МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Комитет образования и науки Волгоградской области

Отдел образования, опеки и попечительства администрации

Иловлинского муниципального района Волгоградской области

МБОУ Иловлинская СОШ №1

РАССМОТРЕНА	СОГЛАСОВАНА	УТВЕРЖДЕНА
МО классный руководителей	Методист по ВР	Директор МБОУ Иловлинской СОШ №1
Волкова Е.В.	Волкова Е.В.	Игнатова Е.П.
Протокол МО №1 от «28» августа 2026 г.	Протокол педагогического совета №1 от «31» августа 2026 г.	Приказ № 271 от «01» сентября 2026 г.

РАБОЧАЯ ПРОГРАММА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ «КиберЩит»

для 8В класса

Программу реализует: Часовская Н.С.
Должность: учитель информатики
МБОУ Иловлинской СОШ №1

р.п. Иловля, 2026

СОДЕРЖАНИЕ КУРСА

Содержание курса «КиберЩит» складывается из пяти содержательных линий и имеет отличия с учетом возрастных особенностей:

- **учитываются возрастные особенности:** самостоятельные действия в сети усложняются в зависимости от уровня образования (от игр и поиска данных к социальным сетям и использованию онлайн-банков);
- **увеличивается подробность материалов:** в 1–4 классах теоретический материал требует более подробного объяснения педагогом, в 10–11 классах часть теоретического материала выделено для внеаудиторной самостоятельной работы;
- **усложняются задания для отработки навыков:** от 1 к 11 классу увеличивается уровень сложности заданий, разнообразие содержания, степень самостоятельности в их выполнении.

Программа курса может быть реализована как самостоятельный учебный курс во внеурочной деятельности детей за один год, а также интегрирована дополнительными содержательными блоками в систему тематических классных часов по модулям календарного планирования программы воспитания (социализации) обучающихся.

Изучение теоретического материала по каждой теме проводится в практико-ориентированном формате в форме фронтальной беседы, диспута, дискуссии или работе в мини-группах (решение ситуационных задач). Практическое занятие по каждой теме может быть проведено не позднее чем через 2 недели после соответствующего теоретического занятия.

Не рекомендуется между теоретическим занятием по теме и его практикумом проводить следующее теоретическое занятие. Для повторения и закрепления учебного материала ученикам доступны задания интерактивного тренажёра, работа с которым возможна в асинхронном формате. Задания асинхронного интерактивного тренажёра на образовательной платформе рекомендуется назначать к самостоятельному выполнению учащимся не ранее 5 класса при условии их готовности к работе в предлагаемом формате.

1 – 4 классы

1. «Личные данные»

Личные данные, выделение ЛД из прочих сведений – работа с текстом, с формами обратной связи, с анкетами, шаблонами. Создание анкеты. Решение проблемных ситуаций: определение ЛД, выделение способов их защиты.

2. «Спам и мошенничество»

Что такое спам и как его избежать. Способы защиты, алгоритмы действий при получении спам-звонка/спам-рассылки.

3. «Цифровой этикет»

Агрессивное поведение в мобильных играх. Алгоритм действий при столкновении с агрессивным поведением в игре.

4. «Безопасность и искусственный интеллект»

Угрозы ИИ. Возможности манипуляции и воздействия на поведение.

5. «Вирусы»

Вирусы при скачивании изображений и музыки. Чем опасно скачивание файлов с незнакомых хостингов. Работа с уведомлениями на скачивание с дополнительными расширениями и разрешениями. Вирусы на мобильных устройствах.

5 – 9 классы

1. «Кибер-гигиена»

Кибер-гигиена и безопасность личных данных. Классификация компьютерных вирусов

2. «Цифровой этикет»

Правила цифрового этикета. Противостояние кибербуллингу в соцсетях, общении на форуме, переписке; ответственность за буллинг (травлю).

3. «Интернет-мошенничество»

Интернет пиратство, фишинг, зеркальные сайты: чем вредят, какое наказание может быть. Виды мошенничества, защита от мошенничества.

4. «Финансовая безопасность»

Личная финансовая безопасность, меры по предотвращению угроз.

5. «Безопасность и искусственный интеллект»

ИИ и его возможности. Безопасность личных данных при работе с ИИ.

10 – 11 классы

1. «Кибербезопасность»

Кибербезопасность, виды киберугроз. Вредоносное ПО, виды: Фишинг, DoS-атаки (атаки типа «отказ в обслуживании»), новейшие киберугрозы.

2. «Цифровой этикет»

Правила цифрового этикета. Границы общения и буллинга; ответственность за буллинг (травлю).

3. «Мошенничество»

Защита от спама и фишинга, защита от программ вымогателей, нарушение приватности при общении.

4. «Финансовая безопасность»

Личная финансовая безопасность, меры по предотвращению угроз.

5. «Безопасность и искусственный интеллект»

ИИ и его возможности ИИ. Искусственный интеллект и мошенничество.

ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

1 – 4 классы: 17 занятий, 6 ак.ч.

