***Ю. С. Бондарева,***

***Е. С. Филиппова***

МБУ ДПО «Центр развития образования
города Челябинска»,
г. Челябинск

# ПОВЫШЕНИЕ ИНФОРМАЦИОННОЙ КОМПЕТЕНТНОСТИ УЧАСТНИКОВ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА С ЦЕЛЬЮ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИСПОЛЬЗОВАНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

*В статье рассматриваются вопросы безопасности в информационном обществе и необходимости защиты персональных данных в сети Интернет. Представлены практические материалы, способствующие формированию знаний и умений по защите персональных данных в информационном пространстве.*

Мы живем в век роста информационных потоков. Сегодня во всем мире Интернетом пользуются более четырех миллиардов человек [13]. Современное общество трудно представить без разнообразных сайтов, поисковых систем, социальных сетей, мессенджеров. Интернет предоставляет множество возможностей для поиска информации, обучения, саморазвития, познания мира. Интернет является обширным пространством для общения. Пользователи глобальной сети активно публикуют информацию о себе, о своей семье, работе, увлечениях, охотно делятся впечатлениями о недавней покупке или путешествии. Интернет является частью жизни многих людей, поэтому мы перестаем замечать грань между частным и публичным.

Участились кибератаки не только на коммуникативные средства связи, но и на различные электронные носители, хакеры взламывают важные файлы, чтобы использовать информацию в корыстных целях. В связи с этим современная жизнь в век информационных технологий диктует нам новые угрозы, о которых мы ранее не задумывались.

В настоящее время объективной реальностью является необходимость обеспечения безопасности личной информации, поскольку информация о человеке сегодня превратилась в дорогой товар. Каждый день пользователи сети Интернет подвержены различным угрозам со стороны злоумышленников, более того сами пользователи могут причинить себе вред, не отдавая отчет тем последствиям, которые могут наступить в результате их собственных поступков и действий. В связи с открытостью современного человека в сети Интернет защита персональных данных может приравниваться к защите личности. Поэтому объективной необходимостью становится повышение информационной компетентности в сфере защиты персональных данных в сети Интернет.

Для решения актуальных задач информационной безопасности в образовательных организациях города Челябинска началась реализация интерактивного образовательного модуля «Кибербезопасность», целью которого является формирование у участников образовательных отношений (педагогов, обучающихся, родителей (законных представителей) компетенций, необходимых для создания безопасной информационной среды в образовательной организации, навыков безопасного поведения в сети Интернет, основ управления персональными данными. Реализация данного модуля представляет собой цикл мероприятий, в ходе которых предполагается дальнейшая трансляция участниками полученного практического опыта.

Одной из форм проведения таких мероприятий является родительское собрание. Цель родительского собрания – повышение информационной компетентности родителей путем определения рисков в сфере приватности и обеспечения безопасности использования персональных данных. Крайне важно донести до родителей (законных представителей) обучающихся ценность личной информации, объяснить возможные последствия неосторожного обращения с ней и научить их эффективным способам защиты персональных данных и управления персональными данными в сети Интернет. Родительское собрание может включать в себя:

- интерактивную лекцию;
- практическое занятие;
- деловую игру;
- дискуссию;
- анкетирование;
- круглый стол.

Во время проведения интерактивной лекции родители (законные представители) знакомятся с основными понятиями Федерального Закона от 27.07.2006г. № 152-ФЗ (в ред. от 31.12.2017г.) «О персональных данных», способами защиты персональных данных, интернет-ресурсами, оказывающими поддержку в вопросах информационной безопасности и защиты персональных данных.

Важным этапом родительского собрания является практическая часть, во время которой родители (законные представители) выполняют упражнения, направленные на расширение представлений о защите своих персональных данных и персональных данных своих детей. В качестве примера можно предложить следующие упражнения.

**Упражнение «Детективное бюро».**

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

Необходимые материалы: карточки с заданиями (приложение 1), комментарии для ведущего.

Время проведения: 20 минут.

Процедура проведения: в начале упражнения ведущий говорит о том, что любое сообщение, опубликованное в сети Интернет, может содержать множество информации о нас. Например, фотография или видеозапись может рассказать о том, как мы выглядим, какой стиль одежды предпочитаем, о семье и друзьях, об обстановке, которая нас окружает. Важно научиться аккуратно

обращаться с личными данными и по ошибке не разместить 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:

*Карточка № 1.* В данном случае можно предположить, что автор поста – молодая девушка или женщина. Она сидит к нам спиной, поэтому мы можем рассказать только о некоторых особенностях ее внешности. Следовательно, идентифицировать ее практически невозможно.

