Министерство просвещение ПМР
ГОУ ДПО «Институт развития образования и повышения квалификации»
Кафедра общеобразовательных дисциплин и дополнительного образования

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЕТЕЙ

Тирасполь
2024

Составитель

***И.А. Гошко**, гл. методист, ст. преподаватель кафедры общеобразовательных дисциплин и дополнительного образования ГОУ ДПО «Институт развития образования и повышения квалификации».*

Рецензенты:

***Н.Г. Пасевина**, вед. методист кафедры общеобразовательных дисциплин и дополнительного образования ГОУ ДПО «Институт развития образования и повышения квалификации»;*

***С.Л. Полозков**, методист-организатор по информатизации образования ГОУ «Тираспольское суворовское военное училище».*

Методические рекомендации по обеспечению информационной безопасности детей (далее – методические рекомендации) разработаны во исполнение плана мероприятий на 2020–2026 годы по реализации Доктрины информационной безопасности Приднестровской Молдавской Республики.

Задачи методических рекомендаций:

1. Оказание методической поддержки педагогических работников и сотрудников организаций образования с целью организации обучения детей и их родителей/законных представителей информационной безопасности.

2. Использование современных технологий и методик в организации обучения детей, в частности в рамках межпредметного обучения, внеурочной деятельности и других форм обучения.

3. Повышение уровня информационной грамотности педагогических работников и сотрудников администрации организаций образования ПМР.

Методические рекомендации ориентированы на педагогических работников:

1) учителя, преподаватели и классные руководители;

2) сотрудники администрации организаций образования по учебно-воспитательной работе и обучающихся;

3) ответственные лица в штате организаций образования в части психологического и воспитательного взаимодействия с обучающимися и педагогами (педагоги-организаторы, психологи, методисты-организаторы по информатизации образования и другие сотрудники организаций образования);

4) ответственные лица в штате организаций образования в части дополнительного образования обучающихся и организации внеурочной деятельности.

Методические рекомендации содержат общие представления о сферах безопасности в информационном пространстве и мерах, которые реализуются в образовательной среде для обеспечения информационной безопасности обучающихся.

Методические рекомендации имеют следующую структуру:

1. Раздел «Актуальность информационной безопасности детей» направлен на ознакомление педагогических работников с основными причинами актуальности информационной безопасности детей.

2. Раздел «Основные аспекты информационной безопасности» содержит описание всех аспектов информационной безопасности, включающих теоретический и практический анализ рисков по информационным, потребительским, техническим и коммуникативным аспектам информационной безопасности, и некоторые вопросы обеспечения информационной безопасности детей для родителей/законных представителей.

3. Раздел «Организация обучения детей и родителей/законных представителей» направлен на предоставление педагогическим работникам и сотрудникам образовательных организаций информации о различных механизмах организации обучения, обучающихся и их родителей/законных представителей.

СОДЕРЖАНИЕ

РАЗДЕЛ 1. АКТУАЛЬНОСТЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЕТЕЙ

Дети и подростки – активные пользователи интернета как в мире, так в Приднестровской Молдавской Республики.

Доступ несовершеннолетних к сайтам в сети Интернет дает им возможность изучать образовательный контент, общаться с ровесниками, самостоятельно обучаться, узнавать о проводимых конкурсах, олимпиадах, принимая в них участие, и использовать сеть Интернет в качестве источника для собственного развития.

Однако использование интернета вместе с возможностями несет и **риски**, такие как:

1) издевательство ровесников и незнакомцев в сети над ребенком;

2) воровство его аккаунтов, денег и личных данных;

3) втягивание ребенка в асоциальную деятельность (группы смерти, группы с рекламой наркотиков и т.д.).

По этой причине организации образования должны осуществлять профилактику и обучение детей навыкам безопасного использования сети Интернет и информирование их родителей/законных представителей о возможных сетевых рисках.

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

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

2) 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;

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

4) содержащая нецензурную брань;

5) содержащая информацию порнографического характера;

6) 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 жительства или место временного пребывания, место его учебы или работы, иную информацию, позволяющую прямо или косвенно установить личность такого несовершеннолетнего.

Оборот такой информации не допускается среди детей в местах, доступных для детей, без применения административных и организационных мер, технических, программно-аппаратных средств защиты детей от такой информации.

Классификация информации по пяти возрастным категориям:

1) информационная продукция для детей, не достигших возраста 6 лет;

2) информационная продукция для детей, достигших возраста 6 лет;

3) информационная продукция для детей, достигших возраста 12 лет;

4) информационная продукция для детей, достигших возраста 16 лет;

5) информационная продукция, запрещенная для детей.

К информационной продукции для детей, не достигших возраста 6 лет, может быть отнесена информационная продукция, содержащая информацию, не причиняющую вреда здоровью и/или развитию детей (в том числе информационная продукция, содержащая оправданные ее жанром и/или сюжетом эпизодические ненатуралистические изображения или описания физического и/или психического насилия (за исключением сексуального насилия) при условии торжества добра над злом и выражения сострадания к жертве насилия и/или осуждения насилия).

К допускаемой к обороту информационной продукции для детей, достигших возраста 6 лет, может быть отнесена следующая информационная продукция:

1) кратковременные и ненатуралистические изображения или описания заболеваний человека (за исключением тяжелых заболеваний) и/или их последствий в форме, не унижающей человеческого достоинства;

2) ненатуралистические изображения или описания несчастного случая, аварии, катастрофы либо ненасильственной смерти без демонстрации их последствий, которые могут вызывать у детей страх, ужас или панику;

3) не побуждающие к совершению антиобщественных действий и/или преступлений эпизодические изображения или описания этих действий и/или преступлений при условии, что не обосновывается и не оправдывается их допустимость и выражается отрицательное, осуждающее отношение к лицам, их совершающим.

К допускаемой к обороту информационной продукции для детей, достигших возраста 12 лет, может быть отнесена следующая информационная продукция:

1) эпизодические изображения или описания жестокости и/или насилия (за исключением сексуального насилия) без натуралистического показа процесса лишения жизни или нанесения увечий при условии, что выражается сострадание к жертве и/или отрицательное, осуждающее отношение к жестокости, насилию (за исключением насилия, применяемого в случаях защиты прав граждан и охраняемых законом интересов общества или государства);

2) изображения или описания, не побуждающие к совершению антиобщественных действий (в том числе к потреблению алкогольной и спиртосодержащей продукции, участию в азартных играх, занятию бродяжничеством или попрошайничеством), эпизодическое упоминание (без демонстрации) наркотических средств, психотропных и/или одурманивающих веществ, табачных изделий при условии, что не обосновывается и не оправдывается допустимость антиобщественных действий, выражается отрицательное, осуждающее отношение к ним и содержится указание на опасность потребления указанных продукции, средств, веществ, изделий;

3) не эксплуатирующие интереса к сексу и не носящие возбуждающего или оскорбительного характера эпизодические ненатуралистические изображения или описания половых отношений между мужчиной и женщиной, за исключением изображения или описания действий сексуального характера.

К допускаемой к обороту информационной продукции для детей, достигших возраста 16 лет, может быть отнесена следующая информационная продукция:

1) изображение или описание несчастного случая, аварии, катастрофы, заболевания, смерти без натуралистического показа их последствий, которые могут вызывать у детей страх, ужас или панику;

2) изображение или описание жестокости и/или насилия (за исключением сексуального насилия) без натуралистического показа процесса лишения жизни или

нанесения увечий при условии, что выражается сострадание к жертве и/или отрицательное, осуждающее отношение к жестокости, насилию (за исключением насилия, применяемого в случаях защиты прав граждан и охраняемых законом интересов общества или государства);

3) информация о наркотических средствах или о психотропных и/или об одурманивающих веществах (без их демонстрации), об опасных последствиях их потребления с демонстрацией таких случаев при условии, что выражается отрицательное или осуждающее отношение к потреблению таких средств или веществ и содержится указание на опасность их потребления;

4) отдельные бранные слова и/или выражения, не относящиеся к нецензурной брани;

5) не эксплуатирующие интереса к сексу и не носящие оскорбительного характера изображения или описания половых отношений между мужчиной и женщиной, за исключением изображения или описания действий сексуального характера.

Информационная продукция, запрещенная для детей, не допускается к распространению в предназначенных для детей организациях образования, детских медицинских, санаторно-курортных, физкультурно-спортивных организациях, организациях культуры, организациях отдыха и оздоровления детей или на расстоянии менее чем сто метров от границ территорий указанных организаций.

Необходимо отметить, что с каждым годом негативные последствия посещения сети Интернет детьми уменьшаются за счет блокировки и недопущения детей до нежелательного и запрещенного контента, активной просветительской работы с детьми и их родителями и увеличения количества пользователей услуг «Родительского контроля» и расширения антивирусных программ.

РАЗДЕЛ 2. ОСНОВНЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1. Информационные аспекты информационной безопасности

Выделяют следующие *категории информации:*

1. Общедоступная информация, которая должна предоставляться свободно всем гражданам;

2. Информация с ограниченным доступом:

– информация, являющаяся объектом гражданских прав. Это такая информация, обладатели которой вправе предоставлять доступ к ней по своему усмотрению, в частности на возмездной (платной) основе. Виды информации, являющейся объектом гражданских прав: произведения, являющиеся объектом авторского права; информация, являющаяся объектом патентного права; товарные знаки, знаки обслуживания и наименования мест происхождения товаров;

– конфиденциальная информация. Это такая информация, доступ к которой ограничивается в целях соблюдения интересов государства или прав и законных интересов их владельцев. К конфиденциальной информации относится государственная тайна, служебная и коммерческая тайны, а также тайны, связанные с правом на неприкосновенность личной жизни: персональные данные, личная и семейная тайны, тайна записи актов гражданского состояния, медицинская тайна и тайна вероисповедания;

– информация нежелательного характера, которая содержит противозаконную, неэтичную и вредоносную информацию.

Некоторые виды информации запрещены для распространения, в частности информация, пропагандирующая потребление и изготовление наркотиков, азартные игры, изготовление взрывчатых веществ, направленная на разжигание межнациональной розни, некоторые виды информации среди детей и отдельных возрастных групп и другая информация.

Неэтичная, противоречащая принятым в обществе нормам морали и социальным нормам, информация не запрещена к распространению, но может содержать информацию, способную оскорбить пользователей и оказать на них вредоносное воздействие, в частности манипулировать сознанием и действиями отдельных граждан или даже групп людей. Примером такой информации может стать нецензурная брань.

Последний вид информации – вредоносный. Данный вид информации характеризуется тем, что распространяется данная информация для заражения компьютера вирусами, например, просмотр тех или иных видеоматериалов приводит к заражению компьютера вирусами. Заражение устройств позволяет злоумышленникам не только получить и украсть важные данные, но и дает им возможность манипулировать ими и действиями зараженного компьютера, в частности получить деньги незаконным способом (фишинг). Примером может стать распространение в сети «пиратского» программного обеспечения, установив которое пользователь может потерять доступ к операционной системе.

Персональные данные

В зависимости от вида собственности, информация может быть отнесена к информации государственной, коммерческой, личной (персональной):

1. Перечень сведений, составляющих государственную тайну, формирует государство в лице его институтов и учреждений. Эти сведения являются обязательной тайной.

2. Перечень сведений, определяющих коммерческую тайну, формируют организации самостоятельно. Он же обеспечивает их сохранность и защиту.

3. Перечень своих персональных данных и личных (персональных) тайн определяет физическое лицо. Гражданин самостоятельно сохраняет и защищает эти данные.

Рассмотрим отдельно такую группу информации, как *персональные данные*.

Персональные данные представляют собой информацию о конкретном человеке. Персональные данные являются любой информацией, относящейся к прямо или косвенно определенному или определяемому физическому лицу. Таким образом, персональные данные – 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.

Персональные данные – это не просто ваши фамилия или имя, персональные данные – это набор данных, их совокупность, которая позволяют идентифицировать вас.

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

К специальным персональным данным относятся: расовая или национальная принадлежность, политические взгляды, религиозные или философские убеждения, состояние здоровья и пр.

По таким данным можно сформировать представление о человеке. Следует заметить, что приведенный перечень персональных данных не является исчерпывающим и может включать в себя еще множество иных идентификационных данных.

В этом контексте необходимо рассмотреть *виды угроз конфиденциальности информации* в целом:

1. Разглашение – это умышленные или неосторожные действия владельца информации с конфиденциальными сведениями, приведшие к ознакомлению с ними лиц, не допущенных к ним. Разглашение может быть выражено в сообщении, передаче, предоставлении, пересылке, опубликовании, утере и в других формах обмена и действий с конфиденциальной информацией. Пример: гражданин потерял в поликлинике свою личную медицинскую карту, оставив ее в фойе поликлиники, в результате чего другие посетители поликлиники смогли ознакомиться с личной историей болезни гражданина.

2. Утечка – это бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она доверена по техническим каналам утечки информации. Пример: злоумышленник установил на Wi-Fi модем вирусную программу, позволяющую фиксировать все действия пользователя в сети Интернет.