№ п/п	Тема занятия	Цель занятия	Вид занятия	Продолжительность занятия
1	Личные данные	формировать представление о ЛД	теория	15
2			практикум	15
3	Защита личных данных	формировать представление о необходимости защиты ЛД	теория	15
4			практикум	15
5	Спам в смс-рассылках и звонках	формировать представление о понятии "спам"	теория	15
6			практикум	15
7	Спам и мошенничество в смс-рассылках и звонках	формировать алгоритм действий при получении спам-звона/спам-рассылки	теория	15
8			практикум	15
9	Цифровой этикет	формировать представление о правилах цифрового этикета	теория	15
10			практикум	15
11	Безопасность в интернете и искусственный интеллект	формировать представление о необходимости критического отношения к получаемым сообщениям; формулировать критерии распознавания мошеннических сообщений; формировать алгоритм действий при получении сообщений сомнительного содержания	теория	15
12			практикум	15
13	Вирусы при скачивании изображений и музыки	формировать представление об опасности работы с не проверенными сайтами	теория	15
14			практикум	15
15	Информационная безопасность	обобщить алгоритмы действий при выявлении случаев кибербуллинга, мошенничества, получения спама	обобщение	30
16	Викторина		викторина	15
17	Проверка знаний		тест	15

5 – 6 классы: 18 занятий, 6 ак.ч.

№ п/п	Тема занятия	Цель занятия	Вид занятия	Продолжительность занятия
1	Кибер-гигиена и безопасность личных данных	формировать представление о понятии "кибергигиена" (правила, сохраняющие ИБ); формировать представление о проблемах, которых помогает избежать соблюдение норм кибергигиены	теория	20
2			практикум	10
3	Компьютерные вирусы	формировать представление о компьютерных вирусах	теория	15
4			практикум	15
5	Цифровой этикет	формировать представление о цифровом этикете как наборе правил, регламентирующих взаимодействие людей в сети	теория	20
6			практикум	10
7	Кибербуллинг и цифровой этикет.	формировать представление необходимости противостояния травле в сети, о способах защиты и мерах наказания за травлю	теория	20
8			практикум	10
9	Интернет-мошенничество (фишинг, зеркальные сайты, пиратство)	формировать представление о мерах пресечения противоправных действий в сети (фишинг, зеркальные сайты, пиратство)	теория	20
10			практикум	10
11	Интернет-мошенничество. Пиратство и зеркальные сайты	формировать представление о способах защиты от мошеннических действий в сети	теория	20
12			практикум	10
13	Финансовая безопасность	формировать представление о личной ФБ; формировать представление об основных угрозах ФБ	теория	20
14			практикум	10
15	Безопасность в интернете и искусственный интеллект	формировать представление об ИИ и сферах его применения	теория	20
16			практикум	10
17	Викторина	обобщить алгоритмы действий при выявлении случаев кибербуллинга, мошенничества, получения спама	викторина	15
18	Проверка знаний		тест	15

7 – 9 классы: 18 занятий, 6 ак.ч.

№ п/п	Тема занятия	Цель занятия	Вид занятия	Продолжительность занятия
1	Кибер-гигиена и безопасность личных данных	формировать представление о цифровом следе пользователя и механизмах сбора персональных данных в интернете	теория	20
2			практикум	10
3	Компьютерные вирусы	формировать представление о компьютерных вирусах	теория	15
4			практикум	15
5	Цифровой этикет	формировать представление о цифровом этикете как наборе правил, регламентирующих взаимодействие людей в сети	теория	20
6			практикум	10
7	Кибербуллинг и цифровой этикет.	формировать представление необходимости противостояния травле в сети, о способах защиты и мерах наказания за травлю	теория	20
8			практикум	10
9	Интернет-мошенничество (фишинг, зеркальные сайты, пиратство)	формировать представление о мерах пресечения противоправных действий в сети (фишинг, зеркальные сайты, пиратство)	теория	20
10			практикум	10
11	Интернет-мошенничество. Пиратство и зеркальные сайты	формировать представление о способах защиты от мошеннических действий в сети	теория	20
12			практикум	10
13	Финансовая безопасность	формировать представление о личной ФБ; формировать представление об основных угрозах ФБ	теория	20
14			практикум	10
15	Безопасность в интернете и искусственный интеллект	формировать представление об ИИ и сферах его применения	теория	20
16			практикум	10
17	Викторина	обобщить алгоритмы действий при выявлении случаев кибербуллинга, мошенничества, получения спама	викторина	15
18	Проверка знаний		тест	15

10 – 11 классы: 17 занятий, 6 ак.ч.

№ п/п	Тема занятия	Цель занятия	Вид занятия	Продолжительность занятия
1	Кибербезопасность и личные данные	формировать понятие "кибер-безопасность" формировать представление об основных видах киберугроз	теория	20
2			практикум	10
3	Вирусы	формировать представление о видах вредоносного ПО	теория	15
4	Виды вредоносного ПО		практикум	15
5	Кибербуллинг и цифровой этикет	научить отличать травлю от конфликтной ситуации	теория	20
6			практикум	10
7	Цифровой этикет	формировать представление о правилах цифрового этикета и важности их выполнения	теория	15
8			практикум	15
9	Мошенничество	формировать представление о мошеннических действиях в сети и наказании за участие в противоправных действиях	теория	15
10	Дискуссия: кибермошенничество		дискуссия	15
11	Финансовая безопасность	формировать представление о видах ФБ и мерах по предотвращению угроз личной ФБ	теория	15
12			практикум	15
13	Искусственный интеллект и кибербезопасность	формировать представление о развитии технологий ИИ и сферах его применения	теория	15
14			практикум	15
15	Дискуссия: Безопасность в интернете и искусственный интеллект	формировать представление об использовании ИИ в мошеннических действиях и наказании за совершение противоправных действий с применением ИИ	дискуссия	30
16	Викторина	обобщить алгоритмы действий при выявлении случаев кибербуллинга, мошенничества, получения спама	викторина	15
17	Проверка знаний		тест	15