Медведева Екатерина Андреевна
бакалавр, учитель
МБОУ «Яльчикская СОШ
им. Героя России Н.А. Петрова»
с. Яльчики, Чувашская Республика

DOI 10.21661/r-588285

ФОРМИРОВАНИЕ НАВЫКОВ ИНТЕРНЕТ-БЕЗОПАСНОСТИ У ШКОЛЬНИКОВ: ПЕДАГОГИЧЕСКИЙ ОПЫТ

Аннотация: *в статье рассматривается тема повышения цифровой грамотности и формирования безопасного поведения в интернете для защиты персональных данных и цифровой репутации. Актуальность темы обусловлена ростом киберпреступности и повсеместной цифровизацией всех сфер жизни. Автор предлагает сценарий познавательной беседы с молодежной аудиторией, в ходе которой в формате живого диалога разбираются основные виды киберугроз: социальная инженерия, фишинг, кэтфишинг и кибербуллинг. Особое внимание уделяется выработке критического мышления и практическим навыкам распознавания мошеннических схем.*

Ключевые слова: *профилактика, социальная инженерия, фишинг, подростки, кибербезопасность, цифровая грамотность, защита персональных данных, киберугрозы, кибербуллинг, цифровая репутация, безопасное поведение в интернете, кэтфишинг.*

Цель.

Повысить цифровую грамотность пользователей, сформировать осознанное и безопасное поведение в интернете для защиты персональных данных и цифровой репутации от современных киберугроз.

Задачи:

– информировать аудиторию о спектре основных киберугроз: фишинг, социальная инженерия, кража личных данных, мошенничество в соцсетях;

– сформировать критическое мышление для оценки достоверности информации и распознавания мошеннических схем.

Актуальность.

Рост киберпреступности: объем и изощренность кибератак растут с каждым годом.

Повсеместная цифровизация: банкинг, госуслуги, общение, работа и хранение личных фото – вся жизнь переместилась в онлайн, что делает защиту цифровой идентичности критически важной.

Защита детей и подростков: подрастающее поколение, являясь активными пользователями сети, особенно уязвимо для кибербуллинга, кэтфишинга и нежелательного контента.

Целевая аудитория.

Родители и педагоги: лица, ответственные за безопасность детей в интернете, нуждающиеся в знаниях о родительском контроле и основах цифрового воспитания.

Подростки и студенты: активные пользователи соцсетей и онлайн-игр, часто недооценивающие последствия неосторожного поведения в сети (размещение личной информации, общение с незнакомцами).

Форма занятия.

Познавательная беседа, живой диалог. Акцент делается на обмен мнениями, разбор конкретных ситуаций из жизни и совместный поиск безопасных решений.

Ход разговора.

Вступление.

– Ребята, поднимите руку, кто сегодня уже заходил в интернет. Соцсеть, игру, либо просто что-то гуглил... Практически все. А теперь поднимите руку, кто уверен, что интернет – это безопасно, и там нет вещей, которых нужно бояться?

– Вижу, что уверенности меньше. И это нормально и даже правильно.

– Интернет – как большой город. В нём есть библиотеки, парки развлечений, школы, кинотеатры, место для шоппинга или встречи с друзьями. Но есть и тёмные переулки, в которые лучше не сворачивать.

Основная часть.

Опрос ребят.

– А что это за тёмные переулки? Какие опасности нас могут поджидать в огромном городе «Интернет»?

– (*ответы ребят*) мошенники, хейтеры, взломщики и другие.

– Были ли у вас подобные случаи? Расскажите!

– *(ответы ребят)* приходят сообщения с подозрительной ссылкой, с просьбой проголосовать в конкурсе, сообщения о взломе или блокировке и т. п.

Характеристики угроз.

– Все эти угрозы можно распределить на группы.

Угроза №1. «Социальная инженерия».

– Ребят, слышали об этом? Это психологическая манипуляция, обман, игра на доверии или чувствах, чтобы мы сами отдали свои данные или деньги. Классика жанра: «Ваш родственник в беде»

– (*ответы ребят*) записывают голосовое: «Сынок, срочно нужны деньги на неотложное дело на карту…». А голос точь-в-точь мамин!

– Что делаем? *Немедленно звоним по телефону напрямую человеку!*

– «Привет, срочно! Скинь, пожалуйста, код из SMS, мне нужно войти в вк с другого телефона, мой телефон сейчас сядет».

