Комитет по делам образования города Челябинска

Муниципальное бюджетное учреждение
дополнительного профессионального образования
«Центр развития образования города Челябинска»

Сборник методических материалов, разработанных в рамках реализации интерактивного образовательного модуля «Кибербезопасность»

Учебно-методическое пособие

Челябинск
2019

Рецензенты:

И. Л. Качуро, кандидат педагогических наук, начальник отдела Комитета по делам образования города Челябинска.

С. В. Мачинская, Почетный работник сферы образования Российской Федерации, директор МБУ ДПО «Центр развития образования города Челябинска».

Е. Н. Бобер, заместитель директора по информатизации и информационно-методической деятельности МБУ ДПО «Центр развития образования города Челябинска».

С. А. Зайкова, заместитель директора по учебно-методической деятельности МБУ ДПО «Центр развития образования города Челябинска».

Редактор: Ю. С. Бондарева, начальник отдела информационно-методического сопровождения образовательных организаций Тракторозаводского района МБУ ДПО «Центр развития образования города Челябинска».

Рекомендовано к печати Методическим советом МБУ ДПО «Центр развития образования города Челябинска».

Протокол № от

Сборник методических материалов, разработанных в рамках реализации интерактивного образовательного модуля «Кибербезопасность»: учебно-методическое пособие – Челябинск: МБУ ДПО «Центр развития образования города Челябинска», 2019. – 116 с.

Данное методическое пособие посвящено вопросам безопасности в информационном обществе. В пособии излагаются основные элементы понятийного аппарата информационной безопасности, рассматриваются теоретические основы защиты персональных данных в сети Интернет, представлены методические и справочные материалы в сфере управления персональными данными в Интернете. В основу данного пособия положен ценностный взгляд на важность и необходимость защиты персональных данных.

Пособие также знакомит читателей со способами исключения утечки информации и ее несанкционированного использования. Содержит игровые элементы, способствующие формированию знаний и умений по защите персональных данных в информационном пространстве.

Пособие адресовано руководителям образовательных организаций, их заместителям, педагогическим работникам, родителям (законным представителям). Полезно оно будет всем заинтересованным лицам, которые интересуются вопросами медиабезопасности.

Содержание

Пояснительная записка

На сегодняшний день современное информационное общество – наиболее развитая фаза современной цивилизации, наступающая в результате информационно-компьютерной революции, когда стали использоваться информационные технологии, «интеллектуальные» системы, автоматизация и роботизация всех сфер и отраслей экономики и управления, создания единой новейшей интегрированной системы связи, предоставляющей каждому человеку любую информацию и знания, обусловливает радикальные изменения во всей системе общественных отношений, благодаря чему обеспечиваются наибольший прогресс и свобода личности, возможность ее самореализации.

Умение эффективно работать с информацией в современном мире является одним из важнейших факторов успеха. Мы живем в век информационного общества и не может не замечать, что стираются границы между абстрактной категорией «информация» и носителем этой информации. Виртуальный мир в современных реалиях представляет угрозу личности, собственности.

Защита информации в сети Интернет стала особенно актуальна в последнее время. Участились кибератаки (о которых мы узнаем из телепередач) не только на коммуникативные средства связи, но и данные на различных электронных носителях; хакеры взламывают важные файлы, чтобы использовать данные в корыстных целях. В связи с этим современная жизнь в век информационных технологий диктует нам новые угрозы, о которых мы ранее не задумывались.

Основные понятия

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

КВЕСТ-ИГРА ДЛЯ УЧАЩИХСЯ ПО ТЕМЕ «БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННОМ ОБЩЕСТВЕ»

Цель занятия: формирование у участников навыков безопасного поведения в информационной среде и основ безопасного использования персональных данных.

Задачи:

1. Определить понятие «персональные данные».
2. Сформировать понятийный аппарат по вопросам защиты персональных данных.
3. Сформировать представления об основных механизмах защиты своих персональных данных.
4. Сформировать навыки безопасного поведения в информационной среде.

Форма: квест.

Планируемые результаты

В результате игры учащиеся:

− изучат понятия в сфере защиты персональных данных;

− научатся использовать основные механизмы защиты своих персональных данных;

− приобретут навыки безопасного поведения в информационной среде.

Введение в тему

Среди экспертов в области информационных технологий бытует мнение, что, при сохранении тенденций и темпов развития интернета, уже в недалеком будущем частная жизнь станет прозрачной и публичной «по умолчанию» –персональную информацию будет невозможно не открыть государству или корпорациям, а справляться с вопросами ее безопасности будет все сложнее.

Именно поэтому важно привлечь внимание школьников, да и взрослых людей, к проблемам и последствиям ненадлежащей обработки персональных данных и широкого распространения личной информации в информационной среде. Актуальность профилактики необдуманного распространения своих персональных данных возрастает в подростковом возрасте с получением паспорта гражданина РФ.

Теоретические основы

Что такое персональные данные? (рассуждение участников квеста).

Демонстрация видеоролика, размещенного на сайте федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций – https://pd.rkn.gov.ru/multimedia/video114.htm

Таких идентифицирующих данных огромное множество, к ним относятся: фамилия, имя, отчество, дата рождения, место рождения, место жительства, номер телефона, адрес электронной почты, фотография, возраст и пр.

Так, если мы кому-то скажем, свои фамилию, имя, отчество и адрес места жительства, то нас вполне можно будет опознать как конкретное лицо.

Получается, что персональные данные – это не просто ваши фамилия или имя, персональные данные – это набор данных, их совокупность, которые позволяют идентифицировать вас, понять, что вы – это вы.

Вывод: персональные данные представляют собой информацию о конкретном человеке. Это те данные, которые позволяют нам узнать человека в толпе, идентифицировать и определить, как конкретную личность.

Рассмотрим виды персональных данных:

Регистрационные данные (паспортные данные, пароли, пин-коды).

Существуют персональные данные, которые представляют собой набор цифр. Благодаря такому набору цифр нас можно определить, как конкретного человека, установить нашу личность.

Такими персональными данными являются: номер и серия паспорта, страховой номер индивидуального лицевого счета (СНИЛС), индивидуальный номер налогоплательщика (ИНН), номер банковского счета, номер банковской карты.

Физические характеристики (внешность, пол, рост, вес, здоровье).

Биометрические персональные данные представляют собой сведения о наших биологических особенностях. Эти данные уникальны, принадлежат только одному человеку и никогда не повторяются.

Биометрические данные заложены в нас от рождения самой природой, они никем не присваиваются, это просто закодированная информация о человеке, которую люди научились считывать. К таким данным относятся: фотография, отпечаток пальца и пр.

Геолокация (определяет ваше текущее местоположение).

Финансы (дом, квартира, дача, зарплата родителей, дорогие вещи показывают, что у вас есть ценного).

Статусы (достижения, награды и пр., показывают в какой области у вас достижения, что вы умеете и ваши возможности).

Общественные связи (информация о родственниках, друзьях, знакомых, принадлежность к различным формальным и неформальным группам), распространение которых создаст угрозу не только для вас, а также для ваших близких прежде всего.

Когда размещается фото друзей, необходимо спросить у них, а хотели бы они, чтобы эти фото были в сети. Нужно быть вежливым не только в обычной реальности, но и в виртуальной реальности.

Образ жизни и поведение (вероисповедание, интересы, хобби, социальные привычки и действия, настроения, вкусы) позволяют сделать выводы в какое время и куда вы ходите, в какие секции и по какому адресу. Также сюда можно отнести такие данные как: расовая или национальная принадлежность, политические взгляды, религиозные или философские убеждения, состояние здоровья и пр.

Эти специальные данные характеризуют наши взгляды, убеждения, мировоззрение, они определяют нашу социальную принадлежность к определенным группам. Например, человек может сказать: «Я демократ или я христианин». По таким данным можно сформировать представление о человеке.

Психологические особенности (черты характера, способности, знания, умения, навыки, личностные черты) позволят манипулировать вами.

Например, легко замотивировать пойти на какое-нибудь мероприятие, которое будет связано с тем, что человека интересует.

Хроника личных событий позволяет отследить каждое действие. Это, например, личный блог.

Вывод очень простой – чем больше мы публикуем о себе информации, тем больше о нас узнают другие пользователи (приложение 1). Одно дело, когда это ваши эмоции, общение, и совсем другое, когда это информация о ваших планах или о ваших данных, которые можно использовать против вас.

Стоит отметить, что о некоторых видах данных мы не задумываемся, когда публикуем их в сеть Интернета. Утечка важной и значимой информации может негативно отразиться на нашей жизни, поэтому обратите внимание на то, что вы размещаете.

Основные понятия, используемые в квесте

Аккаунт, учетная запись (англ. account) – хранимая в компьютерной системе совокупность данных о пользователе, необходимых для его опознавания (аутентификации) и предоставления доступа к его личным данным и настройкам.

Аватарка – это маленькое изображение для идентификации себя в различных форумах и других социальных проектах. Аватаркой может быть маленькая фотография или небольшой рисунок.

Пароль – персональные данные, которые мы храним, нуждаются в защите. С этой целью доступ к информации ограничен паролем – набором символов.

«Придумайте сложный пароль» – это словосочетание можно увидеть при регистрации на сайте или создании аккаунта. Легкий пароль часто служит оружием для взлома электронной почты, аккаунтов социальных сетей. Чтобы избежать постороннего доступа, рассмотрим несколько правил составления надежных паролей:

1. Надежный пароль должен:

− состоять из 8–16 символов;

− включать в себя буквы, цифры и специальные символы;

− включать в себя символы в верхнем и нижнем регистре клавиатуры.

2. Не следует использовать слова, словосочетания, а также комбинации, которые можно легко угадать (например, ФИО).

3. Для каждого аккаунта необходимо иметь свой пароль.

4. Необходимо менять пароли ко всем аккаунтам один раз в 3–6 месяцев.

5. При столкновении с попыткой взлома одного из аккаунтов, необходимо поменять пароли на всех аккаунтах.

Фишинг (англ. phishing, от fishing – «рыбная ловля, выуживание») – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям. Достигается путем проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков или внутри социальных сетей. В письме часто содержится прямая ссылка на сайт, внешне не отличимый от настоящего, либо на сайт с *редиректом (redirect)*. После того как пользователь попадает на

поддельную страницу, мошенники пытаются различными психологическими приемами побудить пользователя ввести на поддельной странице свои логин и пароль, которые он использует для доступа к определенному сайту, что позволяет мошенникам получить доступ к его аккаунтам и банковским счетам.

Геолокация – определение реального географического местоположения электронного устройства, например, радиопередатчика, сотового телефона или компьютера, подключенного к сети Интернет.

Практическая часть

По маршрутным листам прохождение 5 станций (примерно 8 человек – одна команда) по типу «вертушки». Названия станций: «Аккаунт», «Аватарка», «Пароль», «Фишинг», «Геолокация». Время выполнения заданий на каждой станции – до 8 минут

На каждой станции дается задание, а по окончании удачного его выполнения – ключ (пин-код, состоящий из 2 знаков. Таким образом, к концу квеста каждая команда получает суммарный пин-код, состоящий максимально из 10 знаков).

Каждое задание станции выполняется командой, т.е. всей группой.

Задание 1 станции («Аккаунт»):

1) Заполнить бланк с персональными данными по плану (приложение 2): ФИО, внешность: цвет глаз, волос, рост; телефон, адрес, эл. почта, хобби и интересы, вероисповедание, особенности личности, внешности, характера.

2) Собрать все работы.

3) Зачитать каждую страничку (без ФИО) и командой попытаться отгадать, о ком речь в тексте.

4) Озвучить написанные ФИО.

5) Чем быстрее угадывается персонаж, тем менее защищены его персональные данные.

6) Раздать работы.

7) Скорректировать каждому участнику информацию так, чтобы она стала безопасной для автора странички.

Данные теперь защищены? Так как обезопасить их от мошенников?

Задание 2 станции («Аватарка»):

Представьте себе, что на фотокартинах изображены вы.

1) Нужно дифференцировать предложенные фотокартины; с одной стороны, разложить те, которые участники квеста считают незащищенными от мошенников, с другой стороны те, которые, по их мнению, безопасны. Объяснить выбор. Сделать коллаж (на ватмане приклеить безопасные аватарки).

2) Сделать селфи безопасное и сделать провокационное селфи. Объяснить продукт деятельности. Незащищенное удалить.

Задание 3 станции («Пароль»):

Предлагается зашифровать номер телефона, где

8 – хлопнуть в ладоши

9 – притопнуть двумя ногами в прыжке

0 – мяукнуть

8* – прорычать
0) – просвистеть
0+ – щелкнуть пальцами
4 – прогудеть
2 – пролаять
3 – чихнуть
7 – кашлянуть
3! – сказать «чпок»

За 5 секунд вам нужно набрать этими звуками номер телефона. Засекаем время. Добиваемся результата за указанное (5 секунд!) время, чтобы получилось четко и быстро (может быть 2–3 попытки).

Попытайтесь теперь при помощи телефона набрать этот номер (не получается).

Значит, пароль удачен! В нем есть тайна! Четыре последние цифры расположены в неправильном порядке. Догадайтесь, как нужно! (Дети звонят, у ведущего проходит звонок).

А теперь издайте этот номер вновь звуками в нужной последовательности за 5 секунд. Получилось!

Удачно зашифрован номер телефона? Почему? Где знания этой станции можно и нужно использовать?

Задание 4 станции («Фишинг»):

1) Предложить участникам прочитать 3-(5) вариантов текста. Два (три-четыре) из них – мошеннического содержания, один-(два) – безопасный.

2) Нужно найти безопасный вариант и доказать фишинг других вариантов.

3) Предложить каждому участнику придумать свой безопасный логин и пароль. В группе выявить самый удачный вариант. Посоветовать другу из команды, как изменить его логин и пароль для большей безопасности.

Задание 5 станции («Геолокация»):

Нарисовать свое местоположение «здесь и сейчас» (командой) с точностью до метра в радиусе 500 метров

Вывод: так же точно интернет-ресурс видит ваше местоположение. Когда это необходимо, а когда опасно? Что делать?

Заключение

Каждая команда в финале квеста, набирая пин-код на компьютере, имеет возможность посмотреть видеоролик о кибербезопасности в сети Интернет.

Демонстрация видеоролика, размещенного на сайте федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций – https://pd.rkn.gov.ru/multimedia/video114.htm

СЕМИНАР-ПРАКТИКУМ ДЛЯ ПЕДАГОГИЧЕСКИХ РАБОТНИКОВ ПО ТЕМЕ «БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННОМ ОБЩЕСТВЕ»

Цель: формирование компетенций, необходимых для создания безопасной информационной среды в образовательных организациях.

Задачи:

1. Изучить содержание нормативно-правовых документов по вопросам безопасности персональных данных.
2. Определить понятие «персональные данные».
3. Сформировать понятийный аппарат по вопросам защиты персональных данных.
4. Сформировать представление об основных механизмах защиты персональных данных.

Форма: семинар-практикум, очная.

Методы:

– интерактивная лекция;

– доклады;

– практические занятия.

Аудитория: заместители директоров по воспитательной работе, классные руководители, педагоги-психологи, социальные педагоги, учителя информатики, педагоги-организаторы, руководители органов ученического самоуправления, руководители детских СМИ, педагоги дополнительного образования.

Планируемые результаты

В результате участники семинара-практикума:

– изучат содержание нормативно-правовой базы по теме;

– овладеют понятийным аппаратом по вопросам безопасности персональных данных;

– приобретут навыки трансляции полученных компетенций для всех участников образовательных отношений, используя различные формы и методы обучения.

Актуализация темы

Стремительное развитие современных телекоммуникационных и информационных технологий привело к становлению нового общества – информационного. Использование информационных технологий значительно изменяет не только то, как производятся продукты и услуги, но и то, как все мы живем. С 2014 года утверждена программа на государственном уровне о стратегии развития информационного общества.

– Указ Президента РФ от 09.05.2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы»;

– Постановление Правительства РФ от 15.04.2014 г. № 313 (ред. от 25.09.2018 г.) «Об утверждении государственной программы Российской Федерации «Информационное общество (2011–2020 годы)»;

– Государственная программа Челябинской области «Развитие информационного общества в Челябинской области на 2016-2018 годы» (изм. на 20.06.2018 г.) (Постановление от 17.11.2015 года № 571-П).

Сегодня термины информационное общество и информатизация прочно заняли свое место, причем не только в лексиконе специалистов в области информации, но и в лексиконе политических деятелей, экономистов, преподавателей и ученых.

Технологическая составляющая общественного и экономического развития государств сегодня очень существенна, при этом скорость происходящих под ее воздействием изменений настолько велика, что даже на глазах одного поколения происходит несколько циклов технологического обновления. Актуальное вчера, сегодня уже теряет свое значение.

Каждый из нас уже не представляет жизнь без информационных технологий.

Обратите внимание на слайд (рис. 1). Что здесь представлено?

В контакте	Инстаграмм	Твитер	Фэйсбук	Одноклассники	Ютюб

Рисунок 1 – Популярные онлайн ресурсы

Это популярные онлайн ресурсы. А что они нам дают? Общение и прочее. Но самое основное они «сливают» все наши данные, которые мы сами размещаем в соцсетях о себе.

Демонстрация видеоролика «Персональные данные», размещенного на сайте федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций – https://pd.rkn.gov.ru/multimedia/video114.htm

Интернет сегодня является самым востребованным кластером у большинства населения планеты, что вызывает определенные сомнения по поводу безопасности в сети.

Современная жизнь в век информационных технологий диктует нам новые угрозы, о которых ранее никто не задумывался.

Мы не можем не замечать, что стираются границы между абстрактной критерией «информация» и носителем этой информации. Виртуальный мир в современных реалиях представляет угрозу личности, собственности, общественному порядку и государственной безопасности. Так защита той или иной информации может быть приравнена к защите ее материального эквивалента.

Обеспечение информационной безопасности требует от каждого человека внимательного отношения, так как даже сделки, касающиеся покупки бытовой техники либо мебели, постепенно переходят в сеть, а сохранение своих сбережений в сложной системе связано с большим объемом рисков. Безопас-

ность в сети Интернет необходима для организации конфиденциальности сделок и частной переписки, которая может быть перехвачена в случае некачественного контроля со стороны пользователя. Интернет служит для заключения сделок и покупок, а также для получения информации, поэтому среднестатистическому жителю обходиться без глобальной паутины трудно.

В Интернете кроются и отрицательные моменты, которые не дают возможности обеспечить качественную защиту личных данных:

– большинство информации в интернете предоставляется без цензуры с расчетом на широкую аудиторию;

– моментальное распространение вирусов через сеть;

– невозможность проследить исходящие данные с дальнейшей их корректировкой;

– официальная регистрация пользователей не является обязательной, что приводит к возможности скрыться после совершения мошенничества.

Кибермошенничество

Фишинг, фармин, вишинг, смишинг, нигирийские письма, интернет-аукционы, хайп и прочее.

Преступления, совершенные в сети Интернет, не всегда можно классифицировать, поэтому привлечь к ответственности за них достаточно сложно. Наличие всех этих факторов заставляет пользователей задумываться о самостоятельном решении проблем, а также применять программы, которые будут отвечать за безопасность информации.

В настоящее время объективной реальностью является необходимость обеспечения безопасности личной информации, поскольку информация о человеке сегодня превратилась в дорогой товар. Защита личной информации может приравниваться к защите личности, при этом степень угрозы безопасности личности (частная жизнь, личная, семейная тайна, жизнь и здоровье личности, собственность и прочее) может определиться в каждом конкретном случае незнакомого использования информации о личности.

Для решения проблем защиты участников сети Интернет была создана четыре года назад специальная организация – Лига безопасного интернета. Цель деятельности данного объединения заключается в противодействии хакерским атакам, а также в распространении программ контроля над популяризацией в Интернете запрещенного видео. Лигу учредили с надеждой на решение глобальных проблем сети, связанных с распространением вирусных ботов и незаконного контента.

А также на государственном уровне сформирована Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Но прежде всего, мы должны сами себя защищать в информационном обществе, знать свои права и обязанности в данном направлении, то есть нормативно-правовую базу.

Нормативно-правовые документы по вопросам безопасности персональных данных, зоны риска

«У того, кто решит изучать законы,
не останется времени их нарушать»
И.В. Гете

Информационная безопасность вызывает огромный интерес, потому что информация окружают нас повсюду. Однако правильно работать с информацией и безопасно – это искусство. Необходимо знать основные законодательные акты и нормативные документы по данному вопросу.

В современном мире к информационной безопасности относятся очень серьезно, особенно к защите персональных данных. Нормативные акты, регулирующие обеспечение их сохранности предусмотрены не только национальным законодательством, но и международными актами, например, Всеобщая декларация прав человека (принята резолюцией 217 А (III) Генеральной Ассамблеи ООН от 10.12.1948) является одним из важнейших документов в истории человечества. Статья 12 Всеобщей декларации прав человека гласит:

Статья 12 «Никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произвольным посягательствам на неприкосновенность его жилища, тайну его корреспонденции или на его честь и репутацию. Каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств».

Сохранность персональных данных обеспечивается следующими нормативными актами Российской Федерации:

Конституция Российской Федерации от 12.12.1993 г. (с изм. от 30.12.2008 г. № 6-ФКЗ, от 30.12.2008 г. № 7-ФКЗ, от 05.02.2014 г. № 2-ФКЗ, от 21.07.2014 г. № 11-ФКЗ).

В ее положениях признается не только само право на неприкосновенность личной жизни, личную и семейную тайну (ч.1 ст.23), но и обеспечивающие это право дополнительные гарантии (ч.2 ст.23) (все эти права можно рассматривать как право на приватность). В соответствии со ст.2 Конституции РФ «человек, его права и свободы являются высшей ценностью. Признание, соблюдение и защита прав и свобод человека и гражданина – обязанность государства».

Таким образом, Российская Федерация не только устанавливает право, но и обязуется защищать его; ставит интересы человека и гражданина на ступень выше, чем интересы государства, общества, либо общественных или коммерческих организаций. Часть 1 ст.24 Конституции РФ запрещает сбор, хранение, использование и распространение информации о частной жизни лица без его согласия. И, наконец, согласно ст.46 каждому гарантируется судебная защита его прав, в том числе в межгосударственных органах.

Статья 2 «Человек, его права и свободы являются высшей ценностью. Признание, соблюдение и защита прав и свобод человека и гражданина – обязанность государства».

Статья 23 «Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени.

Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения».

Статья 24 Конституции РФ в действующей редакции на 2018 год:

Часть 1 «Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются».

Глава 2 Ст.46:

– «Каждому гарантируется судебная защита его прав и свобод».

– «Решения и действия (или бездействие) органов государственной власти, органов местного самоуправления, общественных объединений и должностных лиц могут быть обжалованы в суде».

– «Каждый вправе в соответствии с международными договорами Российской Федерации обращаться в межгосударственные органы по защите прав и свобод человека, если исчерпаны все имеющиеся внутригосударственные средства правовой защиты».

Кроме того, данную сферу регулирует Федеральный закон от 25.02.1995 г. № 24-ФЗ «Об информации, информатизации и защите информации». В частности, ч.1 ст.11 Федеральный закон от 25.02.1995 г. № 24-ФЗ «Об информации, информатизации и защите информации» определяет, что персональные данные являются конфиденциальной информацией, а ч.3 этой же статьи предупреждает о наступлении ответственности юридических и физических лиц за нарушение режима защиты, обработки и порядка использования этой информации.

Статья 11 «Информация о гражданах (персональные данные)»:

Часть 1. Перечни персональных данных, включаемых в состав федеральных информационных ресурсов, информационных ресурсов совместного ведения, информационных ресурсов субъектов Российской Федерации, информационных ресурсов органов местного самоуправления, а также получаемых и собираемых негосударственными организациями, должны быть закреплены на уровне федерального закона. Персональные данные относятся к категории конфиденциальной информации.

Часть 3. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации (за нарушение режима защиты, обработки и порядка использования этой информации) и соответствующим перечнем, дает им следующее определение:

Понятие «персональные данные»

Для начала необходимо определиться, что такое персональные данные? В Федеральном законе от 25.02.1995 г. № 24-ФЗ «Об информации, информатизации и защите информации».

Статья 2 «Термины, используемые в настоящем Федеральном законе, их

определения: информация о гражданах (персональные данные) – сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность». В соответствии со ст.3 «Основные понятия, используемые в настоящем Федеральном законе» от 27.07.2006 г. № 152-ФЗ «О персональных данных», они понимаются еще шире. Основу этого Закона составляют базовые принципы и условия обработки персональных данных.

Статья 3 «Основные понятия, используемые в настоящем Федеральном законе». Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Такое широкое толкование позволяет относить к персональным данным практически любую информацию о человеке: сведения о его ФИО, поле и возрасте, образовании, месте жительства, семейном положении и др. Помимо этого к персональным данным относится и изображение человека, с помощью которого можно установить его личность – например, фотография, видеозапись или портрет (разъяснения Роскомнадзора от 30 августа 2013 г. «Разъяснения по вопросам отнесения фото-, видеоизображений, дактилоскопических данных и иной информации к биометрическим персональным данным и особенностей их обработки»), а также биометрические персональные данные – физиологические данные (дактилоскопические данные, радужная оболочка глаз, анализы ДНК, рост, вес и другие), а также иные физиологические или биологические характеристики человека, в том числе изображение человека (фотография и видеозапись), которые позволяют установить его личность и используются оператором для установления личности субъекта.

Обработка биометрических персональных данных может осуществляться только при наличии согласия в письменной форме субъекта персональных данных.

В настоящее время закон от 25.02.1995 г. № 24-ФЗ «Об информации, информатизации и защите информации» не действует, его заменил Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями и дополнениями).

В статье 2 нового закона от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями и дополнениями) рассмотрены основные понятия, используемые в данном законе, а в ст.3 говорится о правовом регулировании отношений, возникающих в сфере информации, информационных технологий и защите информации. В этой статье говорится о том, что ограничения доступа к информации может устанавливаться только федеральным законом. Конкретного понятия персональных данных в этом законе нет, очевидно, потому что был утвержден Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных».

В статье 5 ФЗ «Об информации, информационных технологиях и защите информации», сказано: «информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа)».

Общедоступная информация – это та информация, которую нельзя скрывать от общества. Примером может служить информация о состоянии окружающей среды, о деятельности органов государственной власти и органов местного самоуправления, документы, накапливаемые в открытых фондах библиотек и архивов. Так же в эту категорию можно отнести нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина, правовое положение организаций и полномочия государственных органов, органов местного самоуправления.

Информацией ограниченного доступа является информация представляющая ценность для ее владельца, доступ к которой ограничивается на законном основании. В свою очередь информация ограниченного доступа подразделяется на информацию, составляющую государственную тайну и информацию, соблюдение конфиденциальности которой установлено федеральным законом (конфиденциальная информация).

Перечень сведений конфиденциального характера опубликован в Указе Президента РФ от 06.03.1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» (с изменениями и дополнениями от 23.09.2005 г., 13.07.2015 г.) (информация о частной жизни гражданина отнесена к сведениям конфиденциального характера, следовательно, разглашению и несанкционированному сбору не подлежит).

К видам конфиденциальной информации можно отнести следующее:

– персональные данные – сведения о фактах, событиях и обстоятельствах частой жизни гражданина, позволяющие идентифицировать его личность, за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;

– тайна следствия и судопроизводства – сведения, составляющие тайну следствия и судопроизводства, а также сведения о защищаемых лицах и мерах государственной защиты, осуществляемой в соответствии с ФЗ от 20 августа 2004 г. № 119-ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства» и другими нормативными правовыми актами Российской Федерации;

– служебная тайна – служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами;

– профессиональная тайна – сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений и т.д.);

– коммерческая тайна – сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами;

– сведения о сущности изобретения – сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

Обработка персональных данных, их хранение и использование

Все персональные данные на конкретного человека могут быть подвергнуты необходимой обработке (например, формирование списков обучающихся в организации, сотрудников, по полу, возрасту, профессии, образованию и т.п.; подготовка работодателем списков работников, подлежащих медицинским осмотрам, и другое). Основное требование при обработке персональных данных работника – соблюдение конституционных норм, гарантирующих охрану прав и свобод человека и гражданина.

