**МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОСНОВАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ОБУЧАЮЩИХСЯ ОБЩЕОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЙ С УЧЁТОМ ИНФОРМАЦИОННЫХ, ПОТРЕБИТЕЛЬСКИХ, ТЕХНИЧЕСКИХ И КОММУНИКАТИВНЫХ АСПЕКТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

**Сокращенный вариант.**

Методические рекомендации по основам информационной безопасности для обучающихся общеобразовательных организаций с учётом информационных, потребительских, технических и коммуникативных аспектов информационной безопасности (далее – методические рекомендации) разработаны в соответствии с пунктом 8 приказа № 88 Минкомсвязи России 27 февраля 2018 года «Об утверждении плана мероприятий по реализации Концепции информационной безопасности детей на 2018-2020 годы».

Методические рекомендации направлены на организацию преподавания основ информационной безопасности в общеобразовательных организациях Российской Федерации.

Методические рекомендации разработаны Временной комиссией Совета Федерации по развитию информационного общества совместно с ФСБ России, Минобрнауки России, Минкомсвязи России, Роскомнадзором, МЧС России и Минздравом России.

Задачи методических рекомендаций:

1. Оказание методической поддержки педагогических работников и сотрудников образовательных организаций России 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 общеобразовательных организаций Российской Федерации в части тематических положений приказа Министерства труда и социальной защиты РФ от 18 октября 2013 г. N 544н"Об утверждении профессионального стандарта "Педагог (педагогическая деятельность в сфере дошкольного, начального общего, основного общего, среднего общего образования) (воспитатель, учитель)", ФГОС ООО, ФГОС НОО и ФГОС СОО;
4. Оказать методическую помощь администрациям субъектов Российской Федерации, органам местного самоуправления и администрациям образовательных организаций в организации обучения детей, их родителей (законных представителей) и педагогических работников информационной безопасности;
5. Формирование тем и вопросов по вопросам информационной безопасности для включения в тематические учебники, учебные пособия и другие учебно-методические материалы.

Методические рекомендации направлены на организацию обучения детей по следующим направлениям:

1. Организация обучения в рамках действующих учебных предметов и(или) использования межпредметного обучения;
2. Организация обучения в рамках части основной образовательной программы, формируемой участниками образовательного процесса, включая организацию отдельных учебных предметов, учебных курсов и внеурочную деятельность;
3. Организация обучения в рамках дополнительного образования.

Методические рекомендации ориентированы на следующие аудитории (далее - педагогические работники):

1. Учителя, преподаватели и классные руководители;
2. Сотрудники администрации образовательных организаций по учебно-воспитательной работе, по воспитательной работе и безопасности образовательного процесса и обучающихся;
3. Ответственные лица в штате образовательных организаций в части психологического и воспитательного взаимодействия с обучающимися и педагогами (педагоги-организаторы, психологи, методисты и другие сотрудники образовательных организаций);
4. Ответственные лица в штате образовательных организаций в части дополнительного образования обучающихся и организации внеурочной деятельности.

Кроме этого, данные методические рекомендации могут быть использованы:

1. администрациями учреждений для детей-сирот и детей, оставшихся без попечения родителей;
2. организациями дополнительного образования;
3. профессиональными образовательными организациями;
4. и другими организациями, осуществляющими образовательную деятельность для несовершеннолетних обучающихся.

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 разработаны по методологии международного исследовательского проекта Еврокомиссии «EU KidsOnline II» (2010-11 гг.), согласно которой риски (опасности) по данной классификации разделяются на четыре типа: контентные, коммуникационные, электронные (технические) и потребительские. Данная методология была использована при формировании заданий и продемонстрировала эффективность квеста по цифровой грамотности «Сетевичок», проводимого на площадке Временной комиссии Совета Федерации по развитию информационного общества с 2014 года в рамках Единого урока по безопасности в сети «Интернет».

