Рабочая программа модулей дополнительной общеобразовательной общеразвивающей программы “Безопасный кибермир для пожилых людей”

Аннотация

Дополнительная общеобразовательная общеразвивающая программа “Безопасный кибермир для пожилых людей” представляет собой обучающий курс, который состоит из 4 занятий и рассчитан на 1 месяц. Уроки проходят 1 раз в неделю и длятся по 2 академических часа, с перерывом в 15 минут между ними.

Программа предназначена для людей старшего возраста, которые хотят освоить основы безопасного использования интернета и электронных устройств.

Участники получат знания о том, как защитить свои личные данные, как избежать мошенничества в интернете и телефонного мошенничества, как использовать социальные сети безопасно, как защитить свою персональную информацию.

Занятия проводятся в формате лекций и практических занятий, где участники могут задавать вопросы и получать ответы от опытных специалистов в области психологии и информационных технологий. Программа также включает встречу с представителями правоохранительных органов, которые расскажут о том, как защитить себя от киберпреступников и куда обращаться за помощью в случае необходимости.

Максимальное количество учеников в группе - 10 человек.
Возраст: 50+

Срок реализации: 1 месяц

Учебно-тематический план

Тема	Виды учебных занятий, учебных работ	Содержание
Тема 1. Основы безопасности в IT		
Урок № 1.	2	1. Вредоносное ПО Что такое вредоносное ПО, каким оно может быть, как попадает на

		наши устройства. Что делать, чтобы защитить себя. 1.1 Антивирусы Что это такое, как работают и каким функционалом обладают. Какими они бывают и как правильно ими пользоваться.
		2. Аутентификация 2.1 Аутентификация, логины и пароли. Как это работает и почему это важно. Как правильно выбрать пароль. Примеры плохих и хороших паролей. 2.2 Менеджеры паролей. Что это такое, какими бывают и как работают. Можно ли им доверять и как выбрать. 2.3 Двухфакторная аутентификация Что это такое, какие у неё преимущества, какой она бывает, как её настроить.
		3. Электронная почта. Почему она так важна, и как её защитить. 3.1 Письма-вирусы 3.2 Письма-спам 3.3 Черные списки и спам списки. Что это такое, как пользоваться на телефоне и на разных сервисах.
		4. Сайты 4.1 Поддельные сайты. Что это такое, зачем их создают и как их распознать. Примеры фейковых и настоящих сайтов. 4.2 Поддельные ссылки. Какая в них опасность, как распознать и что с ними делать. 4.3 Сокращенные ссылки. Что это такое и для чего используется. Какие сервисы для этого бывают, примеры. 4.4 Безопасное соединение, протокол HTTPS. Что это, для чего нужен, где он указан.
		5. Приложения 5.1 Установщики приложений и места их получения. Где и как можно безопасно скачать

		приложение, как его установить. 5.2 Сбор данных приложениями. Какие данные собирают приложения, как можно это проверить и на что обратить внимание. 5.3 Пользование публичными сетями для доступа в приложения и на сайты. 5.4 Геопозиция. Что это, для чего нужно и как не раскрывать её без необходимости. 5.5 Размещение личное информации в соц.сетях и мессенджерах. Личная информация в закрытых чатах или серверах. 5.6 Разрешения для приложений. Что это такое, как контролировать и настраивать.
		6. Конфиденциальные данные 6.1 Опасности хранения конфиденциальных сведений на устройствах, в приложениях и электронной почте. 6.2 Запрос СМС на сайтах. В чем опасность. 6.3 «Бесплатные» предложения. 6.4 Пользование облаками для хранения данных.
Тема 2. Психология и безопасность в цифровом мире		
Урок №2	2	**Виды мошенничества в интернете:** 1. Онлайн-инвестиции: Мошенники могут предлагать пожилым людям инвестировать в различные проекты, которые на самом деле являются мошенническими. 2. Онлайн-знакомства: Мошенники могут создавать фальшивые профили и обманывать пожилых людей, предлагая им знакомства или романтические отношения. 3. Лотерея: Мошенники могут предлагать пожилым людям участвовать в лотереях, которые на самом деле являются мошенническими. 4. Поддельные лекарства по рецептам: Мошенники могут предлагать пожилым людям поддельные лекарства по рецептам, которые на самом деле не работают или могут быть опасными.