В Европейском Союзе вопросам защиты интересов владельцев персональных данных, которые были подвергнуты электронной обработке, посвящена Конвенция Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных», подписанная в Страсбурге (Франция) в 1981 году. Федеральный закон о ратификации Конвенции был подписан Президентом РФ 19 декабря 2005 года Федеральным законом РФ от 19.12.2005 г. № 160-ФЗ.

Конвенция о защите физических лиц при автоматизированной обработке персональных данных (ETS N 108) (рус., англ.) (от 28.01.1981 г. с изменениями, внесенными Международным договором от 15.06.1999 г.). Ратифицирована Федеральным законом РФ от 19.12.2005 г. № 160-ФЗ.

Под обработкой персональных данных Конвенция Совета Европы «О защите личности в связи с автоматической обработкой персональных данных» от 28 января 1981 г. понимает накопление данных, проведение логических и (или) арифметических операций с такими данными, их изменение, стирание, восстановление или распространение.

Статья 2 «Определения. Для целей настоящей Конвенции»:

– «персональные данные» означают информацию, касающуюся конкретного или могущего быть идентифицированным лица («субъекта данных»);

– «автоматизированная база данных» означает любой набор данных, к которым применяется автоматическая обработка;

– «автоматическая обработка» включает следующие операции, если они полностью или частично осуществляются с применением автоматизированных средств: накопление данных, проведение логических или/и арифметических операций с такими данными, их изменение, стирание, восстановление или распространение;

– «обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных» (Федеральный Закон «О персональных данных» от 27.07.2006 г. № 152-ФЗ).

Обработка указанных специальных категорий персональных данных допускается в случаях, если субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных.

Что значит, дать согласие на обработку персональных данных? Статья 5 Закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» устанавливает шесть принципов обработки персональных данных, защищающих персональную информацию человека; данные принципы схожи с принципами, содержащимися во многих европейских правовых актах. Во-первых, персональные данные должны собираться и использоваться законно и добросовестно. Эта норма говорит о том, что персональные данные должны быть собраны и использованы в соответствии с законодательством РФ и только с согласия субъекта персональных данных, но за исключением случаев, четко оговоренных в части 2 статьи 6 Закона, когда такое согласие не требуется.

В соответствии с гл.2. ст.9 «Согласие субъекта персональных данных на обработку его персональных данных» Федерального Закона «О персональных данных» от 27.07.2006 г. № 152-ФЗ, каждая школа разрабатывает локальный акт, который конкретизирует сведения, относящиеся к персональным данным, кто имеет доступ к персональным данным обучающегося, права и обязанности работников, получивших доступ к персональным данным ученика и утверждает форму Согласия родителя (законного представителя) на обработку персональных данных. Согласие на обработку своих персональных данных субъект персональных данных должен дать в письменной форме; содержание этого документа четко установлено в п.4 статьи 9 Закона. К примеру, в письменном согласии субъекта должна быть обязательно указана цель обработки персональных данных и их перечень, а также срок, в течение которого действует согласие и порядок его отзыва.

Согласно Главе 2. ст.9. ч.4. «Согласие субъекта персональных данных на обработку его персональных данных» должно включать в себя, в частности:

– фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

– фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

– наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;

– цель обработки персональных данных;

– перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

– наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;

– перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

– срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;

– подпись субъекта персональных данных.

В случаях, предусмотренных Федеральным Законом, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью.

Ответственность. Лицам, нарушившим требования Федерального Закона «О персональных данных» от 27.07.2006 г. № 152-ФЗ, в зависимости от конкретных обстоятельств и серьезности деяния может грозить не только административная и уголовная ответственность, но также гражданско-правовая и даже дисциплинарная. При этом административная ответственность с 1 июля 2017 г. ужесточилась – вместо одного состава правонарушения ст.13.11 КоАП РФ теперь предусматривает семь, а максимальный штраф составляет 75 тыс. руб.

Наказание за разглашение персональных данных по ст.137 УК РФ варьируется от штрафа до лишения свободы. Совершение ничем не отягченного преступления (ч. 1 ст. 137 УК РФ) грозит одним из следующих наказаний:

– штрафом в размере до 200 000 руб. (как вариант, в размере полуторагодовой зарплаты виновного);

– обязательными или исправительными работами на срок до 360 часов или до 1 года соответственно;

– до 4 месяцев ареста;

– до 2 лет лишения свободы.

Для лиц, допустивших разглашение конфиденциальных сведений о личности в связи со своим служебным положением, наказание будет строже:

– минимальный размер штрафа в этом случае составит 100 000 руб., максимальный – 300 000 руб.;

– обязательные работы в ч.2 ст.137 не предусмотрены, а срок принудительных увеличен до 4 лет;

– продолжительность ареста продлена до 5 месяцев, срока лишения свободы – до 5 лет.

Самые суровые последствия ждут виновных в разглашении данных о несовершеннолетних:

– согласно ч.3 ст. 37 УК РФ им придется заплатить от 150 000 до 350 000 руб. штрафа или принудительные работы до 6 лет;

– в качестве альтернативы возможен арест на срок до полугода или до 6 лет тюрьмы.

Статья 137 УК РФ – одна из наиболее сложных норм с точки зрения квалификации преступления. Для ее правильного толкования необходимо учитывать требования смежных отраслей законодательства. В частности, не избежать обращения к законам, регламентирующим обращение с персональны-

ми данными, регулирующим деятельность различных ведомств и раскрывающим понятие тайны.

Гражданский кодекс РФ, Часть 1, Раздел I, Глава 8, Статья 152 «Защита чести, достоинства и деловой репутации». Ответственность за распространение недостоверных, но не порочащих сведений. Ранее распространение недостоверных, но не порочащих честь, достоинство и деловую репутацию сведений не считалось нарушением. Новая норма п.10 ст.152 Гражданского кодекса РФ позволяет требовать:

– прекращение распространения любых не соответствующих действительности сведений;

– опровержения сведений;

– опубликования своего ответа;

– компенсации убытков и морального вреда.

В норме устанавливается специальный срок исковой давности в один год на случай распространения недостоверной информации в СМИ.

Напомним, что, если недостоверные сведения порочат честь, достоинство и деловую репутацию, именно ответчик (распространитель) должен доказать их соответствие действительности (п.1 ст.152 Гражданского кодекса). В случае оспаривания недостоверных сведений, которые не порочат, бремя доказывания перенесено на истца. Именно истец должен доказать, что распространенные сведения не соответствуют действительности.

Федеральный Закон от 29.12.2010 г. № 436-ФЗ (ред. от 29.07.2018) «О защите детей от информации, причиняющей вред их здоровью и развитию». Закон издан на 29 страницах, состоит из 7-ми глав и 23 статей. Суть закона в следующем: все дети поделены на четыре «информационно-возрастные» категории:

– до шести лет;

– от шести до двенадцати;

– от двенадцати до шестнадцати;

– достигшие шестнадцати лет.

Для каждой категории закон определяет, какую информацию можно ей предоставлять, а какую запрещается. Федеральный закон направлен на защиту детей от разрушительного, травмирующего их психику информационного воздействия, переизбытка жестокости и насилия в общедоступных источниках массовой информации, от информации, способной развить в ребенке порочные наклонности, сформировать у ребенка искаженную картину мира и неправильные жизненные установки. Информационная безопасность детей – это состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией, в том числе распространяемой в сети Интернет, вреда их здоровью, физическому, психическому, духовному и нравственному развитию (Федеральный закон от 29.12.2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»).

Итак, какую же информацию считают «вредной» и «травмирующей».

Статья 5 «Виды информации, причиняющей вред здоровью и (или) развитию детей».

К информации, причиняющей вред здоровью и (или) развитию детей, относится:

– информация, предусмотренная частью 2 настоящей статьи и запрещенная для распространения среди детей;

– информация, которая предусмотрена частью 3 настоящей статьи с учетом положений статей 7-10 настоящего Федерального Закона и распространение которой среди детей определенных возрастных категорий ограничено.

К информации, запрещенной для распространения среди детей, относится информация:

– побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству;

– способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;

– обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным, за исключением случаев, предусмотренных настоящим Федеральным законом;

– отрицающая семейные ценности, пропагандирующая нетрадиционные сексуальные отношения и формирующая неуважение к родителям и (или) другим членам семьи;

– оправдывающая противоправное поведение;

– содержащая нецензурную брань;

– содержащая информацию порнографического характера;

– о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), включая фамилии, имена, отчества, фото- и видеоизображения такого несовершеннолетнего, его родителей и иных законных представителей, дату рождения такого несовершеннолетнего, аудиозапись его голоса, место его жительства или место временного пребывания, место его учебы или работы, иную информацию, позволяющую прямо или косвенно установить личность такого несовершеннолетнего.

К информации, распространение которой среди детей определенных возрастных категорий ограничено, относится информация:

– представляемая в виде изображения или описания жестокости, физического и (или) психического насилия, преступления или иного антиобщественного действия;

– вызывающая у детей страх, ужас или панику, в том числе представляемая в виде изображения или описания в унижающей человеческое достоинство форме ненасильственной смерти, заболевания, самоубийства, несчастного случая, аварии или катастрофы и (или) их последствий;

– представляемая в виде изображения или описания половых отношений между мужчиной и женщиной;

– содержащая бранные слова и выражения, не относящиеся к нецензурной брани.

В Федеральном Законе от 29.12.2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию, введено понятие информационной безопасности детей, рассмотрены виды информации, причиняющей вред здоровью и (или) развитию детей». Федеральный закон, посвященный защите детей от вредной информации, и даются принципы организации защиты детей.

Указ Президента РФ от 09.05.2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы». Зачем принята стратегия?

«Стратегия развития информационного общества» – политический документ, определяющий цели, задачи и меры по реализации внутренней и внешней политики РФ в сфере применения ИКТ».

Президент в своем указе, утверждающем «Стратегию развития информационного общества», говорит, что «Стратегия» нужна как условие формирования в стране «общества знаний». Определение последнего понятия таково: «общество, в котором преобладающее значение для развития гражданина, экономики и государства имеют получение, сохранение, производство и распространение достоверной информации с учетом стратегических национальных приоритетов РФ».

«Стратегия» в нынешней редакции посвящена главным образом технологиям, информационным и телекоммуникационным как важнейшему элементу национальной инфраструктуры. Построение общества знаний и создание в России цифровой экономики в документе неоднократно упоминаются - как цель развития информационного общества.

Цель формирования информационного пространства знаний, записано в «Стратегии», состоит в «обеспечении прав граждан на объективную, достоверную, безопасную информацию и создании условий для удовлетворения их потребностей в постоянном развитии, получении качественных и достоверных сведений, новых компетенций, расширении кругозора». Отдельно говорится, в частности, об информационной безопасности детей, о «продвижении» русского языка в мире и о поддержке «традиционных», т.е. существовавших задолго до Интернета, «форм распространения знаний».

«Стратегия» прежде всего обращает внимание на безопасность информационной и телекоммуникационной инфраструктуры страны, т.е. «недопущение подмены, искажения, блокирования, удаления, снятия с каналов связи и иных манипуляций с информацией».

Для устойчивого функционирования информационной инфраструктуры предлагается, в частности, обеспечить централизованное управление ею, постепенно перевести на госорганы и ОМСУ на использование инфраструктуры электронного правительства (ее также предусматривается использовать для предоставления гражданам иных, негосударственных сервисов).

Персональные данные и их защита в сети Интернет

Одно из неотъемлемых прав каждого интернет-пользователя – право на защиту персональных данных.

По данным ряда опросов, больше половины россиян не знают о своих правах в Интернете. Нет среди пользователей и точного понимания того, что такое «персональные данные».

Так, в нашей стране в течение 2015 г. Роскомнадзором зарегистрировано приблизительно 33 тыс. обращений от граждан с жалобами на нарушения, связанные с публикацией их личных данных в Интернете.

С развитием Интернета вопросы защиты персональных данных попали в число самых актуальных вопросов безопасности не только взрослых, но и детей.

Именно поэтому важно привлечь внимание обучающихся к проблемам и последствиям ненадлежащей обработки персональных данных и широкого распространения личной информации в информационной среде.

Одним из ключевых направлений работы по защите прав субъектов персональных данных становится информационно – просветительская деятельность, в рамках которой особое внимание уделяется несовершеннолетним пользователям интернета как одной из наиболее уязвимых категорий пользователей. Главная задача – донести до российских учителей и их учеников необходимость защиты личной информации и объяснить правила безопасного управления персональными данными в Интернете.

В целях осуществления профилактических мер, направленных на популяризацию правил защиты персональных данных несовершеннолетних лиц Роскомнадзор в 2014г. провел первый «Всероссийский День защиты персональных данных детей», а также разработал информационно-развлекательный портал для педагогов, родителей и детей http://персональныеданные.дети/ направленный на изучение вопросов, связанных с защитой персональных данных при использовании цифровых технологий.

На сайте размещены информационные материалы для детей, которые могут быть использованы как в рамках школьных уроков по теме персональных данных, так и просто в виде интересной и познавательной информации. Все материалы разрабатывались с учетом ошибок детей в онлайн среде.

Что такое персональные данные? Персональные данные – это любая информация, которая имеет отношение к конкретному человеку. Персональные данные – это совокупность данных, которые необходимы и достаточны для идентификации какого-то человека.

Идентифицирующие данные: фамилия, имя, отчество, дата рождения, место рождения, место жительства, номер телефона, адрес электронной почты, фотография, возраст и прочее

Получается, что персональные данные – это не просто ваши фамилия или имя, персональные данные – это набор данных, их совокупность, которые позволяют идентифицировать вас, понять, что вы – это вы.

Виды персональных данных:

– Регистрационные идентификационные данные (паспортные данные, пароли, пин-коды, СНИЛС, индивидуальный номер налогоплательщика (ИНН), номер банковского счета, номер банковской карты).

– Физические характеристики (внешние данные, биометрические данные, состояние здоровья и др.).

– Пространственная локализация (фиксация местоположения и перемещения).

– Материально-экономическое положение (движимое, недвижимое имущество, зарплата, накопления и др.).

– Официальные статусы (семейное положение, достижения, награды, наличие судимостей и т.д.).

– Профессиональная занятость (включая образование).

– Социальные связи (информация о родственниках, друзьях, знакомых, принадлежность к различным формальным и неформальным группам).

– Образ жизни и поведенческие установки (мировоззрение, ценности, интересы и хобби, социальные привычки и действия, настроения, вкусы, особенности).

– Психологические особенности (черты характера, способности, знания, умения, навыки, личностные черты).

– Хроника личных событий (личный блог, сайт и т.д.).

Основные понятия в рамках безопасного обращения с персональными данными в сети Интернет:

Акка́унт, учетная запись (англ. account) – хранимая в компьютерной системе совокупность данных о пользователе, необходимых для его опознавания (аутентификации) и предоставления доступа к его личным данным и настройкам.

Кибербу́ллинг (англ. cyberbulling) – намеренное и регулярное причинение вреда (запугивание, унижение, травля, физический или психологический террор) одним человеком или группой людей другому человеку с использованием электронных форм контакта.

Конфиденциа́льность (англ. confidence – «доверие») – необходимость предотвращения разглашения, утечки какой-либо информации.

Фи́шинг (англ. phishing, от fishing – «рыбная ловля, выуживание») – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям. Достигается путем проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, социальных сетей.

Вывод очень простой – чем больше мы выкладываем о себе, тем больше о нас информации узнают другие пользователи.

Стоит отметить, что о некоторых видах данных мы не задумываемся, когда выкладываем их в сеть Интернета. Утечка важной и значимой информации может негативно отразиться на нашей жизни, поэтому необходимо обратить внимание на то, что вы размещаете.

Механизмы защиты персональных данных

Существуют «Три кита» защиты персональных данных:

1. Надежный пароль. Надежные пароли позволят защитить от третьих лиц ваши аккаунты на онлайн-ресурсах и в приложениях.

2. Управление уровнями доступа к персональным данным (настройки приватности). Настройки приватности дадут вам возможность определить уровень доступа других пользователей к вашим персональным данным, размещенным на различных онлайн-ресурсах.

3. Сознательное отношение к информации, размещаемой в интернете. Правила управления персональными данными помогут вам понять, как персональные данные, размещенные в интернете, влияют на вашу репутацию в сети.

Правила защиты персональных данных в сети Интернет:

– Ограничьте объем информации о себе, находящейся в Интернете. Удалите лишние фотографии, видео, адреса, номера телефонов, дату рождения, сведения о родных и близких и иную личную информацию.

– Не отправляйте видео и фотографии людям, с которыми вы познакомились в Интернете и не знаете их в реальной жизни.

– Отправляя кому-либо свои персональные данные или конфиденциальную информацию, убедитесь в том, что адресат – действительно тот, за кого себя выдает.

– Если в сети Интернет кто-то просит предоставить ваши персональные данные, например, место жительства или номер школы, класса иные данные, посоветуйтесь с родителями или взрослым человеком, которому вы доверяете.

– Используйте только сложные пароли, разные для разных учетных записей и сервисов.

– Старайтесь периодически менять пароли.

– Заведите себе два адреса электронной почты – частный, для переписки (приватный и малоизвестный, который вы никогда не публикуете в общедоступных источниках), и публичный – для открытой деятельности (форумов, чатов и так далее).

Прежде чем вводить свои персональные данные в интернете, необходимо убедиться, что вы находитесь именно на том ресурсе, на который хотели попасть, а не на поддельной (фишинговой) странице, созданной мошенниками. Существует несколько простых способов убедиться в подлинности ресурса:

– Всегда обращайте внимание на адресную строку браузера. Адрес поддельной странички может отличаться всего на одну букву, которую легко не заметить.

– Не стоит переходить на ресурсы по ссылкам, которые вы получили по электронной почте или в личной переписке и которые требуют ввода персональных данных — многие из них ведут на поддельные сайты. Забейте адрес в адресную строку самостоятельно, а еще лучше – используйте для поиска нужных ресурсов надежные поисковые системы, например, Яндекс.

– Убедитесь, что ресурс, на котором вы находитесь, использует защи-

щенное соединение. Если в адресной строке браузера присутствует иконка замка, а сам адрес начинается с аббревиатуры https:// вместо привычной http://, то такое соединение использует шифрование при передаче ваших персональных данных. В этом случае злоумышленникам будет гораздо сложнее перехватить ваши персональные данные и воспользоваться ими.

– Комплексные антивирусные программы также могут помочь защититься от мошенников.

Защита персональных данных на своем устройстве:

– Для удаления «цифровых следов» с компьютера после работы в интернете очистите журнал посещений (в браузере) и историю поисковых запросов.

– В настройках программ сетевой защиты также можно установить запрет на загрузку временных файлов и cookies с незнакомых сайтов, ограничившись лишь проверенными и надежными ресурсами.

– Будьте внимательны с настройками мобильных приложений: отключите опцию «автосинхронизации» данных, автоматического проставления «геометок» и т. д., если хотите избежать случайного попадания персональных данных в сеть.

Защита персональных данных на чужом устройстве:

– При входе в свой аккаунт с чужого устройства всегда выбирайте опцию «чужой компьютер», «не сохранять пароль», «безопасный ввод» и т. д. (на странице онлайн-ресурса). В этом случае вы можете быть уверены, что никто не войдет в ваш аккаунт после вас.

– Чтобы не оставить цифровых следов на чужом устройстве, используйте режим инкогнито (в браузере). Благодаря ему история поисковых запросов и посещенных страниц не сохраняется в браузере, а сайты не загружают cookies на устройство.

Защита персональных данных от третьих лиц:

– Используя вкладку «настройки приватности» (на странице онлайн-ресурса), запретите другим пользователям отмечать вас на фотографиях и упоминать в постах. Ограничьте круг лиц, которые могут комментировать ваши записи. Как правило, добавление пользователя в «черный список» автоматически лишает его возможности просматривать и комментировать ваши посты, а также упоминать вас в своих постах.

– Если другой пользователь использует ваши персональные данные, например фотографии, без вашего согласия, вы можете пожаловаться в службу поддержки ресурса (на странице онлайн-ресурса), приложив доказательства нарушения. Если другой пользователь, разместив недостоверную или устаревшую информацию, нанес существенный урон вашим чести и достоинству, вы можете обратиться в суд.

С развитием Интернета, уже в недалеком будущем частная жизнь станет прозрачной и публичной «по умолчанию» – персональную информацию будет невозможно не открыть государству и различным организациям, а справляться с вопросами ее безопасности будет все сложнее.

Безопасная информационная среда образовательной организации, система работы

Массовое внедрение компьютерной техники и использование сети Интернет в образовательных организациях добавляют еще один важный вопрос к комплексной безопасности организации и заставляет нас, заместителей директоров по воспитательной работе, заботиться о безопасности информационной среды в своих учреждениях. Организационной структурой, обеспечивающей решение этой задачи в школе, выступает образовательная система, она включает в себя представителей администрации школы, учителей-предметников, социально-психологическую, педагогическую службу, социальных партнеров, родителей сутью которых является создание образовательной среды, через создание и обеспечение качества условий, процесса, результата.

В образовательной среде имеются как внешние, так и внутренние факторы по отношению к образованию. Особенностью современной образовательной системы являются активно протекающие процессы информатизации, именно поэтому образовательная среда трансформировалась в информационно-образовательную. В научно-педагогических трудах, посвященных разработке понятийного аппарата информатизации образования, в последние годы широко обсуждается термин «информационно-образовательная среда».

Согласно О. А. Ильченко, под информационно-образовательной средой понимается системная и организованная совокупность информационного, технического, учебно-методического обеспечения, неразрывно связанная с человеком, как субъектом образовательного процесса.

Коротенков Ю.Г. в учебном пособии «Информационная образовательная среда основной школы» дает такое определение: информационно-образовательная среда – это область и интегрированное средство (ресурс) осуществления и реализации образовательного процесса и образовательного взаимодействия, которое под воздействием информатизации стало информационно-образовательным, информационно-познавательным, информационно-деятельностным и информационно-коммуникативным.

В соответствии с требованиями федерального государственного образовательного стандарта среднего (полного) общего образования информационно-образовательная среда образовательного учреждения включает:

– комплекс информационных образовательных ресурсов, в том числе цифровые образовательные ресурсы;

– совокупность технологических средств информационных и коммуникационных технологий: компьютеры, иное информационное оборудование, коммуникационные каналы;

– систему современных педагогических технологий, обеспечивающих обучение в современной информационно-образовательной среде.

Информационно-образовательная среда образовательной организации должна обеспечивать:

– информационно-методическую поддержку образовательного процесса; планирование, организацию образовательного процесса и его ресурсного обеспечения;

– проектирование и организацию индивидуальной и групповой деятельности;

– мониторинг и фиксацию хода и результатов образовательного процесса;

– мониторинг здоровья обучающихся;

– современные процедуры создания, поиска, сбора, анализа, обработки, хранения и представления информации;

– дистанционное взаимодействие всех участников образовательного процесса (обучающихся, их родителей (законных представителей), педагогических работников, органов, осуществляющих управление в сфере образования, общественности), в том числе с применением дистанционных образовательных технологий;

– дистанционное взаимодействие образовательного учреждения с другими образовательными учреждениями, учреждениями культуры, здравоохранения, спорта, досуга, службами занятости населения, обеспечения безопасности жизнедеятельности.

Каждая школа должна самостоятельно выстроить локальную (частную) систему безопасности как через обучение и воспитание, так и через решение задач технического развития. Отсюда возникает необходимость контролировать и анализировать ситуацию с информационной безопасностью и корректировать, соответственно, методы и способы обеспечения безопасности информационной среды образовательной организации и личной информационной среды каждого обучающегося. Достичь поставленной цели возможно при создании инфобезопасной среды в каждой образовательной организации.

Инфобезопасная среда образовательной организации – это информационно-образовательная среда, дополненная аппаратными, программными и организационными средствами и способами защиты от негативной информации, которая обеспечивает безопасность и защиту личностной информационной среды всех субъектов образовательного процесса в целях создания условий для наиболее полноценного развития и реализации их индивидуальных способностей и возможностей.

Модель информационной безопасности школьников. Объектом информационной безопасности в данной модели является личная информационная среда школьника. В условиях школьного образования обеспечение информационной безопасности личной информационной среды учащихся предлагается рассматривать как совокупность деятельности по недопущению вреда здоровью, сознанию и психике ребенка. Общая структура угрозы складывается из объекта угрозы, ее источника и проявления угрозы.

В образовательной организации должны быть созданы необходимые педагогические условия обеспечения информационной безопасности школьника. Создание и внедрение программ обучения детей и подростков правилам безопасного поведения в интернет-пространстве, профилактики интернет-зависимости, предупреждения рисков вовлечения в противоправную деятельность, порнографию, участие во флешмобах и т. п.

Правовое обеспечение информационной безопасности – это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту личной информационной среды учащегося на законодательной и правовой основе для реализации единой государственной политики в сфере защиты детей от информации, причиняющей вред их здоровью и развитию.

Нравственный и этический контроль подразумевает соблюдение школьниками при осуществлении информационной деятельности норм и правил поведения в обществе, а также сетевой культуры и этики, которые складываются по мере распространения информационных технологий в современном информационном обществе.

Защита психики и здоровья ребенка – меры направлены на актуализацию потребности школьников в хорошем здоровье, физическом благополучии, как средств достижения жизненно важных ценностей, снижение и профилактика компьютерной и интернет-зависимости среди учащихся, педагогическая и психологическая помощь в вопросах уменьшения информационных опасностей в жизнедеятельности школьников.

Организационная защита – это регламентация информационной деятельности подростков, контроль использования сетевых сервисов и сообществ, исключающие или ослабляющие нанесение вреда личной информационной среде школьника.

Воспитательные меры по обеспечению информационной безопасности – необходимо формировать у подрастающего поколения культуру безопасности, ответственность за осуществленные действия в информационном пространстве, воспитывать и укреплять духовно-нравственные ценности, патриотизм, готовить родителей и педагогов к принятию позиции ребенка и уважению его самостоятельности.

Техническое и программное обеспечение информационной безопасности – это использование различных аппаратных и программных средств, препятствующих нанесению материального или морального ущерба личной информации, программ Родительского контроля, сетевых фильтров, технических средств защиты информации.

Это задача выполняется при взаимодействии субъектов информационной образовательной среды, которые разрабатывают единую программу действия по информационной безопасности, выполняя каждый свои функции в работе по данному направлению.

Просмотр видеоролика «Тысяча друзей» – https://www.youtube.com/watch?v=2Re7ErX9Ay8

МЕДИА-ОБРАЗОВАНИЕ КАК ОДИН ИЗ ИНСТРУМЕНТОВ ПОВЫШЕНИЯ МЕДИА-ГРАМОТНОСТИ

XXI век – век телекоммуникаций и интернет-технологий. Человечество тонет в потоке информации. Ежедневно нам приходится отбирать информацию из различных медиа-источников.

Как научить современного ребенка свободно ориентироваться в информационном пространстве? Как обезопасить его пребывание в Интернете? Как научить делать правильный выбор? На эти вопросы отвечает новое направление в образовании – медиа-образование.

Основные понятия:

Медиа-образование представляет собой процесс образования и развития личности, направленный на формирование культуры восприятия, анализа, интерпретации и критического осмысления медиа-текстов, а также обучение способам самовыражения с использованием медиа-технологий.

Медиакомпетентность личности – совокупность ее мотивов, знаний, умений, способностей (показатели: мотивационный, контактный, информационный, перцептивный, интерпретационный/оценочный, практико-операционный/деятельностный, креативный), способствующих выбору, использованию, критическому анализу, оценке, созданию и передаче медиа-текстов в различных видах, формах и жанрах, анализу сложных процессов функционирования медиа в социуме.

Медиа-образование сегодня это необходимость. Современному школьнику крайне необходимо умение критически анализировать то, что посмотрел, прочитал или услышал из средств массовой информации и умение создавать самостоятельно медиа-продукт. Умение находить «иголку в стоге сена» среди потока медиа-информации, которую мы потребляем каждый день. Умение отбирать и формировать уникальную информацию для определенной аудитории.

Информационная культура личности – одна из составляющих общей культуры человека; совокупность информационного мировоззрения и системы знаний, умений, обеспечивающих целенаправленную самостоятельную деятельность по оптимальному удовлетворению индивидуальных информационных потребностей с использованием как традиционных, так и новых информационных технологий. Эта составляющая является важнейшим фактором успешной профессиональной и непрофессиональной деятельности, а также социальной защищенности личности в информационном обществе.