3. Несанкционированный доступ – это овладение конфиденциальной информацией лицом, не имеющим права доступа к охраняемым секретам. Пример: компьютерный взлом социальной сети и кража персональных данных пользователей этой сети.

Достоверность информации

В работе с информацией из любых источников необходимо помнить о необходимости проверки ее истинности, установление достоверности представленных фактов и сведений.

Специалисты определяют данный процесс термином «Верификация информации».

Основным механизмом проверки информации является критический анализ и восприятие информации, предполагающий изучение информации на предмет исторической верности, признаков субъективности и наличия признаков подделки.

Наиболее простой метод проверки информации – это перекрестная, то есть многократная проверка интересующей информации с использованием независимых источников.

Критика информации состоит из определения:

– времени и места появления информации или создания ее источника;

– автора текста или публикатора. Необходимо убедиться в компетентности автора, разбирается ли он в данном вопросе;

– полноты информации. Отвечает ли текст на ключевые вопросы: Что? Где? Когда? При каких обстоятельствах? Кто главные действующие лица?

– полноты доказательств. Какие доказательства использует автор? Видел ли он это сам или пересказывает чьи-то слова?

– надежности источников, поскольку одним из доказательств достоверности является наличие ссылок на источники. Важным критерием является наличие ссылок на официальные сайты органов власти или организаций. Если в качестве доказательства достоверности предоставляют фотографии или видео, то необходимо найти первоисточник и дату публикации изображения видео и соотнести с источником информации;

– изучение обстоятельств появления или публикации информации, а также цели создания этой публикации.

В противном случае, такая информация должна восприниматься не иначе, как авторский вымысел, и ей не нужно уделять большого внимания.

Нельзя использовать интернет как единственный источник информации, необходимо проверять информацию по другим источникам, особенно если эта информация касается жизненно важных моментов в жизни человека, например, здоровья, обучения, нормативно-правовых актов и других, поскольку в интернете не существует служб редакторов и корректоров, которые бы проверяли информацию на достоверность, корректность и полноту.

2.2. Потребительские аспекты информационной безопасности

Сетевое мошенничество

С развитием сети Интернет его стали осваивать и мошенники.

Злоумышленники могут использовать различные методы социальной инженерии (угрозы, шантаж, игру на чувствах жертвы – например, жадности или сочувствии), чтобы выманить деньги и получить личные и конфиденциальные данные: к таким данным относятся логины и пароли от различных сервисов, в том числе банковских, номера и пин-коды банковских карт и другие персональные данные.

Сетевое мошенничество имеет множество *методов*.

Фишинг (англ. phishing, от fishing – рыбная ловля, выуживание) предполагает за счет использования различных методов заманивания пользователя на поддельный сайт, например, через ссылку в письме, баннер или ссылку в тексте.

Иногда вредоносная ссылка маскируется под правильную ссылку – так злоумышленники часто используют похожие имена сайтов, чтобы ввести жертву в заблуждение с помощью опечатки в адресе сайта, или сайты, копирующие интерфейс известных ресурсов.

На подобных сайтах пользователю предлагается ввести логин и пароль или данные счета, после чего зачастую происходит перенаправление на реальный сайт, но данные уже попадают в руки мошенников.

Вишинг является разновидностью фишинга, в которой используется телефон. Мошенник может позвонить и представиться сотрудником банка или платежного сервиса и попросить продиктовать какие-либо платежные данные, например, пароль или код, пришедший на телефон. Его цель – выманить платежные данные, с помощью которых можно украсть деньги с карты или кошелька. Часто дополнительно присылается СМС со ссылкой, которая ведет на фишинговый сайт.

Фарминг или скрытое перенаправление является также разновидностью фишинга, но направляет пользователя вирус или взломанная программа на поддельный сайт, являющийся полной копией официального ресурса.

Сетевое мошенничество имеет также множество *видов*, в частности:

1. Липовые акции и фальшивые выигрыши в лотереи. Пользователь может получить сообщение (по телефону, почте или СМС), что выиграл некий приз, а для его получения необходимо «уплатить налог», «оплатить доставку» или просто пополнить какой-то счет. Признаки фальшивой лотереи: пользователь никогда не принимал участие в лотерее; пользователь никогда не оставлял своих личных данных на этом ресурсе; почтовый адрес отправителя – общедоступный почтовый сервис, например, gmail.com, mail.ru, yandex.ru

2. Просьба «друзей» сообщить пароль, когда знакомый в социальной сети сообщает о потере телефона, просит напомнить ваш номер, вам приходит СМС с неким кодом, а тот же друг в социальной сети сообщает, что заказывает товар или регистрируется на сайте и случайно указал ваш телефон вместо своего. Он просит сообщить пришедший код. Таким образом, ваш номер будет подключен к платной подписке и с вас начнут списывать деньги.

3. Ложная блокировка аккаунта в социальной сети: на баннере подробно расписан вариант «спасения» от блокирования страницы в социальный сети, который включает отправку СМС на «короткий» номер или введение кода подтверждения. В первом случае происходит разовое списание денег, а во втором оформляется ежедневная подписка на какую-либо платную услугу.

4. Рекламные сообщения и баннеры о необходимости обновления браузера имеют риск подписаться на платную загрузку или получить вирус с архивом платной программы.

5. Бесплатное скачивание файлов и просмотр каких-либо файлов с подпиской по номеру телефона, после чего включится подписка и с указанного номера могут начать списываться деньги.

6. Пользователю предлагается бесплатный антивирус, под видом которого на устройство попадет вредоносная программа, либо создается иллюзия, что компьютер уже заражен и для уничтожения угрозы нужно воспользоваться специальным антивирусом, который, опять же, окажется вирусом. Примером является появление надписи на экране компьютера о блокировке операционной системы, устранить которую можно только при отправке СМС с кодом, пришедшим на телефон при подтверждении, – после чего запускается сам вирус.

7. Предложения очень выгодных покупок, реклама больших скидок или анонс распродаж, которые размещаются на сайтах, в социальных сетях и присылаются СМС или на электронную почту. Такие предложения обычно предполагают перевод денег на банковскую карту, электронный кошелек или мобильный номер. В настоящее время стала актуальна следующая разновидность данной угрозы – пользователям рассылаются на оплату мобильного телефона, домашнего интернета и т.д. Зачастую мошенники направляют поддельные квитанции раньше официальной даты оплаты, чтобы успеть собрать свои платежи.

8. Мошенник может попросить денег в долг под видом знакомого, например, через взломанный аккаунт в социальных сетях. При этом перевести деньги он может попросить любым удобным способом – на электронный кошелек, банковскую карту, через интернет-банк.

Особо актуальной проблемой в сфере сетевого мошенничества стало стремление злоумышленников получить доступ к аккаунтам жертвы, например, в социальных сетях, почтовых и других сервисах. Украденные аккаунты они используют, например, для распространения спам-писем и вирусов.

Мошенники могут получить доступ к учетной записи жертвы следующими *способами:*

1) заставить жертву ввести свои данные на поддельном сайте;
2) подобрать пароль жертвы, если он не является сложным;
3) восстановить пароль жертвы с использованием «секретного вопроса» или введенного ящика электронной почты;
4) перехватить пароль жертвы при передаче по незащищенным каналам связи.

Какие меры помогут бороться с мошенничеством в сети?

1. Внимательно проверять доменное имя сайта и особенно доменные имена сайтов, на которых вводятся учетные данные.

2. Использовать проверенные и безопасные веб-сайты, в том числе интернет-магазинов и поисковых систем. Использовать закладки в браузере часто посещаемых сайтов.

3. При переходе по ссылке из сомнительных источников, в частности e-mail, форумы, сообщения в социальных сетях и всплывающие окна, вы рискуете попасть на «фишинговый сайт».

4. Помнить, что платежные сервисы и банки никогда не рассылают сообщения о блокировке счета по электронной почте, а также никогда не просят сообщать – ни по почте, ни по телефону – пароль, пин-код или код из СМС. Нельзя переходить по ссылкам из таких писем и вводить свои пароли на посторонних сайтах, даже если они очень похожи на сайт банка или платежного сервиса.

5. Не указывать свой мобильный номер на незнакомых сайтах.

6. Не переходить по ссылкам в сообщениях электронной почты и сообщениях из социальной сети.

7. Не размещать личную информацию в интернете. Даже маленькие кусочки личных данных могут быть использованы в преступных целях.

8. Никому не сообщать пароли, пин-коды и коды из СМС, которые приходят на мобильный номер от банков, платежных сервисов, мобильных операторов и других организаций.

9. Не поддаваться на провокации злоумышленников, например, с требованием перевести деньги или отправить СМС, чтобы снять блокировку компьютера.

10. Не открывать файлы и другие вложения в письмах, даже если они пришли от друзей и знакомых. Необходимо уточнить у них, отправляли ли они эти файлы.

11. Не доверять объявлениям о подозрительно дешевых товарах, акциях и распродажах на малознакомых сайтах. Перед покупкой необходимо прочитать отзывы в интернете о сайте или частном продавце, а в случае их отсутствия отказаться от покупки.

12. Проверять реквизиты, указанные в платеже, перед оплатой. Если они не совпадают с заявленными ранее, то отказаться от покупки.

13. Настроить онлайн-платежи на заранее проверенные реквизиты (автоплатежи).

14. В случае просьб от друзей и знакомых о деньгах необходимо лично перезвонить и уточнить необходимость в помощи, а в случае отсутствия возможности позвонить, задать какой-либо проверочный вопрос, ответ на который может знать только данный человек.

Что делать если уже возникли проблемы?

1. Если СМС-подписка была оформлена, то необходимо обратиться по телефону в службу поддержки оператора и попросить отключить ее.

2. Если аккаунт был взломан, то необходимо заблокировать аккаунт, сообщить администрации сайта о взломе, поменять пароль к сайту, а также предупредить всех своих знакомых о том, что произошел взлом и, возможно, от вашего имени будет рассылаться спам и ссылки на фишинговые сайты.

3. Если деньги или другие важные данные вашей банковой карты были предоставлены неизвестным лицам, то необходимо как можно быстрее обратиться в банк для блокировки карты и возврата средств.

Онлайн-игры

Современные онлайн-игры – это красочные, захватывающие развлечения, объединяющие сотни тысяч человек по всему миру. Игроки исследуют данный им мир, общаются друг с другом, выполняют задания, сражаются с монстрами и получают опыт.

Игры разделяют на следующие *категории:*

1. *Платные* – доступ к самой игре осуществляется после оплаты единожды либо согласно лимиту (день, неделя, месяц и т.д.), а сама игра не содержит платных дополнительных услуг и предложений.

2. *Бесплатные* – доступ к игре предоставляется бесплатно, а сама игра не содержит платных дополнительных услуг и предложений.

3. *Условно-бесплатные:* доступ к игре предоставляется бесплатно, однако игра содержит платные дополнительные услуги и предложения (например, улучшить ваш персонаж или получить какие-либо игровые привилегии) за счет внесения реальных денег.

При этом важно понимать цель игр платных и условно-бесплатных – получение прибыли. Однако полученные средства разработчиками игр также идут на поддержание и развитие игры, а также на совершенствование системы безопасности: совершенствуются системы авторизации, выпускаются новые патчи (цифровые заплатки для программ), закрываются уязвимости серверов. Кроме этого, на полученные средства нанимаются разработчики и специалисты, осуществляющие в частности поддержку пользователей.

В подобных играх стоит опасаться не столько своих соперников, сколько кражи пароля, на котором основана система авторизации большинства игр.

Основные советы по безопасности своего игрового аккаунта:

1. Если другой игрок создает неприятности, оскорбляет и нарушает своим поведением правила игры, заблокируй его в списке игроков и сообщи в администрацию о поведении данного игрока, в том числе со скринами. Такое действие позволяет администрации игр находить подобных игроков и исключить их из игры, что обычно предусмотрено правилами каждой игры для развития самой игры – ведь никто не будет играть в игру, когда в ней имеются такие игроки.

2. Не рекомендуется указывать личную информацию о себе в аккаунте и распространять ее среди других игроков, поскольку она может привести к различным негативным последствиям в реальной жизни.

3. Необходимо соблюдать правила игры и уважать других игроков, в частности создавать неприятности и оскорблять их.

4. Во время игры не стоит отключать антивирус, поскольку во время игры компьютер, смартфон или планшет могут быть заражены.

5. Необходимо всегда контролировать потраченное в игре время и деньги, поскольку это позволяет оценить свои действия корректно.

6. Нельзя приобретать дополнения к играм, оплачивать подписки и внутриигровые предметы на сторонних ресурсах, поскольку часто злоумышленники получают ваши деньги и доступ к карточкам оплаты и электронным кошелькам.

Спам

В свою очередь юридически спам можно определить как рекламу, распространяемую без предварительного согласия абонента или адресата.

