Департамент труда и социальной защиты населения г. Москвы

Государственное бюджетное образовательное учреждение

г. Москвы

Центр реабилитации и образования №7

Принято	Согласовано	Утверждаю
на педагогическом совете	Зам.директора по УВР	Директор ГБОУ ЦРО № 7
Пр. №1 от 30.08.24г.	_____ И.В. Рибелка	_____ С.А. Войтас
_____ /Т.Г. Жаркович	«30» августа 2024г	«30» августа 2024г.

Программа комплексной реабилитации

«Семь байтов»

на 2024-2025 учебный год

(социально-педагогическая реабилитация)

Составитель:

педагог дополнительного образования

ГБОУ ЦРО № 7

Саласина.А.А.

2024г

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Программа: Название: "7 байтов"

Целевая аудитория: Ученики 1-11 классов

В современном мире, с нарастающей зависимостью от цифровых технологий, безопасность в интернете становится вопросом первостепенной важности. Каждый день миллионы людей по всему миру используют интернет для обмена информацией, общения, совершения покупок и выполнения множества других задач. Однако с ростом возможностей, которые предоставляет интернет, растет и количество угроз для личной безопасности и конфиденциальности.

Информационная безопасность в интернете охватывает широкий спектр мер и практик, направленных на защиту личных данных, предотвращение кибератак, обеспечение конфиденциальности и этичного поведения в онлайн-пространстве. Она становится особенно актуальной в контексте растущей цифровизации общества и увеличения числа онлайн-угроз, таких как киберпреступность, кибербуллинг, кража личной информации и многие другие.

Важно осознать, что безопасность в интернете не ограничивается простым избеганием определенных веб-сайтов или скачиванием антивирусного программного обеспечения. Это комплексный подход, который включает в себя обучение основам цифровой грамотности, развитие критического мышления, а также понимание основных принципов защиты данных и конфиденциальности.

В данном курсе ученики смогут рассмотреть основные аспекты информационной безопасности в интернете и получить инструменты и знания, необходимые для эффективной защиты себя и своей личной информации в онлайн-среде. Разберемся в опасностях, с которыми они смогут столкнуться в интернете, научатся распознавать угрозы и применять практические стратегии, чтобы оставаться безопасными в цифровом мире.

ФОРМА ПРОВЕДЕНИЯ УЧЕБНЫХ ЗАНЯТИЙ

Занятия проводятся в групповой форме и состоят из теоретической и практической части. Практические упражнения предполагают коллективную или индивидуальную работу. При этом занятие построено так, чтобы уделить время каждому воспитаннику.

УЧЕТ РАБОЧЕЙ ПРОГРАММЫ ВОСПИТАНИЯ

Особое внимание уделяется эстетическому воспитанию обучающихся. Формируется чувство ответственности за обеспечение безопасности данных и информации в цифровом пространстве. При выборе учебного материала учитываются современные требования к кибербезопасности, а также принципы этичности и социальной ответственности.

Практические упражнения направлены на развитие навыков применения инструментов и методов защиты информации. При этом стимулируется коллективное решение задач и индивидуальное освоение техник безопасного взаимодействия в онлайн-среде.

СОДЕРЖАНИЕ ПРОГРАММЫ

Классы 1-4:

1. Введение в безопасность в интернете;
2. Основные правила безопасного поведения в сети;
3. Знакомство с понятием "личная информация" и ее значением;
4. Защита личной информации;
5. Правила безопасного общения в онлайн-среде;
6. Как сохранять конфиденциальность своих данных;
7. Опасности в интернете;
8. Понимание различных видов онлайн-угроз: вирусы, кибербуллинг и др.;
9. Развитие навыков распознавания потенциально опасных ситуаций;
10. Этичное поведение в интернете;
11. Почему важно быть доброжелательным и вежливым в онлайн-общении;
12. Понятие интернет-этики и основные принципы ее соблюдения.

Классы 5-7:

1. Кибербезопасность: Основы;

2. Расширенное изучение видов онлайн-угроз и способов защиты;

3. Практические упражнения по созданию сильных паролей и защите учетных записей;

4. Кибербуллинг и онлайн-безопасность;

5. Понимание понятия кибербуллинга и методов его предотвращения;

6. Роль социальных сетей в безопасном общении;

7. Безопасность в онлайн-играх;

8. Основные правила безопасности в многопользовательских играх;

9. Понимание рисков и возможностей виртуального общения;

10. Безопасность в Интернете для детей и подростков;

11. Опасности, с которыми сталкиваются дети и подростки в онлайн-среде;

12. Воспитание цифровой грамотности и этичного поведения в сети для подростков.