Медиа-культура (*media culture*) – совокупность материальных и интеллектуальных ценностей в области медиа, а также исторически определенная система их воспроизводства и функционирования в социуме; по отношению к аудитории *медиа-культура* (или, к примеру, *аудиовизуальная культура*) может выступать системой уровней развития личности человека, способного воспринимать, анализировать, оценивать медиа-тексты, заниматься медиа-творчеством, усваивать новые знания в области медиа.

Понятие *информационная культура* шире, чем *медиа-культура*, так как первое относится к сложным взаимоотношениям личности с любой инфор-

мацией, включая, разумеется, медийную, а второе – только к сфере контактов человека со средствами (массовой) коммуникации.

Деловая игра «Медиа-образование» разработана с учетом последних тенденций в области медиа-образования, а также на основании медиа-потребностей учащихся. Рекомендуется к проведению для учащихся в рамках воспитательной работы школы.

Практическая часть

Цель деловой игры: повышение уровня медиа-компетенций учащихся школы.

Задачи:

1. Развивающая:

– развитие способности критического мышления, которая дает возможность учащимся сформировать независимые суждения о содержании медиа-ресурса;

– развитие способности размышлять о медиа-текстах критически, независимо от того, насколько влиятельны их источники;

– развитие умений анализировать и обсуждать медиа-тексты.

2. Образовательная:

– формирование навыков отбора достоверной информации в сети Интернет;

– формирование у обучающихся навыков безопасного пребывания в сети Интернет;

– формирование культуры поведения в социальных сетях.

3. Воспитательная:

– воспитание социально активной и самостоятельной личности с нравственной позицией и нравственным самопознанием;

– воспитание в детях уважения к себе и к другим пользователям сети Интернет.

Форма: марш-старт.

Участники делятся на 6 команд по количеству станций. Каждой команде выдается маршрутный лист, где указана последовательность станций:

– Дебаты;

– Мафия;

– Селфи;

– Верю – не верю;

– Куплю – не куплю;

– Медиа-безопасность.

Последовательность прохождения этапов не должна совпадать, чтобы команды одновременно не пришли на одну станцию.

На каждой станции за хорошо выполненную работу выдается…

Описание станций

«Дебаты». Команда приходит на станцию и вытягивает одну из тем. Необходимо разделиться на две команды. Одна команда пишет аргументы «за», другая «против». Побеждает та команда, которая более грамотно, выстроит свою аргументацию – факты, ссылки на опросы общественного мнения, экспертизы и т.п.

Темы: вейперы, смертная казнь, Томинский ГОК, школьная форма, использование готовых домашних заданий, использование социальный сетей.

«Мафия». Ребята, добрый день! Знаете ли вы, что такое персональная, личная информация? *(отвечают)*.

Вы правы. Есть такая информация, которую мы с вами никому про себя не можем рассказывать. Например, незнакомцу нельзя говорить свой номер телефона, адрес и многое другое. А есть темы, на которые можно говорить с кем угодно: например, о погоде, домашнем задании. Это не персональная информация.

Сейчас мы проверим, насколько хорошо вы это понимаете. Мы поиграем в «Наш город». Мне нужно четыре человека. Кто хочет поиграть? *(выбираем четырех участников)*.

Итак, сейчас я выдаю вам карточки, где указаны ваши роли в игре. Вам нужно прочитать и сыграть эту роль. А мы вместе с оставшимися ребятами будем играть жителей города. Наша задача – угадать, кто вы, и понять, какую информацию вы пытаетесь у нас выведать – персональную или нет. Кто начнет? Ну что, наши уважаемые персонажи, с чем вы сегодня решили обратиться к нам, жителям города? *(персонажи по очереди исполняют свои роли)*.

Спасибо вам большое! Теперь, уважаемые жители, наша задача – угадать, что же это были за персонажи. Вспомним, о чем нас просил Петя. Кем он был? *(ведущий по очереди спрашивает у ребят, кто какие просьбы озвучивал, и уточняет, можно ли отвечать на такие просьбы, нет ли в них персональной информации. Совместно выясняют, что шутник и продавец выведывали личную информацию, а организатор и эколог просто приглашали на школьные мероприятия, им больше доверия).*

Молодцы! Мы всех рассекретили!

Содержание карточек:

1) Ты – продавец.

Задача: узнать у ребят их телефоны и домашние адреса, чтобы прислать какую-то посылку с одеждой (придумай, какой именно). На самом деле, они ее даже не заказывали.

2) Ты – шутник, «тролль».

Задача: попросить у ребят их личные фотографии, подшучивать над всеми без причины.

3) Ты – организатор школьного концерта.

Задача: пригласить ребят на новогодний концерт. Чтобы заинтересовать всех, придумай, что будет на концерте: интересные конкурсы, песни, танцы. Узнай у ребят, смогут ли они прийти.

4) Ты – эколог.

Задача: пригласи ребят на субботник недалеко от школы. Узнай, смотрели ли ребята прогноз погоды, и смогут ли прийти на субботник.

«Селфи». Ребята, добрый день! Для проведения следующей игры мне понадобится один помощник. Кто тут самый активный, у кого хороший голос? *(выбираем)*.

Как тебя зовут? *(говорит. например, Петя)*.

Итак, здравствуйте, уважаемые гости студии! Я, (ведущий называет свое имя) и Петр, ведущие ток-шоу «Мой выбор». И сегодня тема нашей передачи – селфи. Петя, посмотри пожалуйста сценарий, и задай нашим зрителям первый вопрос. Только первый, будь внимателен. *(Петя читает: Ребята, вы часто делаете селфи? отвечают, ведущий поддерживает диалог)*.

А как ваши родители и учителя относятся к этому увлечению? *(отвечают)*.

Петя, давай зададим нашим зрителям еще вопрос. *(читает: Предлагаю посмотреть на экран. Это страница известного блогера Кати Клэп. Знаете такую? Сотрите, у нее на странице «ВКонтакте» много селфи)*.

Ну что, вам интересно смотреть на страницу Кати? Теперь предлагаю посмотреть еще одну. Это просто девушка из Интернета. Мы с ребятами с факультета журналистики нашли ее страницу, пока готовились к сегодняшнему мероприятию. Что мы здесь видим? *(слайд. разные фото: она рисует, она на прогулке и т.п.)*.

Петя, тебе слово. *(читает: Предлагаю подвести итоги. Как вы считаете, нужно ли размещать в социальных сетях только селфи? А какие фотографии можно постить?)*.

Отлично! Теперь задание: нам с вами нужно сделать общее фото. Я возьму телефон, а вы выстройтесь так, чтобы было видно, какое интересное сегодня мероприятие, куда вы пришли. А я вас сфотографирую. Должно получиться не селфи, а классная, интересная фотография со всеми вами! Ну, строимся! *(общее фото, ведущий помогает ученикам)*.

Молодцы! Мы всех рассекретили! Теперь я хочу выдать вам звездочки за работу. (одна – удовлетворительная работа, две – хорошая, три – активная, отличная работа).

«Верю – не верю». На данной станции используются изображения (рис. 2).

Ребята, добрый день! Вы всегда верите информации, которая вас окружает? *(отвечают)*.

Молодцы! Сейчас в Интернете столько разной информации – не всегда можно понять, правдивая ли она. Я нашел(ла) в Интернете несколько сообщений. Давайте проверим, правду ли они нам сообщают.

Какой-то Рома Петров пишет, что школьную столовую закроют на месяц! Вот это беда, ребята, как же мы теперь будем обедать? Посмотрим, что еще у нас есть.

А здесь – страничка вашего школьного журнала «Взгляд». Пишут, что в столовой подорожают обеды. Это говорит директор. Будем надеяться, что ненамного.

Ребята, ну что, чьему сообщению у нас больше доверия? Ромы Петрова или школьного журнала? *(отвечают. Аргументы: мы не знаем Рому, он не*

указал номер школы и, главное, источник информации – откуда он об этом узнал? В сообщении журнала информация другая, и в тексте все обосновано – есть комментарий директора).

Вы большие молодцы! Предлагаю посмотреть еще пару картинок. Здесь телеведущий сообщает, что школу закрывают на карантин: «Школы Челябинска закрыли на неделю. Температура – -35 С. Карантин. Об этом говорит главный врач челябинской городской больницы Иван Иванов».

А здесь Оля пишет, что школу закрывают на карантин.

Ну что, ребята, где аргументированная информация, а где – непроверенная? *(отвечают. В телесообщении есть ссылка на главврача, указан источник информации)*.

Молодцы! Мы всех рассекретили! Теперь я хочу выдать вам звездочки за работу. (одна – удовлетворительная работа, две – хорошая, три – активная, отличная работа).

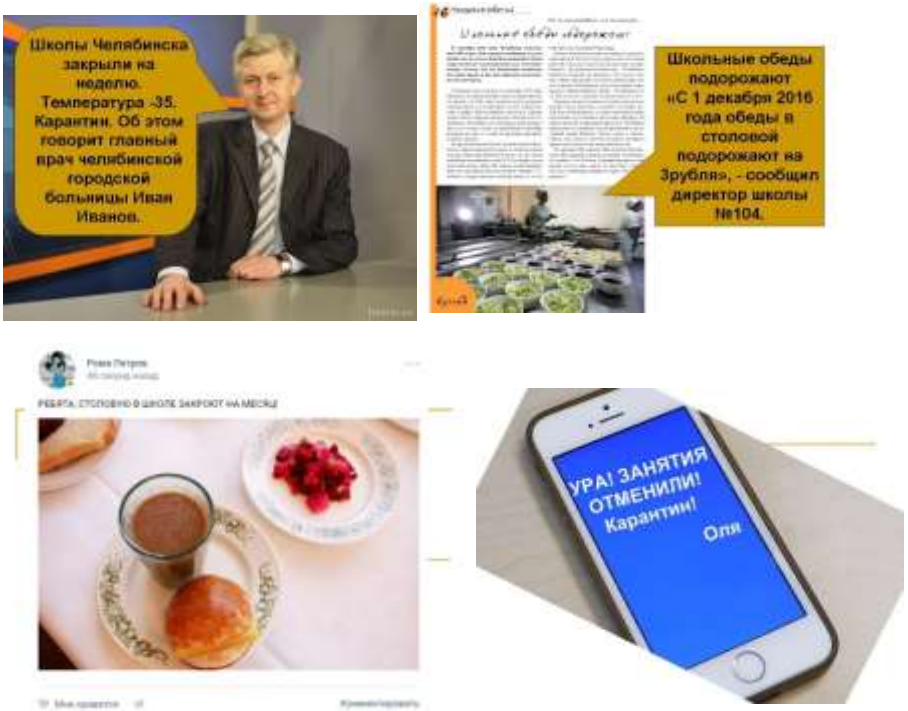


Рисунок 2 – Изображения для станции «Верю – не верю»

«Куплю – не куплю». Ребята, добрый день! Нас окружает много рекламы, заметили? Где вы видите рекламу каждый день? *(отвечают)*.

Сейчас мы с вами поделимся на две команды. Каждой я дам по два текста. Прошу вас определить, где рекламный текст, а где объективный – то есть, в нем представлена проверенная информация, и никто не заставляет нас что-то покупать спонтанно. *(раздает карточки)*. У вас три минутки. *(время прошло, начинаем обсуждение)*.

Информация на карточках:

1) Джинсы «джинс» – лучшие в мире!

В ноябре 2016 года в Челябинске появились джинсы «Джинс». Это самые модные джинсы осени. Их покупают Дима Билан и певица Елка. Приходите в магазин «Глория» на Гагарина, 28, и покупайте модные штаны!

2) Рейтинг джинсов: в каких ходить удобнее?

Редакция журнала «Анютка» провела собственное расследование и выяснила, какие джинсы можно выбрать, чтобы в них было удобно ходить в школу.

– джинсы марки «Престиж». Журналистка Катя Иванова ходила в них целый месяц, и штаны не порвались и не растянулись. Ставим им пятерку!

– джинсы марки «Джинс». Наш корреспондент Кирилл Мамаев сразу заметил, что они сильно растянулись и чуть не упали. Ставим двойку, лучше не носить такие штаны.

3) Книжный магазин «Люблю читать»: единственный книжный в Челябинске.

24 ноября 2016 года в книжный магазин «Люблю читать» пришли новые книги. Больше в Челябинске ходить за книгами некуда, поэтому ждем вас на улице Ленина, 45.

4) Какой книжный лучше: «Люблю читать» или «Книга в подарок»?

Редакция газеты «Ведомости» проверила, в каком магазине больше выбор книг. Согласно нашим подсчетам, магазин «Люблю читать» предоставляет широкий выбор книг. Всего их здесь 450. Есть и детская литература. И классика, и новые книги. В магазине «Книга в подарок» выбор книг нас не порадовал: их всего 100, многие повторяются. Советуем идти за интересной литературой в «Люблю читать».

«Медиа-безопасность». Предлагаю написать синквейн на тему медиабезопасности. Кто знает, что такое синквейн?

Синквейн – это не простое стихотворение, а стихотворение, написанное по следующим правилам:

1 строка – одно существительное, выражающее главную тему синквейна.

2 строка – два прилагательных (или причастия), выражающих главную мысль.

3 строка – три глагола (или деепричастия) описывающие действия в рамках темы.

4 строка – фраза, несущая определенный смысл (раскрывает отношение к теме; возможно, афоризм или пословица).

5 строка – заключение в форме существительного (ассоциация с первым словом).

Составлять синквейн очень просто и интересно. К тому же, работа над созданием синквейна развивает образное мышление и критическое мышление: требуется найти и выделить в рассматриваемой теме самые важные элементы, проанализировать их, сделать выводы и коротко сформулировать, основываясь на основных принципах написания стихотворения.

Пример синквейна на тему «Форум»

Форум (существительное, выражающее главную тему).

Шумный, интересный (два прилагательных, выражающих главную мысль).

Развлекает, развивает, веселит (три глагола, описывающие действия в рамках темы).

Хорошее место для знакомств (фраза, несущая определенный смысл).

Общение (заключение в форме существительного).
Пример синквейна на тему «Жизнь»:
Жизнь.
Активная, бурная.
Воспитывает, развивает, учит.
Дает возможность реализовать себя.
Искусство.
Пример синквейна на тему «Медиа-безопасность»
(написано участниками данной деловой игры)
Медиа-безопасность.
Актуальная, современная.
Просвещая, развивает, защищает.
Дело, важное для каждого.
Новая реальность.

КОМИКС И СОЦИАЛЬНЫЙ ТЕАТР КАК ТЕХНОЛОГИИ ПРОФИЛАКТИКИ КИБЕРБУЛЛИНГА

Предлагаемая методическая разработка представляет собой набор тренинговых упражнений и может стать основой для профилактической системной работы по проблемам школьной травли для разных специалистов – классных руководителей, педагогов-организаторов, педагогов-психологов, педагогов дополнительного образования и др.

Надо отметить, что именно «тренинг», как обучающая технология, является очень удачной формой воспитательной работы по этой, безусловно, актуальной проблеме.

Главной особенностью тренингового подхода является принцип «обучение через опыт», где после каждого упражнения, проигрывания ситуации, следует всестороннее обсуждение и личная оценка результатов и полученных впечатлений. Важное место занимают этапы рефлексии и формулировки выводов.

Обсуждение ситуаций агрессии, особенно в школьном коллективе – довольно сложная задача. Травля – это проблема школьного коллектива, и в то же время – проблема взаимоотношений отдельных личностей. Здесь требуется аккуратный, личностный подход, знания психологии, конфликтологии, знание элементарных понятий о правах человека, хранении персональных данных, кибербезопасности в целом. В конце разработки приведены ссылки на различные методические материалы других авторов, которые обязательно пригодятся для работы педагога по этой теме.

Буллинг (от англ. Bullying) – травля одного человека другим, агрессивное преследование одного ребенка другими детьми. Проявляется во всех возрастных и социальных группах. В сложных случаях может принять некоторые черты групповой преступности.

О травле в образовательных, закрытых и иных детских организациях было известно давно в разных странах, включая Россию. Тем не менее, реальное изучение буллинга началось лишь в конце 20 века. В современном

мире школьный буллинг рассматривается как серьезная социально-педагогическая проблема, которую нужно признать и принимать меры по профилактике. Профилактика буллинга (мероприятия по его предупреждению или снижению уровня агрессии, насилия) поможет снизить масштабы данного негативного явления, сократить количество вовлеченных в него «агрессоров» и «жертв», наладить взаимоотношения между детьми с учетом индивидуальных особенностей каждого.

В воспитательной работе важно уделить внимание именно профилактике буллинга, так как работать с последствиями намного труднее. *Кибербуллинг*, как явление отличает от буллинга лишь цифровая среда, где современный ребенок становится все более уязвимым.

Хочется акцентировать ваше внимание на том, что именно тренинг, при грамотном использовании, позволяет обратиться его участникам, к самому важному фундаменту своей личности – ценностям. Именно поэтому важно не свести беседу с воспитанниками к формальному разговору.

В кратком виде, систему занятий можно разделить на следующие части:

1 блок – Информационный.

Введение и актуализация. Общее понятийное поле. Понятия «буллинг», «травля», «кибербуллинг», «пирамида ненависти», «стереотип», «предубеждение», «насилие», критерии буллинга его признаки и роли.

2 блок – Практический.

Последствия буллинга для «жертвы», «обидчика», «свидетелей» и других участников. Распознавание ситуаций травли. Признаки. Сценарии поведения.

3 Рефлексия. Формулировка групповых правил.

Кодекс общения. Правила коммуникации.

Целесообразно разделить темы на занятия продолжительностью не менее 1 часа. Конечно, на свое усмотрение, педагог может включать и другие блоки, соответствующие упражнения.

Все занятия необходимо проводить, учитывая принципы тренинговых занятий:

– активность участников группы;

– исследовательская позиция;

– партнерское общение;

– участие может быть только добровольным;

– участникам предоставляется полная информация о целях и способах проведения тренинга.

Особенностью проведения данной серии тренингов по этой теме является использование комиксов, рисованных историй.

Комикс (от англ. comic – смешной) – серия рисунков с краткими текстами, образующая связное повествование.

На первом и втором занятии рекомендуется использовать комиксы проекта RESPECT. Цель данного проекта – посредством комиксов поговорить с молодежью на понятном и интересном для нее языке на такие темы, как уважение, отношение к людям разных взглядов, а также этнических, религиозных и социальных групп.

Создатели историй и художники подготовили замечательное методическое пособие, которое можно скачать совершенно бесплатно, как и все комиксы на сайте http://www.respect.com.mx/ru.

Обсуждение прочитанного комикса строится на всестороннем диалоге. Как пишут сами разработчики технологии: «Одна из задач «респект-занятий» – научить рассуждать самостоятельно, формировать собственное мнение и признаваться, когда его нет, выслушивать мнение и признаваться, когда его нет, выслушивать мнения других, не перебивать и не кидаться в спор, не дослушав и не осознав, о чем говорит оппонент.

Позиция ведущего – непривычна для школьной системы, поскольку предполагает возможность интересных, необычных и неожиданных мнений со стороны школьников. То есть эти занятия проводятся не для того, чтобы научить, но для того, чтобы вместе задавать вопросы и вместе искать на них ответы».

Обсуждение прочитанного комикса опирается на основные вопросы, как правило, открытого типа. В методическом пособии по работе с рисованными историями подробно описаны примеры беседы с обучающимися во время занятий.

Цель: повышение толерантности и эмпатии, профилактика конфликтов в межличностных отношениях учащихся, формирование основных принципов и норм коммуникации в коллективе.

Задачи:

1. Снижать агрессию и враждебные реакции подростков.
2. Формировать навыки конструктивного реагирования в конфликте.
3. Содействовать улучшению социального самочувствия.
4. Оптимизировать межличностные и межгрупповые отношения.
5. Изменить представление о самом себе и об отношениях с окружающими.
6. Устранить психотравмирующие и социально опасные ситуации.

Материально-техническое обеспечение (на всех занятиях): стулья по количеству участников группы, листы ватмана, цветные стикеры, клей, скотч, маркеры или фломастеры, листы формата А3 для правил, распечатанные комиксы, ноутбук, проектор.

Первый блок (информационный).

Цель: выявить признаки буллинга, его причины, последствия для разных «ролей», последствия для общества, сформировать понимание, что «травля – болезнь коллектива/класса/группы».

На начальном этапе ведущему необходимо задать вопросы, помогающие актуализировать проблему для каждого участника, например:

– Слышали ли вы когда-нибудь о таких понятиях как травля, буллинг?

– Были ли свидетелями такого поведения?

– Считаете ли вы такое поведение жестокостью? Насилием?

– Как вы думаете, кто виноват в таких ситуациях?

Упражнение «Белый стикер»

Участников тренинга просят закрыть глаза и приклеивают к голове каждого цветной стикер (любых цветов). Одному человеку из группы не достается цветного стикера и ему приклеивают белый. Затем всех участников просят открыть глаза и объединиться в группы. Как правило деление происходит по цветам стикеров. Без группы остается лишь тот участник, которому достался белый стикер. Обсуждение, получившейся, ситуации можно построить по следующим примерным вопросам:

– По какому принципу вы решили объединиться?

– Легко ли вам было найти свою группу?

– Как ты понял(а), что не сможешь ни с кем объединиться?

– Что ты чувствуешь после того, как не нашел себе компанию?

– Часто ли мы судим о человеке только по первому взгляду на него?

– Встречались ли вы с подобными ситуациями в жизни? и др.

Далее всем следует внимательно прочитать комикс «Рыбный день» (или посмотреть его анимированную версию на Youtube, это удобнее, так как можно делать паузу и обсуждать произошедшие изменения).

Обсуждение комикса удобно выстраивать по плану:

– Как вы себя чувствуете?

– Понравился ли вам мультимедийный комикс? Почему?

– Может быть, кто-то что-то хочет прокомментировать? Кому-то что-то было непонятно в комиксе?

– Напоминает ли этот сюжет какие-либо исторические события?

– Что тогда происходило? Кто были действующие лица? Когда это было? В чем причина? (Здесь у педагога есть возможность актуализировать предметные знания по истории) и др.

В процессе обсуждения можно обратиться к иллюстрации «Пирамида ненависти» (рис. 3) и попросить участников привести известные им примеры. Этот небольшой теоретический блок поможет осознать участникам последствия травли в обществе, вред от следования стереотипам и предрассудкам.

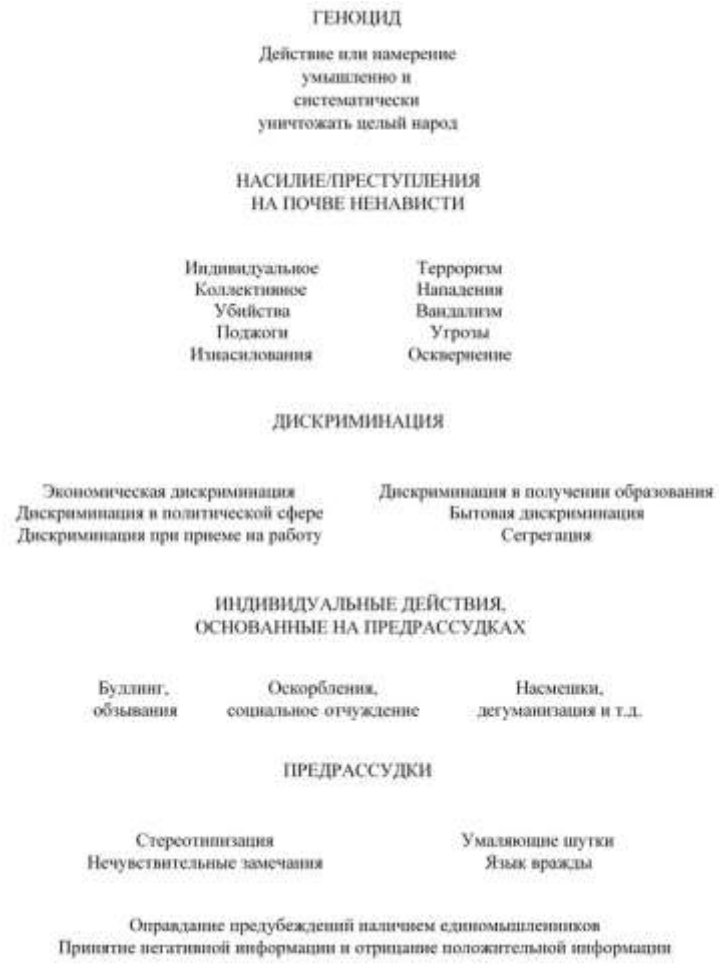


Рисунок 3 – «Пирамида ненависти»

В ходе обсуждения группа может сформулировать следующие выводы:

– Буллинг = Насилие и это ненормальное явление в нашем обществе.

– В ситуации травли всегда есть:

«Агрессор» – человек, который преследует и запугивает жертву.

«Жертва» – человек, который подвергается агрессии.

«Защитник» – человек, находящийся на стороне жертвы и пытающийся оградить ее от агрессии.

«Агрессята» – люди, участвующие в травле, начатой агрессором.

«Сторонники» – люди, находящиеся на стороне агрессора, непосредственно не участвующий в издевательствах, но и не препятствующий им.

«Наблюдатель» – человек, знающий о деталях агрессивного взаимодействия, издевательств, но соблюдающий нейтралитет.

– Типичные признаки буллинга – «Конкретное действие», «Агрессивное поведение», «Периодичность», «Угрозы», «Оскорбления», «Сарказмы» и др.

– Буллинг оказывает тяжелое психологическое воздействие и причиняет вред здоровью. Травля так же опасна, как и физическое насилие.

– Обзывание = избиение. Нельзя преуменьшать это явление и нельзя оставаться равнодушным.

На данном этапе рекомендуется так же использовать комикс «В темноте».

Своеобразным «домашним заданием» для участников может стать просьба ведущего составить список часто встречающихся ситуаций травли.

Второй блок (практический).

Главная задача участников на этом этапе – научиться распознавать ситуации травли и разные ее степени, адекватно реагировать и оставаться неравнодушными к проблеме буллинга в коллективе.

Условно, занятие можно разделить на три части:

– Примеры и ситуации из жизни.

– Чтение и обсуждение комикса «Достается всегда слабым» и\или «Мальчик из Швеции».

– Распознавание ситуаций буллинга.

Суть упражнения в следующем: ведущий зачитывает заранее подобранные ситуации травли и после каждой истории просит определиться участников так, чтобы те, кто считает ситуацию насилием, отходили к одной стене, а те, кто не считает ее таковой, – к другой.

Можно использовать те примеры, которые подготовили сами участники. По ходу определения участников можно вспомнить признаки и критерии буллинга, последствия для разных ролей.

В конце упражнения следует провести обсуждение в группе. Примерные «истории» для обсуждения:

1) Педагог в течение года при всем классе говорит: «Ну да, Петрова, ты в своем стиле, красиво пишешь, жаль, что все неправильно», половина класса смеется в ответ и оборачивается на Петрову...

2) В возрасте 10–14 лет, во дворе меня обзывали бомжом, не потому что я жила на улице. А потому что мне вещи покупали в конфискате или отдавали мамины знакомые. А девочке, с которой я общалась покупали вещи в нормальных магазинах. У нее и мама и папа работают и поэтому они ее балуют. В нашей семье такое позволить не могли, мама одна работает. Но я б не сказала, что мы в нищете жили, все хватало. Не вещи ж главное в жизни, а человек...

3) В начальных классах (с 1 по 4) меня травили за мою фамилию. Придумывали разные прозвища и т.д. Это был не 1 человек, а больше половины класса. Дошло все до того, что одна девочка даже как-то раз таскала меня за волосы за то, что я заступилась за саму себя. Все это закончилось, когда я переехала в другой город (чисто по семейным обстоятельствам). После этого меня не травил никто.

4) В классе шутят про фамилию одного ученика Петушкова. Обращаются к нему «Эй ты, петушок», «Петушочек наш» и пр.

Социальный театр

Одной из интересных и привлекательных форм работы для подростков является «социальный театр». Уникальность театральной методики состоит в том, что она легко адаптируется к тем целям и задачам, которые ставит перед собой специалист по профилактике негативных социальных явлений среди детей и подростков, созданию адекватного информационного поля.