Важно, что допускается реклама при условии предварительного согласия абонента, причем согласие должно быть не устным, а в спорных ситуациях, касающихся рассылок, распространитель обязан доказать наличие такого согласия.

Необходимо:

1. В электронном сообщении найти кнопку «Отказаться от рассылки», пройдя по которой подтвердить отказ от получения рекламных сообщений.

2. По телефону или электронной почте организации или лицу, направившему сообщение СМС, или в мессенджере, сообщить о необходимости исключить из рекламной рассылки.

Также сервисы электронной почты и мессенджеры позволяют отметить сообщение или адресата как спам или распространитель спама соответственно. Для этого необходимо выделить нужное письмо и нажать кнопку «Это спам», после чего письмо или сообщение будет перемещено в папку «Спам» или удалено. При этом администрация сервиса сможет отследить отправителя спама и заблокировать распространение данной информации или отправителя для других пользователей.

2.3. Технические аспекты информационной безопасности

Правила использования персональных устройств и программного обеспечения

Причинение вреда и неаккуратное использование компьютера приводит к потере личных данных, поэтому необходимо внимательное отношение к собственным устройствам или устройствам своих близких.

Здоровье компьютера зависит от двух главных вещей:

1. *Первое* – это порядок в программах и в той информации, которая на компьютере хранится.

2. *Второе* – это порядок и чистота внутри и снаружи компьютера.

Главные причины поломок из-за отсутствия чистоты внутри и снаружи компьютера:

1. Из-за пыли части компьютера не могут достаточно охлаждаться, перегреваются и выходят из строя. Кроме этого, из-за пыли сами вентиляторы могут перестать вращаться.

2. Части компьютера при работе выделяют много тепла, которое отводится с помощью кулеров/вентиляторов и за счет свежего прохладного воздуха в помещении. В жарком помещении компьютеры очень быстро нагреваются до недопустимой температуры.

3. Сырость, в том числе если пары воды конденсируются в компьютере, это может привести к короткому замыканию, и компьютер перегорит.

При чистке компьютера нужно соблюдать правила:

1) чистить только выключенный компьютер;
2) протирать монитор специальными салфетками или слегка влажной чистой тканью;
3) не использовать для чистки такие вещества как спирт или ацетон;
4) чистить клавиатуру и ежедневно протирать кнопки;
5) почаще протирать «мышь» влажной тканью или специальными средствами;
6) чистить не менее раза в месяц системный блок внутри, делая это осторожно с помощью пылесоса и мягкой кисточки;
7) протирать корпус снаружи мягкой влажной тканью.

Необходимо помнить, что клавиатура и мышь пачкаются больше всего, в результате чего на них скапливается грязь, которая может привести к отключению их функционала. Для избежания этого *рекомендуется* не браться за мышь и клавиатуру мокрыми, жирными или просто грязными руками.

Компьютер или ноутбук *рекомендуется:*

1) не держать в пыльном месте, около батареи или на солнце, что может быстро перевести к перегреву и запылению;

2) не держать в тесноте и заваливать его части посторонними предметами, например, складывать книги на системный блок.

Кроме этого, как и каждая техника компьютер имеет свой срок службы. Нужно соблюдать временные ограничения и не оставлять его включенным все время, поскольку чем дольше компьютер работает зря, тем быстрее он сломается просто от «старости».

Современные смартфоны и планшеты содержат функционал, позволяющий им конкурировать со стационарными компьютерами.

Для защиты информации от утери специалисты *рекомендуют* делать резервные копии ценных данных, поскольку вредоносные программы портят данные, шифруют жесткие диски и предлагают разблокировать их за деньги. Резервное копирование информации может осуществляться на другие носители, например, диски и флеш-накопители, так и сетевые носители, например, облачные сервисы, которые позволяют загружать файлы в сеть на свой аккаунт и иметь к ним доступ с любого устройства.

Особый вид программ – браузеры, позволяющие непосредственно посещать сайты и сервисы, поэтому не следует пренебрегать возможностью защиты браузера.

Браузеры имеют различные настройки безопасности:

1. Браузер может предотвратить установку дополнений для браузера.
2. Браузер может блокировать сайты, подозреваемые в атаках и мошеннических действиях.
3. Браузер может сохранять пароли либо никогда их не запоминать. Кроме этого, все браузеры предоставляют возможность ознакомиться лично с перечнем сохраненных паролей и логинов и лично их удалить.
4. И другие.

Рекомендуется использовать максимальные настройки браузера и запретить браузеру сохранять пароли и другую информацию.

Часто при посещении различных сайтов можно увидеть «Наш сайт использует файлы *„cookie”*».

Куки (cookie) – это информация, оставляемая веб-сайтом на компьютере пользователя. Куки способны хранить данные для аутентификации пользователя, персональные данные (если они представлены самим пользователем), сведения о предпочтениях пользователя (используются веб-сервером для улучшения обслуживания), статистическую информацию и т.д. Эти сайты следят за вашими посещениями, предпочтениями, покупками, а затем могут продать все эти сведения, например, рекламодателям.

Браузер при обращении к сайту пересылает куки веб-серверу в составе Http-запроса. Куки дают определенные удобства при постоянной работе с одними и теми же ресурсами (например, чтобы не вводить постоянно имя и пароль). Куки требуются не всем сайтам, обычно они нужны сайтам с ограничением доступа, где требуется регистрация.

Существуют куки от сторонних сайтов, присылаемые тогда, когда на текущем сайте находятся ссылки на другие ресурсы (например, в виде кнопок «понравилось»). Такие сторонние куки могут использоваться рекламодателями. Сами по себе куки безопасны, но могут служить источником информации о пользователе.

Как и другое программное обеспечение, браузеры необходимо обновлять. Зачастую браузеры обновляются автоматически при перезагрузке, однако если это не происходит, то лучше скачать последнюю версию на официальном сайте и установить ее самостоятельно.

Сейчас особенно актуальны следующие *сетевые риски для браузеров* пользователей:

1. Нежелательные расширения, которые представляют собой программы, открывающие различные рекламные блоки или использующие для организации фишинга. Для борьбы с ними необходимо скачивать и устанавливать расширения только из официальных магазинов приложений браузеров.
2. Вредоносный код, используемый в интерпретаторах Java Script и Java, а также плагинах для воспроизведения Flash и отображения PDF. Рекомендуется отключить их работу или отображение соответственно в браузере.

Персональное устройство и программное обеспечение без выхода в сеть Интернет сегодня не рассматриваются. Доступ в сеть Интернет становится обязательным правом каждого человека.

Однако подключение к сети Интернет и работа в ней также имеет риски технического характера.

Wi-Fi – это товарный знак альянса производителей техники, поддерживающего беспроводную связь нескольких стандартов. Символ Wi-Fi устанавливается на оборудование, которое специально протестировано и гарантированно будет работать в сетях с другими устройствами Wi-Fi.

Сети Wi-Fi за счет возможности предоставить множеству пользователей сразу выход в сеть становятся все более популярными, и многие торговые точки предоставляют бесплатный доступ для привлечения клиентов.

Однако нужно быть осторожным. При работе в сети Wi-Fi персональное устройство подобно радиопередатчику передает сигнал прямо в эфир и получает сигнал из эфира. Это значит, что этот сигнал может быть перехвачен. Таким образом, первый и основой риск – это перехват незашифрованных или слабо зашифрованных данных, подмена точки доступа и взлом Wi-Fi-сетей.

Перехват данных, как правило, осуществляется специальными сканерами, которыми злоумышленники перехватывают всю информацию и потом расшифровывают ее. Как правило, в открытых сетях без пароля информация передается в незашифрованном виде, в том числе логины и пароли для доступа к электронной почте и социальным сетям.

Для того чтобы обезопасить себя, достаточно соблюдать *простые правила использования Wi-Fi в общественных местах:*

1. Для начала нужно удостовериться, что есть подключение к официальной сети Wi-Fi заведения. Обычно такие сети имеют пароль или требуют авторизацию по номеру мобильного телефона.

2. Желательно передавать свою личную информацию, в частности пароли доступа, логины и какие-то номера только при наличии знака безопасного соединения (https) либо использование двухэтапной авторизации. Рекомендуется не проводить через публичные сети никакие финансовые операции на сайтах или приложениях.

3. При использовании Wi-Fi необходимо отключить функцию «Общий доступ к файлам и принтерам». Данная функция закрыта по умолчанию, однако некоторые пользователи активируют ее для удобства использования в работе или учебе.

4. В мобильном телефоне необходимо отключить функцию «Подключение к Wi-Fi автоматически», которая не позволит автоматического подключения устройства к сетям Wi-Fi без согласия пользователя.

5. В домашней сети Wi-Fi необходимо использовать надежные пароли и регулярно менять пароль.

Установка и использование пароля

Пароль – условное слово или набор знаков, предназначенный для подтверждения личности или полномочий. Появилось от французского слова «Parole» – слово.

Пароль устанавливается:

1. При заходе в операционные системы любых персональных устройств: компьютер, смартфон, планшет и т.д.
2. При заходе в отдельные программы.
3. При заходе в профайл сайтов, сервисов и приложений.
4. Для банковских карт, платежных сервисов и др.

Получение пароля позволяет осуществлять любые действия от вашего имени, поэтому его безопасность – важнейший вопрос.

Пароль не должен быть простым, поскольку простой пароль – это наибольшая угроза вашей учетной записи. Обычные слова (marina, begemot), а также предсказуемые сочетания букв (qwerty, 123456) могут быть легко подобраны программами для взлома паролей. Особенно популярный пароль, содержащий данные ФИО, дату, месяц и год рождения, например, пароль «Ivan1996».

Важно обеспечить сложные и разные пароли, поскольку в случае взлома злоумышленники получат доступ только к одному профилю в сети, а не ко всем.

Специалисты рекомендуют использовать *два вида* паролей:

1) для платежных систем длинные и сложные пароли, которые состоят как минимум из 10 символов, включают буквы верхнего и нижнего регистра, цифры и специальные символы, не содержат имя пользователя и известные факты о нем;

2) простые и легко запоминающиеся для форумов и других сайтов, не представляющих опасности для денег.

Для того чтобы создать сложный пароль, следует использовать и прописные, и строчные латинские буквы; цифры; знаки пунктуации (допускаются знаки ` ! @ # $ % ^ & * ( ) _ = + [ ] { } ; : « \ | , . < > / ?).

Хороший вариант для пароля – написать какое-нибудь русское словосочетание в английской раскладке клавиатуры. Такой пароль легко запомнить, и в то же время сложно взломать. Например, буквосочетание «вишневый пирог» в английской раскладке выглядит как «dbiytdsq gbhju».

Кроме этого, возможно написание слова и цифр задом наперед, например, ьтсонсапозебребик_8102 (кибербезопасность_2018).

Надежным пин-кодом, состоящим из 4 цифр, может быть сумма цифр, которую знает только владелец, например, год покупки смартфона, первой поездки в летний лагерь, появление домашнего питомца и др.

Кроме этого, необходимо *обеспечить конфиденциальность паролей,* в частности:

1) не сообщать их другим людям;

2) не хранить список паролей в файле на компьютере или на бумаге;

3) в браузере отключить автоподстановку и сохранение паролей;

4) не сохранять пароль на чужом или общественном компьютере, использовав специальную функцию «Чужой компьютер», которая позволяет сервису забыть ваш аккаунт после закрытия браузера;

5) не передавать учетные данные (логины и пароли) по незащищенным каналам связи, которыми являются открытые и общедоступные Wi-Fi-сети.

Рекомендуется обновлять пароли каждые 3–4 месяца.

Для восстановления пароля возможно использовать различные средства, среди которых привязка аккаунтов к мобильному номеру телефона, другая электронная почта и использование контрольного вопроса:

1) привязка аккаунта к мобильному номеру телефона может быть использована при условии указания в настройках аккаунта актуального и работающего номера телефона;

2) привязка аккаунта к другой электронной почте актуальна для почтовых сервисов, что позволяет в случае утери одной почты восстановить ее через другую;

3) контрольный вопрос представляет собой перечень заранее подготовленных вопросов, на которые пользователь дает свой ответ. Например, «Девичья фамилия матери», «Кличка первого животного» и пользователь вводит, например, следующие ответы «Иванова», «Шарик». Таким образом, выбрав функцию восстановления пароля сервис предложит ответить на контрольный вопрос. Рекомендуется не выбирать простые и нейтральные вопросы, ответ на которые легко подобрать или найти, например, в социальной сети.

Необходимо помнить, что восстановить пароль к вашему аккаунту также могут попытаться злоумышленники, а в случае неудачи вы можете потерять свой аккаунт, поэтому к вопросам восстановления необходимо отнестись ответственно.

Как и в случае пароля, так и контрольного вопроса необходимо помнить, что нужно использовать слово или словосочетание, цифру или комбинацию цифр, которые известны и понятны только пользователю, чтобы их можно было легко запомнить.