Классы 8-9:

1. Введение в безопасное поведение в сети;

2. Основные правила безопасного поведения в сети;

3. Поведение в электронной почте;

4. Безопасное поведение в социальных сетях;

5. Защита от вирусов и вредоносных программ;

6. Методы обнаружения вредоносных программ;

7. Развитие навыков предотвращения и обнаружения вирусных атак;

8. Основные принципы работы антивирусных программ;

9. Защита конфиденциальности в онлайн-сервисах;

10. Как управлять настройками приватности в социальных сетях и других онлайн-платформах;

11. Оптимальные стратегии сохранения конфиденциальности;

12. Защита от вирусов и вредоносных программ.

Классы 10-11:

1. Юридические аспекты онлайн-безопасности;

2. Законы и политики, регулирующие интернет и онлайн-безопасность;

3. Понимание своих прав и ответственностей в цифровом пространстве;
4. Практические навыки в области кибербезопасности;
5. Обзор инструментов и техник защиты информации;
6. Сценарные упражнения и ролевые игры для тренировки умений в ситуациях реального времени;
7. Безопасность в сфере медицины и финансов;
8. Рассмотрение уязвимостей и угроз в сферах медицинских информационных систем и финансовых учреждений;
9. Обсуждение методов защиты медицинских данных и финансовых транзакций от кибератак;
10. Юридические аспекты онлайн-безопасности;
11. Законы и политики, регулирующие интернет и онлайн-безопасность;
12. Понимание своих прав и ответственностей в цифровом пространстве.

ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

Данный план рассчитан на 3 занятия в неделю. В случае составления расписания в разрезе 2 часов в неделю, темы объединяются и проводятся по 2 темы в рамках 1 занятия.

1-4 класс

№	Название темы	Количество часов		Форма проведения
		Всего	Практические работы	
1	Введение в безопасность в интернете	1	1	Теория
2	Основные правила безопасного поведения в сети	1	1	Игра
3	Знакомство с понятием "личная информация" и ее значением	1	1	Практика
4	Защита личной информации	1	1	Игра
5	Правила безопасного общения в онлайн-среде	1	1	Практика
6	Как сохранять конфиденциальность своих данных	1	1	Практика
7	Опасности в интернете	1	1	Игра
8	Понимание различных видов онлайн-угроз: вирусы, кибербуллинг и др.	1	1	Игра
9	Развитие навыков распознавания потенциально опасных ситуаций	1	1	Игра
10	Этичное поведение в интернете	1	1	Игра
11	Почему важно быть доброжелательным и вежливым в онлайн-общении	1	1	Игра
12	Понятие интернет-этики и основные принципы ее соблюдения	1	1	Практика

5-7 класс

№	Название темы	Количество часов	Форма проведения

		Всего	Практические работы	
1	Кибербезопасность: Основы	1	1	Теория
2	Расширенное изучение видов онлайн-угроз и способов защиты	1	1	Игра
3	Практические упражнения по созданию сильных паролей и защите учетных записей	1	1	Практика
4	Кибербуллинг и онлайн-безопасность	1	1	Игра
5	Понимание понятия кибербуллинга и методов его предотвращения	1	1	Практика
6	Роль социальных сетей в безопасном общении	1	1	Практика
7	Безопасность в онлайн-играх	1	1	Игра
8	Основные правила безопасности в многопользовательских играх	1	1	Игра
9	Понимание рисков и возможностей виртуального общения	1	1	Игра
10	Безопасность в Интернете для детей и подростков	1	1	Игра
11	Опасности, с которыми сталкиваются дети и подростки в онлайн-среде	1	1	Игра
12	Воспитание цифровой грамотности и этичного поведения в сети для подростков	1	1	Практика

8-9 класс

№	Название темы	Количество часов		Форма проведения
		Всего	Практические работы	
1	Введение в безопасное поведение в сети	1	1	Теория
2	Основные правила безопасного поведения в сети	1	1	Игра
3	Поведение в электронной почте	1	1	Практика
4	Безопасное поведение в социальных сетях	1	1	Игра
5	Защита от вирусов и вредоносных программ	1	1	Практика

