Утверждаю:
Приказ № 01 от «01» декабря 2024 г.
ИП Черных И.В.

ДОПОЛНИТЕЛЬНАЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ОБЩЕРАЗВИВАЮЩАЯ ПРОГРАММА

Безопасный кибермир для пожилых людей

Возраст обучающихся: 50+
Срок реализации: 1 месяц

г. Псков
2024 г.

Раздел 1. Пояснительная записка

1.1. Актуальность программы

Цифровая безопасность - это набор мер и практик, которые помогают защитить личные данные, деньги и устройства от злоумышленников в цифровом мире. Для пожилых людей, которые могут быть менее знакомы с цифровыми технологиями и более уязвимы для мошенничества, цифровая безопасность особенно важна.

Одной из основных угроз для пожилых людей в цифровом мире является мошенничество. Злоумышленники могут использовать различные методы, чтобы получить доступ к личным данным пожилых людей, таким как номера банковских карт или пароли. Цифровая безопасность помогает пожилым людям защитить свои данные от таких атак.

Еще одной угрозой является фишинг. Фишинг - это метод мошенничества, при котором злоумышленники пытаются получить доступ к личным данным, отправляя поддельные электронные письма или сообщения. Цифровая безопасность помогает пожилым людям распознавать и избегать таких атак.

Вредоносные программы также могут нанести серьезный ущерб компьютеру или мобильному устройству. Цифровая безопасность помогает пожилым людям защитить свои устройства от таких программ.

Кроме того, злоумышленники могут использовать украденные личные данные для совершения преступлений, таких как кража личности или мошенничество. Цифровая безопасность помогает пожилым людям защитить свои данные от кражи.

Наконец, хакеры могут получить доступ к компьютерам или мобильным устройствам пожилых людей и использовать их для совершения преступлений. Цифровая безопасность помогает пожилым людям защитить свои устройства от хакерских атак.

В целом, цифровая безопасность помогает пожилым людям оставаться активными, защищенными и информированными в современном цифровом мире. Она позволяет им использовать цифровые технологии для общения, управления финансами, слежения за здоровьем и образования, не опасаясь стать жертвами мошенников или злоумышленников.

1.2. Направленность программы

Направленность программы - техническая (информационные технологии).

1.3. Цель реализации программы

Цель реализации программы "Безопасный кибермир для пожилых людей” заключается в повышении уровня цифровой грамотности и безопасности среди этой группы населения. Программа направлена на обучение пожилых людей навыкам использования цифровых технологий, включая социальные сети, онлайн-банкинг, электронную почту и другие инструменты, а также на предоставление информации о рисках и угрозах в цифровом мире и способах их предотвращения.

1.4. Задачи реализации программы

1. Ознакомление пожилых людей с основами цифровой грамотности и безопасности в киберпространстве.
2. Обучение пожилых людей навыкам критического мышления и оценки информации в интернете.

3. Развитие у пожилых людей умений и навыков безопасного использования различных цифровых инструментов и технологий.
4. Обучение пожилых людей распознаванию и противостоянию телефонному мошенничеству, онлайн-мошенничеству и другим формам интернет-угроз.
5. Формирование у пожилых людей навыков безопасного общения и взаимодействия в социальных сетях и других формах онлайн-коммуникации.
6. Обучение пожилых людей основам информационной безопасности и защиты персональных данных в цифровом мире.

1.5. Адресат программы

Возраст обучающихся по программе - старше 50 лет.

Пожилые люди наиболее уязвимы перед мошенниками в жизни и интернете по нескольким причинам:

1. Недостаток знаний: Пожилые люди могут не иметь достаточных знаний о цифровых технологиях и не знать, как защитить свои личные данные и деньги от мошенников.

2. Доверие: Пожилые люди могут быть более доверчивыми и не подозревать, что кто-то может попытаться обмануть их.

3. Одиночество: Пожилые люди могут быть более одинокими и искать общения, что может сделать их более уязвимыми для мошенников, которые могут использовать это в своих интересах.

4. Финансовые проблемы: Пожилые люди могут иметь финансовые проблемы и быть более уязвимыми для мошенников, которые могут предложить им помощь или обещания, которые не могут быть выполнены.

5. Недостаток поддержки: Пожилые люди могут не иметь поддержки со стороны близких или друзей, которые могли бы помочь им в случае мошенничества.

Все это делает необходимым обучение пожилых людей цифровой грамотности и безопасному поведению в интернете для защиты их от возможных рисков и угроз.

1.6. Планируемые результаты обучения

В результате обучения у обучающихся будут сформированы следующие навыки:

1. Увеличение уровня цифровой грамотности среди пожилых людей: Пожилые люди будут иметь базовые знания о том, как использовать компьютер, интернет и мобильные устройства, а также как защитить свои личные данные и деньги от мошенников.
2. Уменьшение количества случаев мошенничества: Пожилые люди будут более осведомлены о различных видах мошенничества и способах их предотвращения, что приведет к уменьшению количества случаев мошенничества.
3. Улучшение качества жизни пожилых людей: Пожилые люди будут иметь возможность использовать цифровые технологии для улучшения своей жизни, например, для общения с друзьями и семьей, управления своими финансами и отслеживания своего здоровья.
4. Увеличение уровня безопасности в цифровом мире: Пожилые люди будут знать, как защитить свои личные данные и деньги от мошенников, что приведет к увеличению уровня безопасности в цифровом мире.
5. Улучшение психологического состояния пожилых людей: Пожилые люди будут чувствовать себя более уверенно и защищенно в использовании цифровых технологий, что может улучшить их психологическое состояние.

1.7. Форма обучения

Форма обучения: очная.

1.8. Режим занятий

Срок реализации программы: 1 месяц, 4 занятия

Количество часов по программе – 8 академических часов.

Занятия проводятся 1 раз в неделю, по 2 академических часа с перерывами между академическими часами 15 минут. Академический час равен 40 минутам.

Занятия - групповые, сочетается принцип группового обучения с индивидуальным подходом.

Количество обучающихся в группе - до 10 человек.

Раздел 2. Учебный план программы

№	Наименование разделов (модулей) и тем	Всего ак. часов	Виды учебных занятий, учебных работ		Неделя обучения
			Теор. занятия	Практ. занятия	
1	Тема 1. Основы безопасности в IT	2	2	0	1
2	Тема 2. Психология и безопасность в цифровом мире	2	2	0	2
3	Тема 3. Встреча с правоохранительными органами	2	2		3
3	Итоговая аттестация: проверка полученных знаний	2	0	2	4
	Итого	8	6	2	

Раздел 3. Календарный учебный график

Календарный учебный график формируется при осуществлении обучения в течение всего календарного года. По мере набора групп слушателей по программе составляется график, учитывающий объемы лекций, практики, самоподготовки.

Количество занятий: 4 по 2 академических часа.
Количество занятий в неделю: 1

Раздел 4. Рабочая программа

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	

Раздел 5. 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.

Раздел 6. 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.

6.1 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.