Методический материал для разработки занятий по информационной безопасности для обучающихся образовательных организаций Республики

Саха (Якутия) с учетом информационных, потребительских, технических и коммуникативных аспектов информационной безопасности

Методический материал для разработки занятий по информационной безопасности для обучающихся общеобразовательных организаций с учётом информационных, потребительских, технических и коммуникативных аспектов информационной безопасности направлен на организацию преподавания основ информационной безопасности в образовательных организациях Республики Саха (Якутия).

Задачи:

1. Оказание методической поддержки специалистам социально-психологических служб и педагогических работников образовательных организаций Республики Саха (Якутия) 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 специалистов социально-психологических служб и педагогических работников образовательных организаций Республики Саха (Якутия) 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 муниципальным управлениям в сфере образования и образовательным учреждениям республики в организации обучения детей, их родителей (законных представителей) и педагогических работников информационной безопасности.

Методический материал *направлен* 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.
Методический материал *ориентирован* на следующие аудитории (далее -

педагогические работники):
1. Учителя, преподаватели и классные руководители;

Приложение 3

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 материалы *могут быть использованы:*
1. Администрациями учреждений для детей-сирот и детей, оставшихся без

попечения родителей;
2. Организациями дополнительного образования;
3. Профессиональными образовательными организациями;
4. Другими организациями, осуществляющими образовательную

деятельность для несовершеннолетних обучающихся.
Методический материал содержит общие представления о сферах

безопасности в информационном пространстве и мерах, которые реализуются в образовательной среде для обеспечения информационной безопасности обучающихся.

Структура:
1. Раздел «Актуальность информационной безопасности детей» направлен

на ознакомление педагогических работников с основными причинами актуальности информационной безопасности детей, действующим

законодательством и положениями нормативно-правовых актов, затрагивающих данную сферу;

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);

4.В приложении представлен перечень источников, используемых при подготовке методического материала, и перечень рекомендуемых сайтов в сети «Интернет» для использования заинтересованными лицами и организациями.

1. Актуальность информационной безопасности детей

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

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

1. *Издевательство* ровесниками и незнакомцами 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);
4. Прочтение детьми информации, вредящей их *мировоззрению и*

психотическому состоянию.

По данным исследования «Образ жизни российских подростков в сети» у 87% процентов детей возникали различные проблемы в сети «Интернет» только за последний год, однако только 17% рассказали о них своим родителям по следующим причинам:

1. Уверенность детей в незнании родителями решения их проблем;
2. Страх перед родителями;
3. Отсутствие возможности рассказать и поделиться с родителями

своими проблемами.
По этой причине органы государственной власти и местного

самоуправления, образовательные организации должны осуществлять

профилактику и обучение детей навыкам безопасного использования сети «Интернет» и информирование их родителей (законных представителей) о возможных сетевых рисках.

Нормативно-правовые акты:

• *Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и защите информации»* определяет механизм физического ограничения доступа к запрещенной информации в сети «Интернет»;

• *Федеральный закон от 29.12.2010 N 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»* регулирует отношения, связанные с защитой детей от информации, причиняющей вред их здоровью и (или) развитию, в том числе от такой информации, содержащейся в информационной продукции;

• *Федеральный закон No436* определяет перечень запрещенной для детей информации, возрастные категории детей и виды информации, разрешенной для той или иной категории, а также требования к обороту информационной продукции.

• *Согласно ч. 3 ст. 16 Федерального закона No 436-ФЗ* информационная продукция, запрещенная для детей, не допускается к распространению в предназначенных для детей образовательных организациях, 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;

• *Согласно пункту 1 статьи 14 Федерального закона от 24.07.1998 N 124-ФЗ "Об основных гарантиях прав ребенка в Российской Федерации"* органы государственной власти Российской Федерации принимают меры по защите ребенка от информации, пропаганды и агитации, наносящих вред его здоровью, нравственному и духовному развитию, в том числе от национальной, классовой, социальной нетерпимости, от рекламы алкогольной продукции и табачных изделий, от пропаганды социального, расового, национального и религиозного неравенства, от информации порнографического характера, от информации, пропагандирующей нетрадиционные сексуальные отношения, а также от распространения печатной продукции, аудио- и видеопродукции, пропагандирующей насилие и жестокость, наркоманию, токсикоманию, антиобщественное поведение.

Непосредственно обеспечение защиты детей в качестве государственной задачи нашло отражение в разделе *«III. Доступность качественного обучения и воспитания, культурное развитие и информационная безопасность детей». Подраздел «Обеспечение информационной безопасности детства путем реализации единой государственной политики в сфере защиты детей от информации, причиняющей вред их здоровью и развитию»* включал перечень мер, направленных на обеспечение информационной безопасности детства.

• *Письмом Минобрнауки России от 28.04.2014 N ДЛ-115/03 "О направлении методических материалов для обеспечения информационной безопасности детей при использовании ресурсов сети Интернет"* был сформирован перечень информации, не соответствующей задачам образования.

2. Основные аспекты информационной безопасности

В данном разделе будут рассмотрены все аспекты информационной безопасности, включающие теоретический и практический анализ рисков по информационным, потребительским, техническим и коммуникативным аспектам информационной безопасности

2.1. Информационные аспекты информационной безопасности

В данном подразделе будут рассмотрены виды информации и вопросы работы с информацией и ее защиты.

2.1.1. Основы информации

Согласно Федеральному закону от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и защите информации» *информация – это сведения (сообщения, данные) независимо от формы их представления.*

Выделяют следующие категории информации:

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

2. *Информация с ограниченным доступом*;

2.1. 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;

2.2. *Конфиденциальная.* 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.

