Осин Алексей Константинович
канд. пед. наук, доцент
Базарбаева Нилуфав
студентка
Шуйский филиал ФГБОУ ВО «Ивановский государственный университет»
г. Шуя, Ивановская область

АКТИВНЫЕ ФОРМЫ ПРОВЕДЕНИЯ ЗАНЯТИЙ ПРИ ОБУЧЕНИИ БЕЗОПАСНОМУ ПОВЕДЕНИЮ В ИНТЕРНЕТЕ

Аннотация*: статья посвящена вопросу обучения безопасному поведению в Интернете посредством активных форм проведения занятий.*

Ключевые слова*: безопасность в Интернете, кибербезопасность.*

Россия, как и многие страны, идет в своем развитии к цифровому обществу, которое характеризуется, в первую очередь, высокой скоростью коммуникационных процессов, обеспечивающийся информационными технологиями и сетью Интернет. Интернет, являясь средством многократного увеличения возможности и скорости осуществления коммуникаций, решает одну из важнейших проблем цифрового общества – генерации, обработки и передачи огромного массива информации, которая становится главным ресурсом в современном обществе.

Анализируя материалы электронного ресурса «Вся статистика – интернета и соцсетей – цифры и тренды в мире и в России» понятно, что сегодня в мире насчитывается 4,20 млрд пользователей социальных сетей, а это около 53,6% всего населения мира.

Для человека, особенно в условиях пандемии, Интернет создал уникальные возможности для саморазвития, образования, самообразования и трудовой деятельности, информационного обмена, социальной коммуникации и сотрудничества. Данная сеть наполнена не только полезной информацией, она одновременно выступает каналом трансляции угроз и рисков, которые практически

беспрепятственно существуют в Интернете и активно воздействуют на различные категории пользователей. Это порождает проблему информационной безопасности, которая охватывает все области общественной жизни, поэтому компетенции в сфере защиты информации требуются не только от IT-специалистов, но и от любого пользователя персональным компьютером, что отражено в стратегии развития информационного общества РФ на период с 2017 до 2030 года.

В силу возраста наиболее уязвимой категорией в области информационной безопасности выступают подростки, для которых сеть Интернет стала естественной коммуникационной средой, оказывающей влияние на их мировоззрение и поведение. Сегодня 56% школьников в мире имеют собственные аккаунты в социальной сети, за последние три года, как отмечает Росстат, количество домашних хозяйств в России с доступом в интернет выросло в среднем на 4%, из них с помощью мобильного устройства на 15%. Средний возраст школьников, которые входят в учетную запись, составляет 12 лет. Но при всем этом уровень их компетенции в сфере информационной безопасности недостаточный для того, чтобы безопасно использовать привычные и наиболее популярные информационные ресурсы.

Так опасности, с которыми сталкиваются школьники в сети со стороны СМИ, сектантов, «сообществ смерти», активно провоцирующих суицидальные действия, тематических групп, стимулирующих различного рода аддикции, а также вредоносный контент, могут оказать неисправимое на них воздействие. Например, количество сексуальных домогательств, совершенных против несовершеннолетних, с 2014 года выросло на 44%, жертвами интернет-мошенников стали 54% опрошенных детей в возрасте до 18 лет. Следовательно, наибольшей опасностью развития цифровых технологий является разрастающаяся проблема обеспечения информационной безопасности на всех уровнях – от личной до государственной. Комплекс законодательных и организационно-правовых мер в данной сфере направлен на снижение риска негативного влияния, которое может получить ребенок в сети Интернет [1].

Анализ научной литературы позволяет констатировать, что проблема информационной безопасности является междисциплинарной. Так, общим вопросам информационной безопасности посвящены исследования Э. Брандмана, Г.Г. Гафарова, Д.П. Зегжда, В.П. Петрова, С.В. Петрова, С.П. Расторгуева, В.В. Смелянской и др. В данных работах раскрыты информационные угрозы, факторы их вызывающие, а информационная угроза рассматривается как состояние защищенности жизненно важных интересов государства, общества и личности в информационной сфере от влияния внешних и внутренних факторов [2–5 и др.]. Изучению информационной безопасности личности посвящены исследования многих ученых. Причем, если еще лет пять назад основное внимание ученых было направленно на обсуждение вопросов подготовки студентов и старшеклассников к безопасному использованию сети Интернет, то сегодня информационная безопасность подростков становится приоритетной задачей не только государства, но и педагогической науки.