Используя театральную технологию, специалист может во время работы над созданием спектакля помочь участникам пережить сложные моменты во

взаимоотношениях, помочь найти выход из сложной ситуации. Решение проблем личности через театральный персонаж безопаснее для подростка. Социальный театр способен усилить эмоциональную и психологическую составляющую обращения к аудитории и стать эффективным средством, позволяющим рассматривать, в том числе деликатные вопросы, в том числе и вопросы межличностных взаимоотношений. Социальный театр учит видеть и решать общие проблемы жизни, такие как толерантное отношение к другому мнению.

Суть технологии – предварительно распределение ролей и проигрывание заданных ситуаций, с последующим обсуждением в группе.

Можно использовать ситуации из второй части занятий, можно придумать новые истории. Рассматривая ситуации кибертравли, можно использовать живые примеры из сети Интернет, скриншоты переписок из социальных сетей.

Главное на этом этапе – проигрывать одну и ту же историю каждый раз по-разному, меняться ролями, принципиально менять поведение основных участников «истории». Именно такой подход позволит посмотреть на ситуации буллинга с разных позиций и оценить различные сценарии поведения, способы реакций. Лучше дать возможность каждому побыть в разной роли: «обидчика», «жертвы» и «свидетеля».

Очень важно проводить обсуждение после каждого «проигрывания» или смены ролей. Ориентирующими вопросами могут быть:

– Как вам исход событий? Довольны ли результатом?

– Удалось избежать конфликта?

– Почему не получилось? (или – Почему получилось?)

– Что было сложнее всего?

– А кому было труднее в данной ситуации?

– Могла ли история пойти в другую сторону?

– Что для этого должно было произойти? и др.

Третий блок (Рефлексия. Формулировка групповых правил).

Занятие можно начать с прочтения комикса «Такой же, как и все». Как и положено, провести обсуждение истории, опираясь на впечатления участников и личный опыт.

На данном этапе взаимодействие с группой строится на диалоге и обсуждении опыта, полученного в предыдущие занятия.

Главные выводы, к которым ведущий может подтолкнуть участников тренинга:

– Называть явление открыто. Не преуменьшать значение.

– Всегда давать однозначную оценку. (Насилие – это насилие).

– Высказывать свое мнение о ситуациях буллинга.

– Травля – проблема класса\группы\коллектива.

– Нет равнодушию.

– Важно поддержать человека, А НЕ МНЕНИЕ.

– Права человека – ЗАКОН.

– «Другой – не значит опасный».

– Понимать, что разные и уважать чужое мнение.

– «Пока я здесь, это – неприемлемо».

В процессе обсуждения ведущему важно направить группу на решение проблем в общении так, чтобы они сами инициировали правила общения, коммуникации в своем коллективе. Это может быть свой «Закон о дружбе» или «Кодекс общения 9 "А" класса». Правила должны всерьез приниматься всеми участниками группы. Можно даже ввести игровые «санкции» за нарушение правил.

Участникам тренинга, особенно старшеклассникам важно быть мультипликаторами полученного опыта. Необходимо объяснить ребятам, что одно из важнейших условий предотвращения ситуаций травли в школе – открыто рассказывать своим сверстникам о правах человека, борьбе со стереотипами и предрассудками, распространять знания о разрешении конфликтов.

Необходимо помнить о эмоциональных чувствах всех сторон конфликта, как «обидчика», так и «жертвы». Старшие ребята могут быть лучшими защитниками для младших, чем кто-либо. В некоторых школах даже создаются так называемые «Команды взаимопомощи» (LinkCrew), где старшие следят за младшими и при необходимости помогают разрешить конфликты и предотвратить ситуации буллинга. Поговорите со своей группой о создании такой команды.

Заключение

Профилактические мероприятия такого рода позволят создать в образовательной организации безопасное психологическое пространство.

Формируются устойчивые доброжелательные отношения в группе подростков.

Приобретается навык конструктивного реагирования в конфликте, снижается агрессия, изменяются представления о самом себе, о правах человека.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В РАБОТЕ ПЕДАГОГА-ПСИХОЛОГА, ЗОНЫ РИСКА И СПОСОБЫ ИХ УМЕНЬШЕНИЯ

Цель: разработать рекомендации для педагогов по работе с детьми, оказавшимися в группе риска.

Задачи:

1. Определить признаки в поведении учащегося группы риска.
2. Выработать алгоритм действий педагога.
3. Разработать план мероприятий.

Педагогам-психологам будет предложена такая ситуация: учитель заметил, что поведение ребенка изменилось. На что может обратить внимание учитель?

Задание группе 1: определить признаки в поведении учащегося, попавшего в группу риска.

Задание группе 2: выработать алгоритм действий педагога в сложившейся ситуации.

Задание группе 3: разработать план мероприятий педагога-психолога в данной ситуации.

Работа в течение 10 минут. Затем представление результатов и выработка рекомендаций для педагогов.

КАК ПОМОЧЬ РЕБЕНКУ ИЗБЕЖАТЬ ОПАСНОСТИ, ПОДСТЕРЕГАЮЩЕЙ В СЕТИ ИНТЕРНЕТ

Цель: повышение уровня информационной компетентности социальных педагогов по вопросу безопасного использования мобильного устройства и хранения в нем персональных данных.

Задачи:

1. Сформировать понятийный аппарат по вопросам защиты персональных данных.
2. Сформировать представление об основных механизмах защиты своих персональных данных в мобильном устройстве.
3. Сформировать навыки безопасного использования мобильного устройства и основы безопасного использования персональных данных.

Форма: практическое занятие.

Методы:

– беседа;

– игра.

Планируемые результаты

В результате проведенного мероприятия социальные педагоги научатся:

– научиться использовать основные механизмы защиты своих персональных данных;

– приобретут навыки трансляции полученных компетенций для участников образовательных отношений, используя различные формы и методы обучения.

Введение в тему

Упражнение «Никто, кроме моего смартфона, не знает, что я...»

Цель: знакомство с вариантами распространения персональных данных через мобильные приложения.

Задача: помочь участникам разминки осознать, какие персональные данные хранятся на их смартфоне.

Необходимые материалы: небольшой мячик.

Время проведения: 5 минут.

Процедура проведения.

«У каждого из нас есть мобильный телефон или смартфон, в котором хранится много важной и полезной информации, в том числе и наши персональные данные. Записная книга хранит контакты, мессенджеры – переписку с друзьями, игровые приложения – историю наших побед и поражений и т.д. Иногда создается впечатление, что наш телефон знает о нас гораздо больше, чем наши родственники и друзья».

Ведущий предлагает учащимся сыграть в следующую игру.

Ведущий берет мяч в руки и говорит фразу, начинающуюся со слов *«Никто, кроме моего смартфона, не знает, что я…»* (возможные варианты ответов: *выиграл в онлайн-шахматы 90 партий из 100*, *переписываюсь с другом из Люксембурга, пробежал в прошлое воскресенье 25 км и т.д.*). Затем ведущий бросает мяч любому участнику группы. Задача участника – придумать свое окончание фразы *«Никто, кроме моего смартфона, не знает, что я...»* и передать мяч следующему игроку.

Игра продолжается до тех пор, пока все учащиеся не скажут свой вариант ответа.

Вопросы для обсуждения:

– Легким или сложным показалось вам это упражнение? Почему?

– Какой из вариантов фразы показался самым необычным или запомнился больше всего? Почему?

– Как по-вашему, то, что наши смартфоны так много знают о нас – хорошо или плохо? Почему?

Теоретическая часть

В соответствии со статьей 7 Федерального закона «О персональных данных» от 27 июля 2006 года № 152-ФЗ (далее – Закон) лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных. В настоящее время все чаще номера телефонов передаются и используются без согласия абонента, так как в законодательстве четко не указано, что они являются персональными данными.

Казалось бы, набор цифр номера телефона никак не может персонифицировать субъекта персональных данных, он полностью обезличен. Но добавьте к этим цифрам ФИО, и ситуация в корне изменится. Плюс, если этот номер закреплен за конкретным физическим лицом по договору с оператором связи, то говорить об обезличенности набора цифр вовсе не приходится.

И действительно, согласно ст. 3 Закона, персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных), то есть его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, в связи с чем можно сделать вывод, что номер мобильного телефона также является персональными данными.

Но ст.3 Закона также вводит понятие обезличивания персональных данных, которое включает в себя действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных. Сам по себе номер телефона без указания сведений о его владельце, является информацией обезличенной, то есть набор цифр нельзя признать персональной информацией.

А вот если номер телефона использован с указанием на ФИО его владельца, то такая информация уже носит характер конфиденциальной, и может

быть использована только с согласия субъекта персональных данных на обработку его персональных данных.

Статья 44.1. Закона «О связи» 07.07.2003 № 126-ФЗ с изменениями, вступившими в силу 21.10.2014г., также закрепляет, что если по номеру телефона можно как-либо идентифицировать абонента, то необходимо согласие абонента, например, на рассылку рекламной информации.

Выводы:

1. Номер телефона является персональными данными.

2. Передача персональных данных третьим лицам без согласия субъекта персональных данных незаконна.

3. Использование номеров телефонов в случае отсутствия дополнительных сведений об их владельцах также требует согласия**.**

Какие персональные данные хранит само мобильное устройство?

Что нужно сделать чтобы защитить персональные данные, которые находятся в телефоне?

Обновление операционной системы и используемых приложений

Включите автоматическое обновление приложений на вашем телефоне или попросите систему уведомлять вас о наличии новинок, чтобы не упустить момент. И всегда загружайте обновления операционной системы, как только вам будет предложено это сделать.

Зачем это нужно? Чтоб предотвратить взлом телефона через уязвимости в операционной системе и приложениях. Когда авторы программ и игр обновляют свой софт до более новых версий, они составляют отчет об исправленных ошибках. Результаты исправлений они выкладывают на всеобщее обозрение, поэтому хакеры берут эти данные и направляют свои атаки на тех пользователей, которые операционную систему либо приложения не обновили и оставили свои смартфоны или аккаунты в социальных сетях уязвимыми.

Загрузка приложений

1. При загрузке приложений пользуйтесь только проверенными магазинами вроде AppStore и GooglePlay – это официальные источники, где приложения проверяют перед выставлением на всеобщее обозрение и скачиванием обычных пользователей. Поэтому там гораздо меньше шансов нарваться на вредоносное программное обеспечение. Когда же программа скачана с неофициального магазина или сайта, где размещают нелицензионные материалы, то последствием может стать взлом телефона.

2. Подозрительные приложения могут иногда попадаться даже в официальных магазинах. Чтоб избежать обмана, внимательно изучайте информацию о приложении, смотрите на отзывы пользователей, количество скачиваний и общий рейтинг программы.

3. Следите за разрешениями, которые у вас просят приложения при установке или запуске. Это может быть доступ к личным фото, смс-переписке, совершению звонков и особым функциям, например, к функциям разработчика. Всего одно неверное решение – и мошенники смогут получить удаленный доступ к вашему смартфону.

Отказ от получения Root-прав

В Интернете вы могли встречать обсуждения преимуществ, которые дает установка специальных приложений, дающих пользователю операционной системы AndroidRoot-права. Это означает, что с их помощью можно полностью редактировать «внутренности» смартфона, удалять приложения, которые обычно нельзя удалить, например, стандартные, получить доступ к системным папкам и файлам, улучшить производительность устройства.

Однако вместе с неограниченными возможностями вы делаете свой смартфон уязвимым к хакерским атакам. В случае, когда такие права получит вредоносное приложение, оно будет иметь доступ ко всем файлам на вашем мобильном устройстве, даже к таким, как чтение sms для восстановления доступа к аккаунту и подтверждение банковских операций.

Осторожность в использовании публичного Wi-Fi

Когда вы однажды подключитесь к какой-либо беспроводной сети, ваш смартфон запомнит пароль и при нахождении этой сети во второй раз подключится к ней автоматически. Если сеть не защищена паролем, то и запоминать ничего не придется. Казалось бы, очень удобно, но есть один момент. Мошенники могут создавать свои горячие точки вместо знакомых вам точек с Wi-Fi, и называть их тем же именем. Если вы подключитесь к такой точке, то злоумышленник получит доступ ко всем передаваемым данным и будут следить за вашими действиями в сети Интернет, а позже, по собранным сведениям, смогут осуществить взлом телефона.

Чтобы такого не произошло, не следует подключаться к публичным беспроводным сетям, не защищенным паролем, а также очищать список всех сетей, которые «запомнил» ваш телефон. Не ленитесь записать пароли к используемым вами точкам и вводите его каждый раз при подключении, чтобы защитить смартфон от взлома.

Когда же есть необходимость использовать публичные Wi-Fi сети, пользуйтесь VPN-сервисами, которые шифруют ваше интернет-соединение и защищают ваши данные, чтоб их нельзя было перехватить и осуществить взлом.

Отключение сетей Wi-Fi и Bluetooth

Снизить риск взлома телефона поможет отключение сетей Wi-Fi и Bluetooth, когда вы ими не пользуетесь. Тогда у хакера не будет возможности осуществить удаленный доступ к вашему мобильному устройству. С одной стороны, злоумышленник может дождаться момента, когда вы вновь подключитесь к одной из сетей, но с другой – не сумев взломать ваш телефон, он может бросить эту затею, если его цель – массовый взлом аккаунтов, а не именно вы.

Контроль SMS-переписок

Игнорирование подозрительных ссылок, sms-сообщений – тоже хорошая защита от взлома. Многие хакерские атаки и распространение вирусов начи-

нались именно переходом невнимательных пользователей по вредоносным ссылкам. Но осторожным нужно быть, не только открывая ссылки в Интернете, а и получая sms. Обращайте внимание на подозрительные сообщения со странными запросами, даже когда они пришли от вашего друга – его смартфон тоже могли взломать.

Использование сложного пароля

Как утверждает статистика, 80% всех паролей – это простые слова: имена, марки телефона или машины, имя кошки или собаки, а также пароли вроде 123. Такие пароли сильно облегчают работу взломщикам. В идеале пароли должны состоять минимум из семи, а лучше двенадцати символов. Время на подбор пароля из пяти символов – два-четыре часа, но, чтобы взломать пароль из семи символов, потребуется два-четыре года. Лучше использовать пароли, комбинирующие буквы разных регистров, цифры и разные значки.

Заключение

Смартфоны и другие «умные» устройства все активнее проникают в нашу жизнь, делая ее более комфортной и удобной. Однако за это удобство нам приходится платить – нашими персональными данными. Без преувеличения можно сказать, что наши смартфоны порой знают о нас больше нас самих. Поэтому мы должны с осторожностью использовать смартфоны и другие гаджеты, защищать их антивирусными программами и надежными паролями. Устанавливая новые приложения на смартфон, следует внимательно ознакомиться с условиями, предлагаемыми разработчиками.

КАК РЕАЛИЗОВАТЬ ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ?

В эпоху Интернета и цифровых технологий персональная информация человека находится под угрозой. Публикуя личные данные на страницах многочисленных социальных сетей, в резюме сайтов по поиску работы, да и просто заполняя опросный лист интернет-магазинов, пользователь рискует тем, что опубликованные сугубо личные данные могут быть использованы мошенниками в противозаконных действиях. Мы не задумываемся, где оставляем информацию о себе и своей жизни, а также, кто из доверенных субъектов может передавать ее третьим лицам.

Персональные данные представляют собой информацию о конкретном человеке. Это те данные, которые позволяют нам узнать человека в толпе, идентифицировать и определить, как конкретную личность.

Таких идентифицирующих данных огромное множество, к ним относятся: фамилия, имя, отчество, дата рождения, место рождения, место жительства, номер телефона, адрес электронной почты, фотография, возраст и пр**.**

Так, если мы кому-то скажем, свои фамилию, имя, отчество и адрес места жительства, то нас вполне можно будет опознать как конкретное лицо. Но если мы исключим из этого набора данных фамилию или адрес места жительства, то понять, о каком человеке идет речь будет невозможно.

Получается, что персональные данные – это не просто ваши фамилия или имя, персональные данные – это набор данных, их совокупность, которые позволяют идентифицировать вас.

В целом можно сказать, что персональные данные – это совокупность данных, которые необходимы и достаточны для идентификации какого-то человека.

Общие правила защиты персональных данных

Защита персональной информации может обеспечиваться несколькими источниками права:

– Первым источником защиты является ФЗ № 152-ФЗ «О персональных данных», в котором закреплены гарантии, нормы, правила регуляции обмена и открытой публикации материалов.

– Вторым источником является система организационно-правовых отношений, устав образовательной организации, политика конфиденциальности, общепринятая в данной сфере.

– Третьим фактором служит право на защиту личной информации, гарантированное Конституцией РФ каждому ее гражданину.

Начнем с правил создания и хранения сложных и надежных паролей. Вы, конечно же, придумали себе пароль, возможно даже не один, но обязательно используйте эти правила, убедитесь, что ваш пароль можно назвать сложным и надежным.

Кто-то скажет «у меня в Интернете ничего ценного, поэтому пароль 123456», но ничего хорошего в этом нет, так как вашими данными с радостью воспользуются злоумышленники (например, для того чтобы выманить деньги с ваших родственников и знакомых):

1. Пароль должен быть сложным (рис. 4). Все знают, что пароль должен быть достаточно сложным, но что это значит?

– Хороший пароль должен содержать минимум 10 символов, чтобы его было сложно взломать (посчитайте, сколько символов в вашем пароле к социальной сети?).

– Надежный пароль должен содержать 12 символов и более (ваш пароль на основную почту должен быть именно таким длинным).

– Сложный пароль должен содержать три набора символов: большие и маленькие буквы, цифры, специальные символы (PochtiSlozhniyParol123%!).

– Пароль должен быть без общедоступной информации (имя, фамилия, ник, важные даты, номера телефонов, ИНН, адреса, как свои, так и родственников – это не для пароля! [MarinaAV1965 – плохой вариант]).

– Пароль должен быть без словарных слов и без простых сочетаний слов (используйте малораспространенные слова или вообще несуществующие слова [Абырвалг]).

Рисунок 4 – Образец сложного пароля

2. Для разных сайтов – разные пароли. Возможно, вы скажете: «Зачем мне столько паролей?» Давайте посмотрим, зачем это нужно.

Самое важное в Интернете – это ваш e-mail, так как почти все сервисы в Интернете привязаны к вашей электронной почте. Если кто-то получит доступ к вашей электронной почте, то сможет получить доступ ко всему остальному. Поэтому наибольшая степень защиты должна быть у вашего почтового ящика. Например, двухфакторная аутентификация или генерирование сложного пароля.

На малонадежных сайтах e-mail и пароль лежат рядом. Если такой сайт взломают, первое что сделают – проверят, подходит ли пароль к вашей электронной почте, затем попробуют получить доступ к аккаунту в социальной сети и средствам онлайн-оплаты.

Злоумышленники продают друг другу базы взломанных аккаунтов, поэтому риск взлома всех ваших аккаунтов резко возрастает.

Как же быть? Есть простой способ упростить задачу, разделив все сервисы на две группы:

– для обычных аккаунтов использовать более простые, похожие пароли;

– для важных аккаунтов (e-mail, интернет-банкинг) использовать сложные, уникальные пароли и менять их не реже, чем раз в три месяца.

3. Храните пароль надежно. Память инструмент не самый надежный, поэтому лучше использовать один из нескольких проверенных способов надежного хранения паролей.

– Бумажный блокнот – да, даже ведущие специалисты по информационной безопасности признают этот вариант. Вот только храните такой блокнот подальше от любопытных глаз, да и пароли в нем храните в непонятном или зашифрованном виде.

– Менеджер паролей – специальная программа, которая помнит пароли за вас, вам лишь нужно помнить один пароль для доступа к остальной базе.

– Текстовый документ – не самый удачный вариант хранения паролей, но его тоже можно использовать, если вы сможете хранить документ безопасно: в архиве под паролем, но это уже вариант менеджера паролей.

Для каждого способа обязательно используйте резервное копирование.

Как нельзя хранить пароли:

– на бумажке, прикрепленной к монитору или лежащей на столе под клавиатурой (есть прецеденты государственных масштабов);

– в текстовом документе на рабочем столе (с именем «Пароли» или на флэшке, карте памяти телефона и т.д.);

– в браузере тоже не рекомендуется хранить пароли. Особенно на рабочем компьютере, где доступ имеют несколько человек (учителей).

4. Проверьте параметры восстановления пароля. Вашу почту могут попытаться взломать, попытавшись восстановить пароль. Если у вас для восстановления доступа используется ответ на секретный вопрос, его можно угадать или найти ответ в социальных сетях через личные связи. Например, девичья фамилия или день рождения матери.

Ответ на секретный вопрос должен быть стойким к угадыванию (используйте неожиданные ответы, например: «Ваш любимый цвет» – «Закат»).

Если же для восстановления используется второй e-mail, все правила из этой статьи тоже должны относиться к нему.

E-mail для восстановления должен быть надежно защищен (проверьте параметры безопасности сейчас, не откладывайте).

5. Используйте двухфакторную аутентификацию. Для важных аккаунтов используйте двухэтапную или двухфакторную аутентификацию. Например, вы вводите пароль, а с помощью телефона получаете дополнительный одноразовый код для доступа к онлайн-сервису (это может быть sms или сгенерированный в приложении код). В этом случае взломать ваш аккаунт будет значительно сложнее.

Еще одна проблема, с которой можно столкнуться – это размещение персональных данных будущих первоклассников на стендах школы в приказах о приеме в первый класс.

В этом случае можно сказать с уверенностью, что специалист, издающий приказы, не ознакомлен с процедурой охраны персональных данных в образовательной организации, отсутствует соответствующий регламент издания приказов.

Заключение

Незнание закона не снимает ответственность, что очень важно в эпоху Интернета и высоких технологий. Уследить за всеми законодательными аспектами и нюансами невозможно, однако систематизировать и структурировать процессы обработки, хранения и предоставления данных, во избежание проблем с законом – вполне реально.

НАУКА КРИПТОГРАФИЯ

Надежный пароль – это не просто пароль, который сложно угадать, это еще и пароль, который легко запомнить. Хотя сегодня и существуют специальные программы, позволяющие генерировать и хранить сложные пароли на компьютере, гораздо надежнее хранить пароль в голове.

Цель: познакомиться с основами криптографии (метод тайнописи).

Задачи:

1. Ввести участников в тему мероприятия.
2. Познакомить с критериями надежности паролей.
3. Познакомить со способами составления надежных паролей и приемами, позволяющими запомнить составленные пароли.

Необходимые материалы: белые листы бумаги формата А4, цветные карандаши, фломастеры, маркеры и т.д.; памятка «Правила составления надежных паролей» (приложение 3) по количеству участников.

Введение в тему практикума. Блиц-опрос

Участникам предлагается принять участие в блиц-опросе по теме информационной безопасности (приложение 4). Опрос проводится с помощью Google форм в сети Интернет. Выход в Интернет возможен с мобильных устройств участников практикума.

Защита персональных данных с помощью пароля в сети Интернет

Дом, в котором мы храним личные вещи, нуждается в прочной двери и надежном замке. Ключ от дома защищает наши ценности в реальном мире, а пароль защищает в мире виртуальном. Так же и наши персональные данные, которые мы размещаем в социальных сетях или облачных сервисах, должны храниться под замком, ключом к которому является пароль.

По данным Международного союза электросвязи, в 2015г. Интернетом пользовались более 3,2 млрд. человек по всему миру, и, конечно, у всех этих людей имелся хотя бы один аккаунт и пароль к нему. Поскольку пользователей Интернета так много, неудивительно, что пароли, которые они используют, могут повторяться.

Чтобы узнать, какие же пароли чаще всего используют в Интернете, ведущий дает несколько минут на то, чтобы придумать как можно больше ответов на вопрос: «Какой пароль – самый популярный среди пользователей Интернета?». Он напоминает, что все пароли записываются латиницей и предлагает участникам практикума написать на выданных листах пароли. Участники предлагают свой вариант ответа. Повторяться или давать сходные ответы нельзя. Ответы слушателей помещаются на магнитной доске, при этом ведущий следит, чтобы пароли не дублировались. По ходу ведется обсуждение способа составления такого пароля.

Когда все участники предложили свой вариант ответа, ведущий показывает и озвучивает 10 самых популярных паролей интернета (приложение 5).

Практикум по составлению паролей

Ведущий предлагает участникам разделиться на микрогруппы (2-3 человека). Каждому участнику выдается памятка с рекомендациями по составлению надежного пароля. Группам предлагается придумать надежный пароль с помощью одного из методов.

После окончания работы, каждая группа по очереди представляет свой пароль на доске, а другие участники должны попытаться угадать, какое «послание» было зашифровано при составлении этого пароля (иными словами, понять, как он был получен). Если другим участникам это не удается, группа в качестве подсказки может назвать способы шифрования, использованные для составления пароля. В конце упражнения методом открытого голосования выбирается самый удачный пароль – надежный и запоминающийся (голосовать за свой пароль нельзя).

Заключение

Обсуждение результатов блиц-опроса (приложение 6).

РОДИТЕЛЬСКОЕ СОБРАНИЕ ПО ТЕМЕ «Я – В СЕТИ!»

Цель: актуализация у родительского сообщества проблематики безопасности детей в информационной среде.

Задачи:

1. Привлечь внимание родителей к данной проблематике.
2. Сформировать понятийный аппарат по вопросам информационной безопасности.
3. Познакомить с законодательной базой в области защиты персональных данных.
4. Актуализировать знания в области профилактики интернет-зависимости.

Форма: семинар-практикум.

Формы и методы:

− интерактивная лекция;

− практическое занятие;

− дискуссия;

− самостоятельная работа (анализ теоретического и практического материала).

Планируемые результаты

В результате проведенного мероприятия родители:

– обратят внимание на данную проблематику;

– познакомятся с понятийным аппаратом и законодательной базой в области защиты персональных данных;

– актуализируют свои знания по безопасному поведению в сети Интернет.

Введение в тему

Важно привлечь внимание родителей к проблемам и последствиям ненадлежащей обработки персональных данных и широкого распространения личной информации в информационной среде.

Необходимо разобрать теоретические аспекты данной проблематики путем обсуждения продемонстрированного социального ролика (демонстрация социального ролика, размещенного на сайте федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций – https://pd.rkn.gov.ru/multimedia/video114.htm).

Практическая часть. Описание

Станция «Ловушки и капканы»

Упражнение «Цифровой след».

Задача: показать, какие «цифровые следы» могут храниться в компьютере и других устройствах, а также познакомить родителей с тем, какими способами персональные данные попадают в Интернет.

Необходимые материалы: набор из 9 карточек со скриншотами «цифровых следов» (приложение 7), лист с правильными ответами и пояснениями для ведущего (приложение 8).

Время проведения: 15 минут.

Процедура проведения.

Упражнение состоит из двух этапов.

Первый этап. Аудитория делится на подгруппы по 3–4 человека. Если родительская аудитория небольшая, то можно работать в парах и даже по одному. Каждая группа получает карточку с изображением скриншота, содержащего «цифровой след» пользователя. Задача – определить, какой вид персональной информации содержит скриншот. Для того чтобы родители поняли алгоритм выполнения задания, ведущий приводит пример анализа одной из карточек по выбору, пользуясь ключами. На выполнение задания отводится 5 минут. Затем каждая подгруппа по очереди озвучивает свой ответ. Ведущий сверяет ответы с ключами и в случае необходимости задает участникам наводящие вопросы.

Второй этап. Все карточки выкладываются на один стол или прикрепляются на доску. Ведущий обращает внимание группы на то, что карточки имеют разную маркировку (белый, серый или черный квадрат в верхнем левом углу) и предлагает участникам определить, по какому принципу маркированы карточки. Если группа не может дать правильный ответ, его дает ведущий. Затем ведущий подводит итоги данного этапа.

Обсуждение:

– О каких способах попадания информации в Интернет вы узнали впервые, а о каких уже знали?

– Как вы думаете, каким способом информация чаще всего попадает в сеть? Почему?

– Как вам кажется, каким способом ваша персональная информация чаще всего попадает в сеть? Почему?