Гигиенические требования к организации занятий с использованием цифровых средств обучения

Использование цифровых средств – обязательная составляющая современного образования и досуга детей. Наряду с расширением дидактических возможностей преподавания, увеличением объема получаемой информации, индивидуализацией обучения внедрение этих средств как персонального, так и коллективного пользования в учебный процесс имеет ряд негативных особенностей.

К ним в первую очередь относятся: интенсификация и формализация интеллектуальной деятельности учащихся, обуславливающие увеличение нервной и зрительной нагрузки, психологический и зрительный дискомфорт, малоподвижность, воздействие электромагнитных излучений, связанных в том числе с использованием системы Wi-Fi.

Для предупреждения возможного негативного влияния применения информационно-коммуникационных технологий обучения на здоровье и развитие детского организма организаторы образования и педагоги должны знать особенности влияния цифровых средств обучения (ЦСО) на функциональное состояние, работоспособность и здоровье ребенка; соблюдать гигиенические требования к устройству, оборудованию и содержанию учебных кабинетов, в которых используются эти средства, режиму учебы и отдыха детей. В полной мере безопасность может быть обеспечена только в том случае, если в процессе обучения педагоги и родители смогут сформировать у детей стойкие навыки безопасного использования ЦСО.

Персональные компьютеры (ПК) размещают так, чтобы свет на экран падал слева. Занятия должны проходить в хорошо освещенном помещении. Рабочие места с ПК по отношению к светопроемам располагают так, чтобы естественный свет падал сбоку, преимущественно слева.

Оптимальной является ориентация учебных кабинетов, в которых используется компьютерная техника, на северные румбы горизонта. Главное здесь – исключение прямого солнечного света, что способствует более равномерному освещению помещения. Это позволяет решить проблему засветки и бликования экранов дисплея, а также перегрева помещения. Оконные проемы в помещениях, где используются ПК, должны быть оборудованы светорегулируемыми устройствами типа: жалюзи, занавесей, внешних козырьков.

В качестве источников общего искусственного освещения лучше всего использовать осветительные приборы, которые создают равномерную освещенность путем рассеянного или отраженного света (свет падает на потолок), и исключает блики на экране монитора и клавиатуре.

Расстояние от глаз пользователя до экрана компьютера должно быть не менее 50 см. Одновременно за ПК должен заниматься один ребенок, так как для сидящего сбоку условия рассматривания изображения на экране резко ухудшаются. Если для решения педагогических задач необходимы ситуации, когда за одним монитором занимаются двое, следует помнить, что такие занятия должны быть непродолжительны – не более 15 минут.

Стол и стул должны соответствовать росту ребенка. Поза работающего за компьютером должна отличаться следующим: корпус выпрямлен, сохранены естественные изгибы позвоночника и угол наклона таза. Голова наклонена слегка вперед. Уровень глаз на 15–20 см выше центра экрана. Угол, образуемый предплечьем и плечом, а также голенью и бедром, должен быть не менее 90°. Вертикально прямая позиция позволяет дышать полной грудью, свободно и регулярно, без дополнительного давления на легкие, грудину или диафрагму.

Основные рекомендации по организации рабочего места сводятся к следующему:

1) высота стула (а лучше кресла) должна быть такой, чтобы между ладонью и запястьем не образовывался угол;

2) клавиатуру лучше размещать на несколько сантиметров ниже уровня обычного письменного стола;

3) во время работы за компьютером ноги должны иметь опору, чтобы снизить нагрузку, которую они испытывают;

4) во время набора текста на клавиатуре запястья не должны опускаться, подниматься или отклоняться в стороны;

5) пальцы, запястье и предплечье должны образовывать прямую линию;

6) между локтевым суставом и предплечьем должен образовываться угол в 90°, плечи должны быть опущены и расслаблены.

Согласно современным представлениям рациональное применение цифровых средств в учебном процессе способствует активации умственной деятельности учащихся, оказывает благоприятное воздействие на психоэмоциональное состояние и работоспособность.

Однако активизация познавательной деятельности ученика, которая необходима для формирования оптимального тонуса центральной нервной системы и успешной учебной деятельности, не должна переходить в другую крайность – интенсификацию деятельности, приводящей к переутомлению. И важным инструментом в профилактике этих негативных последствий является регламентация использования ПК на учебных и досуговых занятиях детей.

Непрерывное использование персонального компьютера с жидкокристаллическим монитором на уроке для учащихся 1–2 классов не должно превышать 20 минут; для учащихся 3–4 классов – 25 минут; для учащихся 5–6 классов – 30 минут; для учащихся 7–9 классов – 35 минут. Непрерывное использование ноутбука на уроках в 1–2 классах составляет не более 20 минут, в 3–4 классах – не более 25 минут. Выполнение указанных регламентов должно сочетаться с соблюдением нормативных показателей светового режима, микроклимата в учебных помещениях и других требований, предусмотренных санитарным законодательством.

Внеучебные занятия (дополнительное образование) с использованием компьютеров рекомендуется проводить не чаще 2 раз в неделю общей продолжительностью: для учащихся 2–5 классов не более 60 минут; для учащихся 6 классов и старше – не более 90 минут.

Следует иметь в виду, что при прочих равных условиях степень утомления после уроков с ПК выше у детей с миопией и со сниженным запасом аккомодации.

Проявления утомления при работе на компьютере имеют свои особенности: несовпадение субъективной и объективной оценок состояния организма и индивидуальный характер проявления утомления.

Для педагогов важное значение имеют внешние признаки утомления обучающихся, определение которых доступно в процессе занятий. Эти признаки у детей младшего школьного возраста проявляются в частой смене позы и отвлечениях, разговорах, переключении внимания на другие предметы и др.

В ходе занятий с использованием ПК для профилактики переутомления учащихся необходимо осуществлять *комплекс профилактических мероприятий:*

1) выполнять упражнения для глаз через каждые 20–25 минут работы с компьютером, а при появлении зрительного дискомфорта, выражающегося в быстром развитии усталости глаз, рези, мелькании точек перед глазами и т.п., упражнения для глаз проводить индивидуально, самостоятельно и раньше указанного времени;

2) для снятия локального утомления должны осуществлять физкультурные минутки целенаправленного назначения;

3) для снятия общего утомления, улучшения функционального состояния нервной, сердечно-сосудистой, дыхательной систем, а также мышц плечевого пояса, рук, спины, шеи и ног следует проводить физкультпаузы.

Известно, что возможности детей одного и того же возраста могут существенно различаться. Это относится и к выносливости нагрузок, в том числе и занятий за компьютером. Утомительность занятий во многом зависит от их содержания, навыков общения, увлеченности, самочувствия и др. Увлеченность, положительный настрой способствуют активизации работоспособности, отодвигают утомление.

Во время перемен следует проводить сквозное проветривание с обязательным выходом обучающихся из класса/кабинета. Важное значение в профилактике зрительного и общего утомления имеет формирование культуры пользования, обучения навыкам безопасного общения с компьютером и другими ЦСО.

Интерактивная доска (ИД) широко используется в организациях образования, зачастую вытесняя традиционную меловую доску.

При выборе места для ИД нужно руководствоваться теми же соображениями, что и в случае с меловой или маркерной досками. Она должна размещаться на той же высоте, быть хорошо видна и легкодоступна. Если для работы интерактивной доски используется проектор, его размещение должно быть таким, чтобы исключить попадание луча проектора в глаза работающему у доски человеку.

Яркость проектора должна обеспечивать высокую четкость изображения, поскольку полное затемнение учебного помещения невозможно. Следует предусмотреть, чтобы тень от работающего проектора не попадала на доску. ИД проекционного типа нередко используется и в качестве маркерной доски. Однако у такого типа досок есть существенный недостаток – их гладкая поверхность бликует, что ухудшает условия рассматривания размещаемой на ней информации.

Использование ИД предъявляет особые требования к созданию в учебных помещениях комфортных условий для восприятия подаваемой с ее помощью информации. Размещение доски должно обеспечивать благоприятные условия для зрительной работы обучающихся. При использовании интерактивной доски необходимо позаботиться о затемнении окна (окон), ближайшего к доске. Это позволит исключить засветку доски солнечным светом, а также ее бликование.

Предъявляемая на доске информация должна быть четкой, хорошо различимой для всех учащихся независимо от удаленности от доски.

Суммарная продолжительность использования интерактивной доски на уроке в 1–2 классах не должна превышать 25 минут; в 3–4 классах и старше – не более 30 минут. Продолжительность применения ИД в течение учебного дня для 1–2 классов – не более 1 часа 20 минут; для 3–4 классов – 1 часа 30 минут, для средних классов – не более 2 часов.

Для профилактики зрительного утомления у детей работу с ИД следует чередовать с другими видами учебной деятельности и физкультминутками. Если доска не используется, следует ее выключать, чтобы светящийся экран не находился в поле зрения учащихся. Уроки в начальной школе с одновременным использованием 2-х видов ЦСО (интерактивная доска, ноутбук) значительно повышают интенсификацию учебной работы и сопровождаются более выраженным утомлением младших школьников.

Сегодня *мобильный телефон или смартфон* – неотъемлемый атрибут жизни ребенка. Чем дороже телефон, тем больше вероятность того, что он оказывает меньшее неблагоприятное воздействие на организм человека.

Это связано с большей чувствительностью приемника в телефоне, что не только увеличивает расстояние уверенной связи, но и позволяет использовать передатчик меньшей мощности на базовой станции. Однако детям, как правило, приобретают недорогие телефоны.

Учитывая все это, педагогам необходимо объяснять детям *правила безопасного использования сотового телефона:*

1. Разговор по сотовому телефону не должен длиться более 2 минут, а минимальная пауза между звонками должна быть не менее 15 минут. Гораздо безопаснее писать СМС, чем держать трубку возле уха, так что по возможности лучше писать, чем говорить. Если телефон используется для игр, прослушивания музыки, чтения, необходимо перевести его в авиационный режим, когда нет связи с базовой станцией.

2. Держать трубку мобильного телефона нужно на расстоянии от уха, за нижнюю ее часть и вертикально. Затухание радиоволн пропорционально квадрату пройденного расстояния, поэтому, отодвинув трубку от уха всего на сантиметр и увеличив таким образом расстояние до мозга вдвое, можно понизить мощность, излучаемую в мозг, в четыре раза.

3. Подносить трубку к уху лучше после ответа на том конце. В момент вызова мобильный телефон работает на максимуме своей мощности независимо от условий связи в данном месте. В то же время через 10–20 секунд после начала вызова излучаемая мощность снижается до минимально допустимого уровня. Моментально прикладывать телефон к уху бессмысленно еще и потому, что первый длинный гудок появляется не сразу.

4. Многие дети часто отправляют СМС-сообщения или излишне увлекаются играми, встроенными в сотовые телефоны. Такое регулярное и длительное напряжение на растущие кисть и пальцы может вызывать различные нарушения костей и суставов. Кроме того, играя, ребенок вынужден рассматривать мелкое изображение, долго смотрит на подсвеченный экран, все время находящийся на одном расстоянии от глаз. Это является серьезной нагрузкой для глаз и может очень негативно повлиять на зрение.

5. Очки с металлической оправой при разговоре рекомендуется снимать: наличие такой оправы может привести к увеличению интенсивности электромагнитного поля, воздействующего на пользователя.

6. Существует несколько рекомендаций по хранению и переноске телефонов. Специалисты не советуют класть мобильные телефоны рядом с собой во время сна. Также не стоит постоянно держать мобильный телефон при себе, например, в кармане брюк. То есть, контакты с сотовым телефоном стоит ограничить, особенно, если в этом нет никакой необходимости. Носить мобильный телефон лучше в сумке, не стоит держать длительное время сотовый телефон на груди, поясе или в нагрудном кармане.

Упражнения для профилактики развития синдрома запястного канала:

1. Сожмите руки в кулак, поддержите в течение 3 секунд, а затем максимально разожмите и подержите 6 секунд.
2. Вытяните руки перед собой, поднимите и опустите их.
3. Опишите кончиками пальцем круги, будто бы рисуя букву «О».
4. Сделайте круговые движения большими пальцами сначала влево, потом вправо.
5. Методично надавливайте одной рукой на пальцы другой.
6. Энергично несколько раз встряхните руки.

Комплексы упражнений для глаз (профилактика зрительного утомления).

Упражнения выполняются сидя или стоя, отвернувшись от экрана, при ритмичном дыхании, с максимальной амплитудой движения глаз.

Вариант 1:

1. Закрыть глаза, сильно напрягая глазные мышцы, на счет 1–4, затем раскрыть глаза, расслабив мышцы глаз, посмотреть вдаль на счет 1–6. Повторить 4–5 раз.
2. Посмотреть на переносицу и задержать взор на счет 1–4. До усталости глаза не доводить. Затем открыть глаза, посмотреть вдаль на счет 1–6. Повторить 4–5 раз.
3. Не поворачивая головы, посмотреть направо и зафиксировать взгляд на счет 1–4, затем посмотреть вдаль прямо на счет 1–6. Аналогичным образом проводят упражнения, но с фиксацией взгляда влево, вверх и вниз. Повторить 3–4 раза.
4. Перенести взгляд быстро по диагонали: направо вверх, налево вниз, потом прямо вдаль на счет 1–6; затем налево вверх, направо вниз и посмотреть вдаль на счет 1–6. Повторить 4–5 раз.