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

В Российской Федерации 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*. 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, 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. Такие действия преследуются по закону в соответствии со статьями Уголовного кодекса Российской Федерации.

2.1.2. Реклама

Реклама должна быть *добросовестной и достоверной*. Недобросовестная реклама и недостоверная реклама не допускаются.

Недобросовестной признается реклама, которая:

1. *Содержит некорректные сравнения* рекламируемого товара с находящимися в обороте товарами, которые произведены другими изготовителями или реализуются другими продавцами;

2. *Порочит честь, достоинство или деловую репутацию* лица, в том числе конкурента;

3. *Представляет собой рекламу товара, реклама которого запрещена* данным способом, в данное время или в данном месте, если она осуществляется под видом рекламы другого товара, товарный знак или знак обслуживания которого тождествен или сходен до степени смешения с товарным знаком или знаком обслуживания товара, в отношении рекламы которого установлены соответствующие требования и ограничения, а также под видом рекламы изготовителя или продавца такого товара;

4. *Является актом недобросовестной конкуренции* в соответствии с антимонопольным законодательством.

Реклама не должна:

1. Побуждать к совершению противоправных действий;
2. Призывать к насилию и жестокости;
3. Иметь сходство с дорожными знаками или иным образом угрожать

безопасности движения автомобильного, железнодорожного, водного, воздушного транспорта;

4. Формировать негативное отношение к лицам, не пользующимся рекламируемыми товарами, или осуждать таких лиц;

5. Содержать информацию порнографического характера.

В рекламе не допускаются:

1. Использование иностранных слов и выражений, которые могут привести к искажению смысла информации;

2. Указание на то, что объект рекламирования одобряется органами государственной власти или органами местного самоуправления либо их должностными лицами;

3. Демонстрация процессов курения и потребления алкогольной продукции;

4. Использование образов медицинских и фармацевтических работников, за исключением такого использования в рекламе медицинских услуг, средств личной гигиены, в рекламе, потребителями которой являются исключительно медицинские и фармацевтические работники, в рекламе, распространяемой в местах проведения медицинских или фармацевтических выставок, семинаров, конференций и иных подобных мероприятий, в рекламе, размещенной в печатных изданиях, предназначенных для медицинских и фармацевтических работников;

5. Указание на то, что рекламируемый товар произведен с использованием тканей эмбриона человека;

6. Указание на лечебные свойства, то есть положительное влияние на течение болезни, объекта рекламирования, за исключением такого указания в рекламе лекарственных средств, медицинских услуг, в том числе методов

профилактики, диагностики, лечения и медицинской реабилитации, медицинских изделий.

В рекламе не допускается использование бранных слов, непристойных и оскорбительных образов, сравнений и выражений, в том числе в отношении пола, расы, национальности, профессии, социальной категории, возраста, языка человека и гражданина, официальных государственных символов (флагов, гербов, гимнов), религиозных символов, объектов культурного наследия (памятников истории и культуры) народов Российской Федерации, а также объектов культурного наследия, включенных в Список всемирного наследия.

Не допускается реклама, в которой отсутствует часть существенной информации о рекламируемом товаре, об условиях его приобретения или использования, если при этом искажается смысл информации и вводятся в заблуждение потребители рекламы.

Не допускаются использование в радио-, теле-, видео-, аудио- и кинопродукции или в другой продукции и распространение скрытой рекламы, то есть рекламы, которая оказывает не осознаваемое потребителями рекламы воздействие на их сознание, в том числе такое

воздействие путем использования специальных видеовставок (двойной звукозаписи) и иными способами.

Не допускается размещение рекламы в учебниках, учебных пособиях, другой учебной литературе, 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. Создание у несовершеннолетних искаженного представления о доступности товара для семьи с любым уровнем достатка;

4. Создание у несовершеннолетних впечатления о том, что обладание рекламируемым товаром ставит их в предпочтительное положение перед их сверстниками;

5. Формирование комплекса неполноценности у несовершеннолетних, не обладающих рекламируемым товаром;

6. Показ несовершеннолетних в опасных ситуациях, включая ситуации, побуждающие к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью;

7. Преуменьшение уровня необходимых для использования рекламируемого товара навыков у несовершеннолетних той возрастной группы, для которой этот товар предназначен;

8. Формирование у несовершеннолетних комплекса неполноценности, связанного с их внешней непривлекательностью.

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

Из вышеуказанного можно сделать вывод, что информация всегда имеет

владельца.

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

Рассмотрим отдельно такую группу информации как *персональные данные.*

Персональные данные представляют собой информацию о конкретном человеке. Так согласно *Федеральному закону от 27.07.2006 N 152-ФЗ «О персональных данных»* персональные данные являются любой информацией, относящаяся 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.

Так, если мы кому-то скажем, свои фамилию, имя, отчество и адрес места жительства, то нас вполне можно будет опознать как конкретное лицо. Но если мы исключим из этого набора данных фамилию или адрес места жительства, то понять, о каком человеке идет речь, будет невозможно. Получается, что персональные данные - это не просто ваши фамилия или имя, персональные данные - это *набор данных, их совокупность, которая позволяют идентифицировать вас.*

Персональные данные используются и обрабатываются организациями, например, социальными сетями, физическими лицами, например, при заказе услуг, и даже государством, например, при оказании государственных услуг.

Таким образом, персональные данные могут быть использованы как в коммерческих, так и некоммерческих целях.

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.