Ведущая роль в обучении школьников основам информационной безопасности в сети Интернет принадлежит школе, имеющей для этого значительные возможности. Соответственно, возникает проблема эффективного обучения подростков основам информационной безопасности как в рамках уроков информатики, так и неурочной работы. Анализ научно-педагогической и психологической литературы показал, что ученые, рассматривая процесс формирования информационной безопасности школьников, акцентируют внимание, либо на особенностях социализации современных подростков в условиях стремительно нарастающих информационных потоков, их психического состояния, прежде всего в информационном пространстве, либо рассматривают отдельные содержательно-методические аспекты в образовательном процессе.

Так, Е.Г. Белякова, Э.В. Загвязинская и А.И. Березенцева, изучая состояния информационной безопасности школьников, выявили роль внешних ограничений и возможностей внутриличностной фильтрации вредоносного интернет-контента в зависимости от возраста детей [7]. Использованию интерактивных методов при обучении школьников основам информационной безопасности по-

священы исследования Х.Н. Арова, Т.Ю. Денщиковой, М.В. Должиковой, И.А. Глущенко, В.А. Петькова, А.С. Доколин, А.Н. Старков.

Анализ исследований других учёных позволяет говорить о том, что в теоретических исследованиях имеется ряд интересных наработок, однако проблема эффективности обучения школьников основам информационной безопасности в сети Интернет остается недостаточно разработана. Следовательно, можно констатировать противоречие, обусловленное, с одной стороны, процессом информатизации всех сфер жизнедеятельности общества и востребованностью в этой связи субъектов общества, обладающих как знаниями в сфере информационной безопасности, так и способностью обеспечивать собственную технологическую, идеологическую и психологическую безопасность и на этой основе объективно анализировать и оценивать поступающую к ним информацию с учетом содержащихся в ней угроз. С другой – потребностью практики в методическом обеспечении процесса обучения школьников основам безопасности в сети Интернет и недостаточной разработанностью данного вопроса в педагогической науке. Данное противоречие определило проблему исследования, которая заключается в поиске наиболее оптимальной активной формы проведения занятий при обучении безопасному поведению в Интернете.

Одной из активных форм проведения занятий по информатике при обучении безопасному поведению в интернете является сторителинг. Это эффективный метод обучения, который сочетает в себе элементы рассказа и педагогического процесса. С помощью сторителинга обучающиеся лучше понимают материал, что ведет к увеличению их активности на занятиях по информатике.

Сторителинг – это такой метод обучения, при котором преподаватель использует рассказы и истории, чтобы привлечь внимание учеников к материалу. Сторителинг предполагает рассказывание истории со своей точки зрения, и использование воображения, чтобы создать образы и персонажей историй.

Мною классифицированы виды киберугроз и в соответствии с этой классификацией для каждого вида придумана история, которая переведена в формат цифрового повествования. В первой истории рассказывается о девушке, кото-

рая решила купить себе автомобиль на так называемом вторичном рынке. Для этого она зашла на один из самых известных сайтов купли-продажи. Там нашла подходящий себе автомобиль и позвонила первому попавшемуся продавцу ничего не проверив. По телефону они договорились о переводе достаточно большого аванса по банковским реквизитам и договорились о встрече. Девушка ничего не подозревая перевела продавцу деньги и поехала на встречу. Но продавец так не появился и перестал отвечать на звонки. Зачастую на данных сайтах выкладывают ложные объявления люди, которые хотят заработать на доверчивости покупателей. Нужно быть бдительнее и доверять только верифицированным (проверенным) профилям.

Рис. 1. История 1

Вторая история гласит о другой девушке, которая, как и большая половина современного общества, не может обойтись без общения онлайн. У неё есть очень много друзей, с которыми она общается в социальной сети ВКонтакте. Однажды ей написала лучшая подруга с просьбой перевести денег на карту, пообещав, что очень скоро их вернёт. Она написала, что деньги нужно перевести не на её карту, а на карту друга. И героиня истории, ничего не подозревая, сразу же перевела деньги на указанную карту, всё-таки лучшая подруга просит. Потом оказалось, что страницу этой подруги взломали и деньги от её лица просили мошенники, которым наша героиня и перевела свои кровные. Нужно быть бдительнее и проверять достоверность личности, с которой общаетесь.

