Сочинение на тему:
«Безопасный Интернет»

Белендинова Карина

Интернет – это всемирная коммуникационная и информационная сеть, созданная трудами, разумеется, не одного человека, а множества ученых, программистов и инженеров. 29 октября 1969 год – именно этот день принято считать датой основания Интернета.

Роль Интернета в жизни современного человека велика. Пройдя множество ступеней развития, он стал важной частью жизни каждого. Ежедневно люди читают новости, размещенные на различных Интернет-площадках, совершают онлайн-покупки, продают свои услуги, поддерживают связь с друзьями и родственниками независимо от своего местоположения; пользуются безграничным объемом информации, доступ к которой открыт благодаря Интернету. Несомненно, он во многом упрощает нашу жизнедеятельность, но вместе с тем содержит в себе большое количество Интернет-угроз. Под данным понятием имеется ввиду нарушение информационной безопасности тем или иным способом, а также процессы или действия, способные нанести ущерб информационным системам. Виды Интернет-угроз распределяют на преднамеренные и случайные. К первым можно отнести: похищение персональных данных, компьютерные вирусы, мошенничество, троллинг и кибербуллинг, вовлечение в секты и асоциальные сообщества. Ошибки пользователя, ошибки профессионалов, отказы и сбои в работе устройства, форс-мажорные обстоятельства – все это определяется, как случайный вид информационной угрозы. По данным как отечественных, так и зарубежных СМИ, количество так называемых «кибератак» не уменьшается, а наоборот – с каждым годом становится все больше, что подчеркивает актуальность данной проблемы и говорит о том, что столкнуться с ней могут не только крупные организации, но и обычные пользователи сети.

«Как защититься от Интернет-угроз?», – вопрос, возникающий при вышеописанных обстоятельствах. Основным способом их предотвращения являются административные/нормативно-правовые меры, осуществляемые государством посредством издания специальных законопроектов. Кроме того, к методам защиты от информационных угроз относятся: использование и регулярное обновление комплексной системной защиты, посещение и использование исключительно проверенных сайтов, браузеров и приложений, игнорирование незнакомых и подозрительных ссылок, писем и файлов, внимательность при вводе личных данных (никогда не вводите данные о себе и своих учетных записях на неблагонадежных сайтах). Довольно распространенным видом Интернет-угроз является спам – нежелательные письма, кажущиеся на первый взгляд безобидными. Подобные рассылки часто несут с собой не только раздражающий фактор, но и прямую угрозу Интернет-

безопасности пользователя в виде зараженных ссылок и вложений. Что же делать, обнаружив в своей электронной почте письмо с пометкой «Спам»? В первую очередь, обращайте внимание на автоматическую фильтрацию почты (также ее называют «защитой от спама»), которая сейчас присутствует во многих сервисах и службах электронных почт. Далее, не публикуйте свой электронный адрес в открытом доступе, сообщайте его лишь тем людям, которым вы доверяете; используйте максимальный уровень приватности и не переходите по вложениям/ссылкам, содержащимся в подозрительном письме.