Методические рекомендации разработаны на основе:

1. материалов Федерального государственного автономного образовательного учреждения дополнительного профессионального образования «Академия повышения квалификации и профессиональной переподготовки работников образования» (ФГАОУ ДПО АПК и ППРО);
2. материалов порталов "Яндекс" «Сетевичок», «Единое окно доступа к образовательным ресурсам» и «Государственные и муниципальные услуги (функции) в Санкт-Петербурге»;
3. материалов Следственного комитета Российской Федерации;
4. материалов Экспертного совета по информатизации системы образования и воспитания при Временной комиссии Совета Федерации по развитию информационного общества.

Методические рекомендации основаны на положениях курса «Основы кибербезопасности» (далее – курс), разработанного Временной комиссией Совета Федерации по развитию информационного общества.

Курс был одобрен и рекомендован руководителям образовательных организаций высшего образования департаментом высшего образования Минобрнауки России (письмо от 28 июля 2017 г. № 05-11170) для интеграции курса в образовательные программы по УГСН 44.00.00 "Образование и педагогические науки" и реализуется во многих образовательных организациях Российской Федерации согласно рекомендациям парламентских слушаний «Актуальные вопросы обеспечения безопасности и развития детей в информационном пространстве», прошедшие в Совете Федерации 17 апреля 2017 года, и модульной региональной программы обеспечения информационной безопасности детей, производства информационной продукции для детей и оборота информационной продукции, принятой и утверждённой в большинстве субъектов Российской Федерации в качестве региональных программ и планов.

Обновление и актуализация методических рекомендаций будет осуществляться Временной комиссией Совета Федерации по развитию информационного общества до 2020 года включено согласно разделу «Организационно-административные мероприятия Временной комиссии Совета Федерации по развитию информационного общества по реализации методических рекомендаций» методических рекомендаций.

Целью использования методических рекомендаций к 2020 году являются достижение следующих показателей:

1. Охват 100 процентов общеобразовательных организаций системным обучением детей кибербезопасности;
2. Охват не менее 70 процентов педагогических работников, прошедших специальное обучение, курсы и мероприятия, направленные на повышение уровня их знаний и навыков в сфере информационной безопасности;
3. Охват не менее 20 процентов родителей (законных представителей) обучающихся образовательных организаций, прошедших специальное обучение, курсы и мероприятия, направленные на повышение уровня их знаний и навыков в сфере информационной безопасности детей.

**Актуальность информационной безопасности детей**

Дети и подростки — активные пользователи интернета как в мире, так в Российской Федерации.

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.

Определение термина «информационная безопасность детей» содержится в Федеральном законе № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», регулирующим отношения, связанные с защитой детей от информации, причиняющей вред их здоровью и (или) развитию. Согласно данному закону «информационная безопасность детей» - это состояние защищенности, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию.

В силу Федерального закона № 436-ФЗ информацией, причиняющей вред здоровью и (или) развитию детей, является:

1. информация, запрещенная для распространения среди детей;

2. информация, распространение которой ограничено среди детей определенных возрастных категорий.

3. К информации, запрещенной для распространения среди детей, относится:

4. информация, побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в т.ч. причинению вреда своему здоровью, самоубийству;

5. способность вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, пиво и напитки, изготавливаемые на его основе; принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;

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

7. отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи;

8. оправдывающая противоправное поведение;

9. содержащая нецензурную брань;

10. содержащая информацию порнографического характера.

**К информации, распространение которой ограничено среди детей определенного возраста, относится:**

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

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

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

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

**С учетом этого Вам предлагаются правила работы в сети Интернет для различных возрастных категорий, соблюдение которых позволит обеспечить информационную безопасность ваших детей.**

**Общие правила для родителей:**

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. Поощряйте Ваших детей сообщать обо всем странном или отталкивающим и не слишком остро реагируйте, когда они это делают (из-за опасения потерять доступ к Интернету дети не говорят родителям о проблемах, а также могут начать использовать Интернет вне дома и школы).

5. Будьте в курсе сетевой жизни Вашего ребенка. Интересуйтесь, кто их друзья в Интернет так же, как интересуетесь реальными друзьями.