		5. Техническая поддержка: Мошенники могут представляться техническими специалистами и предлагать пожилым людям помощь в решении проблем с компьютером или интернетом, но на самом деле обманывать их. 6. Антивозрастные продукты: Мошенники могут предлагать пожилым людям антивозрастные продукты, которые на самом деле не работают или могут быть опасными. 7. Похороны и ритуальные услуги: Мошенники могут предлагать пожилым людям услуги по организации похорон и ритуальных услуг, которые на самом деле являются мошенническими.
		Манипуляции, используемые мошенниками: 1. Угрозы: Мошенники могут угрожать пожилым людям, чтобы заставить их отдать свои деньги или личные данные. 2. Лесть: Мошенники могут льстить пожилым людям, чтобы заставить их доверять им и отдать свои деньги или личные данные. 3. Сочувствие: Мошенники могут использовать сочувствие, чтобы заставить пожилых людей отдать свои деньги или личные данные. 4. Обещания: Мошенники могут обещать пожилым людям большие выигрыши или другие выгоды, чтобы заставить их отдать свои деньги или личные данные.
		Как правильно реагировать: 1. Умение успокоиться: Пожилые люди должны научиться сохранять спокойствие и не поддаваться на манипуляции мошенников. 2. Скрипт разговора с мошенником: Пожилые люди должны знать, как правильно реагировать на звонки или сообщения от мошенников, чтобы не стать жертвой мошенничества. 3. Цифровая грамотность: Пожилые люди должны знать, как защитить свои личные данные, создавать надежные пароли, не делиться личной информацией в интернете и распознавать фишинговые сайты.
Тема 3. Встреча с правоохранительными органами		
Урок №3	2	1. Рассказ о самых распространенных схемах мошенничества в отношении пожилых людей 2. Ответственность за киберпреступления.

		3. Статистика
Тема 3. Итоговая аттестация: проверка полученных знаний		
Урок №4		Интерактивная игра “Безопасный кибермир”
ИТОГО	**8 ак часов**	

Оценочные материалы

Реализация программы предусматривает текущий контроль, итоговую аттестацию обучающихся.

Текущий контроль проводится в течение освоения каждой темы программы. Текущий контроль включает следующие формы: наблюдение, ответы на вопросы преподавателя.

Итоговый контроль осуществляется в формате соревнования. Обучающиеся разбирают различные ситуации, связанные с безопасностью в сети интернет, устно отвечают на вопросы интерактивной игры, выбирают ответ из предложенных вариантов.

Учебно-методические материалы

1. Бойцев, О.М. Защити свой компьютер на 100% от вирусов и хакеров / Олег Михайлович Бойцев. – Санкт-Петербург : Питер, 2008. – 288 с. : ил.
2. Варюхина, Л. Безопасный интернет. Как избежать беды? / Лилия Варюхина // Наша Молодежь. – 2017. – N 6. – С. 5.
3. Прохоров, А.Н. Интернет : как это работает / А.Н. Прохоров. – Санкт-Петербург : БХВ-Петербург, 2004. – 280 с. : ил.
4. Интернет-энциклопедия. Какие кнопки нажимать / авт.-сост. Виталий Ильич Копыл. – Минск : Харвест, 2006. – 320 с. : ил.

Материально-техническая и ресурсная база

1. Учебная аудитория на 20 человек.
2. Компьютеры по количеству учащихся и для преподавателя. Требование к компьютеру: Процессор Intel Core i3, Оперативная память минимум — 4 ГБ, Общий объём жестких дисков (HDD):500 ГБ, Операционная система: Windows
3. Интерактивная панель для демонстрации презентаций и игры
4. Выделенная линия интернет 10 Мбит/сек.