В связи с появлением и усовершенствованием технологий наше общество приобрело название «информационное» или «постиндустриальное», что характеризует его определенной стадией развития, на которой существенное влияние на основные сферы жизни оказывает использование информационно-коммуникационных технологий. Наверняка вы заметили, что в последнее время увеличилось число юных Интернет-пользователей. Сейчас дети гораздо раньше знакомятся с просторами Интернета, нежели предшествующие им поколения. Данное явление нельзя охарактеризовать однозначно, ведь все зависит от мер осторожности, соблюдаемых родителями и самим ребенком при использовании Мировой сети. Посредством Интернета развивается любознательность детей, появляется возможность решать неограниченное количество логических задач, тренировать мышление, внимательность и память. У юных пользователей Всемирной сети развивается такой важный навык, как умение добывать нужную информацию, что определенно пригодится в будущем. Несмотря на положительные качества использования Интернета детьми, нельзя забывать и о его возможном вреде, ведь чрезмерное увлечение им оказывает влияние на психику ребенка, способствует развитию различных расстройств (например, Интернет-зависимости), утрате навыков общения. В силу детской наивности и неопытности, шанс ребенка столкнуться с Интернет-угрозами значительно выше, нежели у взрослого человека. К примеру, на просторах Интернета можно встретить содержимое, которое должно быть недоступным для юных пользователей сети, но по какой-либо причине не имеет цензуры или возрастных ограничений. Чтобы защитить свое дитя от возможности наткнуться на киберугрозы, родитель должен сделать следующее: рассказать о возможных угрозах в Интернете и их последствиях, согласовать с ребенком правила пользования Интернет-сетью, использовать специальную антивирусную программу, содержащую функцию «Родительский контроль»; контролировать время, проведенное ребенком в сети и просматриваемый им контент (игры, видео и изображения, просматриваемые ребенком в Интернете, должны соответствовать его возрасту).

Теперь поговорим об онлайн-платформах, используемых для взаимодействия людей, изучения новой информации и многого другого. Число пользователей социальных сетей и их актуальность растут с каждым годом, а современные специалисты разделяют их на несколько видов: массовые, тематические и фото-/видео-хостинги. Я, как и многие подростки, являюсь

активным пользователем данных онлайн-платформ. Они помогают мне поддерживать постоянную связь с близкими людьми, вне зависимости от того, как далеко друг от друга мы находимся; повышать уровень своих знаний и навыков в той или иной сфере деятельности, совершать онлайн-заказы, учиться чему-то новому, узнавать последние новости и просто радовать взор просмотром приятного медиа-продукта. Определенно, социальные сети, как и Интернет в целом, делают нашу жизнь гораздо легче, но, будучи их пользователем, нельзя забывать о существующих Интернет-угрозах. На мой взгляд, самой распространенной из них приходится мошенничество, с которым мне и моим знакомым пришлось столкнуться не раз. До установления «двухфакторной аутентификации» интернет-мошенники неоднократно заполучали пароль от моих учетных записей и писали родственникам, друзьям и знакомым с просьбой одолжить определенную сумму денег. К счастью, люди из моего окружения сразу чувствовали неладное и сообщали о подозрительном сообщении мне, что позволяло быстро предотвратить данную махинацию. Но сейчас, защитив все свои аккаунты в социальных сетях, я продолжаю получать подобные сообщения от своих друзей и могу отметить, что от развития технологий не отстают и схемы мошенничества. Теперь вам могут отправить фотографию банковской карты, не принадлежащей конкретному лицу, но с отчетливым указанием его имени и фамилии, что может вызвать доверие получателя сообщения. В таких случаях нельзя сразу удовлетворять просьбу отправителя, а при возможности лучше позвонить действительному владельцу учетной записи и удостовериться в полученной вами просьбе. Если будет установлен факт мошенничества – порекомендуйте родственнику/другу/знакомому улучшить способы защиты личных данных и обратиться в управление МВД России, которое занимается преступлениями, совершенными в Интернете. Также нередко на просторах сети встречается Интернет-угроза под названием «кибербуллинг» – травля в цифровом пространстве, для которой не нужен весомый повод. Рассмотрим наиболее частые причины возникновения данного явления. К первой из них можно отнести межкультурные различия и конфликты (различия в языке, одежде и религии, нестандартный внешний вид). Вторая причина – это страх, под влиянием которого люди (чаще всего подростки) инстинктивно присоединяются к более активной и властной группе с целью обезопасить себя и избежать оскорблений; третья – скука агрессора, его потребность самоутвердиться за счет унижения невинного человека. К моему большому сожалению, с травлей в Интернете может столкнуться каждый, поэтому важно уметь дать отпор злоумышленнику. Во-первых, являясь пользователем социальных сетей, нужно помнить, что нельзя использовать их с целью хулиганства, распространения сплетен/ложной информации и угроз. Во-вторых, не следует отвечать грубостью на грубость; если услышали неприятные слова в свой адрес – сообщите об этом родителям, постарайтесь совместно решить проблему мирным способом или же ограничьте доступ оскорбителя к своей учетной записи. Многие юные пользователи Интернета боятся сообщить о том, что стали жертвой кибербуллинга (некоторые видят в