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, т. е. 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.**

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 подойти еще раз в подобных случаях.

**Информационные аспекты информационной безопасности**

***Основы информации***

Информация – это сведения (сообщения, данные) независимо от формы их представления.

Выделяют следующие категории информации:

1. Общедоступная информация
2. Информация с ограниченным доступом:

- Это такая информация, обладатели которой вправе предоставлять доступ к ней по своему усмотрению, в частности на возмездной (платной) основе.(Пример: произведения, являющиеся объектом авторского права; )

- Конфиденциальная- доступ к которой ограничивается в целях соблюдения интересов государства или прав и законных интересов их владельцев. (государственная тайна, персональные данные, личная и семейная тайны, медицинская тайна)

Необходимо отметить, что имеет место быть информация нежелательного характера, которая содержит противозаконную, неэтичную и вредоносную информацию.

**Противозаконная**- информация, пропагандирующая потребление и изготовление наркотиков, азартные игры, некоторые виды информации среди детей и отдельных возрастных групп и т.д. Распространение данной информации преследуется по закону.

**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. Примером такой информации может стать нецензурная брань. (может повлечь санкции со стороны владельцев сайта, на которых пользователь размещает такую информацию, или со стороны организаций, имеющих возможность ограничить доступ к сайту, содержащего такую информацию).

 **Вредоносная.** Распространяется данная информация для заражения компьютера вирусами. Заражение устройств позволяет злоумышленникам получить и украсть важные данные.

***Реклама***

Особый вид информации – это реклама.

**Реклама не должна:** побуждать к совершению противоправных действий;призывать к насилию и жестокости; содержать информацию порнографического характера.

 В рекламе не допускается использование бранных слов, непристойных и оскорбительных образов, сравнений и выражений.

Не допускается размещение рекламы в учебниках, учебных пособиях, предназначенных для обучения детей по основным образовательным программам начального общего, основного общего, среднего общего образования, школьных дневниках, школьных тетрадях.

В целях защиты несовершеннолетних от злоупотреблений их доверием и недостатком опыта в рекламе не допускаются:

1. дискредитация родителей и воспитателей, подрыв доверия к ним у несовершеннолетних;
2. побуждение несовершеннолетних к тому, чтобы они убедили родителей или других лиц приобрести рекламируемый товар;
3. формирование комплекса неполноценности у несовершеннолетних, не обладающих рекламируемым товаром;
4. формирование у несовершеннолетних комплекса неполноценности, связанного с их внешней непривлекательностью.

***Владелец информации: информация государственная, коммерческая и личная. Персональные данные***

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

Персональные данные представляют собой информацию о конкретном человеке. 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.

Биометрические персональные данные представляют собой сведения о наших биологических особенностях. Эти данные уникальны, принадлежат только одному человеку и никогда не повторяются. Биометрические данные заложены в нас от рождения самой природой, они никем не присваиваются, это просто закодированная информация о человеке, которую люди научились считывать. К таким данным относятся: отпечаток пальца, рисунок радужной оболочки глаза, код ДНК, слепок голоса и пр.

Государство защищает право граждан в защите их права в области персональных данных и отдельно осуществляет защиту следующей информации о гражданах: не допускаются сбор, хранение, использование и распространение информации о частной жизни, а равно информации, нарушающей личную тайну, семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений физического лица без его согласия, кроме как на основании судебного решения.

Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством РФ за нарушение режима защиты, обработки и порядка использования этой информации, в частности предусмотрена административная ответственность.

***Авторское право***

Одной из актуальнейших угроз информации личности, организаций и государства является защита интеллектуальной собственности в сети.

Интеллектуальная собственность регулируется Гражданским кодексом РФ, в которых определены основные понятия.

Автором результата интеллектуальной деятельности признается гражданин, творческим трудом которого создан такой результат. Но это право может быть передано автором другому лицу по договору.

