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

Информационные аспекты информационной безопасности

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

Основы информации

Согласно Федеральному закону от 27.07.2006 N 149-ФЗ"Об информации, информационных технологиях и о 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:

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. 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 (подробная информация представлена в разделе «Актуальность информационной безопасности детей» данных методических рекомендаций).

Распространение данной информации преследуется по закону. В Российском законодательстве есть возможность в соответствии со статьями Кодекса об административных правонарушениях Российской Федерации и Уголовного кодекса

Российской Федерации привлечь к административной и уголовной ответственности за распространение данной информации как владельцев сайтов, на которых размещается данная информация, так и ее авторов, и распространителей.

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.

Изготовление и распространение подобной информации не попадает под действие Кодекса об административных правонарушениях Российской Федерации и Уголовного кодекса Российской Федерации, однако может повлечь санкции со стороны владельцев сайта, на которых пользователь размещает такую информацию, или со стороны организаций, имеющих возможность ограничить доступ к сайту, содержащего такую информацию.

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.

Реклама

Особый вид информации – это реклама.

Согласно федеральному закону «О рекламе» реклама – это информация, распространенная любым способом, в любой форме и с использованием любых средств, адресованная неопределенному кругу лиц и направленная на привлечение внимания к объекту рекламирования, формирование или поддержание интереса к нему и его продвижение на рынке.

Потребители рекламы – это лица, на привлечение внимания которых к объекту рекламирования направлена 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.

Недостоверной признается реклама, которая содержит не соответствующие действительности сведения:

1. о преимуществах рекламируемого товара перед находящимися в обороте товарами, которые произведены другими изготовителями или реализуются другими продавцами;
2. о любых характеристиках товара, в том числе о его природе, составе, способе и дате изготовления, назначении, потребительских свойствах, об условиях применения товара, о месте его происхождения, наличии сертификата соответствия или декларации о соответствии, знаков соответствия и знаков обращения на рынке, сроках службы, сроках годности товара;
3. об ассортименте и о комплектации товаров, а также о возможности их приобретения в определенном месте или в течение определенного срока;
4. о стоимости или цене товара, порядке его оплаты, размере скидок, тарифов и других условиях приобретения товара;
5. об условиях доставки, обмена, ремонта и обслуживания товара;
6. о гарантийных обязательствах изготовителя или продавца товара;
7. об исключительных правах на результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации юридического лица, средства индивидуализации товара;
8. о правах на использование официальных государственных символов (флагов, гербов, гимнов) и символов международных организаций;
9. об официальном или общественном признании, о получении медалей, призов, дипломов или иных наград;
10. о рекомендациях физических или юридических лиц относительно объекта рекламирования либо о его одобрении физическими или юридическими лицами;
11. о результатах исследований и испытаний;
12. о предоставлении дополнительных прав или преимуществ приобретателю рекламируемого товара;
13. о фактическом размере спроса на рекламируемый или иной товар;
14. об объеме производства или продажи рекламируемого или иного товара;
15. о правилах и сроках проведения конкурса, игры или иного подобного мероприятия, в том числе о сроках окончания приема заявок на участие в нем, количестве призов или выигрышей по его результатам, сроках, месте и порядке их получения, а также об источнике информации о таком мероприятии;
16. о правилах и сроках проведения основанных на риске игр, пари, в том числе о количестве призов или выигрышей по результатам проведения основанных на риске игр, пари, сроках, месте и порядке получения призов или выигрышей

по результатам проведения основанных на риске игр, пари, об их организаторе, а также об источнике информации об основанных на риске играх, пари;

17. об источнике информации, подлежащей раскрытию в соответствии с федеральными законами;
18. о месте, в котором до заключения договора об оказании услуг заинтересованные лица могут ознакомиться с информацией, которая должна быть предоставлена таким лицам в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации;
19. о лице, обязавшемся по ценной бумаге;
20. об изготовителе или о продавце рекламируемого товара.

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.

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):

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

2. Перечень сведений, определяющих коммерческую тайну, формируют организации самостоятельно. Он же обеспечивает их сохранность и защиту.
3. Перечень своих персональных данных и личных (персональных) тайн определяет физическое лицо. Гражданин самостоятельно сохраняет и защищает эти данные.

Рассмотрим отдельно такую группу информации как персональные данные.

Персональные данные представляют собой информацию о конкретном человеке. 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.

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

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

Таким образом, специальные данные характеризуют наши взгляды, убеждения, мировоззрение, они определяют нашу социальную принадлежность к определенным группам. Например, человек может сказать: я демократ или я христианин.

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

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

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.

Именно по этой причине перед получением персональных данных лица или организации (законодательством они объединены названием «Операторы персональных данных»), которые хотят получить персональные данные, публикуют политику об обработке персональных данных, в которой отмечена цель их обработки, как они могут быть использованы, как соответственно удалены и другая информация.

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

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

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.

Авторское право

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

Термин "Интеллектуальная собственность" относится к различным творениям человеческого ума, начиная с новых изобретений и знаков, обозначающих собственность на продукты и услуги, и заканчивая книгами, фотографиями, кинофильмами и музыкальными произведениями.

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

Интеллектуальная собственность и отношения в данной области регулируются Гражданским кодексом Российской Федерации, в которых определены основные понятия.

Автором результата интеллектуальной деятельности признается гражданин, творческим трудом которого создан такой результат. Право авторства, право на имя и иные личные неимущественные права автора неотчуждаемы и непередаваемы. Отказ от этих прав ничтожен.

Исключительное право на результат интеллектуальной деятельности, созданный творческим трудом, первоначально возникает у его автора. Это право может быть передано автором другому лицу по договору, а также может перейти к другим лицам.

Гражданин или юридическое лицо, обладающие исключительным правом на результат интеллектуальной деятельности или на средство индивидуализации (правообладатель), вправе использовать такой результат или такое средство по своему усмотрению любым не противоречащим закону способом.

Другие лица не могут использовать соответствующие результат интеллектуальной деятельности или средство индивидуализации без согласия правообладателя.

Каждый из правообладателей вправе самостоятельно принимать меры по защите своих прав на результат интеллектуальной деятельности или на средство индивидуализации.

Интеллектуальные права на произведения науки, литературы и искусства являются авторскими правами. Автору произведения принадлежат следующие права:

1. исключительное право на произведение;
2. право авторства;
3. право автора на имя;
4. право на неприкосновенность произведения;
5. право на обнародование произведения.

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.

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

1. литературные произведения;
2. драматические и музыкально-драматические произведения, сценарные произведения;
3. хореографические произведения и пантомимы;

4. музыкальные произведения с текстом или без текста;
5. аудиовизуальные произведения;
6. произведения живописи, скульптуры, графики, дизайна, графические рассказы, комиксы и другие произведения изобразительного искусства;
7. произведения декоративно-прикладного и сценографического искусства;
8. произведения архитектуры, градостроительства и садово-паркового искусства, в том числе в виде проектов, чертежей, изображений и макетов;
9. фотографические произведения и произведения, полученные способами, аналогичными фотографии;
10. географические и другие карты, планы, эскизы и пластические произведения, относящиеся к географии и к другим наукам;
11. другие произведения.

К объектам авторских прав также относятся программы для ЭВМ, которые охраняются как литературные произведения.

К объектам авторских прав относятся:

1. производные произведения, то есть произведения, представляющие собой переработку другого произведения;
2. составные произведения, то есть произведения, представляющие собой по подбору или расположению материалов результат творческого труда.

Авторские права распространяются как на обнародованные, так и на необнародованные произведения, выраженные в какой-либо объективной форме, в том числе в письменной, устной форме (в виде публичного произнесения, публичного исполнения и иной подобной форме), в форме изображения, в форме звуко- или видеозаписи, в объемно-пространственной форме.