В помощь ведущему: карточки разделены на три группы в соответствии с тем способом, с помощью которого личные данные попадают в сеть:

– 1-ая группа (белый квадрат) – пользователь выкладывает в Интернет информацию о себе сам;

– 2-ая группа (серый квадрат) – информацию об активности пользователя в сети собирают приложения и онлайн-ресурсы;

– 3-ая группа (черный квадрат) – информацию о пользователе в сеть выкладывают третьи лица.

Упражнение «По секрету всему свету».

Задача: помочь родителям в осознании утраты контроля над информацией после того, как она выложена в сеть, а также сложности контроля за персональными данными в сети Интернет.

Необходимые материалы: листы бумаги и ручки по количеству учащихся, клеевой карандаш.

Время проведения: 15 минут.

Процедура проведения.

В качестве разминки ведущий предлагает поиграть. Каждый участник берет небольшой листочек бумаги и записывает на него секрет про себя. Ведущий должен отметить, что секреты не будут зачитываться вслух, но тем не менее они не должны быть слишком личными и значимыми для участников. Затем листочки складываются несколько раз. Их можно также «запечатать» (заклеить) клеевым карандашом. Затем группа садится в круг. По команде ведущего каждый участник передает свой листочек с секретом участнику, сидящему справа, и берет листок у сидящего слева. Через несколько секунд ведущий дает команду, и участники снова меняются секретами. Эти действия продолжаются до тех пор, пока «секреты» не вернутся к своим хозяевам. Теперь участники могут проверить, сохранна ли печать, поставленная клеевым карандашом. На этом игра заканчивается, и можно переходить к обсуждению.

Если в аудитории нет возможности сесть в круг, упражнение можно выполнять, разбившись на пары. В этом случае напарники встают лицом к друг другу, берут листок с секретом в правую руку и подставляют левую руку ладонью вверх. По команде ведущего участники меняются секретами, получая чужой секрет в свою левую руку. Ведущий дает возможность группе побыть в таком состоянии несколько минут. Затем по команде все возвращают секреты обратно. Этот вариант упражнения технически проще и безопаснее. Поэтому если ведущий не уверен, что в группе установился достаточно высокий уровень доверия, лучше выполнять его. Чтобы подстраховаться, ведущий может предложить участникам выбрать себе в пару человека, которому они больше всего доверяют.

В помощь ведущему: когда мы делимся информацией с другими людьми- не важно, лично или выкладывая ее 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 участникам 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 ве-

дущий не уверен в этом, он может предложить участникам выписать на листочек 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? Если бы вы узнали секрет, поделились ли бы вы им с другими? Почему?

– Случалось ли вам выкладывать личную или секретную информацию о другом?

Станция «В гостях у юриста»

Обсуждение и определение нарушения прав человека данной проблематики после демонстрации социального ролика, размещенного на сайте федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций – https://pd.rkn.gov.ru/multimedia/video114.htm

Станция «Паутина»

Встреча с педагогом-психологом по теме «Компьютерная зависимость у подростков». Можно рассмотреть следующие вопросы:

– Понятие «компьютерная зависимость».

– Причины компьютерной зависимости у подростков.

– Симптомы компьютерной зависимости у подростков.

– Способы борьбы с компьютерной зависимости.

Встреча с социальным педагогом по теме «Безопасный поиск в Интернет». Можно рассмотреть следующие вопросы:

– Основные рекомендации родителям о безопасности детей в Интернете (для различных возрастных категорий).

– Способы настройки безопасного поиска в сети Интернет.

Станция «Будь в тренде»

Игра «Оглянись вокруг».

Цель игры: привлечение родителей к проблемам информационной безопасности через укрепление детско-родительских отношений.

Задачи:

1. Познакомить родителей с потенциальными угрозами информационной безопасности.

2. Обратить внимание родителей на необходимость защиты персональных данных.

Оборудование и материалы: набор букв для каждой команды, стикеры с изображением паука, молнии, щита, мультимедийная презентация, компьютеры с доступом в сеть Интернет, онлайн-сервис Learningapps.org.

Ход игры:

Введение. Сегодня мы не представляем свою жизнь без компьютера и сети Интернет. В настоящее время ведется множество неоднозначных раз-

говоров о пользе и вреде всемирной сети. Дети и подростки – активные пользователи интернета, ведь он предоставляет подрастающему поколению невероятные возможности для совершения открытий, общения и творчества. Но у любого явления есть свои светлые и темные стороны, и зачастую дети и молодежь в полной мере не осознают все возможные проблемы, с которыми они могут столкнуться в сети.

Интернет представляет собой открытое окно в мир, который также принадлежит взрослым и содержит материалы, не подходящие для детей, поэтому с использованием киберпространства связаны определенные риски.

Как должны родители и взрослые помочь детям избежать все возможные неприятности, чтобы сделать их пребывание в Интернете более безопасным, научить их ориентироваться во всемирной сети? Простого ответа не существует. Риски могут быть разными в зависимости от возраста и компьютерной грамотности ребенка.

Конечно же, отказ от использования этих современных технологий не является решением проблемы защиты детей в онлайн-пространстве. Это все равно что запретить ездить автотранспорту по улицам и придворовым территориям, чтобы дети не попадали в ДТП. Во избежание несчастных случаев нужно лишь научить ребенка быть осторожным, соблюдать определенные правила, быть ответственным пешеходом, следовать положительному примеру взрослых. Аналогично наиболее важной задачей взрослых является предупреждение детей об опасностях Интернета, чтобы они вели себя осторожно, обдуманно. Кроме того, необходимо обсуждать с детьми все те вопросы, которые могут у них возникнуть при использовании Интернета.

На нашей встрече мы поговорим о возможных рисках, с которыми могут столкнуться наши дети в Интернете.

Современную жизнь трудно представить без компьютера и сети Интернет. Благодаря информационным технологиям мы находим любую информацию, общаемся с друзьями, участвуем в дискуссиях, обсуждаем новости, оставляем комментарии, выкладываем фотографии. Вместе с тем ведется множество разговоров о пользе и вреде всемирной сети.

Интернет представляет собой открытое окно в мир, в котором есть светлые и темные стороны. Интернет предоставляет невероятные возможности для познания, открытий, общения. Но чаще мы не осознаем все возможные проблемы, с которыми мы можем столкнуться в сети.

Как нам избежать всех возможных неприятностей в сети Интернет? Сегодня мы поиграем в игру, которая поможет нам сделать пребывание в Интернете более безопасным.

Основной этап. Перед вами лежит набор букв. Вам необходимо собрать фразу «Оглянись вокруг» *(родители составляют фразу)*. «Оглянись вокруг» – это название игры. Игра «Оглянись вокруг» посвящена безопасности в сети Интернет. Оглянитесь вокруг. Что вы видите? *(на стене приклеены стикеры с изображением паука, молнии, щита)*. Каждое изображение – это явление, происходящее вокруг нас, когда мы входим в сеть Интернет.

Посмотрите на первый слайд. Здесь изображен паук. Паук – это угроза

информационной безопасности. Как вы думаете, какие бывают угрозы информационной безопасности? Упражнение «Классификация угроз информационной безопасности» (https://learningapps.org/1484219).

Выполнив данное упражнение, вы узнали, что существуют угрозы целостности, угрозы доступности и угрозы конфиденциальности. Но существует и иной вид угрозы. Посмотрите на слайд. На слайде изображена молния. Молния означает угрозу под название «Кибербуллинг». Кибербуллинг – это запугивание, унижение, травля. Чтобы узнать, какие бывают виды киербуллинга, необходимо выполнить упражнение «Кибербуллинг и его разновидности» (https://learningapps.org/5314609).

Таким образом, существует множество угроз информационной безопасности. Угрозы направлены на наши персональные данные, которые мы размещаем в сети Интернет. Если личные данные будут открыты, злоумышленники могут воспользоваться ими в своих целях. Поэтому очень важно защищать персональную информацию. На слайде изображен щит. Щит означает безопасность, защиту. Как вы защищаете свои персональные данные в Интернете? Как вы думаете, что можно и нельзя размещать в Интернете? *(родители отвечают на вопросы, затем выполняют упражнение)* «Персональные данные в сети Интернет» (https://learningapps.org/3141917).

Заключительный этап.

На заключительном этапе родители с помощью онлайн-сервиса Learningapps.org создают интерактивное упражнение «Безопасный Интернет».

ЗАНЯТИЕ ДЛЯ ОБУЧАЮЩИХСЯ 5-7-х КЛАССОВ ПО ТЕМЕ «ГИГИЕНА В СЕТИ ИНТЕРНЕТ»

Цель: формирование у подростков представлений безопасного поведения в интернет-пространстве.

Задачи:

1. Информировать обучающихся о безопасных настройках персонального профиля в социальных сетях.
2. Познакомить обучающихся с видами угроз при установке (скачивании) различных приложений (игр) на мобильные устройства.
3. Способствовать формированию безопасного поведения при общении в социальных сетях.

Форма: классный час.

Формы и методы:

– беседа;

– анкетирование;

– дискуссия;

– ролевая игра;

– рефлексия.

Планируемые результаты

В результате занятия обучающиеся:

– приобретут сформированные представления об угрозах в сети Интернет;

– изучат способы безопасного поведения в сети Интернет;

– приобретут навыки безопасного поведения в социальных сетях.

Введение в тему

Интернет сегодня стал неотъемлемой частью жизни людей любого возраста. Он может служить во благо. При помощи сети люди могут общаться, развлекаться, искать нужную информацию и даже зарабатывать деньги. Однако Интернет известен и массой отрицательных проявлений. Они касаются как детей, так и взрослых. Существуют определенные опасности в Интернете. Нежелательный контент, насилие, навязчивое общение – все это может негативно отразиться на психике человека. Также длительное пребывание перед компьютером ухудшает физическое состояние организма. На занятии вы подробнее узнаете, как защитить себя от негативных воздействий всемирной паутины.

Викторина с ответами

Предлагаем ответить на вопросы викторины.

1. Ты зашел на незнакомый сайт. Вдруг на экране компьютера появились непонятные сообщения. Что ты можешь предпринять?

(Если что-то непонятно, всегда зови на помощь родителей!)

2. На уроке биологии тебе задали найти изображение инфузории-туфельки. Ты нашел картинку в Интернете, но для того, чтобы ее сохранить нужно отправить sms на указанный номер в Интернете. Как ты поступишь?

(Никогда не отправляй сообщения на незнакомые номера!)

3. Ты познакомился в Интернете с мальчиком (девочкой), с которым у вас много общего, и вы быстро подружились, но он не учится в твоей школе и живет в другом районе. Он предложил пойти вместе погулять и встретиться в известном тебе месте. Ты пойдешь на встречу?

(Никогда не соглашайся на подобные встречи! Многие люди, с которыми ты общаешься в Интернете, могут оказаться обманщиками!)

4. Новый друг, с которым ты недавно познакомился в Интернете, просит дать твой номер телефона и сказать адрес. Ты согласишься?

(Никогда не рассказывай в Интернете личную информацию о себе! Это должны знать только близкие тебе люди!)

5. После школы ты любишь поиграть в любимую компьютерную игру в Интернете, но тебе постоянно мешают посторонние сообщения, приглашения. Что можно сделать для того, чтобы не получать ненужную тебе информацию?

(Чтобы не сталкиваться с неприятной информацией в Интернете можно установить фильтр или попросить об этом родителей!)

Социальные сети. Настройка профиля

В Интернете есть специальные сайты, смысл которых в том, чтобы объединить людей. Через них можно переписываться, обмениваться фотографиями, слушать музыку, смотреть видео, играть в игры и многое другое. Называются такие ресурсы социальные сети.

Для того, чтобы зарегистрироваться в социальных сетях, необходимо указать свои данные. При этом следует помнить о безопасности своих данных.

Если вы сами не позаботитесь о безопасности своих данных, о ней не позаботится никто. И лучше сделать это раньше, чем злоумышленники получат доступ к вашему аккаунту. Для вашей безопасности соблюдайте несколько правил.

1. Указывайте минимум личных данных в аккаунте.

«Где учился» – школа-ВУЗ, но без подробного направления. Социальные сети предлагают желающим указывать приятелей-подружек, родственников. Зачем тебе это делать? Ты свою семью с родней знаешь отлично, они тебя тоже знают. А чужому народу знать про твои семейные и дружеские отношения ни к чему.

Если все же вы указываете своих родственников и друзей, то сделайте так, чтобы информация вашего профиля была доступна не всем через настройки конфиденциальности.

Вообще, стоит заполнять только обязательные пункты раздела «о себе», которые помечены звездочкой.

2. Чем меньше фото-видео – тем лучше.

Современные гаджеты – смартфоны и планшеты – наряду с доступной интернет-связью облегчают социальные коммуникации в современном обществе. Мода на селфи-фото, видео и текстовое описание своей жизни в социальных аккаунтах, причем в детальных подробностях – современная норма.

«Волшебная жизнь» медийных кумиров из инстаграмма, твиттера или фейсбука манит тебя? Не беспокоишься за выставление своей личной жизни напоказ? Напрасно. У разноплановых «звезд» имеются секьюрити, адвокаты и выгодно оплачиваемые договоренности с соцсетями.

3. Никогда не указывай домашнего адреса.

В рубрике «где живешь» достаточно вписать страну и город. Не указывай район, улицу и, тем более, дом и квартиру.

Адреса в Интернете постят пользователи, которые делают в сети бизнес, а тебе адрес сообщать всему Интернету не нужно.

Тема раскрывается через упражнение «Мой профиль».

Упражнение «Мой профиль»

Задача: объяснить учащимся, что такое персональные данные, и показать, как безличная информация становится персональной.

Необходимые материалы: форма для заполнения по количеству учеников (приложение 2), доска.

Время проведения: 20–25 минут.

Процедура проведения.

Ведущий обращает внимание участников группы на то, что большинство онлай-ресурсов объединяет одна важная особенность – для получения полного доступа ко всем возможностям этих сайтов на них необходимо зарегистрироваться.

Наверняка процедура регистрации хорошо знакома всем участникам: она, как правило, предполагает заполнение регистрационной формы. Чтобы разобраться в этом вопросе более глубоко, ведущий предлагает участникам выполнить следующее задание:

«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».

После этого ведущий раздает участникам формы регистрации и просит их заполнить. На выполнение этого задания отводится 5 минут. Затем ведущий собирает заполненные формы и говорит участникам 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? Чтобы получить ответ на этот вопрос, ведущий в случайном порядке раздает заполненные профили участникам и ставит перед ними задачу: угадать, чей профиль, и написать свою догадку на полученном листке с профилем. На выполнение этой задачи также отводится 5 минут. Важно, чтобы в это время участники не подсказывали друг другу и не высказывали свои догадки вслух.

Когда все участники выполнят задание, ведущий просит каждого по очереди озвучить логин хозяина профиля, а затем высказать и обосновать предположение по поводу его личности. Только после того, как все догадки будут высказаны, ведущий просит хозяев профилей подтвердить или опровергнуть правильность ответов. На эту часть упражнения может уйти от 10 до 15 минут в зависимости от числа участников и активности. Когда все ответы озвучены и проверены, можно переходить к обсуждению результатов упражнения.

После завершения упражнения ведущий возвращает каждому участнику заполненный им профиль и отмечает необходимость бережного обращения со своими персональными данными.

Обсуждение:

– Какой профиль было угадать проще/труднее всего?

– Что помогло/помешало угадать личность хозяина профиля?

– Какими соображениями мы руководствуемся, заполняя профиль?

Таким образом, информация, размещенная в профилях, является персональными данными. Персональные данные позволяют нам установить или идентифицировать личность человека. Чем больше информации о себе размещает человек, тем проще другим людям установить вашу личность. Эта информация может повлиять на вашу репутацию, а также привлечь мошенников. Поэтому надо быть предельно осторожным, когда размещаете о себе информацию в социальных сетях.

Таким образом, информация, размещенная в профилях, является персо-

нальными данными. Персональные данные позволяют нам установить или идентифицировать личность человека. Чем больше информации о себе размещает человек, тем проще другим людям установить вашу личность. Эта информация может повлиять на вашу репутацию, а также привлечь мошенников. Поэтому надо быть предельно осторожным, когда размещаете о себе информацию в социальных сетях.

Угрозы при установке (скачивании) различных видов приложений на мобильные устройства

Использование мобильных устройств в повседневной жизни не ограничивается голосовыми звонками и sms. Возможность загружать и выполнять программы, а также мобильный доступ в Интернет привели к появлению громадного числа мобильных приложений. Функциональность современного смартфона составляют браузеры, клиентские программы социальных сетей, офисные приложения и всевозможные сервисы, работающие в сети. Вместе с мобильными приложениями появились и различные угрозы, знать о которых необходимо, а также уметь себя от них защитить.

Один из видов угроз – это вредоносные программы для смартфонов, которые отправляют sms на premium-номера (за звонок снимается отдельная плата) или звонят без ведома пользователя. Такие программы могут быть замаскированы под любые полезные приложения, распространяемые бесплатно.

Следующую угрозу представляют приложения, установка которых производится не из официального магазина PlayMarket, а из посторонних источников. При этом чаще всего пользователь самостоятельно подтверждает разрешение установки приложений из неизвестных источников в разделе «безопасность» настроек своего телефона. В результате, на смартфон скачивается вирус, а инфицированные телефоны пытаются переводить средства с электронных кошельков или с привязанных карт банков на балансы мошенников.

Кроме этого, следует помнить об основных законах антивирусной безопасности: не следует переходить по ссылкам в sms или мобильной почте, пришедшим с неизвестных номеров или адресов.

Тема раскрывается через упражнение «Лаборатория мобильных приложений».

Упражнение «Лаборатория мобильных приложений».

Задача: помочь учащимся осознать, что при выборе мобильных приложений необходимо ориентироваться на соотношение возможностей, предлагаемых ресурсом, и запрашиваемых им персональных данных.

Необходимые материалы: листы ватмана формата А1, цветные маркеры, наклейки.

Время проведения: 25 минут.

Процедура проведения.

«Существует множество бесплатных «приложений» для смартфонов, которые помогают нам в повседневной жизни и скрашивают досуг. Однако все они являются «бесплатными» лишь условно. На самом деле пользователи расплачиваются за них своими персональными данными. Поэтому нам при-

ходится выбирать между сохранностью персональных данных и нашим удобством». Чтобы этот выбор был осознанным, участникам предлагается встать на место разработчиков мобильных приложений.

Ведущий делит учащихся на несколько микрогрупп, каждая из которых становится «командой разработчиков». Перед ее участниками стоит задача создать мобильное приложение, которое пользовалось бы популярностью у пользователей. Для этого необходимо придумать оригинальную идею приложения и сделать презентацию для потенциальных покупателей. Материал для презентации создается на листах ватмана с помощью маркеров и содержит название приложения, краткое описание основных функций, а также виды персональных данных, которые потребуются при работе с приложением. Участники могут изучить iTunes или Google Play, чтобы понять, какие приложения существуют на рынке, какими они обладают функционалом и как их рекламируют. На выполнение этой части задания отводится 10 минут.

После того как все команды выполнят задание, можно переходить к презентации проектов. Каждая группа получает 2 минуты на выступление и ответы на вопросы. Когда все презентации прозвучали, путем простого открытого голосования выбирается лучшее предложение. Голосовать за свое приложение запрещается.

В помощь ведущему: выбирая мобильное приложение, следует задуматься, какую личную информацию оно запрашивает у пользователя взамен на предоставляемые возможности. Если набор персональных данных соответствует прямому функционалу программы, например, сервис вызова такси онлайн запрашивает информацию о вашем местоположении, то это разумный выбор. Однако если набор персональных данных очень велик и выходит за пределы функционала программы, например, погодный информер требует доступа к вашему аккаунту в социальной сети, то устанавливать ее будет не слишком разумно.

Обсуждение:

– Какое приложение набрало больше всех голосов? Какое – меньше всех? Почему?

– Какими правилами следует руководствоваться, устанавливая приложение на смартфон?

Таким образом, смартфоны и другие «умные» устройства все активнее проникают в нашу жизнь, делая ее более комфортной. Но не следует забывать об угрозах. Поэтому мы должны с осторожностью использовать смартфоны и другие гаджеты, защищать их антивирусными программами и надежными паролями. Устанавливая новые приложения на смартфон, следует внимательно ознакомиться с условиями, предлагаемыми разработчиками.

Что делать, если вас приглашают куда-то в социальных сетях

Тема раскрывается через демонстрацию видеоролика и его обсуждения, размещенного на сайте федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций – https://pd.rkn.gov.ru/multimedia/video114.htm

Заключение

В конце занятия выдается памятка (приложение 10) о безопасном поведении в сети Интернет.

Итоги занятия проводятся в виде вопросов викторины, которая была в начале занятия.

РОДИТЕЛЬСКОЕ СОБРАНИЕ ПО ТЕМЕ «СОВРЕМЕННАЯ ЖИЗНЬ В ОТКРЫТОМ ИНФОРМАЦИОННОМ ОБЩЕСТВЕ»

Цель: повышение информационной компетентности родителей путем определения рисков в сфере приватности и обеспечения безопасности использования персональных данных.

Задачи:

1. Познакомить с понятийным аппаратом в рамках безопасного обращения с персональными данными в сети Интернет.
2. Расширить представления об основных способах защиты своих персональных данных и персональных данных своих детей.
3. Рекомендовать интернет-ресурсы, оказывающие поддержку в вопросах информационной безопасности и защите персональных данных.

Форма: родительское собрание.

Формы и методы:

- интерактивная лекция;
- практическое занятие;
- деловая игра;
- дискуссия;
- анкетирование;
- круглый стол.

Планируемые результаты

В результате проведения родительского собрания родители смогут:

- владеть понятийным аппаратом;
- донести до сознания своих детей последствия неосторожного обращения с информацией личного характера в интернете и необходимости ее защиты;
- управлять персональными данными при работе с различными онлайн-ресурсами, приложениями и устройствами.

В ходе мероприятия родители получат ответы на три вопроса:

1. Что мы знаем о персональных данных?
2. Почему необходимо защищать свои персональные данные и персональные данные своих детей?
3. Каким образом можно управлять персональными данными?

Основная целевая аудитория мероприятия – родители (законные представители) учащихся 6–10-х классов средних общеобразовательных школ (т.к. подросткам чаще бывает проще раскрыться и «излить» душу виртуальному знакомому, чем родным или друзьям. Поэтому крайне важно донести до родителей подростков ценность личной информации, объяснить возможные последствия неосторожного обращения с ней и научить их эффективным способам управления персональными данными).

Введение в тему

В настоящее время объективной реальностью является необходимость обеспечения безопасности личной информации, поскольку информация о человеке сегодня превратилась в дорогой товар. Защита личной информации может приравниваться к защите личности, при этом степень угрозы безопасности личности (частная жизнь, личная, семейная тайна, жизнь и здоровье личности, собственность и пр.) может определяться в каждом конкретном случае незаконного использования информации о личности.

В этой связи вопросы защиты персональных данных получили в последние годы особое звучание – развитие интернет-технологий, широкое распространение персональных гаджетов с разнообразными функциями, в том числе, геолокационными выдвинули эту проблематику в разряд наиболее злободневных.

В силу своей незрелости дети подвержены различным угрозам со стороны злоумышленников, более того дети порой сами могут причинить себе вред, не отдавая отчет тем последствиям, которые могут наступить в результате их собственных поступков и действий.

Так многочисленные исследования свидетельствуют о том, что чрезмерное увлечение общением в информационно-телекоммуникационных сетях крайне негативно сказываются на психологическом и физическом состоянии подрастающего поколения. А ведь помимо прочего это еще и этические проблемы, то есть правила хорошего тона, культурного поведения в сети Интернет. Современным детям нужно объяснять, что размещать фотографии друзей в Интернете без их разрешения также нехорошо, как и читать чужие письма, что свою личную информацию нужно защищать от посягательств со стороны третьих лиц. Так, размещение личной информации о друзьях или себе может привести к ужасным последствиям, когда репутация ребенка будет неисправима.

Распространение личной информации в глобальной сети не только нарушает требование законодательства в области персональных данных, но также может повлечь за собой неблагоприятные последствия для детей и их родителей. Всегда нужно помнить, что злоумышленники, имея свободный доступ к информации о социальном статусе, семейном положении, могут воспользоваться ситуацией и совершить неправомерные посягательства на частную жизнь семьи, здоровье и половую неприкосновенность детей.

Тема раскрывается упражнением «Детективное бюро».

Упражнение «Детективное бюро»

Задача: научить участников определять, какую персональную информацию могут содержать различные материалы, размещаемые в сети Интернет.

Необходимые материалы: карточки с заданиями (приложение 11), комментарии для ведущего (приложение 12).

Время проведения: 20 минут.

Процедура проведения:

В начале упражнения ведущий говорит: «Мы с вами узнали, что существуют разные виды персональных данных. Сообщение, выложенное в Ин-

тернет, 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».

Ведущий предлагает участникам группы разделиться на пять микрогрупп по 3–5 человек. Каждая микрогруппа – это небольшое детективное агентство, которое получает в качестве улики карточку с постом из социальной сети. Задача группы – провести расследование и узнать, как можно больше информации об авторе этого поста. На выполнение задания отводится 5–7 минут. Затем каждая группа кратко представляет результаты своего расследования. Участники других групп могут задавать вопросы и делать свои комментарии. Ведущий в процессе обсуждения сверяется с комментариями (приложение № 12).

Обсуждение:

– 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 о нас то, что мы хотим.

Итоги упражнения.

Подводя итоги, ведущий еще раз напоминает участникам, что существуют разные виды персональной информации. Некоторыми видами данных большинство из нас охотно делится с другими, в том числе в Интернете, 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.

Понятия в рамках безопасного обращения с персональными данными в сети Интернет

Основополагающим законом в области защиты персональных данных является Федеральный закон «О персональных данных» № 152, который был принят Государственной думой 8 июля 2006 года и вступил в силу с 26 января 2007 года. Закон определяет:

– основные понятия, связанные с обработкой персональных данных;

– принципы и условия обработки персональных данных;

– обязанности оператора персональных данных;

– права субъекта персональных данных;

– виды ответственности за нарушение требований ФЗ № 152;

– государственные органы, осуществляющие контроль за соблюдением требований ФЗ-№152.

В соответствии с Законом персональные данные – любая информация, с помощью которой можно однозначно идентифицировать физическое лицо. К персональным данным, в связи с этим могут относиться фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, принадлежащая субъекту персональных данных.

Федеральный закон «О персональных данных» выделяет следующие категории персональных данных.

Общедоступные персональные данные – данные, доступ к которым предоставлен неограниченному кругу лиц с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяются требования соблюдения конфиденциальности. Общедоступные источники персональных данных создаются в целях информационного обеспечения (например, справочники и адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные субъектом персональных данных.

Важно отметить, что сведения о субъекте персональных данных могут быть в любое время исключены из общедоступных источников по требованию субъекта либо по решению суда или уполномоченных государственных органов.

Специальные категории персональных данных – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни. Их обработка допускается только в следующих случаях:

– субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;

– персональные данные являются общедоступными;

– персональные данные относятся к состоянию здоровья субъекта персональных данных и получение его согласия невозможно, либо обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;

– обработка персональных данных членов (участников) общественного объединения или религиозной организации при условии, что персональные данные не будут распространяться без согласия в письменной форме субъектов ПД;

– обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации о безопасности, об оперативно-розыскной деятельности, а также в соответствии с уголовно-исполнительным законодательством Российской Федерации или необходима в связи с осуществлением правосудия.

Биометрические персональные данные – это сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность. Они могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных. Обработка биометрических персональных данных без согласия субъекта персональных данных может осуществляться в связи с осуществлением правосудия, а также в случаях, предусмотренных законодательством Российской Федерации о безопасности, об оперативно-розыскной деятельности, о государственной службе, о порядке выезда из РФ и въезда в РФ, уголовно-исполнительным законодательством.

Определение биометрических данных в российском законодательстве предоставляет оператору персональных данных возможность принятия самостоятельного решения об отнесении тех или иных данных к биометрическим. Это породило немало споров. Рассмотрим пример с фотографией. С одной стороны, она характеризует физиологические особенности человека. Но человек с течением времени может сильно измениться или злоумышленник может подделать внешние признаки под законного субъекта. Так ли однозначно в данном случае установление личности? В настоящее время представители регуляторов подтверждают, что фотография и видеоизображения относятся к биометрическим данным.