*Карточка № 2.* На фотографии изображена семья. Мы можем рассказать об их внешности, семейных отношениях, образе жизни, привычках, об их совместной поездке на природу. Комментарий к фотографии предоставляет нам информацию об именах детей. Исходя из подписи под фото, можно предположить, что автором поста является мама.

*Карточка № 3.* На фотографии изображен автор поста и его невеста. В этом случае мы располагаем информацией об их внешнем виде, семейном положении. Изображение Эйфелевой башни на заднем плане дает возможность установить местоположение пары. Дата, указанная на фото, позволяет установить, когда произошло событие. Кроме того, мы можем сделать вывод о материальном положении пары.

*Карточка № 4.* Скорее всего, на фото изображена автор поста. Мы можем предположить, что фотография сделана на память о выпускном вечере. Изображение Собора Василия Блаженного на заднем плане дает возможность установить, что фото сделано на Красной площади в Москве. Комментарии к

фотографиям, содержащие описание внешнего вида, номер телефона, позволяют нам идентифицировать некоторых людей.

*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.

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.

Информацией о нас, о событиях в нашей жизни мы охотно делимся с друзьями в Интернете, иную информацию мы предпочитаем хранить при себе или вообще не задумываемся, когда публикуем ее в свободном доступе. Каждый из нас имеет право принимать решение, какую информацию сделать доступной, а какую лучше скрыть. Но всегда необходимо помнить, что неосторожное обращение с персональными данными может привести к «утечке» важной и значимой для нас информации. Прежде чем публиковать в сети Интернет какой-либо материал, следует хорошо подумать, какая персональная информация в нем содержится и как она может быть использована другими пользователями [6, с.68].

**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.

**Упражнение «Золотая середина».**

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

Необходимые материалы: бланки с вопросами по количеству участников (приложение 2).

Время проведения: 10 минут.

Процедура проведения: ведущий говорит участникам о том, что в повседневной жизни и в виртуальном пространстве очень важно установить баланс между открытостью и закрытостью, найти «золотую середину», которая у каждого человека может быть своей. «Золотая середина» – это расстояние, на котором нам комфортно и безопасно общаться с разными людьми. В виртуальном пространстве мы устанавливаем «золотую середину» с помощью настроек приватности – системы специальных параметров, позволяющих пользователю онлайн-ресурса настраивать уровень внешнего доступа к различным видам персональной информации. Таким образом, каждый вид или категория персональной информации доступны только определенной аудитории людей.

Первый этап. Индивидуальное заполнение бланка с вопросами каждым участником. Для измерения личного уровня «открытости – закрытости» в виртуальном мире участникам предлагается заполнить бланк с вопросами (приложение 2), 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 3), 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 вопросам 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». Каждый пользователь сети Интернет вправе самостоятельно решать, какая информация будет находится в полюсе «открытости», а какая – в полюсе «закрытости». При этом важно помнить: если информация о нас доступна всем в Интернете, мы становимся уязвимыми; когда же мы, напротив, устанавливаем неприступные барьеры, сохраняем любые сведения в тайне, отгораживая себя от

общения, есть риск лишиться тех возможностей, которые предоставляет нам цифровой мир. Настройки приватности в социальных сетях позволяют нам регулировать личную «золотую середину» – оставаться открытыми для общения с миром и при этом оберегать свое персональное пространство от нежелательного вторжения [6, с.135].

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. Поэтому важную роль в системе обеспечения информационной безопасности играют педагоги. С целью повышения информационной компетентности педагогов в вопросах информационной безопасности предлагается провести семинар-практикум «Школа кибербезопасности». Семинар-практикум разделен на две части – теоретическую и практическую. В теоретической части рассматриваются вопросы «Информационная безопасность в образовательной организации», «Персональные данные, их виды и способы защиты». Практической частью семинара-практикума является 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 (законных представителей);

– 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.*

Он 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 семинара-практикума 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 (приложение 4).

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 (приложение 5).

*Заключительный этап.*

На данном этапе проводится рефлексия занятия в форме устного опроса:

- Какие затруднения возникли у вас при создании плана действий?
- Предложенные интернет-ресурсы помогли вам? Или вы использовали другие источники информации?
- 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.

Стоит упомянуть и о наименее защищенных участниках образовательных отношений от пропаганды – детей и подростков. 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, а справляться с вопросами ее безопасности будет все сложнее.