– И это значит только одно. Что? *Что вашего друга взломали.*

– Код! Это ваше цифровое оружие. Никогда никому ни при каких обстоятельствах не сообщаем код!

Угроза №2. «Фишинг».

– Слышали, ребята? Как понимаете значение слова?

– (*ответы ребят*) ловля данных.

– Верно! Мошенники жаждут украсть нашу «Цифровую личность», а именно: логины, пароли, данные карт.

– Приходят сомнительные ссылки от типа «несомнительных компаний»: Банк, Почта, Теле2, госуслуги, ВКонтакте. Под каким предлогом приходят сообщения?

– (*ответы ребят*) «твой аккаунт взломали, срочно смени пароль!» – и ссылка на фальшивый сайт, похожий на ВК»: vk-security.ru, vk123.com.

– Что происходит, когда человек проходит по ссылке?

– Вводит свои данные и сливает их мошенникам.

Угроза №3. «Кэтфишинг».

– Слышали, ребята?

– Мошенник создаёт вымышленный привлекательный образ, выдавая себя за другого человека. Зачем?

– (*ответы ребят*) получить выгоду, нажиться.

– Где и как? Например, в мессенджерах притворяются богатыми и успешными людьми, которые ищут тех, кто хочет заработать лёгкие деньги.

Угроза №4. «Кибербуллинг».

– Что это значит?

– (*ответы ребят*)

– Хамы, тролли, провокаторы пишут негативные комментарии, отправляют агрессивные сообщения, чтобы вывести вас на эмоции и нанести психологический вред.

– Ситуация: В школьном чате появляется провокатор. Он начинает оскорблять, унижать, выкладывать ваши неприятно переделанные фото. Чего он добивается? Вашей реакции! Чтобы всё, что вы ему ответите, использовать против вас.

– Что делать?

– (*ответы ребят*): лучшая реакция на тролля – игнор. Заблокировать и доложить администрации. Для него наши эмоции – это еда. Не будем его кормить.

Задание для закрепления.

– Соотнесём виды угроз и их значения *(материал выведен на доску/презентация)*.

Таблица 1

Социальная инженерия	Психологический взлом
Фишинг	Кража цифрового «Я»

Кэтфишинг	Опасные знакомства
Кибер-буллинг	Травля

Разбор ситуаций.

Определить:

– вид угрозы;

– признаки;

– дальнейшие действия.

Ситуация №1.

Ответы:

– социальная инженерия;

– ключевое слово «победителем», игра на эмоциях;

– не сообщать код.

Ситуация №2.

Ответы:

– фишинг;

– подозрительная ссылка от «неподозрительного» телеграма;

– заблокировать и не переходить.

Ситуация №3.

Ответы:

– кэтфишинг;

– предлагают им сделать инвестиции с целью приумножения, входят в доверие, присылают первый заработок. Но однажды при переводе крупной суммы деньги так и не возвращаются;

– блок, игнор.

Ситуация №4.

Ответы:

– социальная инженерия;

– личная неприкосновенность, воздействие на эмоции;

– блок, игнор.

Ситуация №5.

Ответы:

– фишинг;

– подозрительная ссылка, от ошибочного «Tiknoff»;

– заблокировать и не переходить.

Ситуация №6.

Ответы:

– кибербуллинг;

– оскорбление, неуважение;

– зафиксировать скрины, доложить администрации школы/игнор.

Ситуация №7.

Ответы:

– социальная инженерия;

– манипуляция;

– блок, игнор.

Заключение.

– Ребята, давайте повторим общие правила безопасного поведения в сети.

(…ответы ребят):

– *сложный пароль* (*с цифрами и символами*);

– *двойная аутентификация* (*чтобы приходил код подтверждения*);

– *не переходить по ссылкам*;

– *не переписываться с незнакомцами*;

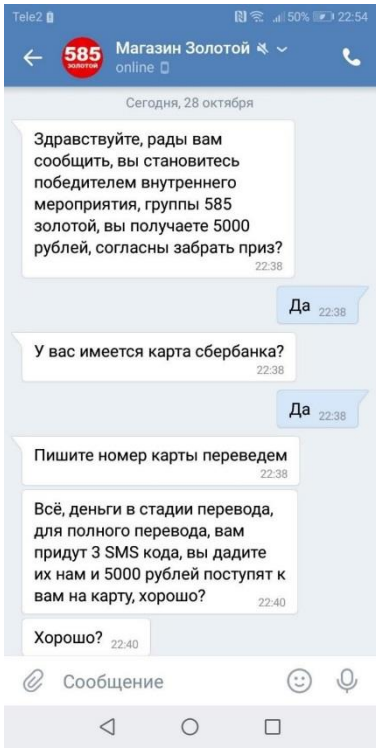
– *не присылать код*;

– *перезванивать близким при сообщениях на тему*: «*Ваш родственник в беде*».