Аккаунт, учетная запись (англ. account) – хранимая в компьютерной системе совокупность данных о пользователе, необходимых для его опознавания (аутентификации) и предоставления доступа к его личным данным и настройкам.

Кибербуллинг (англ. cyberbulling) – намеренное и регулярное причинение вреда (запугивание, унижение, травля, физический или психологический террор) одним человеком или группой людей другому человеку с использованием электронных форм контакта.

Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Фишинг (англ. phishing, от fishing – «рыбная ловля, выуживание») – вид интернет-мошенничества, целью которого является получение доступа

к конфиденциальным данным пользователей – логинам и паролям. Достигается путем проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков или внутри социальных сетей. В письме часто содержится прямая ссылка на сайт, внешне не отличимый от настоящего, либо на сайт с редиректом (redirect). После того как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приемами побудить пользователя ввести на поддельной странице свои логин и пароль, которые он использует для доступа к определенному сайту, что позволяет мошенникам получить доступ к его аккаунтам и банковским счетам.

Хакеры (или крэкерами) называют компьютерных взломщиков – программистов, злонамеренно добывающих конфиденциальную информацию в обход систем защиты.

Тема раскрывается викториной «Пойми меня».

Викторина «Пойми меня»

Для проведения викторины заранее снимается видеоролик.

Задача: познакомить с понятийным аппаратом по вопросам защиты персональных данных.

Необходимые материалы: демонстрация видеоролика, в котором учащиеся описывают понятия, используемые при работе с персональными данными.

Время проведения: 10 минут.

Процедура проведения.

Ведущий просит отгадать основные понятия, которые прокомментировали учащиеся.

Способы защиты персональных данных

Когда-то люди умели хранить секреты. Но с приходом цифровой эры возможностей оставить что-либо конфиденциальным становится все меньше. Данные о наших повседневных действиях: общении с друзьями, поездках в отпуск и покупках – все это и многое другое записывается и хранится на серверах разных компаний и организаций.

Но в наши дни информация не складируется на пыльных носителях где-то в кладовке. Данные хранятся на подключенных к Интернету серверах, их покупают, продают, используют разнообразными способами, а иногда и воруют. И более чем вероятно, что вы не одобрите некоторые сценарии применения ваших данных, если о них узнаете. Всегда неприятно обнаружить, что личные сведения утекли в глобальную сеть и все вокруг обсуждают вашу размолвку с женой, или то, что вы сейчас по уши в долгах, так как вашему ребенку была нужна операция.

Защита личных данных – это важная проблема для людей всех возрастов. Предлагаем вам ознакомиться с простыми правилами, которые помогут вам сохранить конфиденциальность.

1) Каждая социальная сеть – это бесценный источник информации для злоумышленников, собирающих персональные данные, которые они затем

используют для обмана и мошенничества. Поэтому так важно правильно настроить конфиденциальность вашего профиля Facebook, «ВКонтакте», «Одноклассников» и любой другой социальной сети.

2) В вашей почте хранятся «ключи» от большинства ваших учетных записей, так как процедура восстановления пароля чаще всего осуществляется именно с помощью email-сообщений. Поэтому жизненно необходимо обезопасить свой основной почтовый адрес, к которому привязаны интернет-банк и самые важные для вас сайты. Если вы хотите зарегистрироваться на сайте знакомств или в каком-нибудь сомнительном сервисе, лучше создайте второй (а то и третий или даже четвертый) почтовый ящик.

3) Не публикуйте онлайн фотографии ваших документов, билетов и платежных чеков. Также не стоит рассказывать о том, когда вы собираетесь уехать в отпуск или полдня и полночи отрываться в местном ночном клубе. Эти данные очень интересуют как кибермошенников, охотящихся за чужими финансами, так и обычных домушников, ждущих, когда люди уйдут куда-нибудь надолго.

4) Не используйте открытые Wi-Fi-сети. Они могут выглядеть как вполне надежный источник Интернета, предоставленный местным кафе или даже библиотекой, но вам будет сложно отличить «добропорядочный» Wi-Fi от «зловредного». Чтобы создать такую сеть, преступнику понадобятся всего лишь ноутбук и Wi-Fi-адаптер. И мошенники действительно используют этот метод, чтобы перехватить логины и пароли пользователей, пытающихся подключиться к Интернету с помощью их Wi-Fi-сетей.

5) Избегайте ненадежных паролей. Слабые комбинации практически ни от чего не защищают.

6) Помните о том, что для детей проблема конфиденциальности так же актуальна, как и для взрослых. Кибертравля – не миф, от нее страдают множество подростков по всему миру. Поэтому важно не публиковать посты, фото и видео, которые могут смутить вашего ребенка сейчас или в будущем.

7) Вам надоела реклама в Сети? Баннеры могут превратить обычную интернет-страницу в выставку продуктов, которые вам не нужны и неинтересны. А вы знаете, что такие рекламные объявления к тому же шпионят за тем, чем вы занимаетесь онлайн?

8) Интернет-магазины используют ваши данные, чтобы продавать вам больше товаров благодаря персонализированной рекламе, – для этого они отслеживают ваше поведение в сети Интернет.

9) Конечно, маркетинг был бы менее успешным, если бы программы для сбора данных не попадали к нам на ПК довольно незаметным и при этом полностью легальным образом. Когда вы устанавливаете бесплатное ПО, вам часто предлагают поставить дополнительно разнообразные плагины, расширения и панели инструментов. Многие не читают надписи при установке программы, а просто нажимают «Далее». В этом случае вместе с нужной утилитой устанавливается целый пакет бесполезных дополнений, которые способны поменять привычные для вас настройки на незнакомые: например, поставить новую домашнюю страницу и свой сервис поиска.

10) Прежде чем вводить свои персональные данные в интернете, необходимо убедиться, что вы находитесь именно на том ресурсе, на который хотели попасть, а не на поддельной (фишинговой) странице, созданной мошенниками. Существует несколько простых способов убедиться в подлинности ресурса:

– всегда обращайте внимание на адресную строку браузера. Адрес поддельной странички может отличаться всего на одну букву, которую легко не заметить, например: в адресе www.odnoklassniki.ru может быть пропущена всего одна буква «s», но это будет уже совсем другой сайт;

– не стоит переходить на ресурсы по ссылкам, которые вы получили по электронной почте или в личной переписке и которые требуют ввода персональных данных – многие из них ведут на поддельные сайты. Введите адрес в адресную строку самостоятельно, а еще лучше используйте для поиска нужных ресурсов надежные поисковые системы, например, Яндекс.

– прежде чем вводить персональные данные в интернете, убедитесь, что ресурс, на котором вы находитесь, использует защищенное соединение. Если в адресной строке браузера присутствует иконка замка, а сам адрес начинается с аббревиатуры https:// вместо привычной http://, то такое соединение использует шифрование при передаче ваших персональных данных. В этом случае злоумышленникам будет гораздо сложнее перехватить ваши персональные данные и воспользоваться ими.

– комплексные антивирусные программы также могут помочь защититься от мошенников. Многие из них содержат базы данных опасных и ненадежных ресурсов и способны предупреждать о возможной опасности, блокируя переход по фишинговым ссылкам.

11) Для удаления «цифровых следов» с компьютера после работы в интернете очистите журнал посещений (в браузере) и историю поисковых запросов (в аккаунте сайта-поисковика). С помощью средств операционной системы и браузера или специализированных приложений вы можете удалить автономные веб-страницы, временные файлы из интернета, а также cookies (небольшие фрагменты данных, которые отправляются онлайн-ресурсом и хранятся на компьютере пользователя; они помогают сайтам «запоминать» пользователей и их индивидуальные предпочтения), которые также могут многое рассказать о вашей работе в сети. Все это вы сможете сделать, только если обладаете необходимыми правами (например, администратора).

12) В настройках программ сетевой защиты также можно установить запрет на загрузку временных файлов и cookies с незнакомых сайтов, ограничившись лишь проверенными и надежными ресурсами.

13) Будьте внимательны с настройками мобильных приложений: отключите опцию «автосинхронизации» данных, автоматического проставления «геометок» и т.д., если хотите избежать случайного попадания персональных данных в глобальную сеть. Защита персональных данных на чужом устройстве.

14) При входе в свой аккаунт с чужого устройства всегда выбирайте опцию «чужой компьютер», «не сохранять пароль», «безопасный ввод» и т.д. (на странице онлайн-ресурса). В этом случае вы можете быть уверены, что никто не войдет в ваш аккаунт после вас.

15) Чтобы не оставить цифровых следов на чужом устройстве, используйте режим инкогнито (в браузере). Благодаря ему история поисковых запросов и посещенных страниц не сохраняется в браузере, а сайты не загружают cookies на устройство.

16) Используя вкладку «настройки приватности» (на странице онлайн-ресурса), запретите другим пользователям отмечать вас на фотографиях и упоминать в постах. Ограничьте круг лиц, которые могут комментировать ваши записи. Как правило, добавление пользователя в «черный список» автоматически лишает его возможности просматривать и комментировать ваши посты, а также упоминать вас в своих постах.

17) Если другой пользователь использует ваши персональные данные, например, фотографии, без вашего согласия, вы можете пожаловаться в службу поддержки ресурса (на странице онлайн-ресурса), приложив доказательства нарушения. Если другой пользователь, разместив недостоверную или устаревшую информацию, нанес существенный урон вашим чести и достоинству, вы можете обратиться в суд.

При этом важно понимать, что одно только наличие у подростка профиля в данной социальной сети не является непосредственной угрозой его приватности. Вероятность столкновения с рисками, связанными с персональными данными, зависит от навыков безопасного использования сетей. В этом случае особенно важны следующие моменты:

– соблюдает ли подросток правила конфиденциальности в отношении пароля;

– какой доступ установлен к его профилю в целом и к отдельным категориям личной информации в социальной сети;

– какую информацию о себе подросток сообщает незнакомым людям;

– осведомлены ли родители о проблемах своего ребенка, связанных с последствиями неосторожного отношения к персональным данным.

Ключом к личной информации, особенно той, которая предназначена не для всех, является пароль. Именно с утерей конфиденциальности в отношении пароля нередко связаны неблагоприятные последствия в виде взломов профилей, кражи персональных данных, мошенничества и обмана в сети.

Следует помнить о том, что только одновременное соблюдение всех этих правил может надежно защитить от мошенников.

Тема раскрывается упражнением «Золотая середина».

Упражнение «Золотая середина»

Задача: предоставить участникам возможность измерить собственный уровень «открытости – закрытости» в Интернете и найти свою «золотую середину».

Необходимые материалы: бланки с тестом по количеству участников (приложение 13).

Время проведения: 10 минут.

Процедура проведения.

Ведущий говорит участникам о том, что чувствовать себя комфортно

в физическом пространстве и в виртуальном мире возможно, когда установлен баланс между открытостью и закрытостью, найдена «золотая середина», причем у каждого человека она может быть своей. В межличностном общении «золотая середина» означает то расстояние, на котором нам комфортно и безопасно общаться с разными людьми: родителями или одноклассниками, знакомыми или незнакомыми. В виртуальном пространстве мы устанавливаем ее с помощью настроек приватности – системы специальных параметров, позволяющих пользователю онлайн-ресурса настраивать уровень внешнего доступа к различным видам персональной информации. «Золотая середина» в Интернете подразумевает, что пользователь отрегулировал свои настройки приватности так, что каждый вид или категория персональной информации доступны только той аудитории, для которой сам человек хотел бы сделать ее открытой.

Первый этап. Индивидуальное заполнение теста каждым участником. Для измерения личного уровня «открытости – закрытости» в виртуальном мире участникам предлагается заполнить тест (приложение 3), позволяющий оценить уровень внешнего доступа к различным категориям персональной информации об участнике. В каждой строке предложенного бланка необходимо обвести одну цифру напротив каждого вопроса. В последнюю графу нужно вписать сумму набранных баллов. Максимальное количество баллов не может превышать 60.

Второй этап. После подсчета участниками баллов ведущий чертит на доске шкалу «открытости – закрытости» (приложение 14), выделяет на ней пять интервалов в соответствии с приведенными ниже и объясняет, как участники могут оценить полученные результаты.

• Менее 15 баллов – крайне выраженное смещение в сторону полюса «закрытости»; может свидетельствовать о чрезмерной замкнутости и склонности к самоизоляции в сети.

• 15–25 баллов – личный баланс в Интернете смещен в сторону полюса «закрытости».

• 26–34 балла – промежуточное значение, которое может говорить о том, что полюса «открытости/закрытости» в Интернете сбалансированы.

• 35–45 баллов – личный баланс в Интернете смещен в сторону полюса «открытости».

• Более 45 баллов – крайне выраженное смещение в сторону полюса «открытости»; может свидетельствовать о том, что участник склонен сообщать другим пользователям избыточную персональную информацию.

Ведущий называет каждый интервал по очереди и просит участников, набравших сумму баллов из названного диапазона, поднять руку.

Обсуждение:

– Насколько совпадает количество баллов по тесту с тем, какое положение на шкале «открытости – закрытости» вы выбрали?

– В какой диапазон вы попали? Захотелось ли вам поменять что-либо в своих настройках приватности после получения данного результата?

Итоги упражнения.

Каждый человек имеет право на выбор собственной «золотой середины» – личного уровня открытости или закрытости. Мы вправе свободно и самостоятельно решать, какая информация и при каких условиях может быть сохранена в секрете или передана другим людям. При этом следует помнить: если информация о нас лежит на поверхности, мы становимся уязвимыми; когда же мы, напротив, отгораживаемся от людей, устанавливая неприступные барьеры и сохраняя любые сведения в тайне, – есть риск остаться в одиночестве и лишиться тех возможностей, которые предоставляет нам цифровой мир. Настройки приватности в социальных сетях – наши помощники, которые позволяют нам регулировать личную «золотую середину» – оставаться открытыми для общения с миром и при этом оберегать свое персональное пространство от нежелательного вторжения.

Интернет-ресурсы, оказывающие поддержку в вопросах информационной безопасности и защите персональных данных

https://rkn.gov.ru/ – Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций.

http://персональныеданные.дети/ – для несовершеннолетних пользователей Интернета был запущен информационно-образовательный портал «Персональные данные.дети», цель которого в игровой форме объяснить детям и подросткам правила безопасного обращения с персональными данными в сети. Яркие и запоминающиеся герои в живой и понятной форме делятся с посетителями сайта своими историями, рассказывают о последствиях неосторожного обращения с личной информацией и объясняют правила безопасного использования персональных данных, а интерактивные игры и задания помогают школьникам закрепить новый материал. Информация, размещенная на сайте, рекомендована в школах для изучения в рамках уроков безопасного Интернета.

http://detionline.com/ – информация о всероссийской линии помощи «Дети онлайн». Сталкиваясь с проблемами в сети, дети и подростки часто не знают, как поступить в неприятной или опасной ситуации и куда можно обратиться за помощью. 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. Все обращения на Линию полностью анонимны и конфиденциальны.

http://сетевичок.рф/ – сайт международного квеста по цифровой грамотности. Цифровая грамотность – это набор знаний и умений, которые необходимы для безопасного и эффективного использования цифровых технологий и ресурсов интернета. На сайте подробно рассказывается о таких понятиях, как:

– информационная безопасность;

– техническая компетенция;

– цифровое потребление;

– цифровая коммуникация.

http://www.saferunet.ru/ – сайт центра безопасного Интернета в России. Сайт посвящен проблеме безопасной, корректной и комфортной работы в Интернете. Администраторы сайта занимаются интернет-угрозами и эффективным противодействием им в отношении пользователей. Центр был создан в 2008 году под названием «Национальный узел Интернет-безопасности в России». Центр безопасного Интернета в России – организатор мероприятий Международного Дня безопасного Интернета на территории Российской Федерации в форме Недели безопасного Рунета.

Тема раскрывается демонстрацией сайтов, каждому родителю выдается Памятка «Научите своих детей» (приложение 15).

ЗАНЯТИЕ ДЛЯ ПЕДАГОГОВ ПО ТЕМЕ «ШКОЛА КИБЕРБЕЗОПАСНОСТИ»

Цель: повышение информационной компетентности педагогов в вопросах информационной безопасности.

Задачи:

1. Познакомить с понятием «информационная безопасность» и мерами обеспечения информационной безопасности в образовательной организации.

2. Познакомить с понятием «персональные данные» и возможностями обеспечения защиты персональных данных обучающихся в сети Интернет.

3. Применить на практике знания о способах защиты персональных данных и безопасного использования сети Интернет.

Форма: семинар-практикум.

Формы и методы:

− лекция;

− практическое занятие (ролевая игра);

− рефлексия (устный опрос).

Планируемые результаты

В результате проведения семинара-практикума педагоги смогут:

– владеть понятийным аппаратом;

– расширить представления о мерах и возможностях обеспечения информационной безопасности и защите персональных данных;

– использовать в своей практической деятельности способы, методы и приемы обеспечения информационной безопасности и защиты персональных данных.

Введение в тему

Образовательный процесс касается наименее защищенных от пропаганды членов общества – детей и подростков. Поэтому система информационной безопасности образовательной организации должна ограждать учащихся

от любой информации, которая может негативно влиять на сознание, формирование и развитие учащихся. Система информационной безопасности образовательной организации включает в себя не только сохранность баз данных и содержащихся в них конфиденциальной информации, но и комплекс мер и мероприятий, направленных на устранение проблем и трудностей, связанных с использованием сети Интернет в образовательном процессе, а также информационное просвещение участников образовательного процесса.

Теоретические основы

В современной школе информация, информационная инфраструктура, сеть Интернет – одни из главных компонентов учебного процесса. Информация, полученная в сети Интернет, существенно определяет качество знаний, способствует формированию учебных компетенций учащихся. Поэтому обеспечение информационной безопасности образовательной организации является одной из актуальных проблем современного образования.

Информационная безопасность в образовательной организации – это комплексное состояние защищенности информационной среды, обеспечивающее ее формирование, использование и развитие в интересах учащихся.

Информационная безопасность в образовательной организации включает в себя три составляющих:

1) конфиденциальность – защита чувствительной информации обучающихся и обучающих от несанкционированного доступа;

2) целостность – защита точности и полноты информации и программного обеспечения учебного процесса;

3) доступность – обеспечение доступности информации для познавательного процесса, а также основных информационно-библиотечных и иных услуг для пользователя, несовершеннолетнего обучающегося в том числе, и в нужное для него время: в рамках учебного процесса в образовательной организации или вне ее для индивидуальной работы в домашних условиях [1].

Одной из задач информационной безопасности образовательной организации является защита обучающихся от информации, причиняющей вред их здоровью и (или) развитию. Согласно Федеральному закону от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» к информации, запрещенной к распространению среди детей, относится информация:

– побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству;

– способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;

– обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным;

– отрицающая семейные ценности, пропагандирующая нетрадиционные сексуальные отношения и формирующая неуважение к родителям и (или) другим членам семьи;

– оправдывающая противоправное поведение;

– содержащая нецензурную брань;

– содержащая информацию порнографического характера;

– о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), включая фамилии, имена, отчества, фото- и видеоизображения такого несовершеннолетнего, его родителей и иных законных представителей, дату рождения такого несовершеннолетнего, аудиозапись его голоса, место его жительства или место временного пребывания, место его учебы или работы, иную информацию, позволяющую прямо или косвенно установить личность такого несовершеннолетнего.

Таким образом, распространение запрещенной информации является одной из угроз информационной безопасности обучающихся. Также существуют иные формы угрозы информационной безопасности:

– повреждение компьютерной техники в результате механического воздействия, вирусов, по иным причинам;

– повреждение программ, используемых для обеспечения работоспособности системы или в образовательном процессе, в результате вирусов или хакерских атак;

– повреждение данные, хранимые как на жестких дисках, так и на отдельных носителях;

– действия специалистов, отвечающих за работоспособность IT-систем;

– действия обучающихся, подверженных внешнему агрессивному информационному влиянию и способных создать в образовательной организации криминальную ситуацию. В последнее время перечень таких ситуаций существенно расширился, что говорит о возможной целенаправленной психологической атаке на сознание детей и подростков.

Угрозы информационной безопасности могут носить как случайный, так и осознанный преднамеренный характер. Среди угроз, не зависящих от намерения специалистов образовательной организации, учащихся или третьих лиц, можно назвать:

– любые аварийные ситуации, например, отключение электроэнергии или затопление;

– ошибки специалистов образовательной организации;

– сбои в работе программного обеспечения;

– выход техники из строя;

– проблемы в работе систем связи.

Все эти угрозы информационной безопасности носят временный характер, предсказуемы и легко устраняются действиями сотрудников и специальных служб.

Намеренные угрозы информационной безопасности носят более опасный характер и в большинстве случаев не могут быть предвидены. Одной

из самых серьезных угроз является использование образовательного оборудования для вовлечения обучающихся в криминал и терроризм. Компьютерные сети редко подвергаются внешним атакам с целью воздействия на сознание обучающихся, но и это не исключено.

Также к угрозам информационной безопасности относится несанкционированный доступ в компьютерные сети образовательной организации для совершения хищения информации и создания нарушений в системе безопасности. Можно выделить несколько видов несанкционированного доступа:

1. Человеческий. Информация может быть похищена путем копирования на временные носители, переправлена по электронной почте. Кроме того, при наличии доступа к серверу изменения в базы данных могут быть внесены вручную.

2. Программный. Для хищений сведений используются специальные программы, которые обеспечивают копирование паролей, копирование и перехват информации, перенаправление трафика, дешифровку, внесение изменений в работу иных программ.

3. Аппаратный. Он связан или с использованием специальных технических средств, или с перехватом электромагнитного излучения по различным каналам, включая телефонные.

В связи с многообразием атак на информационную безопасность, образовательным организациям необходимо разработать комплекс мер, направленных на защиту информационного пространства и персональных данных. Выделяют следующие меры обеспечения информационной безопасности в образовательной организации:

1. Нормативно-правовой способ обеспечения информационной безопасности. Защита информации опирается на действующие законы, определяющие отдельные ее массивы как подлежащие защите. Законы выделяют те сведения, которые должны быть недоступны третьим лицам по разным причинам (конфиденциальная информация, персональные данные). Кроме законов необходимо выделить действующие в этой сфере ГОСТы, определяющие порядок защиты данных, и применяемые в этих целях методики, и аппаратные средства.

2. Морально-этические средства обеспечения информационной безопасности. В образовательной сфере большую роль играет система морально-этических ценностей. На ней должна основываться система мер, защищающих обучающихся от травмирующей, этически некорректной, незаконной информации. В целях защиты от пропаганды необходимо создавать перечни документов, программ и иных источников, которые могут травмировать психику детей, в целях недопущения их проникновения на территорию учебного заведения. Это станет одной из основ информационной безопасности.

3. Административно-организационные меры. Этот комплекс мер целиком построен на создании внутренних правил и регламентов, определяющих порядок работы с информацией и ее носителями. Это внутренние методики, посвященные информационной безопасности, должностные инструкции, перечни сведений, не подлежащих передаче. Кроме того, эти методики должны

определять порядок доступа детей к сети Интернет в компьютерных классах, возможность защиты некоторых ресурсов неоднозначного характера от доступа ребенка, запрет на пользование собственными носителями информации. Должно быть предусмотрено использование системы родительского контроля над ресурсами сети Интернет.

4. Физические меры. Среди физических мер должна быть предусмотрена пропускная система защиты в помещения, содержащие носители информации, организация контроля доступа посетителей, установления различных степеней допуска. Кроме того, к мерам физической защиты может быть отнесено обязательное копирование значимой информации на диски компьютеров, не имеющих доступа к сети Интернет. Обязательно не только установление паролей, но и их регулярная замена.

5. Технические меры. Комплексную систему защиты всего периметра компьютерной сети должны обеспечивать специализированные программные продукты, выявляющие все возможные угрозы безопасности и применяющие меры по борьбе с ними. Оптимально также ввести полный запрет на копирование любой информации с жестких дисков компьютеров образовательного учреждения. Кроме того, должно быть предусмотрено программное обеспечение, ограничивающее доступ обучающегося на определенные сайты (контент-фильтры).

Информационная безопасность также включает в себя защиту персональных данных обучающихся.

Персональные данные или личностные данные – это любые сведения, относящиеся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Выделяют следующие виды персональных данных:

1. Общие персональные данные – это основная информация о человеке. К ним относят: фамилия, имя, отчество, место прописки и проживания, паспортные данные, образование, ИНН, контактные данные, сведения о работе, доходах и т.д. Не все из них по отдельности можно отнести к персональных данным. Например, точно определить является ли номер телефона персональными данными невозможно, т.к. по номеру невозможно идентифицировать человека. Но номер телефона в связке с ФИО владельца и городом проживания относится к персональным данным.

2. Биометрические персональные данные – это физиологические и биологические характеристики субъекта: группа крови, рост, цвет глаз, вес, анализ ДНК и т. д. К ним относится и информация, которую можно получить по фото- или видеозаписи с человеком. Биометрические персональные данные часто необходимы при лечении или устройстве на работу, оформлении заграничных паспортов и виз.

3. Специальные персональные данные. Раса и национальность, вероисповедание, философские убеждения, состояние здоровья, наличие судимо-

стей относятся к специальным данным. Специальные персональные данные могут содержаться в медицинских справках, личных делах и т. д. Получить доступ к этим данным третьи лица могут только с разрешения субъекта.

4. Обезличенные персональные данные. Такие данные доступны для любого заинтересованного лица. Источниками информации могут быть адресные книжки, справочники, реестры, СМИ.

Таким образом, персональные данные – это любая информация, которая позволяет идентифицировать каждого человека. Развитие сети Интернет и его сервисов приводит к потере приватности, следовательно, к потере персональных данных, т.к. личная информация становится предметом атаки, хищения, манипулирования. Где поджидает опасность?

– *Электронная почта.* Электронную почту используют для регистрации на большинстве сайтов и сервисов, а значит, получив доступ к почте, злоумышленники смогут взломать и другие аккаунты.

– *Аккаунты в игровых сервисах.* Миллионы людей играют в игровые сервисы. Пользователи зарабатывают игровой опыт, внутриигровую валюту, покупают за реальные деньги вещи для игрового инвентаря, сами игры. Взломав игровой аккаунт, злоумышленники украдут купленные лицензионные игры, игровой инвентарь и предметы – и получат за них реальные деньги.

– *Социальные сети и мессенджеры.* Социальные сети и мессенджеры – лучшие объекты для мошенников. Для многих переписка в социальных сетях и мессенджерах заменяет электронную почту – они обмениваются фотографиями, документами, другой конфиденциальной информацией. Если грамотно не защитить свой аккаунт, хищение информации может произойти в любой момент.

– *Цифровая кража телефона.* У всех современных смартфонов есть основная учетная запись: для iOS это Apple ID, для Android – аккаунт Google. Если злоумышленники получат к ним доступ, ценная информация о вас и вашем смартфоне окажется в их руках.

– *Мобильные приложения и игры.* Программы, устанавливаемые из App Store, Google Play или Windows Marketplace, запрашивают доступ к данным: контактам, геопозиции, календарю, платежным данным. К примеру, зачем игре-головоломке знать текущее местоположение или для чего конвертеру величин нужен личный календарь?

– *Незащищенная Wi-Fi-точка.* Злоумышленники используют незащищенность открытых точек и неосторожность пользователей. Злоумышленники подбирают пароли к запароленным точкам. Таким образом они могут подключиться к Wi-Fi, и все, что вы делаете на экране и вводите на клавиатуре, видит злоумышленник.

Персональные данные подвергаются риску каждый день, поэтому важно организовать защиту личной информации. Существуют следующие способы защиты персональных данных:

1. Двухфакторная аутентификация – это двойная защита, первый рубеж которой – обычная комбинация логина и пароля, то есть то, что хранится на сервере, а второй – то, к чему есть доступ только у конкретного пользова-

теля. Например, вы вводите логин и пароль от интернет-банка, после на телефон приходит специальный SMS-код. Это и есть двухфакторная аутентификация.

2. Защищенное соединение. Совершая покупки в Интернете и другие потенциально опасные действия, обратите внимание на значок слева от адресной строки. Если слева в адресной строке указано https, значит сайт, на котором вы находитесь, работает по защищенному соединению.