Именно поэтому важно привлечь внимание учащихся 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.

Формировать у детей навыки безопасного поведения в информационной среде и основ безопасного использования персональных данных можно через следующие формы: внеклассное занятие, деловая игра, ролевая игра, викторина, квест.

Мероприятия могут включать в себя все вышеописанные упражнения и игры, так как их содержание вариативно. Учащимся можно также предложить

игру по составлению надежного пароля средствами криптографии. По окончании мероприятия участникам раздается памятка «Интернет-аксиомы» (приложение 6).

**Упражнение «Занимательная криптография».**

Необходимое оборудование: проектор, экран, доска, мел, ручки, макет клавиатуры (клавиатура).

Задача: познакомить учащихся со способами составления надежных паролей и приемами, позволяющими запомнить составленные пароли.

Время проведения: 20 минут.

Надежный пароль – это не просто набор букв и цифр. Надежный пароль – это пароль, который сложно угадать. Хотя сегодня и существуют специальные программы, позволяющие генерировать и хранить сложные пароли на компьютере, гораздо надежнее хранить пароль в голове. Для того чтобы научиться создавать сложный пароль, ведущий знакомит с основами криптографии (метод тайнописи).

*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.

Учащиеся делятся на группы. Задача группы – придумать самый надежный и вместе с тем запоминающийся пароль.

После окончания работы каждая группа по очереди выписывает свой пароль на доску, а другие участники должны попытаться угадать, что было зашифровано при составлении этого пароля (иными словами, понять, как он был получен).

Обсуждение:

- Какой пароль (способ шифрования) понравился вам больше всего? Почему?
- Какие из предложенных способов шифрования вам уже были знакомы, а о каких вы услышали впервые?
- Планируете ли вы использовать эти правила при составлении паролей к своим аккаунтам? [6, с.112].

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, размещенная в глобальную сеть, может стать причиной серьезных проблем. Наши фамилия, имя, номер телефона помогают злоумышленникам 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, опубликованным в сети 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.

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.

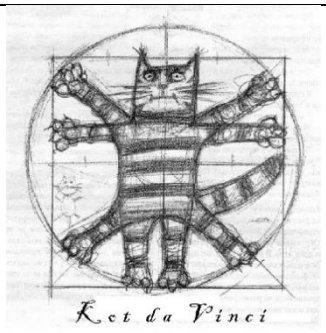
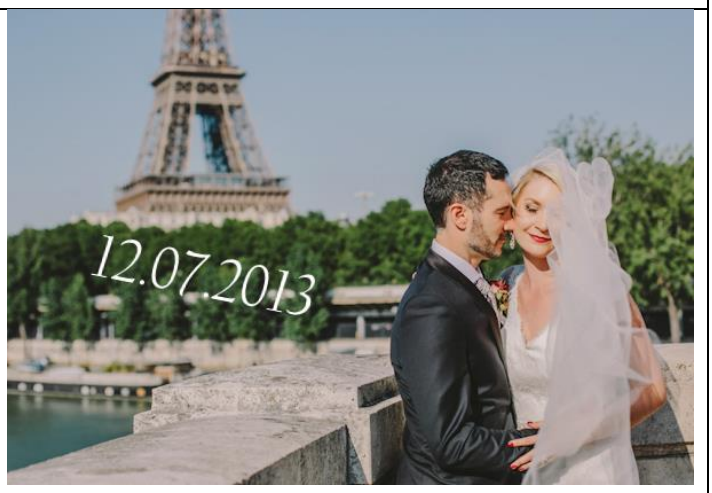
*Приложение 1*

**Карточки с заданиями**

<table>
<tr><td colspan="2">Карточка № 1</td></tr>
<tr><td>  <br>Арина<br>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><td>Карточка № 2</td></tr>
</table>

| | |
|---|---|
|  <br>**Светлана Алексеева**<br>Наконец-то вытащила семью на прогулку!!!)))) |  |
| | **Леночка Иванова:** молодец!!! Так и надо!!! Как Саша и Сережа похожи на папу!!! |

| Карточка № 3 | |
|---|---|
|  <br>**Николай Гусев**<br>Принимаю поздравления! |  |
| | **Свадебный Фотограф**<br>Отличный кадр! Ждем продолжения! |

| Карточка № 4 |
|---|

| | |
|---|---|
|  <br>**ЮльЧИК**<br>Хорошо погуляли! |  |
| | **Машечка:** Точно))))<br>**Вася:** Мне идет черная рубашка!<br>**Ольга:** А мне красный!!!<br>**Федор:** Меня слева почти не видно(((<br>**Вася:** Кто едет в лагерь, звоните мне 89320007722)))) |

| Карточка № 5 | |
|---|---|
|  <br>**Аленка**<br>Еще вопросы будут? |  |
| | **Богдан**<br>Поздравляю! |