Для возникновения, осуществления и защиты авторских прав не требуется регистрация произведения или соблюдение каких-либо иных формальностей.

Авторские права не распространяются на идеи, концепции, принципы, методы, процессы, системы, способы, решения технических, организационных или иных задач, открытия, факты, языки программирования, геологическую информацию о недрах.

Не являются объектами авторских прав:

1. официальные документы государственных органов и органов местного самоуправления муниципальных образований, в том числе законы, другие нормативные акты, судебные решения, иные материалы законодательного, административного и судебного характера, официальные документы международных организаций, а также их официальные переводы;
2. государственные символы и знаки (флаги, гербы, ордена, денежные знаки и тому подобное), а также символы и знаки муниципальных образований;

3. произведения народного творчества (фольклор), не имеющие конкретных авторов;
4. сообщения о событиях и фактах, имеющие исключительно информационный характер (сообщения о новостях дня, программы телепередач, расписания движения транспортных средств и тому подобное).

События и факты, содержащиеся в информационных сообщениях, не получают охраны по авторскому праву в силу того, что являются содержательной частью сообщения, тогда как авторское право охраняет форму произведения, а не его содержание.

Что касается самих сообщений, то они не охраняются авторским правом постольку, поскольку неоригинальны, представляют собой простое, механическое, нетворческое переложение событий и фактов, однако в случае, если форма выражения информационных сообщений является оригинальной, они являются объектом авторского права.

Срок действия авторского права распространяется в течение всей жизни автора и 70 лет после его смерти, однако право авторства, право на имя и право на защиту репутации автора бессрочны. Примером может стать произведение «Война и мир», которое перешло в статус общественного достояния после 70-летия с момента смерти Л.Н. Толстого.

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.

Обладатель авторских прав для оповещения о своих правах вправе использовать знак охраны авторского права, который помещается на каждом экземпляре произведения и состоит из трех элементов:

1. латинской буквы «С» в окружности: © (знак копирайта);
2. имени (наименования) обладателя авторских прав;

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

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

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

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.

Достоверность информации

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

Специалисты определяют данный процесс термином «Верификация информации».

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

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

Критика информации состоит из определения:

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.

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 обратимых 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.

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.

В целом шифрование возникло со времени появления письменности, когда возникла и получила свое дальнейшее развитие потребность в обеспечении стойкости отдельных сообщений, передаваемых почтовыми отправлениями. Первые шифротексты носили некоторый коммерческий характер. В дальнейшем стали шифроваться тексты медицинского характера, купли-продажи скота и недвижимости.

Активное проведение военных действий явилось мощным стимулирующим воздействием на разработку методов шифрования при передаче секретных сообщений. Так, в 56 году до н.э. во времена войны с галлами римский диктатор К. Цезарь при подчинении Риму заальпийской Галлии использовал в системе передачи секретных сообщений шифр замены. Идея шифра замены используется и в современных методах шифрования, так как является частным случаем отображения множества символов

исходного текста на множестве символов зашифрованного текста. Шифрование, применявшееся К. Цезарем, осуществлялось следующим образом. Под символами греческого алфавита приписывался тот же алфавит, но сдвинутый по циклу на "n" позиций (в частности, К. Цезарь в письменности, которая дошла до наших времен, осуществлял сдвиг на три позиции). При шифровании исходного текста буквы открытого текста из верхней строки записи заменялись на буквы нижнего алфавита. В этом случае, ключом шифрования и дешифрования является число сдвигов нижней строки алфавита по отношению к верхней.

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

Существуют персональные данные, которые представляют собой набор цифр, позволяющие определить конкретного человека. Такими персональными данными являются: номер и серия паспорта, страховой номер индивидуального лицевого счета (СНИЛС), индивидуальный номер налогоплательщика (ИНН), номер банковского счета, номер банковской карты. 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 цифровая подпись (ЭЦП).

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

ЭЦП может использоваться физическими и юридическими лицами, органами государственной власти и органами местного самоуправления.

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

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

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

Потребительские аспекты информационной безопасности

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

Электронные деньги и банковские карты

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

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

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.

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

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

Банковские карты содержат следующую информацию на фронтальной стороне:

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

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

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

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

Важно помнить, что для 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.

Покупки в сети

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

Сайты предлагают различные товары и различные услуги, которые предоставляются как в реальной жизни, так и виртуально, например, можно купить смартфон или игровую валюту.

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.

Закон Российской Федерации от 07.02.1992 № 2300-1 «О защите прав потребителей» устанавливает ряд обязательных требований к продавцам в интернете. При продаже товара дистанционным способом продавцом должна быть до продажи покупателю предоставлена следующая информация:

1. об основных потребительских свойствах товара. Данная информация должна позволить потребителю определить, какой именно товар ему необходим;
2. цену в рублях и условия приобретения товаров (работ, услуг), в том числе при оплате товаров (работ, услуг) через определенное время после их передачи (выполнения, оказания) потребителю, полную сумму, подлежащую выплате потребителем, и график погашения этой суммы;
3. каков его состав, последствия его применения (употребления) и т.п. В случае если потребителю оказалось недостаточно представленной информации, то он вправе обратиться к продавцу с просьбой представить ему дополнительные сведения;
4. об адресе (месте нахождения) продавца, при этом должен быть указан как адрес фактического места нахождения продавца, так и его юридический адрес, номер телефона, факс, электронный адрес. Наличие такой информации позволит потребителю в дальнейшем в случае необходимости быстро связаться с продавцом;
5. о месте изготовления товара. Место изготовления товара – это не только страна-изготовитель, но также город, адрес (место нахождения) изготовителя. Такая информация должна быть доведена до потребителя доступным ему

способом, например, закодированная информация в виде штрих-кода не может рассматриваться как факт представления информации о месте изготовления потребителю;

6. о полном фирменном наименовании продавца (изготовителя). Такая информация фактически дополняет информацию о месте нахождения продавца (изготовителя) и также имеет своей целью обеспечить потребителю более быстрое обращение к продавцу (изготовителю) в случае возникновения такой необходимости;
7. о условиях приобретения товара. Данная информация является одной из важнейших составляющих, однако продавцы нередко в целях привлечения большего числа покупателей указывают стоимость товара без учета налогов или без учета почтовой доставки. Сведения об этом приводятся, как правило, мелким шрифтом либо в менее заметных местах рекламного проспекта, каталога. Нередки случаи, когда на товар из каталога предоставляются значительные скидки, однако при этом где-нибудь в незаметном месте указывается, что рекламная кампания действует в течение ограниченного срока;
8. о его доставке. Данный пункт может иметь важное значение, если продавец находится не в месте нахождения потребителя. В этом случае следует тщательно проверить условия доставки товара, входит ли условие о доставке товара в общую стоимость заказа или потребителю придется оплачивать доставку отдельно. При этом может также играть роль удаленность населенного пункта, в котором находится покупатель, от места нахождения продавца. В ряде случаев доставка товара является дополнительной услугой, и покупатель должен дополнительно сообщить о необходимости доставки продавцу. Если потребитель не сделает этого своевременно, то рискует взамен товара получить сообщение, что принадлежащий теперь покупателю товар он может получить в определенном (не всегда удобном для него) месте;
9. о сроке службы, сроке годности и гарантийном сроке. Сведения, перечисленные в данном пункте, должны быть представлены потребителю до заключения договора купли-продажи. Таким образом, до приобретения товара потребитель должен узнать из информации, полученной от продавца, установлен ли на выбранный товар срок службы, срок годности или гарантийный срок, какова его продолжительность, где находятся сервисные центры;
10. о порядке оплаты товара. Продавцом должна быть определена прежде всего форма оплаты: денежный перевод, наличные денежные средства в кассу и т.д. При этом продавец вправе самостоятельно выбрать наиболее приемлемую для него форму оплаты товара или предоставить ее выбор на усмотрение потребителя. Кроме того, должно быть определено, необходима ли предоплата или можно оплатить товар по факту его получения. Если речь идет о предоплате, то продавец вправе предусмотреть как полную, так и частичную предоплату. Подробная информация об этом также должна быть предоставлена покупателю;
11. о сроке, в течение которого действует предложение о заключении договора. Если продавец не представил покупателю информацию о сроке действия его предложения, то считается, что оно действует неопределенный срок, при этом именно на тех условиях, которые стали покупателю известны из рекламного проспекта, каталога и т.п.

