

Программа занятий

в целях создания условий для укрепления здоровья, увеличения периода активного долголетия и продолжительности здоровой жизни граждан старшего поколения в Тюменской области
по направлению просвещение, получение дополнительных знаний по различным направлениям

Паспорт программы

Название Программы	«Кибербезопасность для граждан пенсионного возраста»
Цели и задачи Программы	Цель: Удовлетворение индивидуальных образовательных потребностей граждан старшего возраста в получении основ знаний и навыков в сфере информационной безопасности для успешной адаптации к требованиям жизни в цифровом обществе. Задачи: 1. Повышение грамотности в вопросах безопасного поведения в цифровой среде. 2. Формирование знаний о наиболее распространенных кибератаках, вредоносных программах и методах социальной инженерии. 3. Обучение практическим навыкам защиты устройств, аккаунтов и личных данных. 4. Снижение рисков стать жертвой кибермошенничества через просвещение.
Целевая аудитория	Женщины в возрасте от 55 лет и мужчины от 60 лет (граждане пенсионного возраста), являющиеся пользователями цифровых устройств или планирующие ими пользоваться.
Краткое описание Программы	Образовательный курс, направленный на формирование у пожилых людей компетенций в области кибербезопасности. Программа включает изучение основных киберугроз, правил создания надежных паролей, методов защиты аккаунтов и мобильных устройств, а также алгоритмов действий в случае взлома или попытки мошенничества.
Срок (период) реализации и объем Программы	Срок обучения: 3 месяца. Объем: 40 академических часов (включая лекции, практику и итоговое тестирование).
Формат проведения мероприятий Программы	Очный (с применением компьютерного и мультимедийного оборудования).
Форма проведения мероприятий Программы	Групповые занятия (лекции, мастер-классы, практические занятия с элементами тренинга). Количественный состав группы: до 25 человек.

Периодичность, продолжительность занятий	Занятия проводятся 1–2 раза в неделю в будние дни (дневное время). Продолжительность одного занятия определяется в соответствии с учебным планом
Приемы, методы, методики, использованные в Программе	Информационно-просветительский метод (лекции с презентациями), практико-ориентированный метод (решение ситуационных задач, отработка навыков), наглядный метод (демонстрация схем мошенничества, использование манекенов и реквизита), метод анализа конкретных ситуаций (разбор реальных случаев обмана).
Рекомендации к уровню подготовки (компетенциям, опыту) специалистов, реализующих мероприятия по Программе	Специалисты, имеющие высшее или среднее профессиональное образование и опыт работы в одной из следующих сфер: IT и кибербезопасность, юриспруденция, банковская деятельность, психология, правоохранительные органы, социальное обслуживание. Преподаватели должны владеть актуальными данными о мошеннических схемах и методиками работы с возрастной аудиторией.
Рекомендации (требования) к материально-техническому обеспечению Программы	Оборудованная аудитория с возможностью демонстрации презентаций (проектор/экран, ноутбук), доступ к сети Интернет (по возможности), наглядные пособия (буклеты, памятки, листовки), а также специальный реквизит, используемый для моделирования ситуаций обмана.
Ожидаемые результаты	В результате освоения программы слушатели будут: Знать: основные виды кибератак и вредоносных программ, признаки мошенничества. Уметь: создавать надежные пароли, защищать личную информацию, настраивать безопасность аккаунтов. Владеть: алгоритмами действий при подозрении на взлом устройства, способами резервного копирования данных. Уровень освоения определяется по итогам итогового тестирования.
Информация о разработке Программы	Тюменский региональный благотворительный фонд «Старшее поколение». Автор программы: И.А. Богунова.