3. Контроль доступа мобильных приложений к данным, хранящимся на телефоне. Каждый раз необходимо внимательно читать, к какой информации запрашивает доступ приложение или игра. Если какой-то запрос на доступ вызывает подозрение, необходимо отклонить данный запрос.

4. VPN-сервис. Доступ к Wi-Fi-точке по паролю не гарантирует безопасности. Работая в общественных местах с Wi-Fi, используйте VPN-сервис. Он перенаправляет Интернет-трафик, который не могут отследить злоумышленники.

5. Сложный пароль. «Придумайте сложный пароль» – это словосочетание можно увидеть при регистрации на сайте или создании аккаунта. Легкий пароль часто служит оружием для взлома электронной почты, аккаунтов социальных сетей. Существуют несколько способов создания сложного пароля.

Транслитерация. Это написание русского слова с помощью английской клавиатуры. Например, пароль «кибербезопасность» с помощью метода транслитерации будет выглядеть следующим образом – rb,th,tpjgfcyjcnm. К сожалению, данный способ не подходит для устройств, с виртуальной клавиатурой, где отсутствует двойная подпись клавиш.

Смещение по клавиатуре. Если при написании слова каждый раз смещаться по клавиатуре на одну букву влево, мы используем простое смещение, например, ВПЬЦЩ – это слово «арбуз». Если менять направление смещения по или против часовой стрелки, мы используем сложное смещение, например, ЛПТВЛПР – это слово «барабан».

Акроним. Если взять первые буквы из известных фраз, то мы получаем акроним, который можно использовать в качестве пароля. Например, БПОВТМГ – это первые две строки из стихотворения М. Ю. Лермонтова.

Известные последовательности. Для составления сложного пароля можно использовать первые буквы известных последовательностей слов. Например, ЯФМАМИИАСОНД – это двенадцать месяцев, ДНОСАИИМАМФЯ – это 12 месяцев наоборот.

Чередование символов. Сложный пароль может состоять из последовательности цифр, знаков, чисел, которые можно зашифровать в слове. Например, в пароле С1Л2О3Ж4Н5Ы6Й7П8А9Р1О2Л3Ь зашифровано словосочетание «сложный пароль», к которому добавлено чередование цифр от 1 до 9.

Псевдографика. Достаточно сложный пароль, который представляет собой некое изображение, созданное с помощью символов. Например, пароль _>O:o:O<_ похож на кошачью мордочку.

Размещение личной информации в сети Интернет влечет за собой неблагоприятные последствия для пользователя. Имея открытый доступ к персональным данным, злоумышленники могут воспользоваться ситуацией

и украсть данные для своих целей. Поэтому так важно знать способы защиты информации и уметь применять полученные знания в практической деятельности.

Ролевая игра «Информационная безопасность»

Ролевая игра «Информационная безопасность» представляет собой проблемное задание, выполнение которого направлено на решение вопросов, связанных с обеспечением информационной безопасности и защитой персональных данных. Особенностью данной игры является поиск решения проблемы с использованием ресурсов сети Интернет. Ролевая игра проходит в три этапа: подготовительный, основной, заключительный.

Подготовительный этап.

В образовательной организации создается команда кураторов по обеспечению информационной безопасности. В эту команду входят системный администратор, юрист, классный руководитель, учитель-предметник, педагог-психолог, социальный педагог. Каждому куратору необходимо объяснить его функции:

– заместитель директора по воспитательной работе занимается изучением информационного права, организацией мероприятий по информационной безопасности;

– классный руководитель занимается организацией защиты персональных данных обучающихся и их родителей;

– учитель-предметник занимается организацией работы обучающихся по безопасному поиску и использованию информации в сети Интернет;

– педагог-психолог занимается изучением информационно-психологической безопасности личности и влияния компьютерных технологий на психику человека;

– социальный педагог занимается изучением информационно-педагогической безопасности детей «группы риска».

В ходе подготовительного этапа каждый куратор формулирует проблему, связанную с обеспечением информационной безопасности.

Основной этап.

Основной этап ролевой игры «Информационная безопасность» включает в себя три основных элемента: наличие проблемы, поиск информации, решение проблемы.

Перед началом игры на столе необходимо разложить разноцветные бумажные фигуры: квадрат, треугольник, круг, ромб, шестиугольник. Участники мероприятия выбирают одну из фигур. Таким образом происходит распределение участников по группам, закрепленных за кураторами: «Заместитель директора по ВР», «Классный руководитель», «Учитель-предметник», «Педагог-психолог», «Социальный педагог».

Задание для каждой группы – составить план действий по устранению проблемы, придуманной куратором. В качестве помощи участники мероприятия могут использовать полезные ссылки в сети Интернет (табл. 1).

Таблица 1

Ссылки в сети Интернет

Заместитель директора по ВР	http://cro.chel-edu.ru/New%20Folder/content/Internet-bezopasnost.pdf http://www.consultant.ru/document/cons_doc_LAW_108808/ http://www.consultant.ru/document/cons_doc_LAW_61801/ http://www.consultant.ru/document/cons_doc_LAW_61798/
Классный руководитель	http://cro.chel-edu.ru/services/mediabezopasnost/mediabezopasnost/ https://rocit.ru/knowledge/internet-banking/50-pravil-internet-bezopasnosti https://lifehacker.ru/protecting-your-personal-data/
Учитель-предметник	http://www.bibldetky.ru/bezopasnost/238-internet.html https://libnvkz.ru/chitatelyam/dlia_detei_i_ne_tolko/chitaite-format!/detskie-poiskoviki https://nsportal.ru/shkola/obshchepedagogicheskie-tekhnologii/library/2013/07/10/metodicheskie-rekomendatsii-bezopasnyy
Педагог-психолог	http://bookap.info/psywar/grachev/#o http://psihomed.com/kompyuternaya-zavisimost-u-podrostkov/
Социальный педагог	https://e-koncept.ru/2016/56022.htm http://открытыйурок.рф/статьи/652762/

Время выполнения задания – 60 мин. После выполнения задания участники представляют свой план действий в одной из форм: мультимедийная презентация, выступление, плакат. Каждый план действий оценивается по критериям (табл. 2).

Таблица 2

Критерии оценивания плана действий

Критерий	Отлично	Хорошо	Удовлетворительно
Решение проблемы	План действий структурирован, логичен, дает четкий ответ на поставленный вопрос.	План действий имеет четкую структуру, но недостаточно выражено решение проблемы.	План действий не дает четкого ответа на поставленный вопрос.
Творческий подход	План действий отличается уникальностью, яркой индивидуальностью.	План действий содержит новые походы к решению проблемы, но присутствует заимствование из предложенных источников.	Копирование информации из предложенных источников.

Заключительный этап.

На заключительном этапе проводится рефлексия занятия в форме устного опроса:

1. Были ли затруднения при создании плана действий?

2. Были ли полезны представленные Интернет-ресурсы? Использовали ли вы другие источники информации?

3. Какие трудности могут возникнуть в вашей деятельности по обеспечению информационной безопасности?

Возможен вариант проведения анкетирования. Разработанные планы действий оформляются в виде Справочной информации пользователя сети Интернет.

Заключение

Когда мы делимся информацией с окружающими нас людьми, то теряем над ней контроль, что может вызвать у нас чувство тревоги и дискомфорта. Размещая 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 глобальную 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. Именно поэтому необходимо бережно относиться к персональным данным, попадающим в Интернет. Можно назвать три главные составляющие, обеспечивающие более или менее надежную защиту персональных данных:

1. Надежный пароль.

2. Управление уровнями доступа к персональным данным (настройки приватности).

3. Сознательное отношение к информации, размещаемой в Интернете.

Существует много каналов, по которым наши персональные данные попадают в Интернет. Что-то размещаем мы сами, что-то пишут о нас наши друзья и знакомые, определенную информацию собирают приложения и онлайн-ресурсы. Все наши «цифровые следы» хранятся в наших компьютерах и смартфонах. Если мы хотим сохранить определенный уровень конфиденциальности и хорошую репутацию в сети, эти «следы» необходимо контролировать. Важно знать, что «цифровые следы» также хранятся на серверах разработчиков приложений и онлайн-ресурсов и удалить их оттуда практически невозможно. Поэтому всегда нужно крайне внимательно относиться к той информации, которую мы выкладываем в сеть, а также к тому, что мы делаем в Интернете: какие ресурсы посещаем, какие файлы скачиваем, какие делаем поисковые запросы и т.д. На первый взгляд может показаться, что отдельные «цифровые следы» не представляют угрозы для нашей конфиденциальности. Например, многое ли можно узнать о человеке по его хобби или гастрономическим предпочтениям? Однако важно понимать, что в Интернете потоки персональных данных объединяются друг с другом, как ручьи сливаются в реки, а реки – в моря и океаны. В целом такая обобщенная информация может дать достаточно полное представление о человеке. Современные технические средства легко позволяют объединить «цифровые следы» одного пользователя в единый портрет или профайл и идентифицировать его. Существуют сайты, которые специально собирают информацию о пользователях в коммерческих целях, например, для рекламы, маркетинговых исследований. Сбор персональных данных приложениями и онлайн-ресурсами – условие бесплатного и даже платного использования этих ресурсов, поэтому оградить себя полностью от этого невозможно. Всегда нужно помнить о том, что практически любое наше действие в Интернете оставляет после себя неизгладимый «цифровой след», и по возможности стремиться контролировать свои персональные данные, попадающие в глобальную сеть.

Приложение 1

Правила безопасного Интернета

1. Никогда не давайте частной информации о себе (фамилию, номер телефона, адрес, номер школы) без разрешения родителей.

2. Если кто-либо говорит вам, присылает вам, или вы сами обнаружили в сети что-либо смущающее вас, не старайтесь разобраться в этом самостоятельно. Обратитесь к родителям или учителям – они знают, что надо делать.

3. Встреча в реальной жизни со знакомыми по Интернет-общению не является очень хорошей идеей, поскольку люди могут быть разными в электронном общении и при реальной встрече. Если вы все же хотите встретиться с ними, сообщите об этом родителям, и пусть они пойдут на первую встречу вместе с вами.

4. Не открывайте письма электронной почты, файлы или Web-страницы, полученные от людей, которых вы реально не знаете или не доверяете им

5. Никогда не делайте того, что может стоить денег вашей семье, кроме случаев, когда рядом с вами родители.

6. Всегда будьте вежливыми в электронной переписке, и ваши корреспонденты будут вежливыми с вами.

7. Никому не давайте свой пароль, за исключением взрослых вашей семьи.

Приложение 2

Бланк заполнения персональных данных

Создание учетной записи

Логин* _____

Пол* О Мужской О Женский

Возраст* _____

Электронная почта* _____@_____

Номер мобильного телефона +7 (_____) _____-_____-_____

Пароль* _____

Подтверждение пароля* _____

Страна _____

Город _____

Skype _____

Семейное положение _____

Образование _____

Место работы/учебы _____

Интересы _____

Любимая музыка _____

Любимые книги _____

Любимые кинофильмы _____

Любимые телепередачи _____

Создать четную запись
v

Правила составления надежных паролей

Для получения сложного, но легко запоминающегося пароля можно использовать любое слово, зашифровав его с помощью одного из следующих методов:

1. **Транслитерация.** Если взять любое слово русского языка и набрать его на клавиатуре с латинской раскладкой, то получится бессмысленное сочетание символов. Например, **RJYUHTUFWBZ –** это слово «конгрегация». К сожалению, этот метод плохо подходит для устройств с виртуальной клавиатурой, где отсутствует двойная подпись клавиш.

2. **Смещение по клавиатуре.** Если при написании слова каждый раз смещаться по клавиатуре на одну клавишу влево, мы используем *простое смещение*, например **ВПЬЦЩ** – это слово «арбуз». Если менять направление смещения по или против часовой стрелки, мы используем *сложное смещение*, например, **ЛПТВЛПР** – это слово «барабан».

3. **Акроним.** Если взять первые буквы слов из известной фразы, то мы получаем акроним, который можно использовать в качестве пароля. Например, **МДСЧПКНВШЗ** – это первые две строки из романа А.С. Пушкина «Евгений Онегин».

4. **Известные последовательности.** Также д ля с оставления пароля можно использовать первые буквы известных последовательностей слов. Например, **ЯФМАМИИАСОНД** – это двенадцать месяцев. Всегда можно усложнить последовательность, например, изменив направление и величину шага. **ДОАИАФНСИММЯ** – это последовательность месяцев наоборот и через один.

5. **Чередования символов.** Любой пароль можно усложнить, добавив последовательность цифр или знаков, которые можно чередовать с зашифрованным словом. Например, **П1А2Р3О4Л5Ь6**.

6. **Псевдографика.** Достаточно сложный, но хорошо запоминающийся пароль можно создать с помощью псевдографики — использования символов шрифта для создания графических изображений. Например набор символов **_>(0:o:0)<_** похож на кошачью мордочку.

Чтобы сделать надежный пароль, необходимо использовать несколько различных видов шифрования. Возьмем слово **ПАРОЛЬ**, транслитерируем – **GFHJKM**, добавим через одну букву шесть цифр, но в обратном порядке – **G6F5H4J3K2M1**, а теперь поменяем цифры через одну на соответствующие им символы – **G6F%H4J#K2M!**.

Одну и ту же систему шифрования можно использовать для разных паролей, добавив систему индексов, например, **ПАРОЛЬ**MAIL.RU, **ПАРОЛЬ**GMAIL.COM, **ПАРОЛЬ**VK.COM.

Это существенно упростит процедуру запоминания паролей и сделает их достаточно надежными и безопасными.

Вопросы блиц-опроса

1. **Какая информация может быть отнесена к персональным данным?**

a) Фамилия, имя, отчество.

b) Дата и место рождения.

c) Место учебы.

d) Политические и религиозные убеждения.

e) Все предложенные варианты.

2. **Какие из приведенных персональных данных позволяют однозначно идентифицировать пользователя в нашей стране?**

a) Имя, фамилия, год рождения.

b) Фамилия, год рождения, номер школы.

c) Имя, номер паспорта РФ, город проживания.

d) Имя, фамилия, город проживания.

e) Ни один из предложенных вариантов.

3. **При регистрации на сайте у вас запросили номер телефона. В каком случае это наиболее безопасно?**

a) Вы регистрируетесь на крупном и хорошо известном онлайн-ресурсе, например, на портале Mail.ru.

b) Вы первый раз совершаете покупку в интернет-магазине, на сайте которого размещены положительные отзывы других пользователей.

c) Вы регистрируетесь на игровом портале, который порекомендовали вам ваши друзья и знакомые.

d) Вы хотите скачать новый фильм на файлообменнике, и от вас требуется регистрация во всплывающем окне.

e) Во всех обозначенных выше случаях.

4. **Какой из приведенных паролей можно считать самым надежным?**

a) SupermanVasya2005;

b) QwErTy123456;

c) A!z8@;);

d) Q1jk45)@da;

e) M@$h@2oo!;

5. **Какой из способов хранения пароля от аккаунта можно считать самым надежным?**

a) В записной книжке в нижнем ящике письменного стола.

b) В текстовом файле в скрытой папке на компьютере.

c) В специальной программе, бесплатно скачанной в интернете.

d) Все перечисленные выше способы можно считать полностью надежными.

e) Все перечисленные выше способы считать полностью надежными нельзя.

Приложение 5

Десять самых популярных паролей среди пользователей Интернета

1. **PASSWORD** или слово **ПАРОЛЬ** в транслитерации латиницей (**gfhjkm**).
2. **QWERTY** и другие варианты раскладки клавиатуры.
3. Простые числовые последовательности (**12345678**, **87654321**, **11111111** и т.д.).
4. Сочетание простых числовых и буквенных последовательностей (**абвг1234**, **аааа1111** и т.д.).
5. Сочетание личных имен собственных (имя, фамилия и т.д.) и значимых чисел (года рождения, номера телефона и т.д.), например, **САША2000**, **ИВАНОВ1001010** и т.д.
6. Популярный молодежный сленг, например, **ФИТОНЯШКА**, **ОЛОЛО** и т.д.
7. Фразы типа **ОТКРОЙСЯ**, **ВПУСТИМЕНЯ** и т.д.
8. **ILOVEYOU** или **ЯТЕБЯЛЮБЛЮ** в транслитерации латиницей.
9. Популярные виды спорта, например, **ХОККЕЙ.**
10. Популярные имена, например, **АНАСТАСИЯ**, **ВИКТОРИЯ** и т. д.

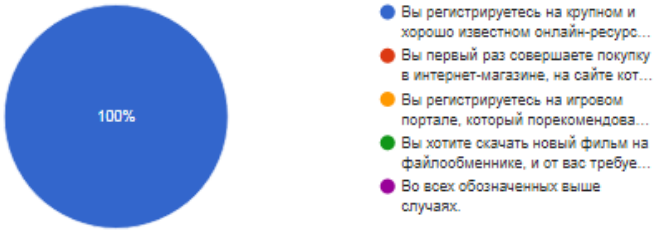
Результаты блиц-опроса

Какие из приведенных персональных данных позволяют однозначно идентифицировать пользователя в нашей стране?

11 ответов

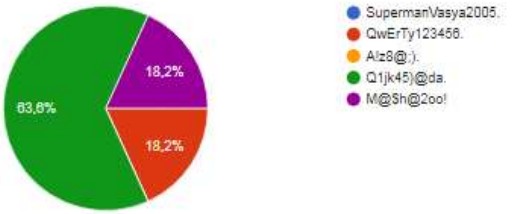
При регистрации на сайте у вас запросили номер телефона. В каком случае это наиболее безопасно?

11 ответов



Какой из приведенных паролей можно считать самым надежным?

11 ответов



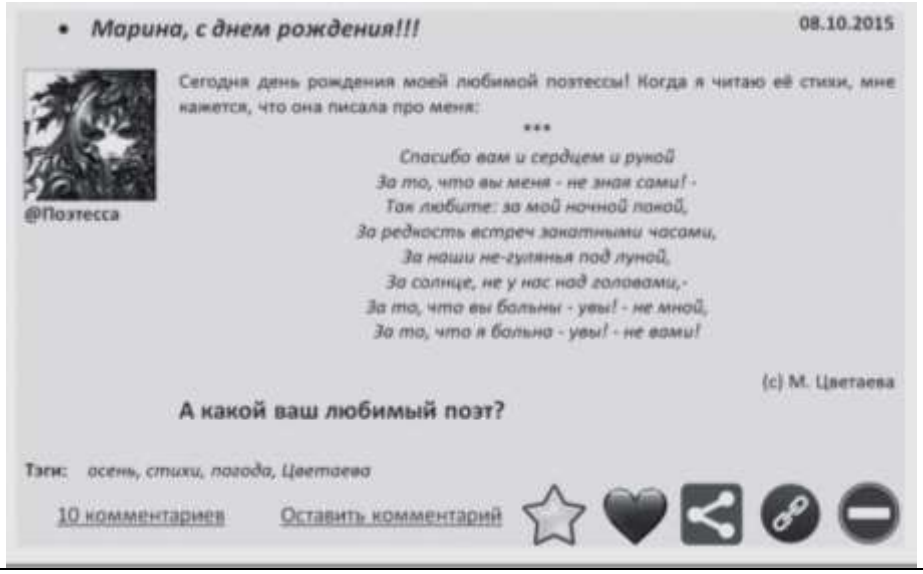
Какой из способов хранения пароля от аккаунта можно считать самым надежным?

11 ответов

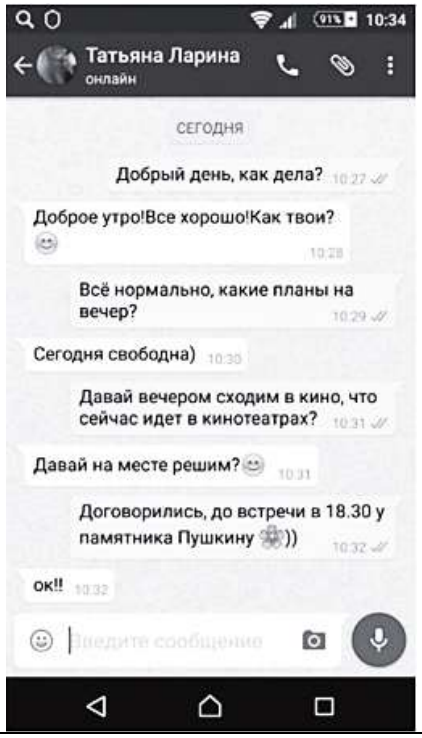
Приложение 7

Карточки с «цифровыми следами»

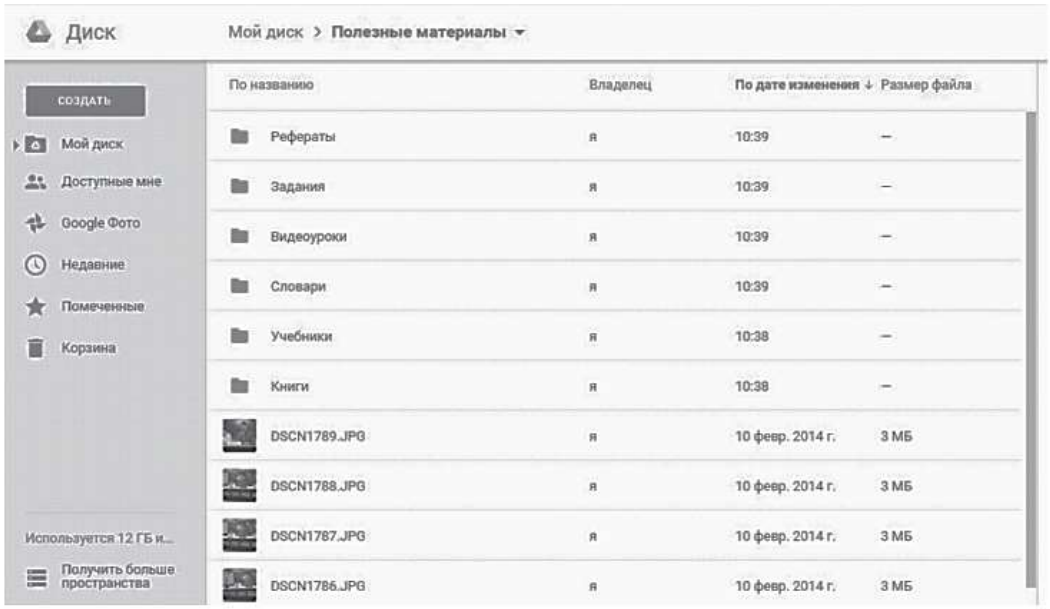
Карточка № 1



Карточка № 2

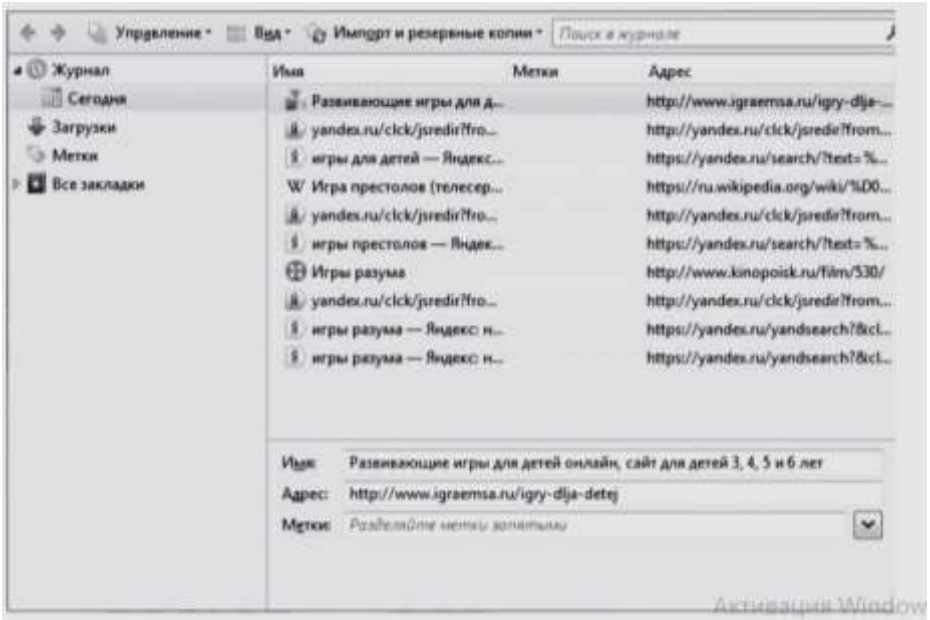


Карточка № 3



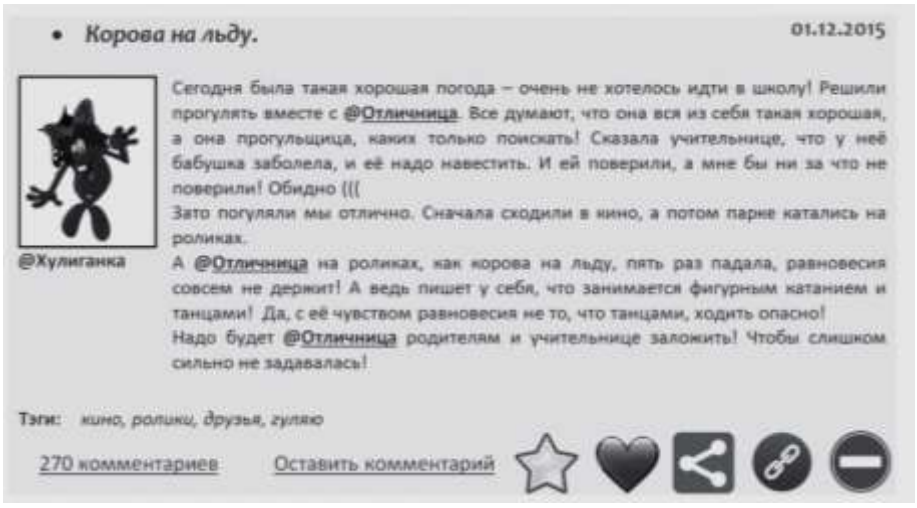
Карточка № 4

Карточка № 5



Карточка № 6

Карточка № 7



Карточка № 8

Карточка № 9

Приложение 8

Правильные ответы и пояснения для ведущего

№ п/п	Информация	Способ попадания в сеть	Способ защиты или удаления информации
1-я группа (маркировка белая): пользователь сам выкладывает в Интернет информацию о себе			
1	Пост, размещенный в одной из социальных сетей, в котором пользователь открыто делится персональной информацией с другими пользователями данного ресурса	Пользователь выкладывает информацию самостоятельно, определяя уровни доступа к посту других пользователей	Содержание поста должно определяться самим пользователем в соответствии с *правилами управления персональными данными*. Доступ к аккаунту защищается *паролем.* Уровни других пользователей к посту определяются *настройками приватности*
2	Личная переписка двух пользователей в мессенджере	Происходит между двумя пользователями. В публичный доступ переписка может попасть, во-первых, в случае перехвата данных, во-вторых, при взломе аккаунта пользователя. В случае если один из аккаунтов будет взломан, злоумышленники получат доступ ко всей истории	Защитить свою переписку можно, используя мессенджеры с шифрованием передачи данных, а также защищая аккаунт ненадежным паролем
3	Папка с файлами, размещенная в облачном хранилище	Пользователь выкладывает самостоятельно, определяя уровни доступа к файлам других пользователей	Доступ к облачному хранилищу, размещенному на удаленном сервере, осуществляется с помощью *пароля*. Уровни доступа к файлам, размещенным в хранилище, определяет сам пользователь в *настройках* приватности.
2-я группа (маркировка серая): информацию об активности пользователя в сети собирают приложения и онлайн-ресурсы			
4	История поисковых запросов (напротив прошлых поисковых запросов стоит надпись	Собирается см помощью инструментов аккаунта пользователя на сайте поисковой системы	Удалить историю поисковых запросов можно в своем аккаунте на сайте поисковика. Чтобы история поис-

№ п/п	Информация	Способ попадания в сеть	Способ защиты или удаления информации
	«Удалить»)		ковых запросов не сохранялась, можно использовать режим *инкогнито* или не заходить в свой аккаунт поискового сервиса при использовании обычного режима браузера
5	Вкладка «Журнал посещения страниц» в браузере, виден список страниц, посещенных пользователем в хронологическом порядке	Собирается браузером, может храниться как на компьютере, так и на удаленном сервере	Удалить лог-файлы, историю посещения страниц, временные файлы из интернета и cookies можно с помощью штатных инструментов операционной системы и браузера или при помощи специализированных приложений. *Программы сетевой защиты* позволяют ограничить загрузку временных файлов из интернета и cookies
6	Вкладка «Загрузки» в браузере- виден список файлов, скаченных пользователем в хронологическом порядке	Собирается браузером и хранится на устройстве в папке «Загрузки»	*Удалить загрузки* можно из вкладки браузера или из папки «Загрузки» на диске
3-я группа (маркировка черная): информацию о пользователе в сеть выкладывают третьи лица			
7	Пост, в котором один пользователь **@Хулиганка** упоминает другого пользователя **@Отличница**, разглашая персональные данные последней	Выкладываются другими пользователями социальных сетей	Если пост, на котором отмечен пользователь, нарушает законодательство и/или правила сообщества, то чтобы его удалить, необходимо обратиться в *службу поддержки социальной сети или к регулятору (в России-Роскомнадзор).* Запретить другим пользователям упоминать себя в их постах можно с помощью *настроек приватности*, например, добавив их «*черный список»*
8	Фотография, размещенная в социальной сети, на которой пользователь	Делаются другими пользователями социальной сети	Запретить другим пользователям отмечать себя на фотографиях можно с помо-

№ п/п	Информация	Способ попадания в сеть	Способ защиты или удаления информации
	@Хулиганка отметил других пользователей: **@Отличница, @Волшебница, @Поэтесса**		щью *настроек приватности*. Если пользователь сообщает ваши персональные данные, необходимо сообщить в *службу поддержки*
9	Комментарии других пользователей к посту **@Волшебница,** которые могут содержать персональные данные автора поста	Делаются другими пользователями социальных сетей	Запретить другим пользователям оставлять комментарии к постам можно в *настройках приватности*. Неприятный комментарий можно просто *удалить*

Приложение 9

ПАМЯТКА «ЭТО ВАЖНО ЗНАТЬ!»