Объектами авторских прав являются произведения науки, литературы и искусства независимо от достоинств и назначения произведения, а также от способа его выражения:,

**Не являются объектами авторских прав:** (официальные документы государственных органов и органов местного самоуправления муниципальных образований , государственные символы и знаки, произведения народного творчества (фольклор), не имеющие конкретных авторов;

Срок действия авторского права распространяется в течение всей жизни автора и 70 лет после его смерти, однако право авторства, право на имя и право на защиту репутации автора бессрочны.

Никто без разрешения автора не может воспроизводить его произведение, распространять, публично демонстрировать, продавать, импортировать, пускать в прокат, публично исполнять, показывать/исполнять в эфире или размещать в Интернете.

Обладатели авторских и смежных прав вправе требовать от нарушителя их права не только признания их права, но и в частности возмещение убытков, включая упущенную выгоду, и выплаты компенсации.

Важно, что нарушением авторского права является не только копирование и распространение, но и незаконное использование – чтение, прослушивание и просмотр.

В повседневной жизни при использовании чужой информации при подготовке, например, статьи, доклада или поста в социальной сети должен указываться источник данной информации.

***Достоверность информации***

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

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

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.

***Основы шифрования***

**Криптографические методы защиты информации:**

1. шифрование, стеганография, кодирование, сжатие

В настоящее время используются два основных метода шифрования – симметричное и асимметричное:

1. В симметричном шифровании один и тот же ключ используется и для шифровки, и для расшифровки сообщений.
2. В асимметричных методах применяются два ключа. Один из них, несекретный, используется для шифровки. другой – секретный – применяется для расшифровки и известен только получателю. Асимметричные методы шифрования позволяют реализовать электронную подпись или электронное заверение сообщения.

Шифрование и криптографию можно увидеть и в обычной жизни каждого человека.

Существуют персональные данные, которые представляют собой набор цифр, позволяющие определить конкретного человека. Такими персональными данными являются: номер и серия паспорта, страховой номер индивидуального лицевого счета (СНИЛС), индивидуальный номер налогоплательщика (ИНН), номер банковского счета, номер банковской карты. Для подписания электронных документов также используются инструменты криптографического преобразования - Электронная цифровая подпись (ЭЦП).

ЭЦП может признаваться равнозначной собственноручной подписи лица и использоваться для подтверждения любой информации, передаваемой в электронном виде. Все экземпляры электронного сообщения, подписанного ЭЦП, имеют силу оригинала.

Для получения ЭЦП гражданину или организации необходимо получить сертификат открытого ключа ЭЦП (сертификат ключа подписи) – это документ, выданный и заверенный специальным удостоверяющим центром, подтверждающий принадлежность ключа ЭЦП лицу.

Несовершеннолетние граждане имеют право на использование ЭЦП и получение сертификата ключа подписи.

**Потребительские аспекты информационной безопасности**

В данном подразделе будут рассмотрены аспекты получения и приобретения различных товаров и услуг в сети «Интернет»

*Электронные деньги и банковские карты*

В Интернете можно осуществлять покупки, различные платежи, оплата игр, участие в различных конкурсах и акциях, а также платежи в благотворительные фонды с помощью банковских карт и электронных денег.

При выборе магазина или организации с которой вы хотите заключить денежный оборот обратите внимание на то что должны быть указаны все данные о ней и ее товаре, услуге. Будьте внимательны до последней информации, где могут быть добавлены рекламы – спамы, пользовательские соглашения и т.д. Если вам не знаком данный магазин или организация попробуйте сначала оформить не значительный заказ, чтоб отследить форму работы организации и качество товара.

В Интернете можно также расплачиваться банковскими картами, которые обычно разделяют на:

1. Зарплатные карты. Их открывает банк по указанию предприятия, которое будет осуществлять выплату заработной платы, аванса, премий, отпускных, командировочных, социальных пособий, положенных работнику;
2. Кредитные карты. Они имеют денежные средства, принадлежащие банку и предоставленные в качестве кредита. Эти деньги предоставляются на определенных условиях и на конкретный срок, в том числе в пределах выделенного лимита;
3. Дебитовые карты. Они открываются для использования и расчетов собственными средствами. На них не установлено кредитного лимита, поскольку клиенту доступен баланс в размере внесенных им денег.