Вся вышеизложенная информация должна быть также предоставлена покупателю в момент доставки товара в письменной форме, а также предоставлены в письменной форме сведения о порядке и сроках возврата товара.

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. В чеке обязательно публикуется следующая информация:

1. наименование документа;
2. порядковый номер за смену;
3. дата, время и место (адрес) осуществления расчета, а также адрес сайта;

4. наименование продавца: наименование организация или фамилия, имя, отчество (при наличии) индивидуального предпринимателя;
5. идентификационный номер налогоплательщика продавца;
6. применяемая при расчете система налогообложения продавца;
7. наименование товаров, работ, услуг, цена за единицу с учетом скидок и наценок;
8. форма расчета (в безналичном порядке) и сумма оплаты в безналичном порядке;
9. адрес сайта уполномоченного органа в сети "Интернет", на котором может быть осуществлена проверка покупки;
10. абонентский номер либо адрес электронной почты покупателя;
11. адрес электронной почты отправителя кассового чека;
12. QR-код.

Согласно закону у покупателя имеется возможность отказаться от товара в любое время до его передачи, а после передачи товара – в течение 7 дней. В случае если продавцом в момент доставки товара не была предоставлена информация в письменной форме о порядке и сроках возврата товара надлежащего качества, то потребитель имеет право отказаться от товара в течение трех месяцев с момента передачи товара.

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 зависимости от наличия недостатков в приобретенном товаре можно выделить две возможных ситуации, в которых процесс возврата товара будет отличаться:

1. возврат товара, в котором нет недостатков, т.е. товара надлежащего качества;
2. в товаре обнаружены недостатки, т.е. передан товар ненадлежащего качества.

Потребитель вправе отказаться от товара, в котором не было обнаружено недостатков, в течение 7 дней с момента получения товара. При этом причины возврата законом не устанавливаются, то есть они могут быть любыми. Важно запомнить, что возврат товара надлежащего качества возможен в случаях, если сохранены его товарный вид, потребительские свойства и документ, подтверждающий факт и условия покупки товара у продавца. В случае если по каким-либо причинам документ, подтверждающий факт покупки товара, у потребителя отсутствует, это не лишает его возможности ссылаться на другие доказательства приобретения товара (свидетельские показания, распечатки с интернет-сайтов и др.).

Также необходимо помнить, что не все товары можно вернуть как товар надлежащего качества – нельзя отказаться от товара, имеющего индивидуально-определенные свойства. Это означает, что данный товар был сделан индивидуально для потребителя, и только он может его использовать. Например, изготовление обуви по меркам, которые предоставлены индивидуально, конкретным потребителем. Продавец возвращает покупателю денежную сумму, уплаченную за товар, за исключением расходов продавца на доставку от покупателя возвращенного товара. Возврат денежных средств осуществляется в течение 10 дней с момента предъявления такого требования.

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.

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. и 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. и 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.

Онлайн-игры

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

Игры разделяют на следующие категории:

1. Платные – доступ к самой игре осуществляется после оплаты единожды либо согласно лимиту (день, неделя, месяц и т.д), а сама игра не содержит платных дополнительных услуг и предложений;
2. Бесплатные – доступ к игре предоставляется бесплатно, а сама игра не содержит платных дополнительных услуг и предложений;
3. Условно-бесплатные: доступ к игре предоставляется бесплатно, однако игра содержит платные дополнительные услуги и предложения (например, улучшить ваш персонаж или получить какие-либо игровые привилегии) за счет внесения реальных денег.

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

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

Основные советы по безопасности своего игрового аккаунта:

1. Если другой игрок создает неприятности, оскорбляет и нарушает своим поведением правила игры, заблокируй его в списке игроков и сообщи в администрацию о поведении данного игрока, в том числе со скринами. Такое действие позволяет администрации игр находить подобных игроков и исключить их из игры, что обычно предусмотрено правилами каждой игры для развития самой игры – ведь никто не будет играть в игру, когда в ней имеются такие игроки;
2. Не рекомендуется указывать личную информацию о себе в аккаунте и распространять ее среди других игроков, поскольку она может привести к различным негативным последствиям в реальной жизни;
3. Необходимо соблюдать правила игры и уважать других игроков, в частности создавать неприятности и оскорблять их;
4. Во время игры не стоит отключать антивирус, поскольку во время игры компьютер, смартфон или планшет 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.

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. При этом администрация сервиса сможет отследить отправителя спама и заблокировать распространение данной информации или отправителя для других пользователей.

В соответствии с ч. ч. 1 и 7 ст. 38 Закона N 38-ФЗ "О рекламе" рассылка физическими и юридическими влечет административный штраф.

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.

Однако каждый пользователь Интернет-сети обязан соблюдать определенные правила безопасности. Пункт 28 Правил оказания телематических услуг связи, утвержденных постановлением Правительства Российской Федерации от 10 сентября 2007 г. № 575, обязывает абонента (пользователя сети): …б) использовать для получения телематических услуг связи пользовательское (оконечное) оборудование и программное обеспечение, которое соответствует установленным требованиям; 33 …д) предпринимать меры по защите абонентского терминала от воздействия вредоносного программного обеспечения; е) препятствовать распространению спама и вредоносного программного обеспечения с его абонентского терминала.

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:

1. Реклама и иные предложения, адресованные неопределенному кругу лиц, рассматриваются как приглашение делать оферты. Содержащее все существенные условия договора предложение, из которого усматривается воля лица, делающего предложение, заключить договор на указанных в предложении условиях с любым, кто отзовется, признается офертой (публичная оферта).
2. Договором присоединения признается договор, условия которого определены одной из сторон в формулярах или иных стандартных формах и могли быть приняты другой стороной не иначе как путем присоединения к предложенному договору в целом. Присоединившаяся к договору сторона вправе потребовать расторжения или изменения договора, если договор присоединения хотя и не противоречит закону и иным правовым актам, но лишает эту сторону прав, обычно предоставляемых по договорам такого вида, исключает или ограничивает ответственность другой стороны за нарушение обязательств либо содержит другие явно обременительные для присоединившейся стороны условия, которые она, исходя из своих разумно понимаемых интересов, не приняла бы при наличии у нее возможности участвовать в определении условий договора.

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.

При этом продолжение использования сайтом или сервисов пользователем после внесения изменений и/или дополнений в Пользовательское соглашение означает принятие и согласие пользователя с такими изменениями и/или дополнениями.

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.

Государственные услуги в интернете

Государственные услуги – это услуги, которые нам оказывают органы власти и государственные организации для решения различных жизненных задач. Например, первой государственной услугой в жизни каждого гражданина является получение свидетельства о рождении.

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.

Получить государственные услуги можно тремя способами: через Интернет, через многофункциональные центры (МФЦ) и в традиционном порядке, посетив государственное учреждение.

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:

1. Получение паспорта гражданина РФ и заграничного паспорта;
2. Получение страхового свидетельства обязательного пенсионного страхования (СНИЛС);
3. Запись на прием к врачу;
4. Результаты государственной итоговой аттестации (ГИА);
5. Результаты вступительных испытаний и о зачислении в образовательные учреждения;
6. Получить направление на временное трудоустройство;
7. Записаться на профессиональную ориентацию;
8. Получение справок для получения государственной социальной стипендии;
9. И многие другие.