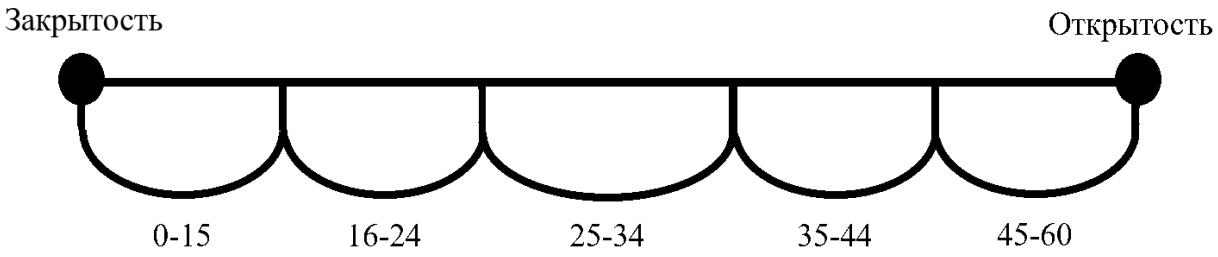
*Приложение 2*

**Бланк с вопросами**

| | | Никто (Только я) | Некоторые друзья или 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 3*

**Шкала «открытости – закрытости»**




*Приложение 4*

**Ссылки в сети Интернет**

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

*Приложение 5*

**Критерии оценивания плана действий**

| Критерий | Отлично | Хорошо | Удовлетворительно |
|---|---|---|---|
| Решение проблемы | План действий структурирован, логичен, дает четкий ответ на | План действий имеет четкую структуру, но недостаточно | План действий не дает четкого ответа на поставленный вопрос. |

| Критерий | Отлично | Хорошо | Удовлетворительно |
|---|---|---|---|
| | поставленный вопрос. | выражено решение проблемы. | |
| 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. |

*Приложение 6*

**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.

*Литература:*

1. 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).

2. Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 29.07.2018) «О защите детей от информации, причиняющей вред их здоровью и развитию».

3. Федеральный закон от 27.07.2006 г. № 152-ФЗ (ред. от 31.12.2017) «О персональных данных».

4. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

5. 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».

6. Солдатова, Г. У., Приезжева, А. А., Олькина, О. И., Шляпников, В. Н. Практическая психология безопасности. Управление персональными данными в интернете: учеб.-метод. пособие для работников системы общего образования [Текст] /Г. У. Солдатова и др. – изд. 2-е, испр. и доп. – М.: Генезис, 2017. – 224 с.

7. 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].– Загл. с экрана (дата обращения: 21.08.2018).

8. Безопасный интернет для детей: законодательство, советы, мнения, международный опыт [Электронный ресурс].– Режим доступа:http://i-deti.org/video/.– Загл. с экрана (дата обращения: 31.08.2018).

9. Как защитить личные данные в Интернете [Электронный ресурс].– Режим доступа: https://lifehacker.ru/protecting-your-personal-data/.– Загл. с экрана (дата обращения: 03.09.2018).

10. Вылегжанина, И. В. Методические рекомендации для образовательных учреждений по проведению родительского всеобуча на тему детской безопасности в Интернете [Электронный ресурс]/ И. В Вылегжанина. – Режим доступа:http://ozyorsk-shkola.ru/wp-content/uploads/2012/05/bezopasnost_rebjonka_v_informacionnom_obshhestve_copy.pdf.– Загл. с экрана (дата обращения: 03.09.2018).

11. Методическое пособие для преподавателей и просветителей [Электронный ресурс].– Режим доступа:http://www.respect.com.mx/ru/technique/191/.– Загл. с экрана (дата обращения: 07.02.2018 г.)

12. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций [Электронный ресурс]: [офиц.сайт]. – Режим доступа:https://rkn.gov.ru – Загл. с экрана (дата обращения: 07.02. 2019 г.).

13. АО «Лаборатория Касперского» [Электронный ресурс]: [офиц.сайт]. – Режим доступа: https://kids.kaspersky.ru/.– Загл. с экрана (дата обращения: 07.02.2018 г.)