6	Методы обнаружения вредоносных программ	1	1	Практика
7	Развитие навыков предотвращения и обнаружения вирусных атак	1	1	Игра
8	Основные принципы работы антивирусных программ	1	1	Игра
9	Защита конфиденциальности в онлайн-сервисах	1	1	Игра
10	Как управлять настройками приватности в социальных сетях и других онлайн-платформах	1	1	Игра
11	Оптимальные стратегии сохранения конфиденциальности	1	1	Игра
12	Защита от вирусов и вредоносных программ	1	1	Практика

10-11 класс

№	Название темы	Количество часов		Форма проведения
		Всего	Практические работы	
1	Юридические аспекты онлайн-безопасности	1	1	Теория
2	Законы и политики, регулирующие интернет и онлайн-безопасность	1	1	Игра
3	Понимание своих прав и ответственностей в цифровом пространстве	1	1	Практика
4	Практические навыки в области кибербезопасности	1	1	Игра
5	Обзор инструментов и техник защиты информации	1	1	Практика
6	Сценарные упражнения и ролевые игры для тренировки умений в ситуациях реального времени.	1	1	Практика
7	Безопасность в сфере медицины и финансов	1	1	Игра
8	Рассмотрение уязвимостей и угроз в сферах медицинских информационных систем и финансовых учреждений.	1	1	Игра

9	Обсуждение методов защиты медицинских данных и финансовых транзакций от кибератак.	1	1	Игра
10	Юридические аспекты онлайн-безопасности	1	1	Игра
11	Законы и политики, регулирующие интернет и онлайн-безопасность	1	1	Игра
12	Понимание своих прав и ответственностей в цифровом пространстве	1	1	Практика

КАЛЕНДАРНО-ТЕМАТИЧЕСКИЙ ПЛАН

1-4 КЛАСС

№	Название темы	Предметные результаты
1	Введение в безопасность в интернете	Ознакомление с основными аспектами безопасности в онлайн-среде.
2	Основные правила безопасного поведения в сети	Усвоение основных правил и рекомендаций для обеспечения безопасности в интернете.
3	Знакомство с понятием "личная информация" и ее значением	Понимание важности личной информации и ее защиты от неправомерного доступа.
4	Защита личной информации	Обучение методам и средствам защиты личных данных в сети.
5	Правила безопасного общения в онлайн-среде	Освоение правил эффективного и безопасного общения в интернете.
6	Как сохранять конфиденциальность своих данных	Обучение методам сохранения конфиденциальности и безопасности данных при использовании интернета.
7	Опасности в интернете	Идентификация основных угроз и опасностей, существующих в онлайн-среде.
8	Понимание различных видов онлайн-угроз: вирусы, кибербуллинг и др.	Изучение различных видов угроз в интернете и способов защиты от них.

9	Развитие навыков распознавания потенциально опасных ситуаций	Тренировка навыков распознавания и предотвращения опасных ситуаций в онлайн-среде.
10	Этичное поведение в интернете	Осознание важности этичного поведения и общения в онлайн-среде.
11	Почему важно быть доброжелательным и вежливым в онлайн-общении	Понимание влияния доброжелательности и вежливости на качество онлайн-общения и общую безопасность интернета.
12	Понятие интернет-этики и основные принципы ее соблюдения	Ознакомление с понятием интернет-этики и основными принципами ее соблюдения для создания безопасной и уважительной онлайн-среды.

5-7 КЛАСС

№	Название темы	Предметные результаты
1	Кибербезопасность: Основы	Изучение основных принципов и понятий в области кибербезопасности.
2	Расширенное изучение видов онлайн-угроз и способов защиты	Глубокое понимание различных типов угроз в сети и эффективных методов их предотвращения.
3	Практические упражнения по созданию сильных паролей и защите учетных записей	Обучение практическим навыкам создания надежных паролей и защите учетных записей от несанкционированного доступа.
4	Кибербуллинг и онлайн-безопасность	Понимание понятия кибербуллинга и методов его предотвращения для обеспечения безопасного онлайн-пространства.
5	Понимание понятия кибербуллинга и методов его предотвращения	Анализ рисков и возможностей, связанных с виртуальным общением, с целью

