопасность компьютера. Защита от сбоев, вирусов и неисправностей:
издательство: ЭКСМО, 2019, 256 с.

Приложение 1

Тест «Сетевой этикет»

Вопрос №1 Что из ниже перечисленного не является основой формирования информационной культуры?

- A) знания об информационной среде
- B) знания о законах функционирования информационной среды
- C) умение ориентироваться в информационных потоках
- D) принцип узкой специализации

Вопрос №2 Информационное общество - это новая историческая фаза развития постиндустриального, в которой главными общества продуктами производства является:

- A) материальные блага и услуги
- B) информация и знания
- C) натуральные продукты
- D) всё вышеперечисленное

Вопрос №3 Что означает фраза, написанная БОЛЬШИМИ БУКВАМИ?

- A) автор смеётся
- B) автор громко кричит
- C) у автора
- D) затрудняюсь ответить

Вопрос №4 Что принято вписывать в поле темы, отвечая на чьё-либо письмо?

- A) Re: Исходная_тема
- B) Re: Любимая_тема
- C) Re: Научная_тема
- D) Re: Новая_тема

Вопрос №5 С чем возникло понятие "сетевой этикет"?

- A) с появлением социальных сетей
- B) с появлением электронной почты
- C) с появлением различных браузеров

Вопрос №6 В чём достоинство Интернета?

- A) расширяет среду общения до размеров земного шара
- B) можно общаться только в отведённых зонах
- C) расширяет среду общения до размеров вселенной

Вопрос №7 В чём заключается основная проблема Интернета?

- A) Интернет не имеет территориальных границ своего распространения
- B) Интернет имеет территориальные границы своего распространения
- C) У Интернета нет проблем

Вопрос №8 Присутствует ли регулирование правовых отношений в Интернете на международном(межгосударственном) уровне?

- A) присутствует
- B) практически отсутствует
- C) полностью исключено

Вопрос №9 Если Вас оскорбили или умышленно или неумышленно обидели, то

- A) обидьтесь и уйдите
- B) ответе в том же стиле
- C) не поддавайтесь на провокацию
- D) пожалуйтесь администратору

Вопрос №10 В чате, форуме, гостевой книге общается большое количество разных людей, с разными мнениями и интересами. Следует быть

- A) тактичным и корректным в своих высказываниях
- B) твердым в своем мнении и убеждать других в нём
- C) вежливым с теми, кто вежлив в тобой
- D) скромным

Вопрос №11 Вставьте пропущенное слово: "Общаясь по электронной почте, личными сообщениями, в чате и т.п. всегда следует _____. Исключения: комментарии и сообщения на форуме."

- A) Писать ИМХО
- B) Троллить
- C) Здороваться
- D) Извиняться

Вопрос №12 Что такое аватар?

- A) Это фильм Джеймса Кэмерона
- B) Это изображение для профиля на сайте
- C) Это квадратный селфи
- D) Это маленькая фотография человека для сайта

Вопрос №13 Что такое электронные деньги?

- A) это как-бы деньги, но как-бы ненастоящие
- B) это баллы на сайте
- C) это реальные деньги, хранящиеся на электронном кошельке
- D) это реальные деньги, хранящиеся в банке

Вопрос №14 Что такое блог?

- A) интернет-дневник, онлайн-дневник, веб-сайт
- B) веб-сайт с мультимедиа
- C) личная статья пользователя
- D) часть сайта в рамке с неизменным содержанием

Вопрос №15 Что такое модерация?

- A) улучшение уже имеющихся материалов
- B) проверка соответствия правилам
- C) увеличенные возможности профиля
- D) редактирование личного кабинета

Вопрос №16 Что такое троллинг?

- A) представитель царства животных
- B) вид виртуального общения, в котором нагнетается конфликт
- C) возможность авторизоваться на сайте
- D) разновидность веб-страниц в которых встроено видео

Вопрос №17 Сокращение "IMHO" (рус. IMХО), используемое в чатах и сообщениях, переводиться на русский в полной форме как

- A) моё сообщение – мои правила
- B) считаю, что автор не прав
- C) к вашему сведению
- D) по моему скромному мнению

Вопрос №18 Сокращение «ROFL», используемое в чатах и сообщениях, переводиться на русский как

- A) катаюсь по полу от смеха
- B) отойду от компьютера
- C) кстати, между прочим
- D) считаю, что автор не прав

Вопрос №19 Сетевой этикет, это

- A) правила общения в жизни
- B) правила поведения в сети
- C) тема сообщения
- D) сервис сети

Вопрос №20 Выберите правильный вариант написания предложения

- A) сетевое сообщение , выходящее за рамки темы общения
- B) сетевое сообщение ,выходящее за рамки темы общения
- C) сетевое сообщение,выходящее за рамки темы общения