Банковские карты содержат следующую информацию на фронтальной стороне:

1. Уникальный номер карты, состоящий из 16 цифр;
2. Имя и фамилию владельца карты;
3. Срок действия карты в формате месяц/год;

На обратной стороне размещены контакты банка, который выдал карту, и в зависимости от вида карты специальные защитные элементы:

1. Магнитная лента черного цвета хранит в зашифрованном виде ключ доступа к счету владельца карты;
2. Посола подписи содержит подпись владельца карты;
3. Защитная голограмма гарантирует подлинность банковской карты;
4. Специальный код безопасности CVC2, который состоит из трех символов.

Многие банковские карты содержат специальный чип, а оплата по ним возможна только введения PIN-кода (пароля). Сейчас особой актуальностью пользуются карты с использованием технологии бесконтактной оплаты, позволяющие оплатить покупку без введения PIN-кода.

Важно помнить, что для различных платежей в Интернете зачастую достаточно знать только номер карты и срок ее действия, чем очень часто и пользуются злоумышленники.

Сервисы электронных денег и банки предоставляют возможность привязки к счету мобильного телефона, что позволяет не только восстановить доступ к счету или карте, а также подтверждать платежи (транзакции) с помощью одноразового пароля. Однако, необходимо в таком случае особенно помнить о безопасности устройства, а в случае его утери необходимости сообщить банку о его потере для блокировки счета.

Электронные деньги - это очень удобный способ платежей, однако существуют мошенники, которые хотят получить эти деньги.

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. Например если вам позвонили и попросили какие – либо данные о карте счет , код ит.д. представляясь сотрудником банка лучше прекратите данный звонок и перезвоните в отделение своего банка и уточните информацию.

Чтобы избежать проблем при использовании карт и электронных денег в сети рекомендуется:

1. Иметь специальную карту или специальный счет электронных денег, на которую можно переводить определенную сумму денег с основной карты или счет только для совершения конкретных транзакций;
2. Использовать одноразовые пароли, которые приходят на номер телефона каждый раз перед оплатой, и в случае их отсутствия платеж не происходит;
3. Не сообщать номер карты другим людям и хранить банковскую карту в надежном месте, в том числе нельзя держать пароли и коды рядом с картой. Никогда нельзя терять из виду карту, когда передаете ее кассиру или официанту и другим лицам;
4. Подключить услугу SMS-уведомлений, чтобы получать сведения о всех совершаемых платежах с карты или счета;
5. Регулярно просматривайте в интернет-банке или аккаунте историю выполненных операций и остаток на карте;
6. Вводить номер карты и срок ее действия только на проверенных сайтах, которые необходимо самостоятельно изучить перед введением данных и соответствующие следующим требованиям:
* Аккредитованные сайты, на которых отображены логотипы VerifiedbyVisa, MasterCardSecureCode и «МИР».
* Подтверждение платежа паролем должно осуществляться на странице банка или сервиса платежей;
* Использующие защищенный протокол https.
1. Использовать специальные программы для интернет-платежей, разработанные производителями антивирусных программ.

**Что делать, если:**

1. Потеряна банковская карта. Сообщить по телефону в банк о произошедшем и попросить ее заблокировать. Банк предложит вместо данной карты выпустить новую карту с новым номером. Пока не будет заблокирована банковская карта, любой, у кого она окажется в руках, сможет воспользоваться ей;
2. Пришло уведомление о платеже, который вы не совершали. Необходимо сообщить в банк или платежный сервис, направив заявление о чарджбеке (отмене операции), в котором максимально подробно описать произошедшее. Банк или платежный сервис рассмотрит обращение и вернет вам деньги в срок от 30 до 60 дней.

Важно помнить, что чем раньше удастся выявить проблему и начать предпринимать меры, то тем больше шансов уменьшить ущерб, который может быть нанесен вам, вашей семье и другим лицам.

