**Учебный план курса «Основы кибербезопасности и искусственного интеллекта»**

**Продолжительность:** 16 академических часов   
**Форма обучения:**лекции, практические занятия, групповые обсуждения   
**Целевая аудитория** : пенсионеры, желающие освоить основы цифровой безопасности и понять, как работает искусственный интеллект (ИИ)

**Модуль 1: Введение в цифровую безопасность (4 часа)**

**Занятие 1: Основы кибербезопасности (2 часа)**

* Что такое кибербезопасность и почему она важна
* Основные угрозы в Интернете: вирусы, фишинг, мошенничество.
* Как защитить свои персональные данные

**Занятие 2: Безопасность безопасного устройства (2 часа)**

* Надежные пароли и двухфакторная аутентификация
* Как распознать мошенничество в интернете
* Безопасность при использовании Wi-Fi и сетей общего пользования

**Модуль 2: Искусственный интеллект и его применение (4 часа)**

**Занятие 3: Что такое искусственный интеллект? (2 часа)**

* Основные понятия: машинное обучение, нейросети.
* Где мы встречаем ИИ в повседневной жизни
* Возможности и ограничения II

**Занятие 4: Опасности и этика II (2 часа)**

* Мошенничество с использованием ИИ
* Фейки и дипфейки: как их распознать
* Этика и границы использования II

**Модуль 3: Практическое использование цифровых технологий (4 часа)**

**Занятие 5: Работа с браузером и безопасный серфинг (2 часа)**

* Как правильно пользоваться поисковыми жизнями
* Расширения для браузера, повышающие безопасность
* Блокировка рекламы и защита от авторитетных сайтов

**Занятие 6: Социальные сети и мессенджеры (2 часа)**

* Настройки конфиденциальности в соцсетях
* Как распознать фейковые аккаунты
* Защита от мошенничества в WhatsApp, Telegram и других мессенджерах

**Модуль 4: Практическое знакомство с искусственным интеллектом (4 часа)**

**Занятие 7: Как ИИ помогает в жизни (2 часа)**

* Голосовые помощники (Алиса, Siri, Google Assistant)
* Автоматические переводчики и генерация текста
* Как использовать ИИ для поиска информации

**Занятие 8: Итоговое занятие и вопросы-ответы (2 часа)**

* Подведение итогов: что важно исправить
* Разработка сложных ситуаций на примерах
* Ответы на вопросы слушателей

**Методы обучения:**

* Демонстрация на экране
* Обсуждение примеров
* Практические задания (создание паролей, проверка сайтов, работа с ИИ)
* Выбор типичных ошибок пользователей

**Результаты курса:**

По окончании курса участники имеют возможность:   
✅ Распознавать основные интернет-угрозы и вирусы от них   
✅ Наладки безопасного прослушиваемого доступа в интернет и соцсети   
✅ Использовать ИИ в повседневной жизни без риска   
✅ Определять фейковые новости и мошенничество

Курс ориентирован на простое объяснение сложной темы, с акцентом на практике. Будет полезно всем, кто хочет уверенно пользоваться интернетом и новыми технологиями!