– Сегодня мы с вами поговорили о том, с какими опасностями можем столкнуться в сети Интернет и как их избежать. Ознакомьтесь с памятками, ребята! *(Раздать памятки на тему: «Правила безопасного поведения в интернете»)*. И пусть бдительность будет всегда рядом с нами, чтобы при прогулке случайно не завернуть ни на один из подобных тёмных переулков.

Приложение

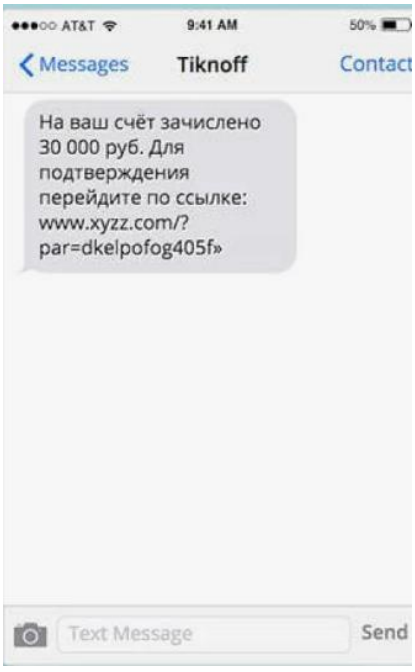
Ситуация №1



Ситуация №2

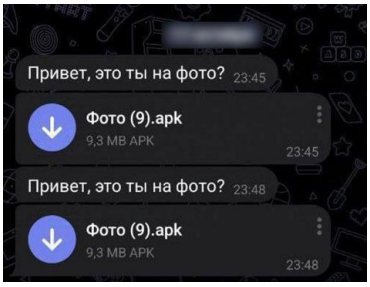
Ситуация №3

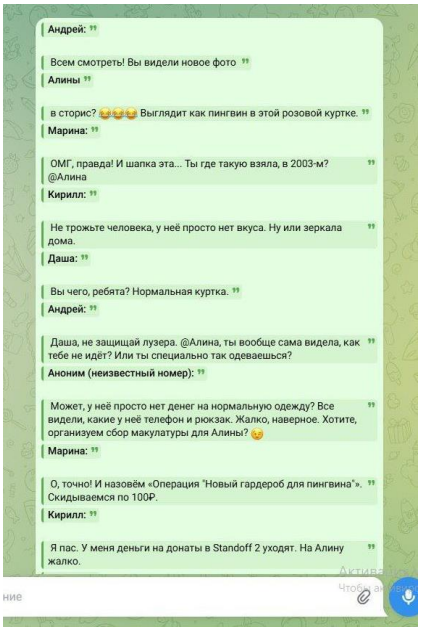
Ситуация №4



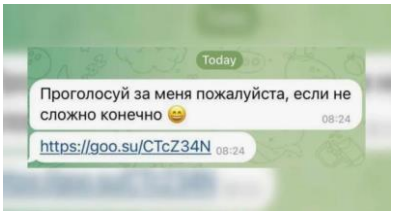
Ситуация №5

Ситуация №6





Ситуация №7



Список литературы

1. Солдатова Г.У. Цифровое поколение России: компетентность и безопасность / Г.У. Солдатова, Е.И. Рассказова, Т.А. Нестик. – М.: Смысл, 2017. – 375 с. EDN XUPTRZ

2. Клименко О.А. Информационная безопасность и защита информации: учеб. пособие / О.А. Клименко. – М.: РИОР: ИНФРА-М, 2020. – 324 с.

3. Бочаров М.И. Технологии защиты информации в интернете: советы профессионала / М.И. Бочаров. – СПб.: Питер, 2019. – 288 с.