*Государственные услуги в интернете*

Получение государственной услуги через Интернет – один из самых простых, удобных и современных способов, поскольку:

1. Электронные государственные услуги экономят время: некоторые предоставляются дистанционно и результат можно получить также дистанционно, а другие в назначенное время без очереди;
2. Возможность проверки статуса заявления;
3. Портал государственных услуг функционирует 24 часа в сутки 7 дней в неделю в праздники или выходные дни, что позволяет подать заявление в любое время.

Государственные услуги предоставляются на сайте gosuslugi.ru

Для получения государственной услуги в сети необходимо в первую очередь зарегистрироваться в ЕСИА – Единой системе идентификации и аутентификации.

ЕСИА представляет собой логин и пароль от всех государственных порталов и сайтов. С его помощью можно подавать электронные заявления, оплачивать счета и штрафы и многое другое.

Зарегистрироваться в ЕСИА могут граждане, достигшие возраста 14 лет и имеющие паспорт. Дети до 14 не могут иметь свою собственную учетную запись.

Для получения ЕСИА необходимо:

1. Заполнить контактные данные на форме регистрации ЕСИА https://esia.gosuslugi.ru/registration.
2. Далее в созданном личном кабинете нужно ввести данные паспорта и номер СНИЛС (он указан на страховом свидетельстве в виде зеленой пластиковой карты);
3. После этого в личный кабинет придет уведомление, что данные документов успешно прошли проверку;
4. Для завершения процесса регистрации нужно подтвердить свою личность. Для этого нужно прийти с паспортом и СНИЛС в любой МФЦ.

Также возможно получить ЕСИА можно сразу в ближайшем отделении МФЦ.

**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.

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

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.

Кратко остановимся на безопасности линий связи, а именно на беспроводной связи, которую мы привычно называем Wi-Fi.

Wi-Fi - это товарный знак альянса производителей техники, поддерживающего беспроводную связь нескольких стандартов

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.

*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.

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/
* Расстояние от глаз пользователя до экрана компьютера должно быть не менее 50 см.
* Стол и стул должны соответствовать росту ребенка.
* Уровень глаз на 15-20 см выше центра экрана.

В ходе занятий с использованием ПК для профилактики переутомления детей 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 физкульт паузы.

**Коммуникативные аспекты информационной безопасности**

В данном подразделе будут рассмотрены различные аспекты коммуникации с другими людьми, а также механизмы и правила общения с ними в сети «Интернет».

*Цифровая репутация*

Старая пословица гласит «Написанное пером, не вырубишь и топором». В Интернете эта пословица получила название «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.

 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.

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 партнёр, 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.

 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.
2. Необходимо следить за формулировками и используемой лексикой, избегать жаргонной и ненормативной лексики и соблюдать правила орфографии и пунктуации.
3. Необходимо правильно выбирать модель поведения, ведь принимаемая в одном месте, она может быть неприемлема в другом.
4. Проверять достоверность фактов и информации перед публикацией.

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 сети «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.

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

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

 Следующим этапом является бан, или внесение в черный список агрессора. В программах обмена мгновенными сообщениями есть возможность блокировки отправки сообщений с определенных адресов.

Пользователь также имеет возможность заблокировать самого хулигана, обратившись с жалобой в адрес администрации сайта.

При наличии угроз жизни и здоровью кибербулинг может перейти в реальную жизнь, вместе с подтверждениями можно обратиться в правоохранительные органы.

*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.

 *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.

 *Интернет-зависимость*

 Фактически интернет-зависимость – это расстройство психики, заключающееся в неспособности человека вовремя выйти из сети, а также в постоянном присутствии желания в нее зайти. Однако с любой проблемой можно справиться, если осознавать в этом необходимость.

**Организация обучения информационной безопасности обучающихся**

Образовательная организация может организовать обучение своих обучающихся информационной безопасности путем:

1. Включения тем информационной безопасности в рамках, действующих в образовательной организации учебных дисциплин;
2. Внедрения в образовательную программу самостоятельной учебной дисциплины или увеличение количества учебных часов на изучение данной проблематики при изучении действующих учебных дисциплин;
3. Организации внеурочной деятельности и дополнительного образования;
4. Организации обучения в рамках программ воспитания и социализации обучающихся.