2.1.4. Авторское право

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

Согласно с*татье 44 Конституции Российской Федерации* каждому гарантируется свобода литературного, художественного, научного, технического и других видов творчества, преподавания.

Автором произведения науки, литературы или искусства признается гражданин, творческим трудом которого оно создано. Лицо, указанное в качестве автора на оригинале или экземпляре произведения либо иным образом считается его автором, если не доказано иное.

Авторские права выступают в качестве гарантии того, что интеллектуальный и (или) творческий труд автора не будет напрасным, и дают ему справедливые возможности заработать на результатах своего труда, а также получить известность и признание.

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.

Таким образом, пользователь должен соблюдать требования в области авторских прав, в частности использовать информацию:

1. Распространяемую бесплатно легально, зачастую при условии обязательного упоминания автора или источника, или на условиях просмотра рекламы, о чем указывается в правилах использования информации на сайте;

2. Распространяемая на основе свободной лицензии, примером которой является всемирная энциклопедия «Википедия».

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

2.1.5. 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».*

Критика информации состоит из определения:
1. *Времени и места* появления информации или создания ее источника; 2. *Автора текста или публикатора*. Необходимо убедиться в

компетентности автора, разбирается ли он в данном вопросе;
3. *Полноты информации*. Отвечает ли текст на ключевые вопросы: Что?

Где? Когда? При каких обстоятельствах? Кто главные действующие лица?

4. *Полнота доказательств*. Какие доказательства использует автор? Видел ли он это сам или пересказывает чьи-то слова?

5. *Надежность 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;

6. *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.

В конце отметим, что 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.

2.1.6. Основы шифрования

Центральное место среди программно-технических средств безопасности занимает *шифрование или криптография.*

Криптографические методы защиты информации:

1. Шифрование;
2. Стеганография;
3. Кодирование;
4. Сжатие.

Процесс шифрования заключается в проведении математических, логических, комбинаторных и других преобразований исходной информации, в результате которых зашифрованная информация представляет собой хаотический набор букв, цифр, других символов и двоичных кодов. Исходными данными для алгоритма шифрования служат информация, подлежащая шифрованию, и ключ шифрования.

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. Основным недостатком симметричного шифрования является то, что секретный ключ должен быть известен и отправителю, и получателю.

2. В *асимметричных методах* применяются два ключа. Один из них, *несекретный*, используется для шифровки и может без всяких опасений передаваться по открытым каналам, другой – *секретный* – применяется для расшифровки и известен только получателю. Асимметричные методы шифрования позволяют реализовать электронную подпись или электронное заверение сообщения.

обратимых

В отличие от других методов криптографического преобразования информации, методы *стеганографии* позволяют скрыть не только смысл хранящейся или передаваемой информации, но и сам факт хранения или передачи закрытой информации.

Содержанием процесса кодирования информации является *замена смысловых конструкций исходной информации* (слов, предложений) кодами. При кодировании и обратном преобразовании используются специальные таблицы или словари.

Сжатие информации может быть отнесено к методам криптографического преобразования информации с определенными оговорками. Целью сжатия является *сокращение объема информации*. В то же время сжатая информация не может быть прочитана или использована без обратного преобразования. Даже если держать в секрете алгоритмы, то они могут быть сравнительно легко раскрыты статистическими методами обработки. Поэтому сжатые файлы конфиденциальной информации подвергаются последующему шифрованию.

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. Такие «кодовые данные» представляют собой некий набор зашифрованной информации о человеке. Шифрование этих данных может производиться государством. Например, когда ребенку исполняется 14 лет, ему выдают паспорт в ФМС. Такой паспорт содержит серию и номер, а также иную информацию.

Для подписания электронных документов также используются *инструменты криптографического преобразования* - Электронная подпись (ЭП).

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

ЭП представляет собой последовательность символов, полученную в результате преобразования исходной информации с использованием закрытого ключа ЭП (последовательность символов, предназначенная для выработки ЭП и известная только владельцу).

2.2. Потребительские аспекты информационной безопасности

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

2.2.1. Электронные деньги и банковские карты

В Интернете можно осуществлять покупки с банковских карт и с помощью электронных денег.

Обычно сервисы электронных денег предлагают клиентам *анонимные и неанонимные аккаунты.* Разница в том, что анонимные - это те, в которых разрешается проводить операции без идентификации пользователя, а в

неанонимных идентификация пользователя является обязательной. Зачастую анонимные аккаунты имеют существенные ограничения в свой работе.

Также следует различать *электронные фиатные деньги*, равные государственным валютам, и электронные нефиатные деньги, которые в свою очередь не равны государственным валютам.

Важно помнить, что для покупок 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.

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

1. Для покупок в Интернете 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;

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:

1. Аккредитованные сайты, на которых отображены логотипы Verified by Visa, MasterCard SecureCode и «МИР».

2. Подтверждение платежа паролем должно осуществляться на странице банка или сервиса платежей;

3. Использующие защищенный протокол https.

7. 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.

2.2.2. Покупки в сети

Сегодня в интернете можно купить буквально все и как в реальной жизни можно столкнуться с различными негативными последствиями.

В основном вся работа с подобными сайтами заключается в следующем: *оформление заказа, оплата заказа и доставка*, которая может осуществляться путем добавления в личный кабинет, например, в игре или доставка на дом товара.

В первую очередь необходимо обратить внимание на устройство, с которого будут осуществляться платежи. Рекомендуется использовать только личное персональное устройство, например, домашний компьютер, смартфон или планшет, имеющий:

1. Включенное антивирусное программное обеспечение;
2. Актуальную версию операционной системы и браузера;

Не рекомендуется оплачивать, проверять баланс счета и проводить другие

финансовые операции на компьютерах с общим доступом и устройствах, подключенных к публичным точкам доступа WiFI.