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.

Для получения ЕСИА необходимо:

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

Также возможно получить ЕСИА можно сразу в ближайшем отделении МФЦ.

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.

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.

Правила использования персональных устройств и программного обеспечения

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

Здоровье компьютера зависит от двух главных вещей:

1. Первое – это порядок в программах и в той информации, которая на компьютере хранится.
2. Второе – это порядок и чистота внутри и снаружи компьютера.

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

1. Из-за пыли части компьютера не могут достаточно охлаждаться, перегреваются и выходят из строя. Кроме этого, из-за пыли сами вентиляторы могут перестать вращаться;
2. Части компьютера при работе выделяют много тепла, которое отводится с помощью кулеров (вентиляторов) и за счет свежего прохладного воздуха в помещении. В жарком помещении компьютеры очень быстро нагреваются до недопустимой температуры;
3. Сырость, в том числе если пары воды конденсируются в компьютере, это может привести к короткому замыканию, и компьютер перегорит.

При чистке компьютера нужно соблюдать правила:

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

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

Компьютер или ноутбук рекомендуется:

1. не держать в пыльном месте, около батареи или на солнце, что может быстро перевести к перегреву и запылению
2. не держать в тесноте и заваливать его части посторонними предметами, например, складывать книги на системный блок.

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

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

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.

В настоящее время представлены различные операционные системы, из которых некоторые распространяются платно, а другие бесплатно. Существуют отдельно операционные системы для смартфона и планшета, имеющие особенность в виде системы управления (не мышь и клавиатура, а сенсор). Пользователь самостоятельно принимает решение какую операционную систему выбрать и использовать.

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 отчески 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.

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

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

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

Настройки браузеров имеют разные период хранения куки:

1. до истечения срока их действия.
2. до закрытия браузера.
3. каждый раз, когда сайт будет присылать куки, браузер будет спрашивать, сохранять ли их.

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

Информационный след также оставляет история браузера, которая сохраняет и формирует каталог ссылок, которые посещал пользователь, время и дату посещения. Эти данные также могут удаляться браузером автоматически, например, при закрытии браузера.

Все браузеры позволяют пользователям, которые не хотят, чтобы посторонние узнали историю посещений, логины и пароли, введенные пользователем, применить функцию «Приватное окно» или «Приватная страница (вкладка)», которая после закрытия не сохраняет на компьютере никакую информацию.

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.

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

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

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

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

Для 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.

Любое действие в интернете — это обмен данными. Обычно обмен данным проходит по протоколу HTTP, который устанавливает правила обмена информацией и обеспечивает загрузку в браузер содержимого сайта. Через данный протокол работают как локальные сети (кабель), так и Wi-Fi.

Однако данные, передаваемые по HTTP, не защищены и передаются в открытом виде, а поскольку информация переходит различные узлы передачи, то существует риск того, что в случае использования и контроля хотя бы одного такого узла злоумышленниками, данные пользователей могут быть переданы им.

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.

Установка и использование пароля

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

Пароль устанавливается:

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

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

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

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

Специалисты рекомендуют использовать два вида паролей:

1. для платежных систем длинные и сложные пароли, которые состоят как минимум из 10 символов, включают буквы верхнего и нижнего регистра, цифры и специальные символы, не содержат имя пользователя и известные факты о нем;
2. простые и легко запоминающееся для форумов и других сайтов, не представляющих опасности для денег.

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

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

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

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

1. Привязка аккаунта к мобильному номеру телефона может быть использована при условии указания в настройках аккаунта актуального и работающего номера телефона;
2. Привязка аккаунта к другой электронной почте актуальна для почтовых сервисов, что позволяет в случае утери одной почты восстановить ее через другую;
3. Контрольный вопрос представляет собой перечень заранее подготовленных вопросов, на которые пользователь дает свой ответ. Например, «Девичья фамилия матери», «Кличка первого животного» и пользователь вводит, например, следующие ответы «Иванова», «Шарик». Таким образом, выбрав функцию восстановления пароля сервис предложит

ответить на контрольный вопрос. Рекомендуется не выбирать простые и нейтральные вопросы, ответ на которые легко подобрать или найти, например, в социальной сети.

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

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

Гигиенические требования к организации занятий с использованием цифровых средств обучения

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

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

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

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

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

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

экране монитора и клавиатуре. Наиболее благоприятные показатели зрительной работоспособности отмечаются при освещенности рабочего места в 400 люкс, а экрана дисплея – 300 люкс.

В настоящее время появилась возможность организации общего освещения с помощью светодиодных источников света. Самое главное преимущество новых ламп – снижение пульсации светового потока в 10 и более раз по сравнению с действующим регламентом.

Поэтому светодиодные установки в школах оказывают более позитивное влияние на зрительный анализатор, обеспечивают более эффективную работоспособность и меньшее утомление школьников. Чистку осветительной арматуры светильников необходимо проводить не реже 2 раз в год и своевременно заменять перегоревшие лампы.

Расстояние от глаз пользователя до экрана компьютера должно быть не менее 50 см.

Одновременно за ПК должен заниматься один ребенок, так как для сидящего сбоку условия рассматривания изображения на экране резко ухудшаются. Если для решения педагогических задач необходимы ситуации, когда за одним монитором занимаются двое школьников, следует помнить, что такие занятия должны быть непродолжительны – не более 15 минут.

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

Основные рекомендации по организации рабочего места сводятся к следующему:

1. высота стула (а лучше кресла) должна быть такой, чтобы между ладонью и запястьем не образовывался угол;
2. клавиатуру лучше размещать на несколько сантиметров ниже уровня обычного письменного стола;
3. во время работы за компьютером ноги должны иметь опору, чтобы снизить нагрузку, которую они испытывают;
4. во время набора текста на клавиатуре запястья не должны опускаться, подниматься или отклоняться в стороны;
5. пальцы, запястье и предплечье должны образовывать прямую линию;
6. между локтевым суставом и предплечьем должен образовываться угол в 90°, плечи должны быть опущены и расслаблены.

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

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

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

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

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

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

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

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

1. выполнять упражнения для глаз через каждые 20-25 минут работы с компьютером, а при появлении зрительного дискомфорта, выражающегося в быстром развитии усталости глаз, рези, мелькании точек перед глазами и т.п., упражнения для глаз проводить индивидуально, самостоятельно и раньше указанного времени;
2. для снятия локального утомления должны осуществлять физкультурные минутки целенаправленного назначения;
3. для снятия общего утомления, улучшения функционального состояния нервной, сердечно-сосудистой, дыхательной систем, а также мышц плечевого пояса, рук, спины, шеи и ног, следует проводить физкультпаузы.

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

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

Интерактивная доска (ИД) широко используется в общеобразовательных школах, зачастую вытесняя традиционную меловую доску. Важное значение имеет размер ИД. Согласно существующим требованиям, ее диагональ должна быть не менее

1900 мм, а размер активной поверхности – не менее 1560х1100 мм. Аппаратное разрешение – не ниже 4000х4000 точек. Активная поверхность доски должна быть износостойкой, твердой, матовой и антивандальной.

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

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

Использование ИД предъявляет особые требования к созданию в учебных помещениях комфортных условий для восприятия подаваемой с ее помощью информации.

Размещение доски должно обеспечивать благоприятные условия для зрительной работы учащихся. При использовании интерактивной доски необходимо позаботиться о затемнении окна (окон), ближайшего к доске. Это позволит исключить засветку доски солнечным светом, а также ее бликование.

Предъявляемая на доске информация должна быть четкой, хорошо различимой для всех учащихся независимо от удаленности от доски. Суммарная продолжительность использования интерактивной доски на уроке в 1-2 классах не должна превышать 25 минут; в 3-4 классах и старше – не более 30 минут. Продолжительность применения ИД в течение учебного дня для 1-2 классов – не более 1 часа 20 минут; для 3-4 классов – 1 часа 30 минут, для средних классов – не более 2 часов.