Вариант 2:

1. Закрыть глаза, не напрягая глазные мышцы, на счет 1–4 широко раскрыть глаза и посмотреть вдаль на счет 1–6. Повторить 4–5 раз.
2. Посмотреть на кончик носа на счет 1–4, а потом перевести взгляд вдаль на счет 1–6. Повторить 4–5 раз.
3. Не поворачивая головы (голова прямо), делать медленно круговые движения глазами вверх-вправо-вниз-влево и в обратную сторону: вверх-влево-вниз-вправо. Затем посмотреть вдаль на счет 1–6. Повторить 4–5 раз.

Вредоносное программное обеспечение

Вредоносное программное обеспечение – это разновидность компьютерных программ, отличительной особенностью которой является способность к размножению, то есть данные программы способны создавать свои копии. При этом копии программ-вирусов сохраняют способность дальнейшего распространения.

Вредоносное программное обеспечение предполагает несанкционированное использование, то есть без согласия и ведома пользователя ресурсов персонального устройства и нейтрализацию средств защиты устройства пользователя. Таким образом, вредоносное программное обеспечение, в том числе вирусы, нарушает конфиденциальность, целостность и доступность информации.

Вредоносное программное обеспечение может причинить персональному устройству не меньший вред, чем человеку – вирус серьезной болезни. В названии скрыта главная особенность программы – они схожи с живыми вирусами, распространяясь и живя, но жертвой являются не люди и животные, а компьютеры.

Значительная часть вредоносного программного обеспечения распространяется через сетевые технологии (сетевые, пакетные, почтовые черви и др.) и с помощью средств переноса информации (флэшек, дисков), что позволяет компьютерам «заражать» друг друга вирусами.

Вредоносное программное обеспечение при проникновении на новый носитель информации применяет средства маскировки: он не имеет какого-либо собственного имени: в одних случаях он добавляет свое «тело» программы к уже имеющимся на нем файлам (тем сам заражая их и выступая в дальнейшем под их прикрытием), в других записывает себя, например, как сбойный (дефектный), в третьих размещается в области так называемых старших адресов адресного пространства носителя (винчестера и т.д.), отведенных под оперативную память устройства и т.д. Обычно вредоносное программное обеспечение воздействует на операционную систему, системные и другие важные для работы устройства файлы и память самого устройства.

После проникновения тем или иным способом на носитель информации вирус начинает осуществлять различные действия, которые были ему поставлены ее разработчиком-злоумышленником.

Вредоносное программное обеспечение может повредить, копировать, подменять и полностью уничтожить все файлы и данные, подконтрольные пользователю, от имени которого была запущена зараженная программа, а также повредить или даже уничтожить операционную систему со всеми файлами в целом. Например, вирусы могут украсть пароли, контакты, реквизиты пластиковых карт, а также писать от имени пользователя сообщения в социальных сетях и многое другое.

Яркими *примерами работы вредоносного программного обеспечения* являются:

1. *Троянский конь.* Этот метод предполагает, что пользователь не заметил, что компьютерная программа была изменена таким образом, что включает в себя дополнительные функции. Программа, выполняющая полезные функции, пишется таким образом, что содержит дополнительные скрытые функции, которые будут использовать особенности механизмов защиты системы (возможности пользователя, запустившего программу, по доступу к файлам).

2. *Бэкдор.* Этот метод основан на использовании скрытого программного или аппаратного механизма, позволяющего обойти методы защиты в системе. Этот механизм активируется некоторым неочевидным образом. Иногда программа пишется таким образом, что специфическое событие, например, число транзакций, обработанных в определенный день, вызовет запуск неавторизованного механизма.

3. *Технология салями.* Названа так из-за того, что преступление совершается понемногу, небольшими частями, настолько маленькими, что они незаметны. Обычно эта технология сопровождается изменением компьютерной программы. Например, платежи могут округляться до нескольких центов, и разница между реальной и округленной суммой поступать на специально открытый счет злоумышленника.

В литературе обычно выделяют следующие *виды вирусов:*

1. *Вирус* – вредоносный код, который нарушает работоспособность системы, например, отключает интернет, устанавливает экран блокировки, стирает или шифрует файлы, включает возможность удаленного управления твоим компьютером или телефоном.

2. *Сетевые черви* – это вирусы, которые могут самостоятельно распространяться, заражая все больше устройств.

3. *Руткиты* – это вирусы, которые маскируют свое присутствие в системе и могут самовосстанавливаться или заражать компьютер при определенных условиях, например, если на компьютере работает администратор.

4. *Загрузочные вирусы* – это вирусы, поражающие загрузочные сектора дисков.

5. *Файловые вирусы* – это вирусы, заражающие исполнительные файлы различных типов.

6. *Шпионские программы* – это вредоносные программы, целью которых является слежка и похищение информации. Они могут копировать пароли, контакты, номера пластиковых карт, делать снимки экрана, запоминать нажатия клавиш и другую важную информацию. Позже эта информация передается на сервера злоумышленников. Некоторые вредоносные программы могут отправлять почту, сообщения в социальных сетях, совершать платные звонки и рассылать СМС скрытно от владельца устройства.

Источниками вирусного вредоносного программного обеспечения являются:

1) получение и просмотр вложенных файлов и ссылок в электронных письмах, в сообщениях в социальных сетях, которые могут быть получены как от постороннего человека, так и от знакомого, но уже зараженного участника социальной сети или почтовой переписки;

2) открытие файлов на съемных носителях (компакт-диски, флешки и т.д.);

3) посещение зараженных сайтов как специально созданных в целях мошенничества, так и обычных, но имеющих уязвимости информационной безопасности;

4) ошибки программного кода программ, установленных на устройстве;

5) клики по рекламным баннерам сомнительного содержания;

6) скачивание и установка программ из непроверенных или нелицензионных ресурсов.

Зараженный вирусом компьютер часто совершает неожиданные и необычные *действия*, которые пользователь может заметить, а при их наличии необходимо провести полную проверку системы на наличие вирусов:

1. Снижается скорость обмена данными с интернетом.
2. Вывод на экран странных сообщений или изображений.
3. Подача странных звуковых сигналов.
4. Неожиданное открытие и закрытие лотка дисковода.
5. Произвольный запуск на компьютере каких-либо программ.
6. Неожиданная перезагрузка и завершение некоторых программ.
7. Повышенная нагрузка и «зависание» устройства.
8. Замедление работы устройства или некоторых программ.
9. Увеличение размера файлов.
10. Появление не существовавших ранее и не создававшихся пользователем файлов.
11. Уменьшение объема доступной оперативной памяти.
12. Искажение содержимого файлов и каталогов или их полное исчезновение.
13. Самопроизвольное появление на экране сообщений или изображений.
14. Странное поведение интернет-браузера.
15. Невозможность перегрузки компьютера (операционная система не загружается).

Вредоносное программное обеспечение как программу сложно обнаружить человеку, а для их выявления и борьбы с ними используются другие программы – антивирусные.

Эти программы в режиме реального времени оценивают все файлы, которые находятся на устройстве, и осуществляют выявление среди них вирусов.

Вирусы постоянно обновляются, совершенствуются, их разработчики нацелены на преодоление антивирусной защиты. Именно по этой причине антивирусные программы имеют базы-энциклопедии вирусов, которые регулярно обновляются, что позволяет производителям антивирусного программного обеспечения оперативно совершенствовать их работу.

Поэтому *антивирусные программы нужно не только устанавливать, но и регулярно обновлять.*

Обновление происходит следующим образом:

1. Антивирусная программа создает барьер для вирусов, распознавая их. Разработчики антивирусной защиты включают коды известных программ-вирусов в базы данных антивирусных программ.

2. По мере появления новых вирусов антивирусные базы обновляются, и именно эту информацию получает пользователь компьютера, устанавливая обновления антивирусных программ.

Если же вирус проник в компьютер, то существуют антивирусные программы, которые могут «лечить» отдельные зараженные файлы или всю систему. Чаще всего они способны сохранить информацию зараженных файлов полностью или частично.

Также антивирусные программы позволяют перед открытием проверять на наличие вирусов все вставленные в компьютер внешние носители, например, флешки или диски.

Многие производители антивирусных программ предлагают как платные, так и бесплатные решения, которые позволяют обеспечить минимальный уровень безопасности устройств.

Необходимо помнить, что мошенники зачастую предлагают под видом зараженного программного обеспечения бесплатно скачать антивирусную программу, которая распространяется платно ее разработчиком.

Чтобы *обезопасить свои устройства от вирусов рекомендуется:*

1. Использовать антивирусное программное обеспечение на всех устройствах с регулярным обновлением базы данных (желательно установить автоматическое обновление) и осуществлять регулярную проверку на наличие вирусов. Никогда не отключать антивирус, даже его работа тормозит работу какой-либо программы. Установить максимальные настройки безопасности.

2. Не открывать вложенные файлы или ссылки, полученные по электронной почте, через социальную сеть или другие средства коммуникаций в интернете, не удостоверившись, что файл или ссылка не содержит вирус. Лучше такое сообщение сразу удалить и очистить корзину.

3. Использовать только лицензионное и актуальное программное обеспечение, в том числе операционную систему и антивирусную программу, и своевременно их обновлять как на компьютере, так и на других устройствах (желательно установить автоматическое обновление или скачивать антивирус только с официального сайта разработчика).

4. Обращать внимание на предупреждения браузера или поисковой машины о том, что сайт может угрожать безопасности компьютера.

5. Не подключать к своему компьютеру непроверенные съемные носители.

6. Включить на компьютере персональный брандмауэр и установить максимальные настройки безопасности.

7. Работать на компьютере под правами пользователя, а не администратора.

8. Ограничить физический доступ к компьютеру для посторонних лиц. Не оставлять без присмотра компьютер с важными сведениями на экране.

9. Регулярно необходимо осуществлять резервное копирование важных данных.

Нужно помнить, что даже антивирусные программы не могут полностью обеспечить и дать стопроцентной гарантии защиты устройства от вирусов, поэтому необходимо внимательно и ответственно использовать сеть Интернет.

2.4. Коммуникативные аспекты информационной безопасности

Цифровая репутация

Цифровая репутация – это негативная или позитивная информация в сети Интернет о пользователе.

Компрометирующая информация, размещенная в интернете, может серьезным образом отразиться на реальной жизни. К такой информации можно отнести место жительства, учебы, финансовое положение, особенности характера и рассказы о близких – все это накапливается в сети. «Цифровая репутация» – это имидж, который формируется из информации в интернете.

Многие молодые люди легкомысленно относятся к публикации личной информации в интернете, не понимая возможных последствий:

1. Уже сегодня существуют программы и сервисы, которые анализируют интересы, записи на стене, увлечения, высказывания, фотографии и другие данные, опубликованные потенциальными кандидатами на работу. В случаях несоответствия описания кандидата результатам, работодатели отказывают в работе.

2. Имеются неоднократные примеры, когда за некорректные комментарии или фотографии уволены сотрудники.

Комментарии, размещенная информация и действия пользователя в сети Интернет не исчезают после их удаления самим пользователем – они сохраняются в поисковых системах и других сайтах, на которых любой желающий может с ними ознакомится, в том числе с намерением причинить вред.

Например, при отправке кому-либо фотографии:

1) ее могут переслать дальше или показать кому-нибудь еще;

2) ее могут разместить в интернете;

3) ее могут увидеть одноклассники, учителя, родители, совершенно чужие люди;

4) ее могут комментировать незнакомые люди, в частности присылать оскорбительные комментарии, подвергнуть унижению и террору и даже звонить;

5) ее могут увидеть ваши дети, ваш партнер, работодатель, коллеги по работе или учебе в будущем.

Кроме этого, публикуя фотографии или другие медиафайлы, на которых вы или ваши друзья показаны не в очень выгодном свете, вы можете испортить репутацию не только себе, но и знакомым.

Необходимо помнить, что действия и слова пользователя в интернете могут повлечь за собой критику как обычных пользователей, так и киберхулиганов.

Отправляя какую-либо информацию незнакомым людям, например, участвуя в каких-либо обсуждениях в комментариях, на форумах и беседах, можно сформировать негативное отношение к себе со стороны других людей, в частности у них может появится желание мести.

Так можно пожалеть о размещении комментария в виде замечания в группе новостей по отношению к человеку и, удалив его, крайне удивиться, что этот комментарий уже прочитан десятками или сотнями людей и столько же людей перенаправили его по разным адресам, а в адрес пользователя поступают угрозы, и он заблокирован сайтом или администрацией данной группы в социальной сети.

Для защиты своей информации в социальных сетях пользователи могут самостоятельно настроить свои настройки приватности, например, ограничив доступ к некоторой или всей информации на своем аккаунте для всех зарегистрированных и незарегистрированных пользователей, для своих друзей и подписчиков или к отдельной группе пользователей.