Сайты и сервисы для защиты своих клиентов при оплате онлайн используют *протокол HTTPS,* который можно увидеть в адресе платежной страницы в браузере, зачастую отмечаемый замком зеленого цвета. Только этот протокол обеспечивает безопасную передачу данных, поэтому рекомендуется оплачивать только на сайтах и сервисах, использующих данный протокол.

При выборе сайта или сервиса, на котором планируется что-либо приобрести, также рекомендуется:

1. *Сравнивать* цены в различных сайтах и сервисах;
2. *Ознакомиться* с отзывами покупателей данного сайта или сервиса;
3. *Избегать* предоплаты;
4. *Уточнить* возможность подать жалобу или/и отменить заказ;
5. *Проверять* реквизиты, название сайта или сервиса и информацию

продавце (как о физическом или юридическом лице);
6. *Проверить* историю сайта или магазина, в частности через поисковые

системы либо по дате регистрации домена.
Если сайт или сервис не соответствует вышеуказанным требованиям, то

лучше исключить возможность покупки на нем.
Особенно рекомендуется обратить внимание и избегать сайты и сервисы:
1. *Продающие технику, на которой отсутствует русификация*. Это

является одним из признаков контрабандного товара либо оборудование уже на заводе не планировалось поставлять в Россию;

2. *Использующие для приема платежей электронные кошельки*, поскольку такие сервисы предоставляют возможность принимать платежи сразу

после регистрации, указав только электронную почту. E-mail нельзя отследить, что сказывается на отсутствие возможности установить личность продавца;

3. *Которые не имеют пунктов самовывоза или своих офисов*.

До покупки необходимо ознакомиться с правилами сайта или сервиса и условиями покупки. Зачастую пользователи не знают о таком праве сайтов как распространять информацию о покупках своих клиентов публично, а многие сервисы предоставляют пробный бесплатный период, по окончании которого включается подписка на платные услуги с автоматическим продлением, от которой сложно отказаться.

Во время покупки или для ее подтверждения администраторы или модераторы сайта или сервиса не могут требовать полные данные счета, пароли и пин-коды для подтверждения платежа. Если кто-то запрашивает подобные данные, то, скорее всего, это мошенники.

После покупки все сайты и сервисы обязаны предоставить пользователю электронный чек, который можно как скачать, так и отправить на адрес электронной почты или смс-сообщением покупателю.

Согласно закону у покупателя имеется возможность отказаться от товара в любое время до его передачи, а после передачи товара – *в течение 7 дней*.

В этой связи *особо важным обстоятельством при покупках в сети является сохранение чеков,* отчетов об оплате и доставке товаров, которые получает покупатель после покупки.

В случае если потребителю был передан товар ненадлежащего качества, т.е. в нем имеются какие-либо недостатки. Потребитель имеет право на предъявление следующих требований:

1. Безвозмездное устранение недостатков;
2. Соразмерное уменьшение покупной цены;
3. Замена на товар аналогичной марки либо на товар другой марки с

соответствующим перерасчетом покупной цены;
4. Отказ от исполнения договора и возврат денежных средств,

уплаченных за товар.

1.2.3. 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. Примеры: http://www.sberbank.ru/ и http://www.sbenbank.ru/ либо www.yandex.ru и www.yadndex.ru.

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 SMS), 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 SMS 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 SMS 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 SMS 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, ЖКХ 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.

Фишинговые сообщения могут содержать:

1. Сведения, вызывающие тревогу, или угрозы, например, закрытие ваших банковских счетов;

2. Обещания большой денежной выгоды с минимальными усилиями или вовсе без них;

3. Сведения о сделках, которые слишком хороши для того, чтобы быть правдой;

4. Запросы о пожертвованиях от лица благотворительных организаций после сообщений в новостях о стихийных бедствиях;

5. Другую информацию.

Отдельным подвидом необходимо рассматривать *мобильное мошенничество,* которое в частности предполагает получение смс-сообщений с незнакомых номеров, которые могут содержать:

1. Ссылки на фишинговые или зараженные ресурсы;
2. Информацию о выигрышах, которых не существует;
3. Ложные просьбы о помощи;
4. О переводе денег на сотовый, прямые просьбы о переводе денег;
5. SMS из несуществующего банка;
6. Просьбы перезвонить на платный номер;
7. Требования выкупа;
8. Просьбы отправить СМС, которые активируют платные услуги;
9. Другую информацию.

Мобильное мошенничество также часто встречается в формах:
1. *Wangiri* («Очень дорогой звонок») – когда человек звонит с

неизвестного номера, но, как только человек берет трубку, звонок внезапно обрывается. Вы перезваниваете на неизвестный номер и попадаете на автоинформатор, задача которого – как можно дольше удержать абонента на линии, пока со счета списываются деньги;

2. *Требования выкупа* – когда кто-то звонит вам с неизвестного номера, но, как только вы берете трубку, звонок внезапно обрывается. Вы перезваниваете на неизвестный номер и попадаете на автоинформатор, задача которого – как можно дольше удержать абонента на линии, пока со счета списываются деньги. Когда вам позвонили или прислали SMS с неизвестного номера с просьбой о помощи близкому человеку: не впадайте в панику, не торопитесь переводить деньги. Перезвоните родным и узнайте, все ли у них в порядке. Уточните, где находятся близкие.

