Семенов Виктор Анатольевич,

преподаватель отдельной дисциплины (математика, информатика и ИКТ),

ФГКОУ «Оренбургское президентское кадетское училище»,

г. Оренбург

ЭЛЕМЕНТАРНЫЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СЕТИ ИНТЕРНЕТ

Аннотация. Статья посвящена основам информационной безопасности в сети Интернет. Несмотря на рост компьютерной грамотности населения, многие, в том числе школьники, забывают об угрозах, существующих в сети. Автор останавливается на основных видах угроз информационной безопасности и предлагает способы их предотвращения.

Ключевые слова: информационная безопасность, угрозы, предотвращение, утечка информации, электронная почта, пароли.

Современные дети с младенчества осваивают технику. Это неотъемлемая часть их жизни. Но они должны обладать знаниями о безопасности в сети. «Как есть уроки «Основы безопасности жизнедеятельности», так и должны быть уроки, посвященные основам информационной безопасности», - Сергей Неверов, лидер фракции «Единая Россия» (https://ria.ru/20190708/1556308891.html)

Уровень компьютерной грамотности населения растет, но все ли осознают, каким рискам и взрослые, и дети подвергаются в Интернете? Интернет – очень полезная вещь, которая дает нам возможность общаться, несмотря на время и расстояние, пользоваться образовательным контентом, также это площадка для саморазвития и самовыражения, но не стоит забывать, что наравне с огромными возможностями мы подвержены таким рискам, как: хищение денег, личных данных, несанкционированный доступ в личные аккаунты, неприемлемый контент для несовершеннолетних, а также втягивание в асоциальную деятельность.

Несмотря на быстрое развитие IT-технологий, не все люди знают и пользуются правилами информационной безопасности в Интернете. Поэтому не стоит забывать об угрозах, которые преследуют нас в сети.

В образовательных организациях в настоящий момент повсеместно применяются технические способы фильтрации информации, на компьютерах в классах разводятся учетные записи учителя, ученика и администратора, в некоторых школах в штатном расписании есть инженер-программист, который помимо технического обслуживания компьютеров регулярно проводит внутренний аудит информационного содержимого техники, передача различных баз данных (для олимпиад, конкурсов, при сдаче различного рода отчетов) осуществляется строго через защищенный канал связи.

Но кроме этого в школах в рамках образовательной программы должна осуществляться профилактика и обучение детей навыкам безопасного использования сети «Интернет», а также информирование их родителей (законных представителей) о возможных сетевых рисках. Для обеспечения безопасности важно вводить модули по обучению информационной безопасности в рамках таких дисциплин, как «Информатика и ИКТ», «Основы безопасности жизнедеятельности» и (если рассматривать вопрос с правовой точки зрения) «Обществознание». В любом случае, к правилам безопасного времяпровождения в Интернете должны относиться с не меньшим вниманием, чем к правилам пожарной безопасности и правилам дорожного движения.

Цель данной статьи – демонстрация основных угроз, которым мы подвергаемся в сети и способы их предотвращения.

Одна из главных угроз – утечка информации, кража личных данных. Под угрозой находятся все ваши данные, которые вы вносили в сеть Интернет. На данный момент одним из эффективным инструментов защиты от кражи и утечки информации является двухфакторная аутентификация. Также стоит следить за историей активности своего аккаунта в сетях и если вы замечаете подозрительную активность (странный IP или другая страна входа, если вы не

пользуетесь VPN), то стоит сменить пароль (пароль должен содержать не менее 10 символов, включая буквы разных регистров, цифры и специальные знаки).

Совершая покупку онлайн, обращайте внимание на защищенность канала передачи данных, не сохраняйте данные карт. Отслеживайте файлы cookies на жестком диске, регулярно проверяйте их принадлежность и удаляйте подозрительные. Для защиты от вирусов, червей и троянов приобретите лицензионный антивирусный пакет и не забывайте своевременно его обновлять и продлевать. А также пользуйтесь только лицензионным программным обеспечением.

Внимательно относитесь ко всем письмам, которые приходят на вашу почту. Не открывайте письма, который пришли к вам с подозрительного сайта, не переходите по подозрительным ссылкам, даже если ее вам прислал хороший знакомый (лучше переспросить у него, точно ли он присылал вам данное письмо).

Если вам приходится очень часто сталкиваться с работой с документами, то создавайте текстовые файлы, которые не позволяют вносить изменения (защита документа, ограничение на редактирование, только чтение). Для своей учетной записи на компьютере/ноутбуке создайте пароль, если вы отлучаетесь, обязательно блокируйте экран. Для противодействия хакерам воспользуйтесь такими простыми правилами: не храните пароли на компьютере/смартфоне, заполняйте их всегда вручную, желательно к каждому ресурсу иметь собственный пароль, при подозрении на хакерскую атаку отключайте Internet, запускайте антивирусную программу, изменяйте пароли, просматривайте чаще системный реестр на предмет подозрительных записей; резервные копии данных, пользуйтесь виртуальными машинами и фаерволами.

Также стоит более скептически относиться ко всей информации, которая циркулирует в сети, проверять ее сразу в нескольких открытых источниках и т.д., это позволит вам избежать дезинформации.