Основные *советы по защите цифровой репутации:*

1. Перед публикацией любой информации, например, публикацией фотографии или осуществлении любого действия, например, комментирования какого-либо поста в сети Интернет, необходимо подумать о возможных последствиях и защите себя и близких сейчас и в будущем.

2. Установить в настройках профиля ограничения на просмотр профайла и его содержимого.

3. Нельзя размещать и указывать информацию, которая может кого-либо оскорбить, обидеть или унизить.

Сетевой этикет. Кибербуллинг

В ходе сетевого общения необходимо придерживаться следующих правил поведения:

1. Помнить о том, что ведется диалог с человеком и не забывать об эмоциональной сфере. В ходе дискуссии можно очень легко ошибиться в толковании слов собеседника, забыв, что собеседник имеет чувства, привычки, позицию и мировоззрение.

2. Необходимо следить за формулировками и используемой лексикой, избегать жаргонной и ненормативной лексики и соблюдать правила орфографии и пунктуации, поскольку любая информация может быть включена в новый контекст и поменять смысл.

3. Необходимо правильно выбирать модель поведения, ведь принимаемая в одном месте, она может быть неприемлема в другом. Оказавшись на новом сайте, в группе или новом блоге, сначала необходимо ознакомиться с правилами и прочитать, как и о чем говорят участники дискуссии, узнать методы и форматы общения и только после этого вступать в дискуссию. Также общение с друзьями может включать в себя некую расслабленность, но в коммуникации с коллегами, начальством или другими лицами – это не допускается. Проверять достоверность фактов и информации перед публикацией. Недостоверная информация способна вызвать негативную оценку со стороны собеседников.

4. Необходимо обратить внимание на логичность текста, который должен быть выстроен так, чтобы в нем не было ни одной «логической дыры» и обобщений, чем могут воспользоваться для опровержения собеседники.

5. Нельзя распространять личные данные, позволяющие идентифицировать пользователя, поскольку в реальной жизни его могут найти для причинения вреда его здоровью, а в сети невозможно быть абсолютно уверенным в том, что собеседник – это тот человек, за которого он себя выдает.

6. Помнить об отсутствии анонимности в сети и действии законов в сетевом пространстве. Выдавая себя за кого-то другого, оскорбляя и запугивая других пользователей, распространяя запрещенную информацию и осуществляя другие действия,

незаконные или запрещенные администрацией сайта или сервиса, помнить о том, что администрация сайта или сервиса и правоохранительные органы могут определить любого пользователя по его IP-адресу.

При ответе на замечания в сети Интернет необходимо придерживаться следующих *правил:*

1) избегать открытого противоречия;
2) сохранять спокойный, доброжелательный тон;
3) с уважением относиться к позиции собеседника;
4) подчеркивать позитивные моменты, признавать правоту собеседника;
5) быть лаконичным.

Однако в интернете пользователь может стать жертвой издевательств, хулиганства и бойкота, а также преследоваться сообщениями, содержащими оскорбления, агрессию и запугивание. Такие действия имеют общее название – это *кибербуллинг* или виртуальное издевательство.

Английское слово *буллинг* (bullying, от bully – драчун, задира, грубиян, насильник) обозначает запугивание, унижение, травлю, физический или психологический террор, направленный на то, чтобы вызвать у другого страх и тем самым подчинить его себе.

Зачастую кибербуллинг рассматривается специалистами как социальное давление, перенесенное в плоскость электронного общения путем использования электронной почты, социальных сетей, СМС-сообщений, мессенджеров и других средств коммуникации в интернете.

Независимо от формы проявления кибербуллинг может причинить значительный вред жертве, а в крайних случаях привести к самым трагическим последствиям.

Обычно выделяют следующие *виды кибербуллинга:*

1. Оскорбление происходит посредством оскорбительных комментариев и вульгарных обращений, происходящих в публичном пространстве интернета.
2. Домогательство от незнакомцев, адресованное конкретно пользователю.
3. Клевета путем выставления жертв в неблагоприятном свете с помощью различных материалов или информацией.
4. Использование фиктивного имени, когда кто-то выдает себя за другого человека, используя пароль жертвы, либо создает поддельную страницу на ее имя, где размещает лживый и унизительный контент или отправляет различные сообщения негативного характера друзьям и знакомым жертвы для ухудшения отношения к жертве.
5. Публичное разглашение личной информации осуществляется путем распространения личной информации для шантажа или оскорбления жертвы.

Чтобы противостоять кибербуллингу, необходимо следовать *ряду правил*.

Одноразовые оскорбительные сообщения лучше игнорировать, поскольку обычно агрессия прекращается на начальной стадии.

В случае их продолжения, в том числе регулярного, необходимо игнорировать такие сообщения и не стоит угрожать хулигану «найти и наказать». Это лишь спровоцирует хулигана на продолжение конфликта и социального давления, что усугубит ситуацию.

Неоднократно в практике имеются случаи, когда киберхулиганы могут специально создавать поводы, заставляя сердиться свою жертву до такой степени, что она рано или поздно отвечает разгневанным или оскорбительным замечанием. После такой реакции киберхулиган уведомляет администраторов сайта или сервиса о недопустимом содержимом и нарушении правил пользования услугами сети, после чего аккаунт жертвы блокируется.

Следующим этапом является бан или внесение в черный список агрессора, функция которого предусмотрена во всех сервисах, имеющих функцию общения. В программах обмена мгновенными сообщениями есть возможность блокировки отправки сообщений с определенных адресов, а для СМС-сообщений для этого достаточно обратиться по телефону в службу поддержки оператора.

Пользователь также имеет возможность заблокировать самого хулигана, обратившись с жалобой в адрес администрации сайта, потребовав применить санкции в отношении обидчика и даже удаление его аккаунта. Жалобу необходимо сопроводить скопированной или сохраненной информацией фактов поступивших сообщений, в частности угроз.

При наличии угроз жизни и здоровью кибербуллинг может перейти в реальную жизнь, вместе с подтверждениями можно обратиться в правоохранительные органы для защиты пользователя и его близких.

Если же пользователь стал свидетелем кибербуллинга, то ему необходимо:

1) выступить против преследователя или хулиганов, указав на правовые последствия данных действий;

2) поддержать жертву, которой нужна психологическая помощь;

3) сообщить администрации сайта или сервиса о случившемся с просьбой предпринять соответствующие меры.

Технологии информационного воздействия

В идеологическом противоборстве большое место занимают технологии информационно-психологического воздействия (манипулирования).

Технология в современной коммуникативной науке – это совокупность приемов, методов и средств, используемых для достижения конкретных целей, в частности для осуществления деятельности на основе рационального ее «расчленения» на процедуры и операции с их последующей координацией, синхронизацией и выбором оптимальных средств и методов их выполнения.

Технологии информационно-психологического воздействия в массовых информационных процессах базируются на использовании возможностей для воздействия на массовое и индивидуальное сознание аудитории и молодежи в частности.

Организации, группы лиц и отдельные лица в сети Интернет зачастую используют в своем арсенале воздействия на личность самые разные средства – от способствующих процессу формирования террористических позиций, так и вызывающих реакции страха, неуверенности, психологической напряженности. Эти технологии применяются в качестве средства разрушения политической стабильности в обществе, а также формирования террористической идеологии.

Инструменты коммуникации: электронная почта, социальные сети и мессенджеры

Электронная почта – это технология и предоставляемые ею услуги по пересылке и получению электронных сообщений, которые распределяются в компьютерной сети.

Обычно электронный почтовый ящик выглядит следующим образом: *имя пользователя@имя домена*. Также кроме передачи простого текста, имеется возможность передавать файлы.

В первую очередь необходимо выбрать правильный сервис электронной почты.

Рекомендуется использовать бесплатные почтовые сервисы, которые представлены на рынке достаточно долгое время и соответствуют следующим условиям:

1) имеют авторизацию через защищенное соединение https;
2) имеют двухэтапную авторизацию;
3) имеют функцию «Секретного вопроса»;
4) имеют функцию отключения рекламы в профайле;
5) имеют возможность привязать к аккаунту номер мобильного телефона;
6) имеют функцию защиты от спама и проверки сообщений, приходящих на почту, на предмет наличия вирусного программного обеспечения.

На следующем этапе необходимо правильно выбрать адрес электронной почты – почтовый адрес должен быть удобен в произнесении и понятен.

В названии своего ящика можно использовать реальные имя и фамилию, что позволит облегчить связь с пользователем, однако в названии почты не стоит употреблять посторонние слова, так как это может скомпрометировать пользователя. Например, если пользователя зовут Екатерина Иванова, то ее почтовый ящик следует назвать KateIvanova или EkaterinaIvanova; если такие почтовые ящики уже существуют, то следует добавить год рождения или две последние цифры (KateIvanova76 или EkaterinaIvanova1976). Неправильным примером может стать электронная почта с названием «Kotenok1976».

Вместе с тем специалисты рекомендуют:

1. Не указывать в личной почте личную информацию, например, лучше выбрать «музыкальный_фанат@» или «рок2013» вместо «Коля2012».

2. Использовать несколько почтовых ящиков: первый для частной переписки с адресатами, к которым имеется доверие, и второй для регистрации на форумах и сайтах.

Не рекомендуется использовать для регистрации на важных сайтах сервисы, предоставляющие адрес электронной почты на время, поскольку в дальнейшем восстановить доступ к такой почте будет невозможно.

После получения адреса электронной почты можно пройти регистрацию в социальных сетях.

Первоначально социальные сети были созданы для упрощения общения между людьми. В них можно делиться своими мыслями, идеями, заводить новые знакомства и поддерживать общение со старыми друзьями.

Теперь страничка в социальных сетях – это не только виртуальное Я человека, но и инструмент формирования имиджа пользователя, поэтому так необходимо внимательно относиться к тому, как она выглядит.

Чтобы обезопасить себя в социальных сетях, пользователю нужно придерживаться *различных правил*.

Перед регистрацией в социальных сетях необходимо ознакомиться с политикой конфиденциальности, условиями использования и безопасности, а также другими условиями, поскольку данному ресурсу будут предоставлены не только персональные данные, но и, скорее всего, через него будут осуществляться покупки.

При регистрации необходимо указание реальных имени и фамилии, поскольку в случае утери доступа к аккаунту паспортные данные пользователя смогут стать подтверждением факта принадлежности аккаунта. При публикации аватара необходимо помнить, что использование для этой цели чужой фотографии может привести к блокировке аккаунта со стороны администрации.

При регистрации в новой социальной сети или сервисе обычно запрашивается возможность поиска друзей или коллег по электронной почте, которые уже зарегистрированы на сайте или сервисе. Рекомендуется не раскрывать адреса электронной почты друзей и знакомых, поскольку, используя полученные данные, сайты или сервисы смогут рассылать электронные сообщения от имени пользователя всем пользователям из списка контактов.

При работе в социальной сети в первую очередь необходимо ограничить список друзей. В друзьях любого пользователя не должно быть случайных и незнакомых людей. Мошенники могут создавать фальшивые профили, чтобы получить от пользователя или его друзей информацию.

Публикуя информацию, необходимо помнить о цифровой репутации и не размещать информацию личного характера, которая может быть использована против пользователя: пароли, телефон, адрес и другую личную информацию, которая позволяет узнать окружение, интересы и виды активности пользователя. Стоит заполнять только обязательные пункты раздела «о себе», которые помечены звездочкой.

В частности, именно через социальные сети злоумышленники ищут данные, которые используются в качестве секретного слова или пароля.

Особенно необходимо обратить внимание на настройки геолокации. Собрав информацию о перемещениях пользователя и его частых местах пребывания, злоумышленники смогут спланировать любое преступление. Кроме этого, лучше избегать размещения фотографий в интернете, где по местности можно определить местоположение, кроме публичных и туристических мест.

Не стоит афишировать свое финансовое благосостояние: информация о приобретении машины, квартиры и путешествии может послужить мотивацией для грабителей. Примером данной ситуации служит история, когда злоумышленники ограбили квартиру во время отпуска ее хозяев, узнав о планируемом отпуске и его сроках из аккаунта сына в социальной сети.

Данное правило также распространяется на всю публикуемую на странице информацию, в том числе на репосты из публичных страниц либо со страниц своих друзей, добавленные видео и фотографии и список групп и страниц, на которые подписан пользователь.

Таким образом, перед публикацией необходимо проводить внутреннюю модерацию, оценивая уровень уверенности, безопасности и адекватности публикуемой информации.

В этой связи особую актуальность приобретает установка настроек приватности, которые рекомендуется установить на максимальном уровне, предоставив возможность доступа к информации, публикуемой на аккаунте, только друзьям. Рекомендуется также разграничить информацию, которую могут увидеть друзья, коллеги или одноклассники, родители, коллеги, педагоги и другие лица, что позволит не смешивать среди ваших друзей работу/учебу и отдых, а некоторые лица не должны знать все.