Мобильное мошенничество имеет *примеры смежных технологий*: пользователю может прийти SMS от банка или платежного сервиса с паролем для совершения платежа, а сразу после этого может позвонить человек, который скажет, что ввел этот номер мобильного телефона по ошибке и попросит сообщить код из SMS, которое только что пришло пользователю. На самом деле код из SMS — это пароль не к счету незнакомца, а к счету пользователя, с помощью которого злоумышленник может поменять настройки кошелька или интернет-банка, украсть деньги и т.д.

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 учётной 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 SMS. 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 не сообщать пароли, пин-коды и коды из SMS, 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 SMS, 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 (авто-платежи).

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 её.

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.

2.2.4. Онлайн-игры

В онлайн-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 может быть заражен;

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.

2.2.5. Спам

Согласно *статье 18 Федерального закона от 13.03.2006 N 38-ФЗ «О рекламе»* распространение рекламы допускается только при условии предварительного согласия абонента или адресата на получение рекламы.

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.

Также согласно закону распространитель такой рекламы обязан немедленно прекратить распространение данной рекламы в адрес лица, обратившегося к нему с таким требованием.

Для этого 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.

Для привлечения к ответственности распространителя спама получателю спама *необходимо обратиться с ФАС России*, сообщив о получении спама, указав на отсутствие согласия на получение таких рассылок, и приложив сообщение, его фотографию или скриншот, содержавший рекламу.

2.2.6. Пользовательское соглашение

Отношения пользователей и различных сайтов и сервисов носят *правовой характер* и имеют форму *Пользовательского соглашения.*

Так данное *Пользовательское соглашение является публичной офертой* или договором присоединения.

Перед регистрацией или использованием пользователь должен *подтвердить свое согласие с условиями «Пользовательского соглашения»*, а в случае несогласия с ними *не имеет права пользоваться сайтом*. Именно поэтому регистрация пользователя означает полное и безоговорочное принятие пользователем пользовательского соглашения.

Кроме этого, зачастую администрация сайтов и сервисов оставляет за собой право *изменить Пользовательское соглашение* в одностороннем порядке без какого-либо специального уведомления, публикуя Пользовательское соглашение в открытом доступе, поэтому рекомендуется регулярно проверять условия Пользовательского соглашения на предмет их изменения и/или дополнения.

В Пользовательском соглашении отражены *различные аспекты работы сайтов или сервисов,* которые включают такие вопросы как порядок регистрации и использования, права и ответственность администрации сайта или сервиса, права и ответственность пользователя, перечень возможностей использования и правил их использования пользователем сайта или сервиса и другие аспекты.

Особую актуальность Пользовательское соглашение приобретает в условиях возможности передачи персональных данных пользователей другим организациям и лицам для коммерческих целей и ответственность пользователя за размещение или предоставление доступа к материалам, нарушающим интеллектуальные права.

2.2.7. Государственные услуги в интернете

Когда гражданину исполняется 14 лет, ему предоставляется право получать государственные услуги самостоятельно, например, получение паспорта, запись на прием к врачу, поиск работы или получение результатов экзаменов.

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

В настоящее время получить государственные услуги можно по различным вопросам, в том числе.

Заявление на предоставление услуги в электронной форме подается онлайн с помощью компьютера, планшета или мобильного телефона, а документы при необходимости прикрепляются в виде скана или фотографии. Прежде чем подать заявление, пользователь может ознакомиться со всей нужной информацией о предоставлении услуги и ответственных организациях онлайн.

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. Например, в некоторых регионах России узнать оценки в электронном дневнике родители могут с

помощью ЕСИА, а учетная запись ЕСИА дает возможность пользоваться бесплатным беспроводным интернетом в метро Петербурга и Москвы.

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

После регистрации в этой системе будет открыт полный доступ к государственным сайтам и порталам, а для получения непосредственно государственных услуг необходимо:

1. *Найти и ознакомься с описанием услуги*. Для этого необходимо выбрать в каталоге на главной странице портала интересующую услугу или найти ее с помощью строки поиска, перейдя к странице с ее описанием. После необходимо изучить информацию на странице, в частности сведения о праве на получение услуги, какие документы необходимы для ее получения, и другую важную информацию. Часто услуга предоставляется разным категориям заявителей: физическим лицам, юридическим лицам и индивидуальным предпринимателям.

2. *Нажать на кнопку «Получить услугу*». После получения информации об услуге можно перейти к ее получению. Чтобы заполнить электронное заявление, необходимо нажать на кнопку «Получить услугу».

3. *Заполнить электронное заявление*. Внесение необходимой информации в поля формы электронного заявления. На любом шаге заполнения заявления возможно создать его черновик, нажав кнопку «Сохранить», и вернуться к подаче заявления в удобное время.

4. *Прикрепление необходимых документов*. На этом шаге потребуется прикрепить документы, необходимые для получения услуги. Возможно прикрепить скан или фотографию документа.

5. *Отправить электронное заявление.* После заполнения всех полей формы заявления необходимо нажать на кнопку «Отправить».

6. *Отслеживание хода оказания услуги*. В личном кабинете или по электронной почте можно отслеживать ход оказания услуги.

7. *Получение результата*. По некоторым услугам получить результат услуги можно онлайн. Но иногда для получения готового документа, например, паспорта, требуется личное обращение в орган власти.

2.3. Технические аспекты информационной безопасности

В данном подразделе будут рассмотрены различные аспекты использования и работы цифровых устройств, в частности вредоносное программное обеспечение, работа в сетях и другие вопросы.