этом проявление слабости), по этой причине необходимо знать некоторые признаки и последствия его проявления: нежелание посещать учебное учреждение, снижение самооценки ребенка, потеря уверенности в себе, психические расстройства, постоянное чувство тревоги и даже попытки самоубийства. Вышеперечисленная информация не имеет конкретных возрастных ограничений, а, следовательно, может коснуться и более старшего поколения. Поэтому, пожалуйста, взрослые и дети, будьте осторожны при использовании Интернета и социальных сетей. Помните о том, что «человек человеку друг, товарищ и брат».

Еще раз убедившись в том, что Интернет содержит в себе не только множество полезной информации, но и угроз, хочется рассказать о своей безопасности в социальных сетях. В защите личных данных мне помогает «двухфакторная аутентификация» – метод идентификации пользователя в каком-либо сервере (как правило, в Интернете); он обеспечивает более эффективную защиту аккаунта от несанкционированного проникновения и доступен на многих Интернет-площадках. В добавок к этому, я отказалась от использования одинаковых паролей для различных социальных сетей/сервисов и не храню их в открытом доступе, на бумаге. Сейчас многие программные обеспечения для просмотра веб-страниц предлагают хранить пароли и другую личную информацию внутри самого браузера, что не является надежным (браузеры не всегда соответствуют требованиям безопасности, а заполучив доступ к вашему устройству, на котором выполнен вход в личный аккаунт, злоумышленник сможет заполучить и другие персональные данные). Поэтому, устанавливайте уникальные пароли, не совпадающие с другими, держите их в секрете от третьих лиц и используйте надежные способы хранения персональной информации. Я не ввожу какие-либо личные сведения на подозрительных сайтах или в неофициальных приложениях, более того, не пользуюсь ими. Онлайн-заказы совершаю исключительно через проверенных продавцов, не контактирую с незнакомыми мне людьми и игнорирую подозрительные или содержащие негативный посыл письма, предложения (за исключением жалоб, отправляемых в службу поддержки той или иной Интернет-площадки с целью предотвращения последующих Интернет-угроз).

Рассказав о некоторых способах защиты личной информации в социальных сетях, хочется поднять еще одну немаловажную тему и звучит она так: «Как сделать Интернет для детей безопасным во всем мире?» Я уже упоминала, что в современном мире дети с ранних лет начинают свое знакомство с так называемым «царством безграничных возможностей». В связи с этим, преимущественно родителям необходимо соблюдать определенные действия, которые помогут предостеречь чадо от Интернет-угроз: контролируйте время, проводимое ребенком в Интернете; используйте средства, способствующие блокировке нежелательной информации и регулярно проводите разговоры на тему безопасности в Интернете. Юные Интернет-пользователи должны понимать, что сообщать о любых тревогах

или угрозах, с которыми они столкнулись – очень важно. Кроме того, не будут лишними специальные уроки или же классные часы, проводимые образовательными учреждениями по всей стране с целью развития детей в вопросе Интернет-безопасности.

Подводя итог своего сочинения, хочется выразить его главную мысль. Безоговорочно, Интернет многое дал человечеству и с каждым днем облегчает наши повседневные задачи. Но в погоне за развитием технологий и идеальными образами, которыми полна сеть, не стоит забывать о реальной жизни. «Имейте в виду: Интернет – не новая форма жизни, а просто новое занятие», – высказывание американской предпринимательницы и общественного деятеля Эстер Дайсон, подтверждающие мои слова. Притом, войдя в цифровое пространство, немаловажно сохранять внимательность, бдительность и ясность ума, которые не позволят вам стать жертвой Интернет-угроз, а также помнить о таком понятии, как «гуманность».