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

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

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

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

1. Разговор по сотовому телефону не должен длиться более 2 минут, а минимальная пауза между звонками должна быть не менее 15 минут. Гораздо безопаснее писать SMS, чем держать трубку возле уха, так что по возможности

лучше писать, чем говорить. Если телефон используется для игр, прослушивания музыки, чтения, необходимо перевести его в авиационный режим, когда нет связи с базовой станцией.

2. Держать трубку мобильного телефона нужно на расстоянии от уха, за нижнюю ее часть и вертикально. Затухание радиоволн пропорционально квадрату пройденного расстояния, поэтому, отодвинув трубку от уха всего на сантиметр и увеличив таким образом расстояние до мозга вдвое, можно понизить мощность, излучаемую в мозг, в четыре раза.
3. Подносить трубку к уху лучше после ответа на том конце. В момент вызова мобильный телефон работает на максимуме своей мощности независимо от условий связи в данном месте. В то же время через 10-20 секунд после начала вызова излучаемая мощность снижается до минимально допустимого уровня. Моментально прикладывать телефон к уху бессмысленно еще и потому, что первый длинный гудок появляется не сразу.
4. Многие дети часто отправляют SMS-сообщения или излишне увлекаются играми, встроенными в сотовые телефоны. Такое регулярное и длительное напряжение на растущие кисть и пальцы может вызывать различные нарушения костей и суставов. Кроме того, играя, ребёнок вынужден рассматривать мелкое изображение, долго смотрит на подсвеченный экран, всё время находящийся на одном расстоянии от глаз. Это является серьезной нагрузкой для глаз и может очень негативно повлиять на зрение.
5. Очки с металлической оправой при разговоре рекомендуется снимать: наличие такой оправы может привести к увеличению интенсивности электромагнитного поля, воздействующего на пользователя.
6. Существует несколько рекомендаций по хранению и переноске телефонов. Специалисты не советуют класть мобильные телефоны рядом с собой во время сна. Также не стоит постоянно держать мобильный телефон при себе, например, в кармане брюк. То есть, контакты с сотовым телефоном стоит ограничить, особенно, если в этом нет никакой необходимости. Носить мобильный телефон лучше в сумке, не стоит держать длительное время сотовый телефон на груди, поясе или в нагрудном кармане.

Упражнения для профилактики развития синдрома запястного канала:

1. Сожмите руки в кулак, поддержите в течение 3 секунд, а затем максимально разожмите и подержите 6 секунд.
2. Вытяните руки перед собой, поднимите и опустите их.
3. Опишите кончиками пальцем круги, будто бы рисуя букву «О».
4. Сделайте круговые движения большими пальцами сначала влево, потом вправо.
5. Методично надавливайте одной рукой на пальцы другой.
6. Энергично несколько раз встряхните руки.
7. Комплексы упражнений для глаз (профилактика зрительного утомления).
8. Упражнения выполняются сидя или стоя, отвернувшись от экрана, при ритмичном дыхании, с максимальной амплитудой движения глаз.

Вариант 1:

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

Вариант 2:

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

Вредоносное программное обеспечение

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

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

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

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

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

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

Яркими примерами работы вредоносного программного обеспечения являются:

1. Троянский конь. Этот метод предполагает, что пользователь не заметил, что компьютерная программа была изменена таким образом, что включает в себя дополнительные функции. Программа, выполняющая полезные функции, пишется таким образом, что содержит дополнительные скрытые функции, которые будут использовать особенности механизмов защиты системы (возможности пользователя, запустившего программу, по доступу к файлам).
2. Бэкдор. Этот метод основан на использовании скрытого программного или аппаратного механизма, позволяющего обойти методы защиты в системе. Этот механизм активируется некоторым неочевидным образом. Иногда программа пишется таким образом, что специфическое событие, например, число транзакций, обработанных в определенный день, вызовет запуск неавторизованного механизма.
3. Технология салями. Названа так из-за того, что преступление совершается понемногу, небольшими частями, настолько маленькими, что они незаметны. Обычно эта технология сопровождается изменением компьютерной программы. Например, платежи могут округляться до нескольких центов, и разница между реальной и округленной суммой поступать на специально открытый счет злоумышленника.

В литературе обычно выделяют следующие виды вирусов:

1. Вирус – вредоносный код, который нарушает работоспособность системы, например, отключает интернет, устанавливает экран блокировки, стирает или шифрует файлы, включает возможность удаленного управления твоим компьютером или телефоном.
2. Сетевые черви – это вирусы, которые могут самостоятельно распространяться, заражая все больше устройств.

3. Руткиты – это вирусы, которые маскируют свое присутствие в системе и могут самовосстанавливаться или заражать компьютер при определенных условиях, например, если на компьютере работает администратор.
4. Загрузочные вирусы – это вирусы, поражающие загрузочные сектора дисков.
5. Файловые вирусы – это вирусы, заражающие исполнительные файлы различных типов
6. Шпионские программы – это вредоносные программы, целью которых является слежка и похищение информации. Они могут копировать пароли, контакты, номера пластиковых карт, делать снимки экрана, запоминать нажатия клавиш и другую важную информацию. Позже эта информация передается на сервера злоумышленников. Некоторые вредоносные программы могут отправлять почту, сообщения в социальных сетях, совершать платные звонки и рассылать СМС скрытно от владельца устройства.

Источниками вирусного вредоносного программного обеспечения являются:

1. получение и просмотр вложенных файлов и ссылок в электронных письмах, в сообщениях в социальных сетях, которые могут быть получены как от постороннего человека, так и от знакомого, но уже зараженного участника социальной сети или почтовой переписки;
2. открытие файлов на съемных носителях (компакт-диски, флешки и т.д.)
3. посещение зараженных сайтов как специально созданных в целях мошенничества, так и обычных, но имеющих уязвимости информационной безопасности;
4. ошибки программного кода программ, установленных на устройстве;
5. клики по рекламным баннерам сомнительного содержания;
6. скачивание и установка программ из непроверенных или нелицензионных ресурсов.

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

1. Снижается скорость обмена данными с Интернетом;
2. Вывод на экран странных сообщений или изображений;
3. Подача странных звуковых сигналов;
4. Неожиданное открытие и закрытие лотка дисковода;
5. Произвольный запуск на компьютере каких-либо программ;
6. Неожиданная перезагрузка и завершение некоторых программ;
7. Повышенная нагрузка и «зависание» устройства;
8. Замедление работы устройства или некоторых программ;
9. Увеличение размера файлов;
10. Появление не существовавших ранее и не создававшихся пользователем файлов;
11. Уменьшение объема доступной оперативной памяти;

12. Искажение содержимого файлов и каталогов или их полное исчезновение;
13. Самопроизвольное появление на экране сообщений или изображений;
14. Странное поведение интернет-браузера;
15. Невозможность перегрузки компьютера (операционная система не загружается).

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

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

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

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

Обновление происходит следующим образом:

1. Антивирусная программа создает барьер для вирусов, распознавая их. Разработчики антивирусной защиты включают коды известных программ-вирусов в базы данных антивирусных программ.
2. По мере появления новых вирусов антивирусные базы обновляются, и именно эту информацию получает пользователь компьютера, устанавливая обновления антивирусных программ.