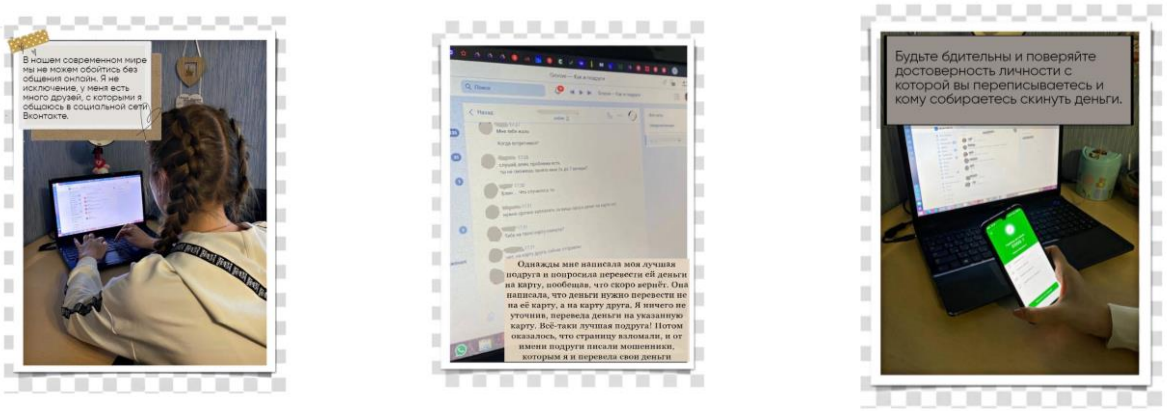

Рис. 2. История 2

Третья история происходит во время каникул. Героиня, занимаясь шопингом, увидела в одном из магазинов телевизор, который ей очень понравился. Но вот цена его была очень высокой. И она решила посмотреть такой же телевизор в интернет-магазине. Не задумываясь, она подключилась к обнаруженной открытой сети «WiFi». Зайдя на сайт интернет-магазина, нашла в точности такой же телевизор, но по цене почти в 3 раза дешевле. Тут же оформила покупку, введя номер банковской карты и трёхзначный код с её обратной стороны. Радовалась героиня истории недолго, так как данными завладели мошенники и с помощью них завладели денежными средствами с карты. Нельзя передавать данные через общественную сеть «WiFi».

Рис. 3. История 3

А в последней истории рассказывается о девушке, которая решила посмотреть фильм. Для этого она зашла на первый сайт в поисковике. Там неожиданно

высветилась реклама, в которой говорилось о тысячах, миллионах рублей. Нажав на эту рекламу, героиня потеряла управление над своим компьютером, как будто кто-то удалённо начал им управлять. Впоследствии оказалось, что от её имени были разосланы письма с просьбой дать денег взаймы. Также были похищены её конфиденциальные данные. Нельзя открывать подозрительные письма и ссылки!

Рис. 4. История 4

Таким образом, сторителинг – это эффективный метод обучения безопасному поведению в Интернете. Он позволяет обучающимся лучше запоминать информацию, развивать критическое мышление.

Список литературы

1. Зегжда Д.П. Основы безопасности информационных систем / Д.П. Зегжда, А.М. Ивашко. – М.: Горячая линия-Телеком, 2000.

2. Осин А.К. Педагогическая система формирования мотивации и самоорганизации учебной деятельности учащихся сельской школы: дис. … канд. пед. наук: 13.00.01 / А.К. Осин. – Шуя, 2000. – 171 с. – EDN NLUAPP

3. Осин А.К. Проектирование внеурочной деятельности в инновационной парадигме новых стандартов / А.К. Осин // Научный поиск. – 2015. – №3.6. – С. 32–38. – EDN UMJXCN

4. Петров В.П. Информационная безопасность человека и общества: учебное пособие / В.П. Петров, С.В. Петров. – М.: ЭНАС, 2007. – EDN SDQVYR

5. Рыбакова О.С. Законодательное регулирование обеспечения безопасности ребенка в интернет-пространстве / О.С. Рыбакова // Правовая информатика. – 2017. – №4. – С. 49–54. – EDN YQRLPB

6. Романова М.В. Методика обучения школьников основам безопасности в сети Интернет / М.В. Романова, Е.В. Чернова [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/metodika-obucheniya-shkolnikov-osnovam-bezopasnosti-v-seti-internet (дата обращения: 10.07.2024).