Тематический план

№ п/п	Наименование темы	Количество часов/форма обучения (очно/заочно/дистант)		
		Лекция	Практическое занятие	Самостоятельн ая работа
Раздел 1. Введение в кибербезопасность				
1.	Основные функции кибербезопасности. Наиболее распространенные кибератаки.	1	1	-
2.	Вредоносные программы и методы	1	1	-

	их распространения.			
3.	Понятие информационной безопасности личности (защита от манипуляций).	1	1	-
Раздел 2. Киберпреступники и методы обмана				
4.	Кибервзломщики и их классификация. Социальная инженерия как основной метод обмана пожилых.	1	-	-
5.	Анализ реальных мошеннических схем: звонки от "родственников", лжесотрудники, СМС-выигрыши.	1	2	-
Раздел 3. Оценка текущего состояния безопасности				
6.	Определение способов защиты. Оценка текущих мер безопасности.	1	2	-
Раздел 4. Безопасность устройств				
7.	Безопасность мобильных устройств. Человеческий фактор и правила использования гаджетов.	1	2	-
Раздел 5. Безопасность аккаунтов				
8.	Стратегии сохранения данных у третьих лиц.	1	2	-
9.	Обеспечение безопасности платежных, банковских и торговых счетов.	1	2	-
Раздел 6. Пароли				
10.	Как создать надежный пароль. Хранение паролей.	1	2	-
11.	Виды аутентификации. Защита от «социальной инженерии» (практика отработки отказов).	1	1	-
Раздел 7. Признаки взлома				
12.	Выявление признаков нарушения кибербезопасности (признаки взлома, вирусы).	1	1	-
13.	Практические методы устранения нарушения (антивирусы, настройки).	1	2	1
Раздел 8. Восстановление после взлома				
14.	Что делать, если компьютер/телефон подвергся взлому (алгоритм действий).	1	2	-
15.	Восстановление устройства без помощи профессионала (сброс, резервное копирование).	1	2	-
16.	Итоговое тестирование (контроль	-	1	-

	знаний)			
	ИТОГО:	15	24	1

Содержание занятий

Раздел 1. Введение в кибербезопасность

Лекция (3 ч.) + Практика (3 ч.). Понятие кибербезопасности, ее роль в жизни пожилого человека. Анализ международной и российской статистики старения населения и рисков, связанных с цифровизацией. Обсуждение уязвимости пожилых людей: доверчивость, низкая компьютерная грамотность, психологические особенности. Вредоносное ПО и классификация кибератак.

Раздел 2. Киберпреступники и методы обмана

Лекция (2 ч.) + Практика (3 ч.). Кто такие социальные инженеры. Разбор типичных сценариев: телефонное мошенничество (звонки из "банка", "полиции"), мошенничество с "выигрышами", визиты лже-сотрудников (соцзащита, ЖКХ, медицина). *Практика: просмотр и обсуждение видеороликов с записями реальных звонков мошенников.*

Раздел 3. Оценка текущего состояния безопасности

Лекция (1 ч.) + Практика (2 ч.). Как проверить свои устройства на уязвимости. Помощь слушателям в оценке их текущих привычек (использование одинаковых паролей, хранение данных). *Практика: заполнение чек-листа "Насколько вы защищены".*

Раздел 4. Безопасность устройств

Лекция (1 ч.) + Практика (2 ч.). Физическая защита смартфонов и компьютеров. Биометрическая защита (отпечаток пальца, Face ID) и ее преимущества. *Практика: настройка блокировки экрана на учебных устройствах.*

Раздел 5. Безопасность аккаунтов

Лекция (2 ч.) + Практика (4 ч.). Защита личных кабинетов на Госуслугах, в банковских приложениях и соцсетях. Риски хранения данных у третьих лиц. *Практика: упражнение по настройке двухфакторной аутентификации (на примере учебного аккаунта).*

Раздел 6. Пароли

Лекция (4 ч.) + Практика (2 ч.). Правила создания сложного, но запоминающегося пароля. Парольные менеджеры: за и против. Защита от фишинга и социальной инженерии. *Практика: тренинг "Угадай пароль" и отработка навыка вежливого отказа мошеннику по телефону.*

Раздел 7. Признаки взлома

Лекция (2 ч.) + Практика (3 ч.) + Самост. (1 ч.). Симптомы заражения устройства: медленная работа, всплывающие окна, подозрительные СМС. Действия при подозрении на утечку данных. *Практика: запуск антивирусного сканирования, обновление операционной системы. Самостоятельная работа: чтение памяток по кибергигиене.*

Раздел 8. Восстановление после взлома

Лекция (2 ч.) + Практика (5 ч.). Алгоритм экстренных действий при взломе (звонки в банк, смена паролей, блокировка сим-карты). Создание и восстановление из резервной копии. *Практика: демонстрация процесса сброса настроек без потери данных.*