Получая от своего друга странное или подозрительное сообщение, нельзя быть уверенным в том, что его аккаунт не был взломан. Также необходимо относиться с осторожностью к приглашениям зарегистрироваться в той или иной социальной сети, вступить в какое-либо сообщество, скачать файл, проверяя ведет ли присланная ссылка на безопасный сайт или страницу. Рекомендуется оперативно связаться с отправителем альтернативным способом, например, по телефону, чтобы убедиться в том, что именно этот человек отправил вам данное сообщение.

Многие социальные сервисы предоставляют возможность использования внутри социальной сети различные приложения, в том числе игры, а авторизацию через социальную сеть использовать при посещении других сайтов. Перед использованием такой функции необходимо удостовериться в безопасности данного приложения или сайта, поскольку через данный канал злоумышленникам могут перейти различные личные данные.

Особая категория аккаунтов в социальных сетях – это *фейки*.

Фейки – это поддельные страницы реальных людей с идентичными фотографиями и данными. Чаще всего фейковые страницы создают под профайлы известных людей. Как отличить фейк от оригинала?

1. Фотографии, «вырванные» из других социальных сетей или поисковых сервисов. Многие социальные сети помечают закаченные фотографии своим логотипом либо уменьшают качество фотографии.
2. Пустой профайл, на котором не указана подробная личная информация.
3. В общении с другими людьми обладатель фейковой страницы обычно пишет общими фразами, никогда не указывает детали.
4. От фейковых страниц приходит много спама, так как многие мошенники создают такие странички для накрутки голосов или приглашения людей на свои сайты или группы.
5. Если указана школа/университет и год окончания, то проверьте, есть ли в друзьях у данного аккаунта пользователи, указавшие данную школу или вуз. Зачастую фейковые аккаунты создают и раскручивают аккаунт в короткие сроки, а фотографии загружают в одно время.

В конце отметим, что необходимо помнить, что быть и казаться – разные понятия.

То, что демонстрируется в социальных сетях, не всегда соответствует реальности.

Вместе с социальными сетями многие пользователи используют различные мессенджеры для общения, однако в большинстве мессенджеров можно не только обмениваться текстовыми и фотосообщениями, но и звонить, подписываться на информационные каналы, общаться в чатах, осуществлять покупки и другие действия.

Как и в социальных сетях, сервисах почт и мессенджерах вопросы сохранения пользовательских данных от коммерческого использования крайне актуальны. Так некоторые сервисы используют полученные данные и продают третьим лицам и рекламодателям, чтобы обеспечить персонализированную рекламу товара или услуги, которой пользователь интересовался или даже обсуждал с другими пользователями.

Необходимо учитывать данный вопрос при выборе сервиса, в частности многие мессенджеры предоставляют функцию сквозного шифрования, предполагающую возможность прочтения текста только отправителем и получателем, и предполагают удаление сообщений и другого контента с серверов после отправления.

Многие мессенджеры предоставляют возможность самоуничтожения сообщений после получения их адресатом. Сообщение будет удалено как на устройстве пользователя, так и устройстве получателя, что позволяет обеспечить безопасность переписки и сохранение личных данных.

Интернет-зависимость

Интернет-зависимость – навязчивое желание войти в интернет, находясь офлайн и неспособность выйти из интернета, будучи онлайн (Гриффит В., 1996).

Фактически интернет-зависимость – это расстройство психики, заключающееся в неспособности человека вовремя выйти из сети, а также в постоянном присутствии желания в нее зайти.

По своим проявлениям она схожа с уже известными формами аддиктивного поведения, например, в результате употребления алкоголя или наркотиков, но относится к типу нехимических зависимостей, то есть не приводящих непосредственно к разрушению организма.

Главной группой риска в этом виде зависимости являются люди, испытывающие проблемы или дефицит реального общения. Отсутствие коммуникативных навыков погружает их в виртуальный мир, заменяющий им круг реальных друзей.

Интернет-зависимым такой стиль жизни легче, поскольку позволяет забыть о проблемах в реальной жизни или разногласиях с друзьями или близкими, что приводит к конфликтам с последними, таким образом поддерживая зависимость.

Зависимость от интернета возникает по ряду причин и может проявляться в различных формах.

Интернет-зависимость опасна по различным причинам, которые приводят:

1) к снижению концентрации внимания;
2) к ухудшению памяти;
3) к мыслительным и психическим расстройствам;
4) к обострению физических заболеваний;
5) к потере времени для жизни.

Известны многие *виды интернет-зависимости:*

1) информационная зависимость (стремление постоянно путешествовать по интернету в бесцельных поисках информации);
2) игровая зависимость, когда пользователь «подсаживается» и не может оторваться от онлайн-игр, тратя реальные деньги;
3) зависимость от интернет-общения;
4) зависимость от азартных игр в интернете. Во многом схожа с обычным пристрастием к игре на деньги. Здесь в качестве главной опасности выступают интернет-казино и другие сайты азартных игр, которые действуют по аналогии с настоящими;
5) стремление к поиску информации агрессивного или непристойного содержания;
6) постоянное стремление к просмотру или скачиванию фильмов и музыки;
7) стремление к совершению вредных действий (целенаправленное нарушение правил сетевого этикета, распространение ненужной или вредной информации и т.п.);
8) хакерство;
9) навязчивое желание тратить деньги и осуществлять ненужные покупки, в частности непроизвольная тяга к покупкам вещей на интернет-аукционах и в онлайн-магазинах;
10) пристрастие к виртуальному общению и виртуальным знакомствам (большие объемы переписки, постоянное участие в чатах, веб-форумах, избыточность знакомых и друзей в сети);
11) бесконечное скачивание с торрент-трекеров и других источников нелицензионного контента и материалов в целях создания собственной базы и т.д.

Интернет-зависимые как большинство психически нездоровых людей не осознают тяжести своего состояния и с раздражением и агрессией относятся к попыткам отвлечь их от источника зависимости, но это происходит, когда болезнь зашла уже слишком далеко. До этого еще можно и самостоятельно обнаружить у себя признаки формирующейся зависимости и, если хватит силы воли, вовремя остановиться.

Для этого состояния характерны следующие *признаки:*

1) потеря ощущения времени при использовании устройства;

2) эйфория при использовании устройства;

3) досада и раздражение при невозможности выйти в интернет, в частности отвращение ко всем остальным видам деятельности;

4) друзья и знакомые перестают общаться, но это не расстраивает;

5) интересует только то, что связано с предметом увлечения – играми, социальными сетями и т.п.;

6) невозможность остановиться при использовании устройства;

7) использование устройства тайно или тайком от посторонних. Интернет-зависимые считают, что следует потратить все деньги на покупку новых игр, на увеличение мощности компьютера и улучшение или приобретение подобных функций; лучшие друзья – те, которых они встретили в виртуальной среде.

Зачастую интернет-зависимые врут о своей зависимости, например, говоря, что занимались чем-то другим, а не проводили время в интернете.

Однако с любой проблемой можно справиться, если осознавать в этом необходимость. Для того чтобы не попасть в компьютерную зависимость, помогут *следующие действия:*

1. Для входа в интернет должна быть обоснованная цель пребывания в интернете. Можно планировать, какие сайты посетить, что там сделать и посмотреть, сколько времени на это выделить. Если работа с устройством в учебных целях, необходимо следить за тем, чтобы не отвлекаться на ненужные ресурсы.

2. Необходимо уменьшать количество времени, которое пользователь проводит в интернете, чтобы в конечном итоге свести его к минимуму. Возможно установление временных интервалов для работы и отдыха в интернете, а смартфон можно ограничить графиком проверки сообщения, например, один раз в полчаса, а ночью выключать его.

3. Если появилось свободное время, то лучше быть на воздухе, двигаться и заниматься спортом, а также лично общаться с друзьями и знакомыми.

4. Необходимо урегулировать режим сна и питания, исключив практику питания за компьютером.

РАЗДЕЛ 3. ОРГАНИЗАЦИЯ ОБУЧЕНИЯ ДЕТЕЙ И РОДИТЕЛЕЙ/ЗАКОННЫХ ПРЕДСТАВИТЕЛЕЙ

3.1. Аспекты информационной безопасности для родителей/законных представителей детей

Вопросы информационной безопасности детей для родителей или законных представителей детей имеют свою специфику, отражающую необходимые им знания для обеспечения защиты детей в информационном пространстве с учетом специфики каждого возраста.

Общие вопросы для родителей можно представить следующими *советами:*

1. Независимо от возраста ребенка используйте программное обеспечение, помогающее фильтровать и контролировать информацию, но не полагайтесь полностью на него. Ваше внимание к ребенку – главный метод защиты.

2. Если ваш ребенок имеет аккаунт на одном из социальных сервисов (LiveJournal, blogs.mail.ru, vkontakte.ru и т.п.), внимательно изучите, какую информацию помещают его участники в своих профилях и блогах, включая фотографии и видео.

3. Проверьте, с какими другими сайтами связан социальный сервис вашего ребенка. Странички вашего ребенка могут быть безопасными, но могут и содержать ссылки на нежелательные и опасные сайты (например, порносайт или сайт, на котором друг упоминает номер сотового телефона вашего ребенка или ваш домашний адрес).

4. Стимулируйте ваших детей сообщать обо всем странном или отталкивающем.

5. Реагируйте, когда они этого не делают (из-за опасения потерять доступ к интернету дети не говорят родителям о проблемах, а также могут начать использовать интернет вне дома и школы).

6. Будьте в курсе сетевой жизни вашего ребенка. Интересуйтесь, кто его друзья в интернете так же, как интересуетесь реальными друзьями.

Советы по безопасности в сети Интернет для детей 7–8 лет

В интернете ребенок старается посетить те или иные сайты, а возможно и чаты, разрешение на посещение которых он не получил бы от родителей. Поэтому родителям особенно полезны будут те отчеты, которые предоставляются программами по ограничению использования интернета, то есть родительский контроль или то, что вы сможете увидеть во временных файлах. В результате у ребенка не будет ощущения, что за ним ведется постоянный контроль, однако родители будут по-прежнему знать, какие сайты посещает их ребенок. Дети в данном возрасте обладают сильным чувством семьи, они доверчивы и не сомневаются в авторитетах. Они любят играть в сетевые игры и путешествовать по интернету, используя электронную почту, заходить на сайты и чаты, не рекомендованные родителями.

Советы по безопасности в сети Интернет для детей 7–8 лет:

1. Создайте список домашних правил посещения интернета при участии детей и требуйте его выполнения.

2. Требуйте от вашего ребенка соблюдения временных норм нахождения за компьютером. Покажите ребенку, что вы наблюдаете за ним не потому, что вам это хочется, а потому, что вы беспокоитесь о его безопасности и всегда готовы ему помочь.

3. Компьютер с подключением к интернету должен находиться в общей комнате под присмотром родителей.

4. Используйте специальные детские поисковые машины.

5. Используйте средства блокирования нежелательного контента как дополнение к стандартному родительскому контролю.

6. Создайте семейный электронный ящик, чтобы не позволить детям иметь собственные адреса.

7. Блокируйте доступ к сайтам с бесплатными почтовыми ящиками с помощью соответствующего программного обеспечения.

8. Приучите детей советоваться с вами перед опубликованием какой-либо информации средствами электронной почты, чатов, регистрационных форм и профилей.

9. Научите детей не загружать файлы, программы или музыку без вашего согласия.

10. Не разрешайте детям использовать службы мгновенного обмена сообщениями.

11. В «белый» список сайтов, разрешенных для посещения, вносите только сайты с хорошей репутацией.

12. Не забывайте беседовать с детьми об их друзьях в интернете, как если бы речь шла о друзьях в реальной жизни.

13. Не делайте «табу» из вопросов половой жизни, так как в интернете дети могут легко наткнуться на порнографию или сайты «для взрослых».

14. Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с интернетом. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам о своих тревогах. Похвалите их и посоветуйте всегда обращаться в подобных случаях.

Советы по безопасности в сети Интернет для детей от 9 до 12 лет

В данном возрасте дети, как правило, уже наслышаны о том, какая информация существует в интернете. Совершенно нормально, что они хотят это увидеть, прочесть, услышать. При этом нужно помнить, что доступ к нежелательным материалам можно легко заблокировать при помощи средств родительского контроля. Советы по безопасности для детей от 9 до 12 лет:

1. Создайте список домашних правил посещения интернета при участии детей и требуйте его выполнения.

2. Требуйте от вашего ребенка соблюдения норм нахождения за компьютером.

3. Наблюдайте за ребенком при работе за компьютером, покажите ему, что вы беспокоитесь о его безопасности и всегда готовы оказать ему помощь.

4. Компьютер с подключением в интернет должен находиться в общей комнате под присмотром родителей.

5. Используйте средства блокирования нежелательного контента как дополнение к стандартному родительскому контролю.

6. Не забывайте принимать непосредственное участие в жизни ребенка, беседовать с детьми об их друзьях в интернете.