Непосредственно уроки и занятия по вопросам информационной безопасности возможно организовать в следующих формах, которые могут быть использованы как отдельно, так и совместно: Дискуссии или дебаты, деловые игры, буклеты, листовки, квесты, премии, конкурсы и олимпиады, анкетирование, исследования и опросы, тесты и викторины, демонстрация мультфильмов и (или) видеоурока, 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.

**Организация обучения информационной безопасности родителей**

Для повышения уровня знаний родителей и законных представителей обучающихся (далее родителей),предпринимаются 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 образовательной организации, в частности для демонстрации видеоматериалов по данным вопросам.
2. Организация индивидуальных и групповых консультаций родителей классными руководителями, специалистами психологической службы и администрации образовательной организации для обеспокоенных родителей и находящихся в группе риска.
3. Проведение семинаров, лекций и вебинаров с участием экспертов и сотрудников правоохранительных органов для родителей.
4. Раздача информационных материалов об обеспечении безопасности детей в сети «Интернет», в частности памятки, флаеры и другие материалы.
5. Проведение анкетирования родителей по вопросам организации дома мер по обеспечению защиты детей в информационном пространстве.
6. Размещение на сайте образовательной организации, средствах массовой информации образовательной организации, сообществах в социальной сети и сервисе электронных дневников для родителей информации по обеспечению информационной безопасности детей.

В ходе мероприятий для родителей 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.

*Информационно-методическое сопровождение организации обучения информационной безопасности обучающихся и их родителей (законных представителей)*

В работе образовательным организациям и педагогическим работникам рекомендуется использовать материалы и информацию, разработанную либо рекомендованную органами государственной власти, органами местного самоуправления, их подведомственными организациями и учреждениям, и научными организациями с целью исключения использования в образовательном процессе материалов и информации, содержащую рекламу коммерческих товаров и (или) услуг.

**Организация организационно-административных мероприятий администрациями субъектов Российской Федерации, органами местного самоуправления и образовательными организациями по реализации методических рекомендаций**

Для организации обучения эффективно и успешно образовательные организации реализуют организационно-административные мероприятия по следующим направлениям.

Образовательные организации обеспечивают в кадровом направлении работы:

1. укомплектованность педагогическими, руководящими и иными работниками, обладающими знаниями в сфере обеспечения информационной безопасности детей и организации обучения детей информационной безопасности;
2. осуществление профессионального развития педагогических, руководящих и иных работников по вопросам обеспечения информационной безопасности детей и организации обучения детей информационной безопасности, в частности:
* прохождения обучения по программам дополнительного профессионального образования;
* участия в деятельности общественных организаций, осуществляющих деятельность по данным вопросам;
* участия в мероприятиях очного, очно-заочного заочного по вопросам информационной безопасности детства.

Для обеспечения вышеуказанных процессов в организационно-административные мероприятия входит создание необходимых финансово-экономических условий для организации обучения, в частности закупка необходимых учебников, учебно-методической литературы, материалов и других средств обучения.

**Организационно-административные мероприятия Временной комиссии Совета Федерации по развитию информационного общества**

Для обеспечения педагогических работников образовательных организаций необходимыми материалами и информацией, сформирована сетевая библиотека.

Данное решение было выбрано с целью:

1. предоставления педагогическим работникам возможности самостоятельно выбрать и использовать наиболее подходящие и различные форматы работы;
2. исключить практику рекомендации единообразных решений и методик, не учитывающих специфику работы каждого педагогического работника и образовательных организаций в целом;
3. стимулировать разработку новых практик, методов и методик организации обучения информационной безопасности, позволяющих учесть новые форматы организации обучения и появление новых технических угроз и возможностей;
4. поддержать и распространить в образовательном пространстве уже имеющиеся разработки и опыт организаций и лиц, уже подтвердивших свою эффективность.