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

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

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

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

Чтобы обезопасить свои устройства от вирусов рекомендуется:

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

2. Не открывать вложенные файлы или ссылки, полученные по электронной почте, через социальную сеть или другие средства коммуникаций в интернете, не удостоверившись, что файл или ссылка не содержит вирус. Лучше такое сообщение сразу удалить и очистить корзину.
3. Использовать только лицензионное и актуальное программное обеспечение, в том числе операционную систему и антивирусную программу, и своевременно их обновлять как на компьютере, так и на других устройствах (желательно установить автоматическое обновление или скачивать антивирус только с официального сайта разработчика).
4. Обращать внимание на предупреждения браузера или поисковой машины о том, что сайт может угрожать безопасности компьютера.
5. Не подключать к своему компьютеру непроверенные съемные носители.
6. Включить на компьютере персональный брандмауэр и установить максимальные настройки безопасности.
7. Работать на компьютере под правами пользователя, а не администратора.
8. Ограничить физический доступ к компьютеру для посторонних лиц. Не оставлять без присмотра компьютер с важными сведениями на экране.
9. Регулярно необходимо осуществлять резервное копирование важных данных.

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

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 Управления «К» 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

Коммуникативные аспекты информационной безопасности

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

Цифровая репутация

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

Цифровая репутация - это негативная или позитивная информация в сети «Интернет» о пользователе.

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

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

1. Уже сегодня существуют программы и сервисы, которые анализируют интересы, записи на стене, увлечения, высказывания, фотографии и другие данные, опубликованные потенциальными кандидатами на работу. В случаях несоответствия описания кандидата результатам, работодатели отказывают в работе.
2. Имеются неоднократные примеры, когда за некорректные комментарии или фотографии уволены стюардессы, учителя, госслужащие, сотрудники крупных компаний.

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

Например, при отправке кому-либо фотографии:

1. Ее могут переслать дальше или показать кому-нибудь еще.
2. Ее могут разместить в интернете.
3. Ее могут увидеть одноклассники, учителя, родители, совершенно чужие люди.
4. Ее могут комментировать незнакомые люди, в частности присылать оскорбительные комментарии, подвергнуть унижению и террору и даже звонить.
5. Ее могут увидеть ваши дети, ваш партнёр, работодатель, коллеги по работе или учебе в будущем.

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

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

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

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

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

Основные советы по защите цифровой репутации:

1. Перед публикацией любой информации, например, публикацией фотографии или осуществлении любого действия, например, комментирования какого-либо поста в сети «Интернет» необходимо подумать о возможных последствиях и защите себя и близких сейчас и в будущем;
2. Установить в настройках профиля ограничения на просмотр профайла и его содержимого;
3. Нельзя размещать и указывать информацию, которая может кого-либо оскорбить, обидеть или унизить.

Сетевой этикет. Кибербуллинг

В ходе сетевого общения необходимо придерживаться следующих правил поведения:

1. Помнить о том, что ведется диалог с человеком и не забывать об эмоциональной сфере. В ходе дискуссии можно очень легко ошибиться в толковании слов собеседника, забыв, что собеседник имеет чувства, привычки, позицию и мировоззрение.
2. Необходимо следить за формулировками и используемой лексикой, избегать жаргонной и ненормативной лексики и соблюдать правила орфографии и пунктуации, поскольку любая информация может быть включена в новый контекст и поменять смысл.
3. Необходимо правильно выбирать модель поведения, ведь принимаемая в одном месте, она может быть неприемлема в другом. Оказавшись на новом сайте, в группе или новом блоге, сначала необходимо ознакомиться с правилами и прочитать, как и о чем говорят участники дискуссии, узнать методы и форматы общения и только после этого вступать в дискуссию. Также общение с друзьями может включать в себя некую расслабленность, но в коммуникации с коллегами, начальством или другими лицами - это не допускается.
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.

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

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

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

Обычно выделяют следующие виды кибербуллинга:

1. Оскорбление происходит посредством оскорбительных комментариев и вульгарных обращений, происходящих в публичном пространстве интернета;
2. Домогательство от незнакомцев, адресованное конкретно пользователю;
3. Клевета путем выставления жертв в неблагоприятном свете с помощью различных материалов или информацией;

4. Использование фиктивного имени, когда кто-то выдает себя за другого человека, используя пароль жертвы, либо создает поддельную страницу на ее имя, где размещает лживый и унизительный контент или отправляет различные сообщения друзьям и знакомым жертвы негативного характера для ухудшения отношения к жертве.
5. Публичное разглашение личной информации осуществляется путем распространения личной информации для шантажа или оскорбления жертвы.

Чтобы противостоять кибербуллингу, необходимо следовать ряду правил.

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

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

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

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

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

При наличии угроз жизни и здоровью 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.

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

1. Манипулирование истинной информацией.
3. Тенденциозный подбор тем и материалов.
4. Эмоциональное комментирование, представление происходящего.
5. Технология влияния на деформацию образов, внедрение в общественное сознание элементов нестабильности, дезорганизованности, хаоса, неуверенности и страха.
6. Использование контента как канала доведения до населения дезинформации.
7. Технологии манипуляции с опросами общественного мнения.
8. «Эффект CNN» (тенденциозное представление информации).
9. Эксплуатация всевозможных слухов, которые могут целенаправленно влиять на информационно-психологический климат в обществе.
10. Использование контента как инструмента непосредственного доведения до отдельной личности, общества и органов государственной власти угроз, ультиматумов, «импульсов» диктата и устрашения.

Рассмотрим некоторые технологии более подробно.

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.

Инструменты коммуникации: электронная почта, социальные сети и мессенджеры

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

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

В первую очередь необходимо выбрать правильный сервис электронной почты. Рекомендуется использовать бесплатные почтовые сервисы, которые представлены на рынке достаточно долгое время и соответствуют следующим условиям:

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

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

В названии своего ящика можно использовать реальные имя и фамилию, что позволит облегчить связь с пользователем, однако в названии почты не стоит употреблять посторонние слова, 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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Особая категория аккаунтов в социальных сетях – это фейки. Фейки - это поддельные страницы реальных людей с идентичными фотографиями и данными. Чаще всего фейковые страницы создают под профайлы известных людей. Как отличить фейк от оригинала?

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

В конце отметим, что необходимо помнить, что быть и казаться – разные понятия. То, что демонстрируется в социальных сетях, не всегда соответствует реальности.

Вместе с социальными сетями многие пользователи используют различные мессенджеры для общения, однако в большинстве мессенджеров можно не только обмениваться текстовыми и 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.

Интернет-зависимость

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

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

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

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

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

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

Интернет-зависимость опасна по различным причинам, которые приводят 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.

Аспекты информационной безопасности для родителей (законных представителей) детей

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

Общие вопросы для родителей можно представить следующими советами:

1. Независимо от возраста ребенка используйте программное обеспечение, помогающее фильтровать и контролировать информацию, но не полагайтесь полностью на него. Ваше внимание к ребенку - главный метод защиты.
2. Если ваш ребенок имеет аккаунт на одном из социальных сервисов (LiveJournal, blogs.mail.ru, vkontakte.ru и т.п.), внимательно изучите, какую информацию помещают его участники в своих профилях и блогах, включая фотографии и видео.
3. Проверьте, с какими другими сайтами связан социальный сервис вашего ребенка. Странички вашего ребенка могут быть безопасными, но могут и содержать ссылки на нежелательные и опасные сайты (например, порносайт или сайт, на котором друг упоминает номер сотового телефона вашего ребенка или ваш домашний адрес).
4. Стимулируйте ваших детей сообщать обо всем странном или отталкивающем.
5. Реагируйте, когда они этого не делают (из-за опасения потерять доступ к Интернету дети не говорят родителям о проблемах, а также могут начать использовать Интернет вне дома и школы).
6. Будьте в курсе сетевой жизни вашего ребенка. Интересуйтесь, кто его друзья в Интернете так же, как интересуетесь реальными друзьями.