2.3.1. Правила использования персональных устройств и программного обеспечения

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

Однако *средств защиты* для подобных устройств пока очень мало. Например, сенсорные экраны плохо работают при низких температурах и требуют дополнительной чистоты рук, а антивирусные программы для смартфонов появились несколько лет назад.

Именно поэтому при использовании смартфонов и планшетов необходимо иметь чехол и соблюдать требования к компьютерам, а также обратить внимание на некоторые меры безопасности своего портативного устройства:

1. *Нельзя загружать приложения* от неизвестного источника, ведь они могут содержать вредоносное программное обеспечение;

2. *Периодически необходимо проверять*, какие платные услуги активированы на номере;

3. *Предоставлять свой номер телефона только людям, которым можно доверять*;

4. *Bluetooth должен быть выключен*, когда им не пользуются, а его отключение необходимо также периодически проверять.

Другая сторона использования персональных устройств - программы, которые мы используем на наших устройствах, в частности *операционные системы.*

При выборе и использовании операционной системы необходимо помнить о необходимости использовать *лицензионную операционную систему*, поскольку нелицензионные операционные системы могут быть заражены вирусами и использованы злоумышленниками, и регулярно обновлять их, поскольку новые пакеты от производителя программного обеспечения закрывают критические уязвимости для своих устройств и другие ошибки технического характера, которые были выявлены в ходе работы.

Зачастую информация о появлении новых обновлений появляется в виде блока уведомления во всех операционных системах, а для обновления

пользователю необходимо только скачать файл обновления и перезагрузить устройство.

Операционные системы имеют *файрвол* (брандмауэр в Windows), который представляет собой межсетевой экран, проверяющий данные, которые обменивает компьютер и подключенная сеть, например, локальная или сеть «Интернет». При выявлении опасных соединений файрвол блокирует данное соединение. Файрвол дополнительно защищает операционную систему от вирусов. Рекомендуется включить файрвол на все виды сетей: доменных, частных и общественных.

Данные правила также распространяются на все программное обеспечение, устанавливаемое и используемое на любых устройствах.

Большинство операционных систем и программ имеют *интуитивно понятный интерфейс,* однако нужно понимать, что изучение правил работы в программе открывает дополнительные возможности и позволяет работать более быстро, эффективно и безопасно.

Актуальными в настоящее время стали приложения, распространяемые на мобильных операционных системах, запрашивающие доступ к таким функциям и информации, которые не соответствуют целям приложения. Например, приложение для обработки фотографий запрашивает доступ к звонкам, смс-

сообщениям и телефонной книге, а программа для чтения электронных книг запрашивает доступ к микрофону и местоположению. Такие права после установки приложения невозможно изменить или обойти, поэтому лучше отказаться от подобного рода приложения.

Для корректной работы и очистки устройства от сетевого мусора рекомендуется использовать программы, позволяющие удалить временные файлы интернета, загруженные файлы программ, автономные веб-страницы, буфер обмена, временные файлы, системные отчеты, эскизы, а также очистить корзину.

В настоящее время все *операционные системы предоставляют возможность использовать учетную запись с ограниченными правами*, которая ограничена полномочиями, что не позволит вирусу внедриться в систему, даже если он проникнет в компьютер.

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.

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.

Большинство браузеров позволяет *отключать куки*, однако, изначально они включены.

Можно *полностью запретить принимать куки* со сторонних сайтов, что рекомендуется осуществлять самостоятельно после посещения сайта, на котором вводилась личная информация.

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 JavaScript 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.

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

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 перехвата данных злоумышленник может разворачивать собственные точки доступа, которые похожи по имени на надежные, и перехватывать чужой сигнал. Данные записываются для последующей дешифровки.

Взлом сетей Wi-Fi, как правило, проводится для подключения к домашней или рабочей сети, чтобы далее появилась возможность удаленного управления компьютерами этой сети и хищения с них информации.

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 её 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*.

Для защиты пользовательских данных был реализован протокол HTTPS – это специальное защищенное соединение, а «s» на конце значит с английского secure «защищенный». HTTPS обеспечивает шифрование данных, создавая фактически специальный канал обмена информацией между пользователем и каким-либо сервисом или сайтом, делая их недоступными для просмотра посторонними.

Перед тем как ввести свою конфиденциальную информацию (пароли, номера кредиток, номер телефона, паспортные данные), *необходимо обратить внимание на адресную строку и убедиться, что имя протокола имеет вид https:// или иногда отображается в браузерах зеленым замком*.

Все браузеры поддерживают одновременно протокол *HTTPS и HTTP.*

Для использования HTTPS организации получают *специальные сертификаты, гарантирующие безопасность ресурса*. До подключения к сайту или сервису браузер пользователя проверяет подлинность сертификата

и, если подлинность сертификата не была подтверждена, выводит соответствующее сообщение и рекомендацию не вводить на данной странице свои личные данные.

2.3.2. Установка и использование пароля

Пароль не должен быть простым, поскольку простой пароль — это наибольшая угроза вашей учетной записи.

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.

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 другие.

Специалисты также отмечают *одноразовые пароли* как один из самых безопасных методов защиты: финансовые сервисы, банки и другие сервисы предоставляют возможность входа в аккаунт с помощью одноразового пароля, который направляется смс-сообщением владельцу аккаунта для подтверждения входа или оплаты.

Объединяют две вышеуказанные технологии *двухэтапная авторизация*, представляющая собой *авторизацию в два этапа:*

1. Введение установленного пользователем пароля;
2. Ввода кода подтверждения, который приходит пользователю в виде

сообщения через мессенджеры, электронную почту или СМС.

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 три или четыре месяца.