		обеспечения безопасного и продуктивного интернет-взаимодействия.
6	Роль социальных сетей в безопасном общении	Изучение влияния социальных сетей на безопасное общение и методов обеспечения безопасности при их использовании.
7	Безопасность в онлайн-играх	Освоение основных правил безопасности в многопользовательских онлайн-играх для защиты от угроз и обеспечения безопасного гейминга.
8	Основные правила безопасности в многопользовательских играх	Обучение правилам безопасного поведения и взаимодействия с другими игроками в многопользовательских играх, чтобы избежать конфликтов и негативного воздействия.
9	Понимание рисков и возможностей виртуального общения	Разбор рисков и возможностей, связанных с виртуальным общением, в том числе распространение личной информации, обман и кибербуллинг, и изучение способов защиты от них.
10	Безопасность в Интернете для детей и подростков	Развитие умения распознавать потенциальные угрозы в Интернете и умений действовать в соответствии с ними.
11	Опасности, с которыми сталкиваются дети и подростки в онлайн-среде	Риски встреч с неприятными людьми или экспонирование вредоносного контента.
12	Воспитание цифровой грамотности и этичного поведения в сети для подростков	Содействие развитию эмпатии и уважительного отношения к другим в онлайн-среде.

8-9 КЛАСС

№	Название темы	Предметные результаты
1	Введение в безопасное поведение в сети	Ознакомление с основными концепциями и принципами безопасности в онлайн-среде.
2	Основные правила безопасного поведения в сети	Изучение основных правил и рекомендаций для обеспечения безопасности при использовании интернета.
3	Поведение в электронной почте	Обучение правилам безопасной работы с электронной почтой и защите от фишинговых атак.
4	Безопасное поведение в социальных сетях	Освоение методов обеспечения безопасности при использовании социальных сетей и защиты личных данных.
5	Защита от вирусов и вредоносных программ	Обучение методам защиты компьютера и устройств от вирусов и вредоносных программ.
6	Методы обнаружения вредоносных программ	Изучение методов обнаружения и удаления вредоносного программного обеспечения.
7	Развитие навыков предотвращения и обнаружения вирусных атак	Тренировка навыков распознавания и предотвращения вирусных атак на компьютер и устройства.
8	Основные принципы работы антивирусных программ	Понимание работы и принципов действия антивирусного программного обеспечения.
9	Защита конфиденциальности в онлайн-сервисах	Обучение методам защиты личной информации и конфиденциальности при использовании онлайн-сервисов.
10	Как управлять настройками приватности в социальных сетях и других онлайн-платформах	Изучение способов управления настройками приватности для обеспечения безопасного и конфиденциального общения в сети.

11	Оптимальные стратегии сохранения конфиденциальности	Обучение оптимальным стратегиям и методам сохранения конфиденциальности данных и личной информации в онлайн-среде.
12	Защита от вирусов и вредоносных программ	Установка и регулярное обновление антивирусного программного обеспечения на всех устройствах

10-11 КЛАСС

№	Название темы	Предметные результаты
1	Юридические аспекты онлайн-безопасности	Анализ законодательства и нормативных актов, касающихся правового регулирования безопасности в цифровом пространстве.
2	Законы и политики, регулирующие интернет и онлайн-безопасность	Изучение основных правовых актов и политик, ориентированных на обеспечение безопасности в интернете.
3	Понимание своих прав и ответственностей в цифровом пространстве	Обучение основам цифровой грамотности и осознанию собственных прав и обязанностей в онлайн-среде.
4	Практические навыки в области кибербезопасности	Развитие навыков обнаружения, предотвращения и реагирования на киберугрозы в реальном времени.
5	Обзор инструментов и техник защиты информации	Изучение современных инструментов и методов защиты данных и сетей от кибератак.
6	Сценарные упражнения и ролевые игры для тренировки умений в ситуациях реального времени.	Проведение тренировочных сценариев и игр для развития навыков принятия решений и действий в случае киберугроз.

7	Безопасность в сфере медицины и финансов	Рассмотрение особенностей и угроз безопасности в медицинских информационных системах и финансовой сфере.
8	Рассмотрение уязвимостей и угроз в сферах медицинских информационных систем и финансовых учреждений.	Изучение потенциальных угроз и уязвимостей, присущих системам обработки медицинских данных и финансовым институтам.
9	Обсуждение методов защиты медицинских данных и финансовых транзакций от кибератак.	Разработка стратегий и методов защиты конфиденциальной информации и финансовых операций от киберугроз.
10	Юридические аспекты онлайн-безопасности	Глубокое рассмотрение правовых аспектов, касающихся безопасности в сети.
11	Законы и политики, регулирующие интернет и онлайн-безопасность	Дополнительное изучение основных правовых и политических мероприятий, направленных на обеспечение безопасности в онлайн-среде.
12	Юридические аспекты онлайн-безопасности	Обсуждение и анализ законодательства и нормативных документов, регулирующих аспекты безопасности в цифровой сфере.