1. Я не скажу о себе ничего (ни адреса, ни телефона, ни других сведений) без разрешения родителей.

2. Я никогда не передам по Интернет своей фотографии.

3. Я никогда не встречусь ни с кем, кого знаю только по Интернет, без разрешения родителей. На встречу я пойду с отцом или с матерью.

4. Я никогда не отвечу на сообщение, которое заставляет меня краснеть, будь то электронное письмо или общение в чате.

5. Я буду разговаривать об Интернет с родителями.

6. Я буду работать только тогда, когда они разрешат мне, и расскажу им обо всем, что я делал в Интернет.

Безопасность при хождении по сайтам и по приему электронной почты:

1. Не посещайте незнакомые сайты

2. Если к вам по почте пришел файл Word или Excel, даже от знакомого лица, прежде чем открыть, обязательно проверьте его на макровирусы.

3. Если пришел exe-файл, даже от знакомого, ни в коем случае не запускайте его, а лучше сразу удалите и очистите корзину в вашей программе чтения почты.

4. Не посещайте сайты, где предлагают бесплатный Интернет (не бесплатный e-mail, это разные вещи).

5. Никогда, никому не посылайте свой пароль.

6. Старайтесь использовать для паролей трудно запоминаемый набор цифр и букв.

Приложение 10

Интернет-аксиомы

1. Никогда не давай интернет-собеседнику частную информации о себе и своих близких (фамилию, номер телефона, адрес, номер школы).

2. Не стесняйся обратиться за помощью к родителям или учителям в случаях, когда кто-либо пишет, присылает тебе негативную информацию.

3. Твой знакомый по интернет-общению предложил тебе встретиться в реальной жизни? Помни, что это не очень хорошая идея. Люди могут быть разными в электронном общении и при реальной встрече.

4. Не открывай письма электронной почты, файлы или Web-страницы, полученные от людей, которых ты реально не знаешь или не доверяешь им.

5. Никогда не делай то, что может стоить денег твоей семье, кроме случаев, когда можешь согласовать эти действия с родителями.

6. Всегда проявляй вежливость в общении, и твои собеседники будут вежливыми с тобой.

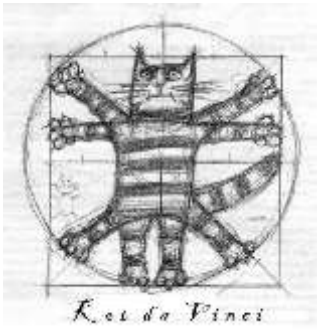
7. Никому не давай свой пароль.

Приложение 11

Карточки с заданиями

<table>
<tr><th colspan="2">Карточка № 1</th></tr>
<tr><td> 
Арина
Как же я люблю это время года!</td><td>  </td></tr>
<tr><td></td><td>Маша: Аринка, отлично выглядишь! Ты это где?)</td></tr>
</table>

<table>
<tr><th colspan="2">Карточка № 2</th></tr>
<tr><td> 
Светлана Алексеева
Наконец-то вытащила семью на прогулку!!!))))</td><td>  </td></tr>
<tr><td></td><td>Леночка Иванова: молодец!!! Так и надо!!! Как Саша и Сережа похожи на папу!!!</td></tr>
</table>

Карточка № 3	
 **Николай Гусев** Принимаю поздравления!	
	Свадебный Фотограф Отличный кадр! Ждем продолжения!

Карточка № 4	
 **ЮльЧИК** Хорошо погуляли!	
	Машечка: Точно)))) **Вася:** Мне идет черная рубашка! **Ольга:** А мне красный!!! **Федор:** Меня слева почти не видно(((**Вася:** Кто едет в лагерь, звоните мне 89320007722))))

Карточка № 5	
 **Аленка** Еще вопросы будут?	
	Богдан Поздравляю!

Комментарии для ведущего

При обсуждении результатов упражнения ведущий должен обратить внимание участников на то, что информация, размещаемая в Интернете, никогда не может быть однозначно интерпретирована на 100%. Всегда существует вероятность того, что мы имеем дело с подставным профилем (фейковым, т.е. фальшивым) или информацией, намеренно искаженной автором. Еще более неоднозначную информацию содержат отдельные посты (публикации), вырванные из ленты. Во всех случаях по комментариям мы можем проследить социальные связи авторов постов.

Карточка № 1. В данном случае можно предположить, что автор поста – молодая девушка или женщина. Мы можем сделать вывод о некоторых особенностях ее внешности, однако идентифицировать ее практически невозможно, т.к. на фото она стоит к нам спиной.

Карточка № 2. Мы можем предположить, что на фотографии изображена семья. Фотографии содержит информацию об их внешности, семейных отношениях, образе жизни, привычках, об их совместной поезде на природу. Комментарий к фотографии предоставляет нам информацию о родственной связи изображенных на ней людей, именах детей. Исходя из подписи под фото, можно предположить, что, скорее всего, автором поста является мама.

Карточка № 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.

Карточка № 4. Скорее всего, на фото изображена автор поста. По-видимому, фотография сделана на память о значительном событии. Изображение Собора Василия Блаженного на заднем плане дает возможность установить, что фото сделано на Красной площади в Москве.

Карточка № 5. Автор поста выложила собственную фотографию и паспорт: мы видим ее паспортные данные (Ф.И.О.; дата и место рождения; номер, серия, место и дата выдачи паспорта). Также мы совершенно точно знаем, как она выглядит.

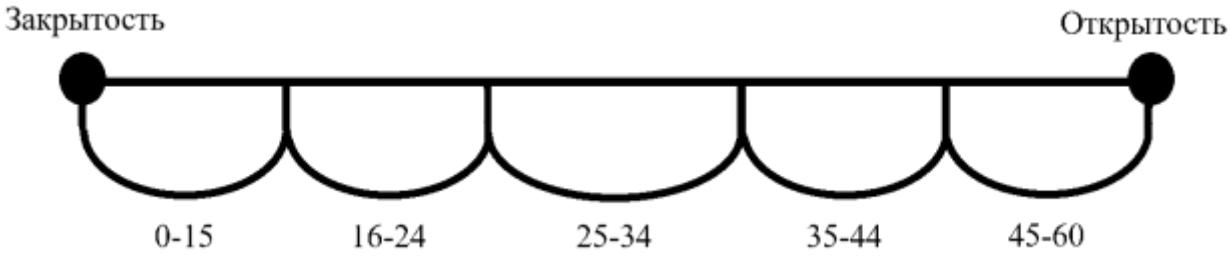
Приложение 13

Тест «Золотая середина»

		Никто (Только я)	**Некоторые или друзья группы друзей**	**Все друзья**	**Друзья и друзья друзей**	**Все пользователи**
Кому Вы позволите видеть следующие типы Вашей персональной информации?						
1.	Список друзей в социальной сети	0	1	2	3	4
2.	Адрес электронной почты	0	1	2	3	4
3.	Номер мобильного телефона	0	1	2	3	4
4.	Связанные аккаунты (веб-сайт, скайп, и др.)	0	1	2	3	4
5.	Домашний адрес	0	1	2	3	4
6.	Фотографии с Вами	0	1	2	3	4
7.	Видеозаписи с Вами	0	1	2	3	4
8.	Список Ваших групп	0	1	2	3	4
9.	Карту с Вашими фотографиями	0	1	2	3	4
10.	Чужие записи на Вашей странице	0	1	2	3	4
11.	Комментарии к Вашим записям	0	1	2	3	4
Кто может осуществлять следующие действия в Вашей социальной сети?						
12.	Оставлять записи на Вашей странице	0	1	2	3	4
13.	Комментировать Ваши записи	0	1	2	3	4
14.	Писать Вам личные сообщения	0	1	2	3	4
15.	Приглашать Вас в сообщество	0	1	2	3	4
Общая сумма баллов:						

Приложение 14

Шкала «Открытости – закрытости»



Памятка «Научите своих детей»

1. Никогда не давать частную информации о себе (фамилию, номер телефона, адрес, номер школы) без разрешения родителей.

2. Не разбираться самостоятельно в случаях, когда кто-либо пишет, присылает ему, или он сам обнаружил в сети Интернет что-либо смущающее его. Нужно обратиться к родителям или учителям – они знают, что надо делать.

3. Не встречаться в реальной жизни со знакомыми по интернет-общению. Это не очень хорошая идея, поскольку люди могут быть разными в электронном общении и при реальной встрече. Если все же ребенок хочет встретиться с ними, необходимо сообщить об этом родителям, и Вам сходить на первую встречу вместе с ребенком.

4. Не открывать письма электронной почты, файлы или Web-страницы, полученные от людей, которых он реально не знает или не доверяет им.

5. Никогда не делать того, что может стоить денег вашей семье, кроме случаев, когда рядом с ним родители.

6. Всегда быть вежливым в электронной переписке, и его корреспонденты будут вежливыми с ним.

7. Никому не давать свой пароль, за исключением взрослых Вашей семьи.

Используемая литература и источники

Нормативно-правовые документы

1. Всеобщая декларация прав человека (принята резолюцией 217 А (III) Генеральной Ассамблеи ООН от 10.12.1948).

2. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ).

3. Конвенция о защите физических лиц при автоматизированной обработке персональных данных (ETS № 108) (рус., англ.) (от 28.01.1981 с изменениями, внесенными Международным договором от 15.06.1999). Ратифицирована Федеральным законом РФ от 19.12.2005 № 160-ФЗ.

4. Указ Президента РФ от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера» (с изменениями и дополнениями от 23.09.2005, 13.07.2015).

5. Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы».

6. Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 29.07.2018) «О защите детей от информации, причиняющей вред их здоровью и развитию».

7. Федеральный закон от 27.07.2006 г. № 152-ФЗ (ред. от 31.12.2017) «О персональных данных».

8. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

9. Письмо Министерства образования и науки Российской Федерации от 14.05.2018 г. № 08-1184 «О направлении информации» (вместе с методическими рекомендациями «О размещении на информационных стендах, официальных Интернет-сайтах и других информационных ресурсах общеобразовательных организаций и органов, осуществляющих управление в сфере образования, информации о безопасном поведении и использовании сети Интернет».

10. Трудовой кодекс Российской Федерации от 30.12.2001 г. № 197-ФЗ (Глава 14 «Защита персональных данных работника»).

11. Гражданский кодекс РФ, Часть 1, Раздел I, Глава 8, Статья 152 «Защита чести, достоинства и деловой репутации».

12. Разъяснения Роскомнадзора от 30 августа 2013 г. «Разъяснения по вопросам отнесения фото-, видеоизображений, дактилоскопических данных и иной информации к биометрическим персональным данным и особенностей их обработки».

13. Практическая психология безопасности. Управление персональными данными в интернете: учеб.-метод. пособие для работников системы общего образования / Г. У. Солдатова, А. А. Приезжева, О. И. Олькина, В. Н. Шляпников. – изд. 2-е, испр. и доп. – М.: Генезис, 2017. – 224 с.

Литература

14. «Буллинг – причины, формы, профилактика» Методический материал (Для педагогов, воспитателей). Разработан: врачом-методистом Ларченко Н. А. Государственное казенное учреждение здравоохранения «Волгоградский областной центр медицинской профилактики». Волгоград, 2015.

15. «Профилактика буллинга в подростковой среде» тренинг для подростков. Баженова В. С. педагог-психолог МБОУ СШ №9 им. И. Ф. Учаева г. Волгодонска, 2017.

16. Баева, И. А. Психологическая безопасность образовательной среды: учеб. пособие / под ред. И. А. Баевой. М., 2009.

17. Бльох Е. А. О возрастающей роли медиа-образования при работе с детскими СМИ / Е. А. Бльох // ЗНАК. Проблемное поле медиа-образования.- 2016 № 2 (16) С.5-12;

18. Бльох Е. А. Формирование медиа-компетенций на занятиях школьного пресс- центра / Е. А. Бльох // Высшее образование для XXI века: XII Международная научная конференция. Москва, 3-5 декабря 2015 г.: Доклады и материалы. Круглый стол «Современные тенденции медиа-образования» / отв. ред. О. Е. Коханая. — М. : Изд-во Моск. гуманит. ун-та, 2015. С. 14-19.

19. Бочаров, М. И. Комплексное обеспечение информационной безопасности школьников. // Применение новых информационных технологий в образовании. 2009.

20. Зазнобина, Л. С. Стандарт медиа-образования, интегрированного в гуманитарные и естественнонаучные дисциплины начального общего и среднего общего образования / Л. С. Зазнобина// Медиа-образование. — М.: Изд-во Моск. ин-та повыш. квалиф. раб-в образ., 1996. - С.72-78.

21. Ильченко, О. А. Организационно-педагогические условия разработки и применения сетевых курсов в учебном процессе (на примере подготовки специалистов с высшим образованием): автореф. дисс. канд. пед. наук. М.: Центр креативной педагогики Московской государственной технологической академии. 2002.

22. Как работать с комиксами проекта «Респект 2.0».

23. Коротенков, Ю.Г. Информационная образовательная среда основной школы М.: Академия АйТи, 2011.

24. Левицкая, А. А. Региональные научно-образовательные центры европейской части России в области медиа-педагогики: сравнительный анализ / А. А. Левицкая // Дистанционное и виртуальное обучение. 2010. № 7. С.60-81.

25. Методические рекомендации по предотвращению буллинга (травли среди сверстников) в детских коллективах. Составители: А. Е. Довиденко, А. П. Третьякова, А. С. Мелях, Л. А. Губарева, М. В. Корба, Н. А. Алексеева, Н. В. Коровина, Т. П. Погадаева. - Екатеринбург, 2014.

26. Минин, А. Я. Информационные технологии в образовании: учеб. пособие. – М.: МПГУ, 2016. – 148 с.

27. Профилактика школьного буллинга. Методические материалы / Автор-составитель: А. Ненашева. – Южно-Сахалинск, 2015.

28. Тоискин, В. С., Красильников В. В. Медиа-образование в информационно-образовательной среде: Учебное пособие. – Ставрополь: Изд-во СГПИ, 2009. -122с.

29. Федоров, А. В. Развитие медиа-компетентности и критического мышления студентов педагогического вуза. М.: Изд-во МОО ВПП ЮНЕСКО «Информация для всех», 2007. 616 с.

30. Федоров, А. В. Словарь терминов по медиа-образованию, медиа-педагогике, медиа-грамотности, медиа-компетентности. / Таганрог : Изд-во Таганрог. гос. пед. ин-та, 2010. – С. 25.

31. Челышева, И. В. Влияние современных масс-медиа на здоровье и развитие подрастающего поколения. / И. В. Челышева // Образование. Медиа. Общество. 2008. № 3. С.14-18.

32. Школа без насилия. Методическое пособие/Под ред. Н. Ю. Синягиной, Т. Ю. Райфшнайдер. — М.: АНО «ЦНПРО», 2015. — 150 с.

Интернет-ресурсы

33. V Международный квест по цифровой грамотности [Электронный ресурс] – Режим доступа: http://сетевичок.рф.

34. Безопасный Интернет – детям! Полезные советы для тебя и твоих друзей. – Лифлет Министерства внутренних дел Российской Федерации. Управление «К». – [Электронный ресурс] – Режим доступа: https://mvd.ru/upload/site1/mvd1/liflets_k_deti_06.pdf.

35. Безопасный интернет для детей: законодательство, советы, мнения, международный опыт [URL: http://i-deti.org/video/] (Дата обращения: 31.08.2018).

36. Веб-квест «Информационная безопасность» [URL: https://kopilkaurokov.ru/informatika/uroki/vieb-kviest-zashchita-informatsii-v-sieti-intierniet] (Дата обращения: 27.06.2018).

37. Вредоносные программы в Интернете. Правила поведения в Интернете. Безопасное использование электронной почты. Защита от вредоносных программ. –Лифлет Министерства внутренних дел Российской Федерации. Управление «К». – [Электронный ресурс] – Режим доступа: https://mvd.ru/upload/site1/mvd/mvd2/mvd3/liflets_out_1.pdf.

38. Информационная безопасность образовательных учреждений [URL: https://searchinform.ru/resheniya/otraslevye-resheniya/informatsionnaya-bezopasnost-obrazovatelnykh-uchrezhdenij/] (Дата обращения: 28.06.2018).

39. Как защитить личные данные в Интернете [URL: https://lifehacker.ru/protecting-your-personal-data/] (Дата обращения: 03.09.2018)

40. Комикс «В темноте». Проект «RESPECT 2.0» http://www.respect.com.mx/ru/comics/246/.

41. Комикс «Всегда достается слабым?». Проект «RESPECT 2.0» http://www.respect.com.mx/ru/comics/207/.

42. Комикс «Мальчик из Швеции». Проект «RESPECT2.0» http://www.respect.com.mx/ru/comics/9/.

43. Комикс «Ощипанная птица». Проект «RESPECT 2.0» http://www.respect.com.mx/ru/comics/8/.

44. Комикс «Рыбный день». Проект «RESPECT 2.0» http://www.respect.com.mx/ru/comics/58/.
45. Комикс «Такой же, как и все». Проект «RESPECT 2.0» http://www.respect.com.mx/ru/comics/7/.
46. Комиксы из разных стран за респект и уважуху. Как работать с комиксами «РЕСПЕКТ». Методическое пособие для преподавателей и просветителей. – Воронеж, 2012 г. – 48 с. http://www.respect.com.mx/ru/technique/111/.
47. МВД РФ предупреждает! Пользователям интернета будьте осторожны! Мошенническое дублирование благотворительных сайтов. – Лифлет Министерства внутренних дел Российской Федерации. Управление «К». – [Электронный ресурс] – Режим доступа: https://mvd.ru/upload/site1/mvd1/liflets_out_3.pdf.
48. Методические рекомендации для образовательных учреждений по проведению родительского всеобуча на тему детской безопасности в Интернете. И.В. Вылегжанина – [Электронный ресурс] – Режим доступа: http://ozyorsk-shkola.ru/wp-content/uploads/2012/05/bezopasnost_rebjonka_v_informacionnom_obshhestve_copy.pdf.
49. Методическое пособие для преподавателей и просветителей http://www.respect.com.mx/ru/technique/191/.
50. Национальная стратегия действий в интересах детей на 2012 - 2017 годы [Электронный ресурс] URL:http://www.soprotivlenie.org.
51. Подростки в сети: методика обнаружения потенциальных угроз. Методические рекомендации. Челябинск: АНО Центр культурно-религиоведческих исследований, социально-политических технологий и образовательных программ. – 8 с. [URL: http://www.resurs-center.ru/sites/default/files/podrostki_v_seti_metodika_vyyavleniya_potencialnyh_ugroz_a4_0.pdf] (Дата обращения: 06.06.2018).
52. Понятие и виды персональных данных [URL: https://otdelkadrov.online/5841-ponyatie-vidy-personalnyh-dannyh] (Дата обращения: 03.09.2018)
53. Сделайте Интернет безопасным для своих детей. – Google Центр безопасности. – [Электронный ресурс] – Режим доступа: http://www.google.ru/safetycenter/families/start/.
54. Уроки мобильной грамотности [URL:https://chelyabinsk.beeline.ru/customers/help/safe-beeline/ugrozy-mobilnykh-moshennikov/uroki-mobilnoi-gramotnosti/] (Дата обращения: 31.08.2018).
55. https://learningapps.org
56. https://www.youtube.com/watch?v=9OVdJydDMbg
57. https://rkn.gov.ru
58. https://pd.rkn.gov.ru/multimedia/video114.htm
59. http://персональныеданные.дети/
60. http://detionline.com/
61. http://сетевичок.рф/

Авторы-составители

1. Абатуров Е. И., заместитель директора по воспитательной работе, МАОУ «СОШ № 98 г. Челябинска», ГМО руководителей ДОО и УСУ.

2. Айчувакова Е. Р., заместитель директора по воспитательной работе, МБОУ «СОШ № 86 г. Челябинска», ГМО классных руководителей.

3. Алтухова Н. А., начальник отдела информационно-методического сопровождения образовательных организаций Калининского района «Центр развития образования города Челябинска».

4. Бабушкина Т. В., социальный педагог, МБОУ «СОШ № 53 г. Челябинска» (филиал), ГМО социальных педагогов.

5. Бондарева Ю. С., начальник отдела информационно-методического сопровождения образовательных организаций Тракторозаводского района «Центр развития образования города Челябинска».

6. Бояркина О. В., учитель информатики, МАОУ «СОШ № 59 г. Челябинска», ГМО учителей информатики.

7. Валитова И. С., методист, МБУДО «ДЮЦ», ГМО ДОО и УСУ.

8. Вершинина Ю. В., заместитель директора по воспитательной работе, МАОУ «СОШ № 62 г. Челябинска», ГМО заместителей директора по ВР.

9. Гребенкина Е. Д., заместитель директора по воспитательной работе, МАОУ «Лицей № 142 г. Челябинска», ГМО заместителей директора по ВР.

10. Дорофеева Н. Н., заместитель директора по воспитательной работе, МБУДО «ЦВР г. Челябинска», ГМО социальных педагогов.

11. Евстифеева А. А., социальный педагог, МБОУ «СОШ № 51 г. Челябинска», ГМО социальных педагогов.

12. Епифанова Л. П., педагог дополнительного образования, МАОУ «СОШ № 147 г. Челябинска», ГМО руководителей ДОО и УСУ.

13. Жадько Н. П., учитель информатики, МБОУ «СОШ №45 г. Челябинска», ГМО учителей информатики.

14. Загитова О. В., начальник отдела информационно-методического сопровождения образовательных организаций ленинского и Советского районов «Центр развития образования города Челябинска».

15. Ильина И. В., заместитель директора по воспитательной работе, МАОУ «СОШ № 46 г. Челябинска», ГМО заместителей директора по ВР.

16. Коробова Ю. В., заместитель директора по воспитательной работе, МБОУ «СОШ № 32 г. Челябинска», ГМО классных руководителей.

17. Лебедева С. С., заместитель директора по воспитательной работе, МБОУ «СОШ № 45 г. Челябинска», ГМО заместителей директора по ВР.

18. Ледкова О. Ю., педагог-психолог, МАОУ «СОШ № 56 г. Челябинска», ГМО педагогов-психологов.

19. Манюк И. И., заместитель директора, МАУ «ЦППМСП Тракторозаводского района г. Челябинска», ГМО педагогов-психологов.

20. Матвеева Н. Ю., учитель информатики, МБОУ «СОШ № 109 г. Челябинска», ШМО информатики и физики.

21. Муталипова Д. А., социальный педагог, МАОУ «СОШ № 5 г. Челябинска», ГМО социальных педагогов.

22. Николаева С. Н., заместителя директора по учебно-воспитательной работе, МБОУ «СОШ № 28 г. Челябинска», ГМО руководителей школьных музеев Муниципальный координатор первичного отдела РДШ.

23. Ордина И. П., педагог-психолог, МАУ «ЦППМСП Центрального района г. Челябинска», ГМО педагогов-психологов.

24. Петрова Ю. А., учитель информатики, МАОУ «Гимназия № 100 г. Челябинска», ГМО учителей информатики.

25. Прокопьева Ю. А., социальный педагог, МАОУ «СОШ № 147 г. Челябинска», ГМО социальных педагогов.

26. Пушнина Н. К., заместителя директора по воспитательной работе, МБОУ «СОШ № 12 г. Челябинска», ГМО классных руководителей.

27. Ратанина А. В., заместитель директора по воспитательной работе, МАОУ «СОШ № 104 г. Челябинска», ГМО заместителей директора по ВР.

28. Ролинская В. Л., заместитель директора по воспитательной работе, МАОУ «СОШ № 148 г. Челябинска», ГМО классных руководителей.

29. Сильнова О. А., заместитель директора по воспитательной работе, МБУ ДО «ЦВР «Истоки», ГМО заместителей директора по ВР.

30. Сироткина Е. А., заместитель директора по воспитательной работе, МБОУ «СОШ № 109 г. Челябинска», ГМО учителей информатики.

31. Скобочкина О. В., учитель начальных классов, МАОУ «СОШ № 5 г. Челябинска», ГМО классных руководителей.

32. Слепова А. В., учитель русского языка и литературы, МАОУ «СОШ № 104 г. Челябинска», ГМО руководителей СМИ.

33. Слуднова Н. В., педагог-психолог, МАОУ «СОШ № 104 г. Челябинска», ГМО педагогов-психологов.

34. Смирнова Т. П., педагог-психолог, МБОУ «СОШ № 55 г. Челябинска», ГМО педагогов-психологов.

35. Солдаткин П. И., учитель истории, педагог-организатор, МБОУ «С(К)ОШ № 127 г. Челябинска», ГМО руководителей детских СМИ.

36. Соловьева М. В., учитель информатики, МАОУ «Гимназия № 80 г. Челябинска», ГМО учителей информатики.

37. Солодова Л. А., заместителя директора по воспитательной работе, МБОУ «СОШ № 137 г. Челябинска», ГМО заместителей директора по ВР.

38. Тащилина М. В., заместитель директора по воспитательной работе, МБОУ «СОШ № 121 г. Челябинска», ГМО руководителей ДОО и УСУ.

39. Третьякова Н. Е., методист отдела информационно-методического сопровождения образовательных организаций Металлургического района «Центр развития образования города Челябинска».

40. Федорова С.Ю., учитель информатики, МАОУ «СОШ № 153 г. Челябинска», ГМО учителей информатики.

41. Филиппова Е. С., начальник отдела информационно-методического сопровождения образовательных организаций Центрального района «Центр развития образования города Челябинска».

42. Черкащенко И. Г., заместитель директора по воспитательной работе, МБОУ «СОШ № 129 г. Челябинска», ГМО руководителей ДОО и УСУ.

43. Шитова Н. Е., социальный педагог, МАОУ «СОШ № 154 г. Челябинска», ГМО социальных педагогов.

44. Шорохова И. А., методист, МБУДО «ДЮЦ», ГМО руководителей детских СМИ.

45. Щелканова Е. Е., начальник отдела информационно-методического сопровождения образовательных организаций Курчатовского района «Центр развития образования города Челябинска».

46. Ялакаева О. В., заместитель директора по воспитательной работе, МБОУ «СОШ № 107 г. Челябинска», ГМО руководителей ДОО и УСУ.

47. Ярушина О. А., социальный педагог, МБОУ «СОШ № 39 г. Челябинска», ГМО социальных педагогов.

Отпечатано в информационно-издательском отделе
МБУ ДПО ЦРО г. Челябинска,
4540007, ул. Первой Пятилетки, 57