7. Настаивайте, чтобы дети никогда не соглашались на личные встречи с друзьями по интернету.

8. Позволяйте детям заходить только на сайты из «белого» списка, который создайте вместе с ними.

9. Приучите детей никогда не выдавать личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в интернете.

10. Приучите детей не загружать программы без вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.

11. Создайте вашему ребенку ограниченную учетную запись для работы на компьютере.

12. Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с интернетом. Напомните детям, что они в безопасности, если сами рассказали вам о своих тревогах и опасениях.

13. Расскажите детям о порнографии в интернете.

14. Настаивайте на том, чтобы дети предоставляли вам доступ к своей электронной почте, чтобы вы убедились, что они не общаются с незнакомцами.

15. Объясните детям, что нельзя использовать сеть для хулиганства, распространения сплетен или угроз.

Советы по безопасности в сети Интернет детей и подростков от 13 до 17 лет

В этом возрасте подростки активно используют поисковые машины, пользуются электронной почтой, службами мгновенного обмена сообщениями, скачивают музыку и фильмы. Мальчикам в этом возрасте больше по нраву сметать все ограничения, они жаждут грубого юмора, азартных игр, картинок «для взрослых». Девочки предпочитают общаться в чатах, при этом они гораздо более чувствительны к сексуальным домогательствам в интернете. Зачастую в данном возрасте родителям уже весьма сложно контролировать своих детей, так как об интернете те уже знают значительно больше своих родителей. Тем не менее, не отпускайте детей в «свободное плавание» по интернету. Старайтесь активно участвовать в общении ребенка в интернете.

Важно по-прежнему строго соблюдать правила интернет-безопасности – соглашение между родителями и детьми. Кроме того, необходимо как можно чаще просматривать отчеты о деятельности детей в интернете. Следует обратить внимание на необходимость содержания родительских паролей (паролей администраторов) в строгом секрете и обратить внимание на строгость этих паролей.

Советы по безопасности детей и подростков в возрасте от 13 до 17 лет:

1. Создайте список домашних правил посещения интернета при участии подростков и требуйте безусловного его выполнения. Обговорите с ребенком список запрещенных сайтов («черный список»), часы работы в интернете, руководство по общению в интернете (в том числе в чатах).

2. Компьютер с подключением к сети Интернет должен находиться в общей комнате.

3. Не забывайте беседовать с детьми об их друзьях в интернете, о том, чем они заняты, но таким образом, будто речь идет о друзьях в реальной жизни. Спрашивайте о людях, с которыми дети общаются посредством служб мгновенного обмена сообщениями, чтобы убедиться, что эти люди им знакомы.

4. Используйте средства блокирования нежелательного контента как дополнение к стандартному родительскому контролю.

5. Необходимо знать, какими чатами пользуются ваши дети. Поощряйте использование модерируемых чатов и настаивайте, чтобы дети не общались в приватном режиме.

6. Настаивайте на том, чтобы дети никогда не встречались лично с друзьями из сети Интернет.

7. Приучите детей не выдавать свою личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в интернете.

8. Приучите детей не загружать программы без вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.

9. Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с интернетом. Напомните детям, что они в безопасности, если сами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте всегда обращаться в подобных случаях.

10. Расскажите детям о порнографии в интернете. Помогите им защититься от спама. Научите подростков не выдавать в интернете своего реального электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.

11. Приучите себя знакомиться с сайтами, которые посещают подростки.

12. Научите детей уважать других в интернете. Убедитесь, что они знают о том, что правила хорошего поведения действуют везде – даже в виртуальном мире.

13. Объясните детям, что ни в коем случае нельзя использовать сеть для хулиганства, распространения сплетен или угроз другим людям.

14. Обсудите с подростками проблемы сетевых азартных игр и их возможный риск. Напомните, что дети не могут играть в эти игры согласно закону.

15. Постоянно контролируйте использование интернета вашим ребенком. Это не нарушение его личного пространства, а мера предосторожности и проявление вашей родительской ответственности и заботы.

3.2. Организация обучения детей и родителей/законных представителей

Образовательные организации с учетом раздела №1 «Актуальность информационной безопасности детей» данных методических рекомендаций должны предпринимать различные меры по повышению уровня знаний обучающихся в сфере информационной безопасности, а для реализации данной функции также взаимодействовать с родителями и законными представителями обучающихся для повышения их уровня знаний в данной сфере.

Важнейшим условием реализации данной работы является соответствие организации образования требованиям для успешной и эффективной организации обучения информационной безопасности обучающихся и их родителей/законных представителей, в частности кадровым, материально-техническим и иным условиям.

Организация обучения информационной безопасности обучающихся

Организация образования может организовать обучение своих обучающихся информационной безопасности путем:

1. Обращения внимания на вопросы обеспечения информационной безопасности в рамках действующих в организации образования учебных дисциплин.

2. Внедрения в образовательную программу самостоятельной учебной дисциплины или увеличения количества учебных часов на изучение данной проблематики при изучении учебных предметов в рамках вариативной части учебного плана образовательной программы.

3. Организации соответствующих мероприятий или обучения в рамках тематической внеурочной деятельности и дополнительного образования.

4. Организации соответствующих мероприятий или обучения в рамках программ воспитания и социализации обучающихся.

Организациям образования и организациям дополнительного образования рекомендуется организовать обучение детей с 1 по 11 классы или до 18 лет включительно, а для профессиональных образовательных организаций до 18 лет включительно и далее на усмотрение администрации организации образования.

Вопросы обеспечения информационной безопасности могут быть изучены во время различных учебных дисциплин как в рамках курса «Информатика», так и других предметных областей, и иной учебной деятельности с учетом межпредметных и метапредметных связей.

При преподавании и изучении обучающимися вопросов информационной безопасности рекомендуется не только рассмотреть информационные, потребительские, технические и коммуникативные аспекты информационной безопасности, но и вопросы практического использования сети Интернет для собственного развития и образования.

Для повышения эффективности занятий могут быть проведены межпредметные и внутрикурсовые уроки: одновременно по двум предметам, одновременно для обучающихся разных возрастов и т.д.

Непосредственно *уроки и занятия* по вопросам информационной безопасности возможно организовать в следующих формах, которые могут быть использованы как отдельно, так и совместно:

1. Дискуссии или дебаты.
2. Деловые игры.
3. Подготовка обучающимися тематических буклетов, листовок и других материалов.
4. Квесты, премии, конкурсы и олимпиады.
5. Анкетирование, исследования и опросы.
6. Тесты и викторины.
7. Демонстрация мультфильмов и/или видеоурока.
8. Семинар, вебинар или занятие с приглашенным экспертом.

При проведении уроков и занятий можно использовать следующие *игровые методики:*

1. Уроки, напоминающие публичные формы общения: пресс-конференция, брифинг, аукцион, бенефис, регламентированная дискуссия, панорама, телемост, репортаж, диалог, «живая газета», устный журнал и т.д.

2. Уроки, основанные на имитации деятельности учреждений и организаций: следствие, органы власти, патентное бюро, ученый совет и т.д.

3. Уроки, основанные на имитации деятельности при проведении общественно-культурных мероприятий: заочная экскурсия, экскурсия в прошлое, путешествие, прогулки и т.д.

Рекомендуется предусмотреть после поведения уроков и занятий раздачу обучающимся листовок об основных аспектах информационной безопасности, которые образовательные организации могут распечатать самостоятельно.

Организация обучения информационной безопасности родителей и законных представителей обучающихся

Организация образования может для повышения уровня знаний родителей и законных представителей обучающихся в вопросах обеспечения информационной безопасности детей предпринимать различные регулярные меры информационного и организационного характера, в частности:

1. Освещение вопросов информационной безопасности детей в рамках проводимых родительских собраний и проведение тематических собраний для родителей с участием педагогических работников и представителей администрации организации образования, в частности для демонстрации видеоматериалов по данным вопросам.

2. Организация индивидуальных и групповых консультаций родителей и законных представителей обучающихся классными руководителями, специалистами психологической службы и администрации организации образования для обеспокоенных родителей и законных представителей обучающихся, а также родителей и законных представителей обучающихся, находящихся в группе риска.

3. Проведение семинаров, лекций и вебинаров с участием экспертов и сотрудников правоохранительных органов для родителей и законных представителей обучающихся.

4. Раздача информационных материалов об обеспечении безопасности детей в сети Интернет, в частности памятки, флаеры и другие материалы.

5. Проведение анкетирования родителей и законных представителей обучающихся по вопросам организации дома мер по обеспечению защиты детей в информационном пространстве.

6. Размещение на сайте организации образования, средствах массовой информации, сообществах в социальной сети и сервисе электронных дневников для родителей и законных представителей обучающихся информации по обеспечению информационной безопасности детей.

В ходе мероприятий для родителей и законных представителей обучающихся рекомендуется отметить следующие *темы:*

1. Важность обеспечения цифровой и информационной грамотности детей и подростков.

2. Рекомендации и советы по обеспечению информационной безопасности личности и детей как особо незащищенных пользователей сети Интернет.

3. Методы и функции родительского контроля.

3.3. Информационно-методическое сопровождение организации обучения информационной безопасности обучающихся и их родителей/законных представителей

Организациям образования и педагогическим работникам рекомендуется учитывать следующие аспекты при выборе учебников, учебно-методической литературы и материалов для организации обучения информационной безопасности обучающихся и их родителей/законных представителей.

Используемые в образовательном процессе учебники, учебно-методическая литература и материалы по содержанию должны соответствовать данным методическим рекомендациям.

ИСТОЧНИКИ И РЕКОМЕНДУЕМЫЕ САЙТЫ В СЕТИ ИНТЕРНЕТ

1. http://festival.1september.ru/articles/612789/ – урок в 9–10 классах. Профилактика интернет-зависимости «Будущее начинается сегодня».
2. http://i-deti.org/ – портал «Безопасный инет для детей», ресурсы, рекомендации, комиксы.
3. http://ppt4web.ru/informatika/bezopasnyjj-internet.html – презентация о безопасном интернете.
4. http://security.mosmetod.ru/ – сайт «Безопасный интернет».
5. http://www.igra-internet.ru/ – онлайн интернет-игра «Изучи интернет – управляй им».
6. http://www.ligainternet.ru/ – Лига безопасного интернета.
7. http://www.microsoft.com/ru-ru/security/default.aspx – сайт Центра безопасности Майкрософт.
8. http://www.nachalka.com/node/950 – видео «Развлечение и безопасность в интернете».
9. http://www.safe-internet.ru/ – сайт Ростелеком «Безопасность детей в интернете», библиотека с материалами, памятками, рекомендациями по возрастам.
10. http://сетевичок.рф/ – «СЕТЕВИЧОК» сайт для детей – обучение и онлайн-консультирование по вопросам кибербезопасности сетевой безопасности.
11. https://staysafeonline.org/ – Stay Safe Online-ресурс, предоставляющий информацию о кибербезопасности для детей, подростков и их родителей.
12. https://www.commonsensemedia.org/ – Common Sense Media-сайт, предоставляющий рекомендации о контенте для детей и семей, а также советы по безопасности в онлайн-мире.
13. https://www.detyvinternete.ru/ – дети в интернете, российский ресурс, посвященный вопросам безопасности детей в сети Интернет.
14. https://www.internet-patrul.ru/ – интернет-патруль, российский проект, направленный на обучение детей и родителей безопасному поведению в интернете.
15. www.1001skazka.com – «1001 сказка». На сайте можно скачать аудиофайлы – сказки, аудиокниги.
16. www.e-parta.ru – блог школьного «Всезнайки» – это ленты новостей по всем школьным предметам, виртуальные экскурсии, психологические и юридические советы по проблемам в школе и на улице, учебные видеофильмы, обзоры лучших ресурсов Всемирной паутины.
17. www.fid.su/projects/saferinternet/year/hotline/ – Линия помощи «Дети онлайн». Оказание психологической и практической помощи детям и подросткам, которые столкнулись с опасностью или негативной ситуацией во время пользования интернетом или мобильной связью. Линия помощи «Дети онлайн» является первым и единственным такого рода проектом в России и реализуется в рамках Года безопасного интернета в России.
18. www.friendlyrunet.ru – Фонд «Дружественный Рунет». Фонд поддерживает проекты, связанные с безопасным использованием интернета, содействует российским пользователям, общественным организациям, коммерческим компаниям и государственным ведомствам в противодействии обороту противоправного контента, а также в противодействии иным антиобщественным действиям в сети.
19. www.membrana.ru – «Люди. Идеи. Технологии». Информационно-образовательный интернет-журнал о новых технологиях.
20. www.nedopusti.ru – социальный проект по защите прав детей «Не допусти» – социальный проект по защите детей от похищений, сексуальной эксплуатации и жестокого обращения.
21. www.newseducation.ru – «Большая перемена» сайт для школьников и их родителей.
22. www.saferunet.ru – Центр безопасного интернета в России. Сайт посвящен проблеме безопасной, корректной и комфортной работы в интернете.