Возраст от 7 до 8 лет

В Интернете ребенок старается посетить те или иные сайты, а возможно и чаты, разрешение на посещение которых он не получил бы от родителей. Поэтому родителям особенно полезны будут те отчеты, которые предоставляются программами по ограничению использования Интернета, т.е. родительский контроль или то, что вы сможете увидеть во временных файлах. В результате у ребенка не будет ощущения, что за ним ведется постоянный контроль, однако родители будут по-прежнему знать, какие сайты посещает их ребенок. Дети в данном возрасте обладают сильным чувством семьи, они доверчивы и не сомневаются в

авторитетах. Они любят играть в сетевые игры и путешествовать по Интернету, используя электронную почту, заходить на сайты и чаты, не рекомендованные родителями. Советы по безопасности в сети Интернет для детей 7 - 8 лет:

1. Создайте список домашних правил посещения Интернета при участии детей и требуйте его выполнения.
2. Требуйте от вашего ребенка соблюдения временных норм нахождения за компьютером. Покажите ребенку, что вы наблюдаете за ним не потому что вам это хочется, а потому что вы беспокоитесь о его безопасности и всегда готовы ему помочь.
3. Компьютер с подключением к Интернету должен находиться в общей комнате под присмотром родителей.
4. Используйте специальные детские поисковые машины.
5. Используйте средства блокирования нежелательного контента как дополнение к стандартному родительскому контролю.
6. Создайте семейный электронный ящик, чтобы не позволить детям иметь собственные адреса.
7. Блокируйте доступ к сайтам с бесплатными почтовыми ящиками с помощью соответствующего программного обеспечения.
8. Приучите детей советоваться с вами перед опубликованием какой-либо информации средствами электронной почты, чатов, регистрационных форм и профилей.
9. Научите детей не загружать файлы, программы или музыку без вашего согласия.
10. Не разрешайте детям использовать службы мгновенного обмена сообщениями.
11. В "белый" список сайтов, разрешенных для посещения, вносите только сайты с хорошей репутацией.
12. Не забывайте беседовать с детьми об их друзьях в Интернете, как если бы речь шла о друзьях в реальной жизни.
13. Не делайте "табу" из вопросов половой жизни, так как в Интернете дети могут легко наткнуться на порнографию или сайты "для взрослых".
14. Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам о своих тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.

Возраст детей от 9 до 12 лет

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

1. Создайте список домашних правил посещения Интернета при участии детей и требуйте его выполнения.
2. Требуйте от вашего ребенка соблюдения норм нахождения за компьютером.
3. Наблюдайте за ребенком при работе за компьютером, покажите ему, что dы беспокоитесь о его безопасности и всегда готовы оказать ему помощь.

4. Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей.
5. Используйте средства блокирования нежелательного контента как дополнение к стандартному родительскому контролю.
6. Не забывайте принимать непосредственное участие в жизни ребенка, беседовать с детьми об их друзьях в Интернете.
7. Настаивайте, чтобы дети никогда не соглашались на личные встречи с друзьями по Интернету.
8. Позволяйте детям заходить только на сайты из "белого" списка, который создайте вместе с ними.
9. Приучите детей никогда не выдавать личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернете.
10. Приучите детей не загружать программы без вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.
11. Создайте вашему ребенку ограниченную учетную запись для работы на компьютере.
12. Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Напомните детям, что они в безопасности, если сами рассказали вам о своих тревогах и опасениях.
13. Расскажите детям о порнографии в Интернете.
14. Настаивайте на том, чтобы дети предоставляли вам доступ к своей электронной почте, чтобы вы убедились, что они не общаются с незнакомцами.
15. Объясните детям, что нельзя использовать сеть для хулиганства, распространения сплетен или угроз.

Возраст детей от 13 до 17 лет

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

Важно по-прежнему строго соблюдать правила Интернет-безопасности - соглашение между родителями и детьми. Кроме того, необходимо как можно чаще просматривать отчеты о деятельности детей в Интернете. Следует обратить внимание на необходимость содержания родительских паролей (паролей администраторов) в строгом секрете и обратить внимание на строгость этих паролей. Советы по безопасности в этом возрасте от 13 до 17 лет:

1. Создайте список домашних правил посещения Интернета при участии подростков и требуйте безусловного его выполнения. Обговорите с ребенком список запрещенных сайтов ("черный список"), часы работы в Интернете, руководство по общению в Интернете (в том числе в чатах).
2. Компьютер с подключением к сети Интернет должен находиться в общей комнате.
3. Не забывайте беседовать с детьми об их друзьях в Интернете, о том, чем они заняты таким образом, будто речь идет о друзьях в реальной жизни. Спрашивайте о людях, с которыми дети общаются посредством служб мгновенного обмена сообщениями, чтобы убедиться, что эти люди им знакомы.
4. Используйте средства блокирования нежелательного контента как дополнение к стандартному родительскому контролю.
5. Необходимо знать, какими чатами пользуются ваши дети. Поощряйте использование модерируемых чатов и настаивайте, чтобы дети не общались в приватном режиме.
6. Настаивайте на том, чтобы дети никогда не встречались лично с друзьями из сети Интернет.
7. Приучите детей не выдавать свою личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернете.
8. Приучите детей не загружать программы без вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.
9. Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Напомните детям, что они в безопасности, если сами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.
10. Расскажите детям о порнографии в Интернете. Помогите им защититься от спама. Научите подростков не выдавать в Интернете своего реального электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.
11. Приучите себя знакомиться с сайтами, которые посещают подростки.
12. Научите детей уважать других в интернете. Убедитесь, что они знают о том, что правила хорошего поведения действуют везде - даже в виртуальном мире.
13. Объясните детям, что ни в коем случае нельзя использовать сеть для хулиганства, распространения сплетен или угроз другим людям.
14. Обсудите с подростками проблемы сетевых азартных игр и их возможный риск. Напомните, что дети не могут играть в эти игры согласно закону.
15. Постоянно контролируйте использование Интернета вашим ребенком. Это не нарушение его личного пространства, а мера предосторожности и проявление вашей родительской ответственности и заботы.

Организация обучения детей и родителей (законных представителей)

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

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.

Вопросы обеспечения информационной безопасности с учетом раздела №1 «Актуальность информационной безопасности детей» данных методических рекомендаций могут быть изучены во время различных учебных дисциплин как в рамках курса «Информатика», так и других предметных областей, и иной учебной деятельности с учетом межпредметных и метапредметных связей.

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

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 №1 «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.

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.

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.

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

Образовательные организации осуществляют обучение обучающихся и просвещение их родителей и законных представителей в соответствии с настоящими методическими рекомендациями.

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

Образовательные организации обеспечивают в кадровом направлении работы:

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

Для обеспечения учебно-методического и информационного сопровождения образовательного процесса образовательные организации:

1. оказывают постоянную научно-теоретическую, методическую и информационную поддержку педагогическим работникам по вопросам обеспечения информационной безопасности детей и организации обучения детей информационной безопасности;
2. обеспечивают укомплектованность соответствующим данным методическим рекомендациям учебниками, учебно-методической литературой и материалами, включающими вопросы, связанные с обеспечением информационной безопасности детей и организации обучения детей информационной безопасности, либо учебниками, учебно-методической литературой и материалами по данным тематикам.

Организационно-административные мероприятия в материально-технической области предполагают соблюдение санитарно-эпидемиологических требований при организации образовательной деятельности с использованием ИКТ-технологий и соответствующего оборудования и регулярный мониторинг в образовательной организации соблюдения данных требований.

Для обеспечения вышеуказанных процессов в организационно-административные мероприятия для образовательных организаций входит создание необходимых финансово-экономических условий для организации обучения детей информационной безопасности в рамках реализации образовательной программы, в частности закупка необходимых учебников, учебно-методической литературы, материалов и других средств обучения.

Образовательные организации для планирования и систематизации реализуемых мер и проводимых мероприятий формируют ежегодный план мероприятий образовательной организации по организации обучения обучающихся информационной безопасности, отражающий все аспекты организации обучения обучающихся и их родителей (законных представителей) информационной безопасности и реализуемые организационно-административные мероприятия.