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

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, цифра или комбинация цифр, *которые известны и понятны только пользователю*, чтобы их можно было легко запомнить.

2.3.3. **Вредоносное программное обеспечение**

Вредоносное программное обеспечение - это разновидность компьютерных программ, отличительной особенностью которой является способность к

размножению, т.е. данные программы способны создавать свои копии. При этом копии программ-вирусов сохраняют способность дальнейшего распространения.

Вредоносное программное обеспечение предполагает несанкционированное использование, т.е. 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.

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».

В конце данного раздела отметим, что за создание программ для ЭВМ или внесение в существующие программы изменений, заведомо приводящих к

несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами предусмотрена уголовная ответственность согласно *статье 273 Уголовного кодекса Российской Федерации*.

Полномочия по борьбе с распространением вредоносных программ и противодействию мошенническим действиям с использованием информационно- телекоммуникационных сетей, включая сеть Интернет, находятся в сфере деятельности Министерства внутренних дел Российской Федерации.

О создании, распространении и использовании вредоносных программ и других противоправных действиях в сети Интернет можно сообщить в Общественную приемную МВД России на Правоохранительном портале Российской Федерации: **www.112.ru**

2.4. 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».

2.4.1. 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.

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.

2.4.2. 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.

4. *Проверять достоверность фактов* и информации перед публикацией. Недостоверная информация способна вызвать негативную оценку со стороны собеседников.

5. *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.

6. *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.

7. *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 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*.

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 кибербулинг может перейти в реальную жизнь, вместе с подтверждениями *можно обратиться в правоохранительные органы* для защиты пользователя и его близких, действия обидчиков могут попадать под статьи действия Уголовного кодекса и Кодекса об административных правонарушениях Российской Федерации.

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.

2.4.3. 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.

Основные технологии воздействия на общественное сознание через Интернет:

Технология «манипулирования с истинной информацией» является одной из наиболее широко распространенных технологий информационно-психологического воздействия на общественное сознание. Так, организованное блокирование части информации или запрет на выражение точки зрения противоположной стороны при акцентировании политически выгодных тем может вызвать у пользователей реакцию, которая будет неадекватной происходящим в действительности событиям.

Технология влияния контента на деформацию архетипических образов – одна из технологий для воздействия на общественное сознание, посредством которой осуществляется внедрение в общественное сознание элементов нестабильности, дезорганизованности, хаоса, неуверенности и страха. Эта технология состоит в воздействии на стереотипы, установки, сложившиеся у населения конкретной страны, в вытеснении из общественного сознания доминирующей национальной идеи, объединяющего морального начала и рассчитана на реализацию в долгосрочном, стратегическом плане.

«Эффект CNN» – одна из технологий для воздействия на общественное сознание через СМИ, заключается в демонстрации потрясающих психику аудитории актуальных событий в реальном масштабе времени. Благодаря эффекту «присутствия» пользователя в гуще событий (например, при бомбардировках городов) достигается эмоциональное усиление оказываемого на аудиторию психологического воздействия, которое закрепляется нацеленным комментарием.

В политических процессах активно используются *манипулятивные технологии*. Все политические технологии манипулирования поведением человека действуют в ограниченном временном и функциональном диапазоне. Степень их эффективности определяется духовной зрелостью людей, их готовностью обманываться. Глубинной основой политических манипулятивных технологий является конструирование мифов, обращение не к разуму человека, а к глубинам подсознания. Люди позволяют собой манипулировать, сбрасывая ответственность за свои поступки на так называемых манипуляторов. Метод политических мифов – направлен на изменение основы ориентации человека, в качестве которой служит складывающаяся в мозгу определенная картина мира, с которой сравниваются явления, наблюдаемые в окружающей среде. Изменение картины мира может происходить внедрением в сознание политических мифов, позволяющих заменить целостное мировоззрение фрагментарным, изменить

объективную картину мира, приводя к неадекватному искаженному пониманию реальности, своего рода психическим сдвигам.

Примеры технологий воздействия, которые могут влиять на ценностные установки пользователей Интернета:

1. *Анонимный авторитет* – излюбленный прием введения в заблуждение, активно используемый в различных группах. Одним из самых эффективных методов влияния является обращение к авторитету, который может быть религиозным или политическим деятелем, ученым или представителем другой профессии.

2. «*Будничный рассказ»* – «будничное» или «обыденное» изложение информации используется, например, для адаптации человека к информации явно негативного, вызывающего отрицание, содержания. Предполагается, что пользователь, многократно сталкиваясь с информацией такого рода, перестает реагировать на самые чудовищные преступления и массовые убийства, происходящие в обществе. Наступает психологический эффект привыкания.

3. *«Забалтывание*» – метод используется, когда необходимо снизить актуальность или вызвать негативную реакцию к какому-либо явлению. Метод «забалтывания» нередко применяется для создания «информационного шума», когда нужно скрыть какое-то важное событие или главную проблему, в его основе лежит эффект размытия внимания, за счет большого объема текста с малой информационной нагрузкой.

4. *Эмоциональный резонанс* – данную технику определяют как способ создания у пользователей определенного настроения с одновременной передачей пропагандистской информации. Эмоциональный резонанс

позволяет снять психологическую защиту, которую на мыслительном уровне выстраивает человек, сознательно пытаясь оградиться от пропагандистского или рекламного «промывания мозгов».

5. *Эффект бумеранга* – организация тотальной травли своего оппонента, она приводит к тому, что в итоге он начинает вызывать жалость и симпатию у широкой аудитории.