D) сетевое сообщение, выходящее за рамки темы общения

Обобщающий тест «Медиабезопасность в сети Интернет»

1. Какие сайты, группы в социальных сетях чаще всего становятся для Вас источником информации?
А) только известные, общепризнанные, проверенные, с большой аудиторией
Б) разные, как общеизвестные, которым доверяют все, так и малоизвестные, с небольшой аудиторией
В) предпочитаю черпать информацию из малоизвестных источников
2. Есть ли в списке Ваших друзей в социальной сети незнакомые Вам люди?
А) Нет, я знаю всех своих интернет-друзей лично
Б) Есть один или несколько человек
В) Да, таких много
3. Доверяете ли Вы всей информации, которая появляется в Вашей ленте в социальной сети?
А) Нет, всегда проверяю
Б) Иногда ищу подтверждения, проверяю
В) Да, полностью доверяю
4. Часто ли Вы переходите по ссылкам на незнакомые сайты?
А) Нет, никогда
Б) Было несколько раз
В) Да, часто
5. Оставляете ли Вы свои личные данные на незнакомых сайтах, форумах, в анкетах и т.д.?
А) Нет, никогда
Б) Было однажды
В) Да, часто оставляю, в этом нет ничего страшного
6. В каком объеме Вы указываете свои личные данные в личных аккаунтах в социальных сетях?
А) По минимуму: ФИО, рабочий телефон, остальные контакты знают те, кому это нужно
Б) ФИО, личный номер телефона
В) Пишу всё о себе: ФИО, личный телефон, адреса, привычки и т.д., люди должны иметь возможность найти меня и узнать все из моей анкеты
7. Распространяете ли Вы информацию о денежных сборах на благотворительность, помощь для операций, лечения и т.д.?
А) Нет, стараюсь не распространять, если не проверенная
Б) Распространяю, если не вызывает вопросов с первого взгляда, но не стараюсь проверить
В) Распространяю, люди должны знать об этом и помогать друг другу
8. Каковы настройки приватности вашей страницы в социальной сети?
А) Страница закрыта, просматривать ее могут только друзья
Б) Страница открыта всем пользователям, но сообщения и комментарии могут отправлять только друзья, просмотр фото и видеоограничен
В) Страница открыта всем пользователям
9. Переводите ли Вы деньги на пожертвования\за услуги или товары по информации в социальной сети?
А) Нет, никогда, стараюсь не пользоваться такими услугами, если нет возможности проверить или оплатить товар после его прихода на почту
Б) Иногда перевожу
В) Часто перевожу, не проверяю, пользуюсь такими услугами, делаю пожертвования
10. Выкладываете ли Вы личные фото или видео в социальные сети?

- А) Стараюсь делать это по минимуму, ограничиваю возможность просмотра в настройках приватности
- Б) Выкладываю, но не очень много, иногда ограничиваю возможность просмотра для самых личных материалов
- В) Выкладываю фото или видео каждого своего шага, ставлю гео-тэги
11. Пароль какого типа Вы используете в своих аккаунтах?
- А) С буквами разного регистра, не связанными в слово, цифрами, от 8 символов
- Б) Только из букв разного регистра \ только из цифр
- В) Простое слово \ простой набор цифр
12. Как часто вы меняете пароли?
- А) Периодически меняю, задаю разные для разных аккаунтов
- Б) Меняю, если меня взломали
- В) Не меняю, у меня вообще один пароль для всех аккаунтов

Подсчитайте баллы.

№ вопроса	Ответ/баллы	№ вопроса	Ответ/баллы
1	А - 3 Б - 2 В - 1	7	А - 3 Б - 2 В - 1
2	А - 3 Б - 2 В - 1	8	А - 3 Б - 2 В - 1
3	А - 3 Б - 2 В - 1	9	А - 3 Б - 2 В - 1
4	А - 3 Б - 2 В - 1	10	А - 3 Б - 2 В - 1
5	А - 3 Б - 2 В - 1	11	А - 3 Б - 2 В - 1
6	А - 3 Б - 2 В - 1	12	А - 3 Б - 2 В - 1

Результаты

Количество баллов: 25-36

Высокий уровень медиабезопасности

Вы знаете, как обезопасить себя в интернете, следите за своими личными данными и тщательно проверяете информацию, ориентируетесь в информационном потоке.

Количество баллов: 13-24

Средний уровень медиабезопасности

Ваше взаимодействие с медиа на среднем уровне безопасности. Вы осмотрительны, следите за своими личными данными, но бдительность можно повысить

Количество баллов: 1-12

Вы небезопасно взаимодействуете с медиа

Вы небезопасно взаимодействуете с медиа. Вам обязательно нужно изменить свое поведение в интернете, быть более осмотрительным, подвергать информацию более тщательной проверке, обратить внимание на безопасность личных данных