В перечень организационно-административных мероприятий администраций субъектов Российской Федерации, органов муниципальных образований и образовательных организаций по реализации методических рекомендаций в области повышения уровня информированности граждан по вопросам информационной безопасности детей входит реализация 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".

К организационно-административным мероприятиям, проводимым администрациями субъектов Российской Федерации и органов муниципальных образований, включая их подведомственные организаций и учреждения, относится:

1. Осуществление в рамках своей компетенции обучения обучающихся и их родителей (законных представителей) информационной безопасности и проведении организационно-административных мероприятий в образовательных организациях, в частности оказывая им необходимое содействие и поддержку;
2. Осуществление методической и информационной поддержки педагогических работников образовательных организаций в организации обучения обучающихся и их родителей (законных представителей) информационной безопасности и проведении организационно-административных мероприятий в образовательных организациях;
3. Организация и проведение регулярного мониторинга реализации положений настоящих методических рекомендаций в образовательных организациях;
4. Разработка и реализация региональных программ обеспечения информационной безопасности детей, производства информационной продукции для детей и оборота информационной продукции и муниципальной программы обеспечения информационной безопасности детей, производства информационной продукции для детей и оборота информационной продукции соответственно на основе модульной региональной программы обеспечения информационной безопасности детей, производства информационной продукции для детей и оборота информационной продукции, утверждённой на парламентских слушаниях «Актуальные вопросы обеспечения безопасности и развития детей в информационном пространстве», прошедших в Совете Федерации 17 апреля 2017 года.

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

Временная комиссия Совета Федерации по развитию информационного общества осуществляет на федеральном уровне координацию и методическое сопровождение реализации данных методических рекомендаций.

В настоящее время Временная комиссия Совета Федерации по развитию информационного общества при поддержке Минпросвещения России и Минкомсвязи России является инициатором и организатором важнейших мероприятий в сфере информационной безопасности детей: Единого урока по безопасности в сети «Интернет» и цикла мероприятий для детей и педагогических работников «Сетевичок».

На площадке Временной комиссии Совета Федерации по развитию информационного общества, руководствуясь рекомендациями парламентских слушаний «Актуальные вопросы обеспечения безопасности и развития детей в информационном пространстве», прошедших в Совете Федерации 17 апреля 2017 года (далее – рекомендации парламентских слушаний), создается и осуществляет свою деятельность детское общественное движение «Страна молодых», реализующее различные программы и проекты для обеспечения безопасности и развития детей в информационном пространстве.

Образовательные организации, органы власти и муниципалитеты могут выступить учредителями регионального отделения Движения в своем субъекте Федерации и принимать участие в инициативах и программах Движения.

Для реализации настоящих методических рекомендаций на площадке Экспертного совета по информатизации системы образования и воспитания при Временной комиссии Совета Федерации по развитию информационного общества (далее – Экспертный совет) реализована программа для образовательных организаций, позволяющая организовать преподавание информационной безопасности обучающимся дистанционно в рамках:

1. таких учебных дисциплин как «Информатика», «Основы безопасности жизнедеятельности» и другие;
2. самостоятельной учебной дисциплины «Информационная безопасность;
3. программы внеурочной деятельности и (или) дополнительного образования;
4. программ воспитания и социализации обучающихся.

Особенностью реализации данной программы является организация образовательной деятельности по основным и дополнительным общеразвивающим программам дистанционно в соответствии с требованиями законодательства, что позволит образовательным организациям использовать современные образовательные технологии при обучении обучающихся информационной безопасности.

Данная программа была реализована в соответствии с рекомендациями парламентских слушаний и поддержана Министерством образования и науки Российской Федерации, а в апробации в формате внеурочной деятельности принимали участие более 800 образовательных организаций.

Для развития образования в области информационной безопасности педагогических работников образовательных организаций на площадке Экспертного совета организованы бесплатные дистанционные программы повышения квалификации, разработанные на основе данных методических рекомендаций.

Программы повышения квалификации включают изучение информационных, потребительских, технических и коммуникативных аспектов информационной безопасности, организацию обучения информационной безопасности обучающихся и их родителей (законных представителей) как на базовом, так и на повышенном уровне. Дополнительно для педагогических работников организованы бесплатные программы повышения квалификации и по другим направлениям и сферам, которые рекомендуется пройти всем педагогическим работникам.

Для обеспечения педагогических работников образовательных организаций необходимыми материалами и информацией, в частности тематическим планированием и рабочими программами, сформирована сетевая библиотека материалов по вопросам обучения информационной безопасности детей и их родителей (законных представителей) (далее – сетевая библиотека).

Данное решение организации методико-информационного сопровождения реализации данных методических рекомендаций было выбрано с целью:

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

В сетевую библиотеку войдут материалы и разработки:

1. Министерства просвещения Российской Федерации, подведомственных организаций и учреждений Министерства просвещения Российской Федерации, в частности ФГАОУ ДПО АПК и ППРО ФГБНУ «Центр защиты прав и интересов детей», других федеральных органов государственной власти и их подведомственных организаций и учреждений;
2. Органов власти субъектов Российской Федерации, муниципальных образований, их подведомственных организаций и учреждений;
3. Образовательных и научных организаций;
4. Педагогических работников.

Данная электронная библиотека реализуется в рамках Электронной библиотеки образования (ЭБО), реализуемой на площадке Экспертного совета по информатизации системы образования и воспитания при Временной комиссии Совета Федерации по развитию информационного общества при поддержке Минобрнауки России.

Материалы по различным направлениям в ЭБО могут включать все педагогические работники и бесплатно получить соответствующий электронный документ о публикации в электронном средстве массовой информации.

Осуществлять модерацию и экспертизу представленных материалов и информации для публикации будут члены методического совета Экспертного совета по информатизации системы образования и воспитания при Временной комиссии Совета Федерации по развитию информационного общества, осуществляющей свою деятельность дистанционно и на некоммерческих началах.

Членами методического совета Экспертного совета по информатизации системы образования и воспитания при Временной комиссии Совета Федерации по развитию информационного общества могут стать педагогические работники в соответствии с положением о Методическом совете Экспертного совета по информатизации системы образования и воспитания при Временной комиссии Совета Федерации по развитию информационного общества.

На основе размещаемой в электронной библиотеке информации либо появления новых актуальных вопросов обеспечения информационной безопасности детей Временная комиссия Совета Федерации по развитию информационного общества после согласования с заинтересованными федеральными органами государственной власти будет расширять данные методические рекомендации новой информацией – дополнительными модулями.

Такой механизм обновления методических рекомендаций позволит обеспечить заинтересованные организации и лица актуальной информацией для организации соответствующей работы или внесения корректировки в процесс обучения соответственно.

Дополнительные модули будут также разрабатываться на основе пожеланий и предложений образовательных организаций, органов местного самоуправления и органов государственной власти, которые будут собираться и анализироваться в рамках проведения мониторинга субъектов Российской Федерации о ходе реализации методических рекомендаций.

Мониторинг субъектов Российской Федерации о ходе реализации методических рекомендаций будет организован ежегодно с целью изучения процесса внедрения методических рекомендаций в работу образовательных организаций и реализацию организационно-административных мероприятий администрациями субъектов Российской Федерации, муниципальными организациями и образовательными организациями.

Результаты мониторинга будут направляться в адрес заинтересованных федеральных органов государственной власти и органов исполнительной власти субъектов Российской Федерации.

Вышеуказанные мероприятия и меры будут реализовываться до 2020 года включительно в соответствии с приказом Минкомсвязи России от 27.02.2018 N 88 "Об утверждении плана мероприятий по реализации Концепции информационной безопасности детей на 2018 - 2020 годы".