6. *Эффект ореола* – базируется на коварном психологическом свойстве – человеческой склонности мыслить «ложными аналогиями» и состоит из двух распространенных стереотипов–заблуждений: 1. «*Рядом – значит вместе».* Вследствие этого феномена нахождение рядом со знаменитым или высокопоставленным человеком несколько повышает статус в глазах окружающих. 2. *Второй стереотип* – человека, добившегося весомых успехов в какой-то конкретной области, окружающие считают способным на большее и в других делах.

7. *Эффект первичности* – в современной пропаганде существует принцип: человек, сказавший миру первое слово, всегда прав. Здесь срабатывает один из эффектов восприятия: мы склонны отдавать предпочтение той информации, что поступила первой. Изменить уже сформировавшееся мнение очень трудно.

8. *Информационная блокада* – замалчивание или заведомо искаженное описание происходящего.

2.4.4. Инструменты коммуникации: электронная почта, социальные сети и мессенджеры

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, т.к. 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.

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 фото сообщениями, 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.

2.4.5. Интернет-зависимость

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 к:

1. Снижению концентрации внимания;
2. Ухудшению памяти;

3. Мыслительным и психическим расстройствам;
4. Обострению физических заболеваний;
5. 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:
1. Следует потратить все деньги на покупку новых игр, на увеличение

мощности компьютера и улучшение или приобретение подобных функций;
2. 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.

3. Организация обучения детей и родителей (законных представителей)

Образовательные организации с учетом раздела No1 «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 их родителями и законными представителями обучающихся для повышения их уровня знаний в данной сфере.

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

3.1. Организация обучения информационной безопасности обучающихся

Образовательная организация может организовать обучение своих обучающихся информационной безопасности путем:

1. Обращения внимания вопросам обеспечения 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 учебных предметов в рамках вариантовой 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.

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

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.*

Образовательные организации организуют в рамках своей компетенции и проводят классные часы, внеклассные мероприятия и другие различные

тематические мероприятия, в частности Единый урок по безопасности в сети «Интернет», квест по цифровой грамотности «Сетевичок» и другие.

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

С учетом раздела No1 «Актуальность информационной безопасности детей» данных методических рекомендаций обучение детей по ступеням обучения имеют следующие *цели:*

1. *Для обучающихся начальной школы* рекомендуется рассмотреть основные аспекты осуществления деятельности в сети «Интернет» и мерах собственной защиты, в частности с учетом отсутствия у многих детей в данном возрасте собственной электронной почты.

2. *Для обучающихся средней школы* вопросы информационной безопасности могут быть расширены за счет изучения психологических и технических аспектов информационной безопасности, вопросов законодательства и ответственности, правил и условий получения, изготовления и распространения информации и других аспектов, позволяющих обучающимся не только знать меры защиты, но и знание источников и принципов работы сетевых рисков.

3. *Для обучающихся старшей школы* вопросы информационной безопасности должны быть изучены в той мере, которая позволит самому обучающему стать источником достоверной информации по вопросам информационной безопасности для своих ровесников и младших.

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.

Самостоятельным направлением работы является *воспитание у детей культуры информационной безопасности при работе в сети Интернет вне образовательной организации:*

1. Вовлечение обучающихся в деятельность детских общественных организаций, реализующих свою деятельность дистанционно, например, детская общественная организация «Страна молодых», Российское движение школьников и другие.

2. Организация и проведение дистанционных мероприятий, посвященных информационной безопасности, например, Всероссийская контрольная работа по информационной безопасности, квест «Сетевичок» и другие, для повышения уровня знаний обучающихся в сфере информационной безопасности и повышения общего уровня ИКТ-компетентности.

3.2. Организация обучения информационной безопасности родителей и законных представителей обучающихся

Образовательная организация 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 образовательной организации, 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 образовательной организации для обеспокоенных родителей и законных представителей обучающихся и 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 образовательной организации*, средствах массовой информации образовательной организации, 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)

Образовательным организациям 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 и учитывать курс для начального, общего и полного среднего образования межпредметной области «Основы кибербезопасности».*

В своей деятельности образовательные и научные организации, педагогические работники, органы власти, органы местного самоуправления и другие заинтересованные организации и лица могут использовать материалы данных методических рекомендаций и методических рекомендаций о размещении на информационных стендах, официальных интернет-сайтах и других информационных ресурсах общеобразовательных организаций и органов, осуществляющих управление в сфере образования, информации о безопасном поведении и использовании сети «Интернет», а также другую информацию из официальных документов и публикуемой на официальных сайтах государственных органов и органов местного самоуправления муниципальных образований.

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.

4. Источники и рекомендуемые сайты в сети «Интернет»

При подготовке методических рекомендаций были использованы следующие источники:

1. http://www.apkpro.ru;
2. https://yandex.ru;
3. http://сетевичок.рф;

4. http://window.edu.ru;
5. https://gu.spb.ru;
6. http://Единыйурок.рф;
7. https://sledcom.ru.

Рекомендуемые сайты в сети «Интернет» для использования в процессе обучения основам информационной безопасности:

1. http://www.apkpro.ru;
2. https://yandex.ru;
3. http://сетевичок.рф;
4. http://window.edu.ru;
5. https://gu.spb.ru;
6. http://Единыйурок.рф;
7. https://sledcom.ru;
8. http://fond-detyam.ru;
9. http://www.ya-roditel.ru;
10. https://edu.gov.ru;
11. https://игра-интернет.рф;
12. https://fcprc.ru;
13. http://www.персональныеданные.дети;
14. https://мвд.рф;
15. http://rospotrebnadzor.ru;
16. http://Единыйурок.дети.