МУ «Отдел образования Ачхой-Мартановского муниципального района»
Муниципальное бюджетное учреждение дополнительного образования
«Детско-юношеский центр Ачхой-Мартановского муниципального района»

Принята на заседании
педагогического совета
Протокол №
от «___» _____202_г

Утверждена
Приказом № ___
от «___» _____202_г
Директор
_____ И.З.Висаитов



Дополнительная общеобразовательная общеразвивающая программа
«Лето кибербезопасности»
Направленность программы: социально-гуманитарное
Уровень программы: Стартовый

Возраст обучающихся 10 – 12 лет
Срок реализации 14 дней

Составитель:
Бакаева Хава Умаровна,
педагог дополнительного образования

г. Ачхой-Мартан, 2026 г.

Программа прошла внутреннюю экспертизу и рекомендована к реализации в МБУ ДО «ДЮЦ Ачхой-Мартановского муниципального района»
Экспертное заключение (рецензия) № __ от «____» _____202___ г.

Эксперт _____ _____
(Ф.И.О.) (должность)

Содержание программы

Раздел 1.	Комплекс основных характеристик дополнительной общеобразовательной общеразвивающей программы	4
1.1.	Нормативно-правовые основы	4
1.2.	Направленность	4
1.3.	Уровень освоения программы	4
1.4.	Актуальность программы	4
1.5	Отличительные особенности программы	5
1.6.	Цель и задачи программы	5
1.7.	Категория учащихся	5
1.8.	Срок реализации и объем программы	5
1.9.	Формы организации образовательной деятельности и режим занятий	5
1.10.	Планируемые результаты освоения программы	5
Раздел 2.	Содержание программы	7
2.1.	Учебный план	7
2.2.	Содержание учебного плана программы	7
Раздел 3.	Форма аттестации и оценочные материалы	9
Раздел 4.	Комплекс организационно-педагогических условий	10
4.1.	Материально–технические условия реализации программ	10
4.2.	Кадровое обеспечение программы	10
4.3.	Учебно-методическое обеспечение	10
	Список литературы	10
	Приложение №1	

Раздел.1. Комплекс основных характеристик дополнительной общеобразовательной общеразвивающей программы

1.1. Нормативно-правовые основы разработки дополнительных общеобразовательных программ.

- Федеральный закон «Об образовании в Российской Федерации» № 273-ФЗ от 29.12.2012г.;
- Приказ Министерства образования и науки РФ от 27 июля 2022 года № 629 «Об утверждении порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам»;
- Концепция развития дополнительного образования детей до 2030 года от 31 марта 2022 года № 678-р; (изм. от 1 июля 2025 г. № 1745-р)
-Постановление Главного государственного санитарного врача РФ от 28 сентября 2020г.№28 «Об утверждении санитарных правил СП 2.4.3648-20 «Санитарно-эпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодежи»;
- Приказ Министерства образования и науки Российской Федерации от 23 августа 2017 г. №816 «Об утверждении Порядка применения организациями, осуществляющими образовательную деятельность электронного обучения, дистанционных образовательных технологий при реализации образовательных программ»;
- Письмо Минобрнауки РФ от 18.11.2015 № 09-3242 «О направлении рекомендаций» (вместе с Методические рекомендации по проектированию дополнительных общеразвивающих программ);
- Распоряжение Правительства РФ от 29.05.2015 №996-р «Об утверждении Стратегии развития воспитания в Российской Федерации на период до 2025 года»;
- Приложение к письму Департамента молодежной политики, воспитания и социальной поддержки детей Минобразования и науки России от 11.12.2006 г. № 06-1844 «О примерных требованиях к программам дополнительного образования детей» (в частях, не противоречащих современному законодательству);
- Приказ Министерства просвещения РФ от 3 сентября 2019 г. №467 «Об утверждении Целевой модели развития региональных систем дополнительного образования детей».

1.2. Направленность программы.

Дополнительная образовательная общеразвивающая программа «Лето кибербезопасности» - социально-гуманитарной направленности. Программа направлена на изучение правил поведения детей вести себя в той или иной сложной ситуации, например, если ребенок столкнулся с телефонным мошенничеством, интернет травлей, а также о том, как проводить время в сети с пользой.

1.3. Уровень освоения программы.

Настоящая программа имеет стартовый уровень в соответствии с Методическими рекомендациями по проектированию дополнительных общеразвивающих программ Министерства образования и науки РФ (письмо от 18 ноября 2015 г. № 09-3242)

1.4. Актуальность программы.

Данная дополнительная общеразвивающая программа соотносится с тенденциями развития дополнительного образования и согласно Концепции развития дополнительного образования способствует созданию необходимых условий для личностного развития обучающихся. Воспитывая будущих цифровых граждан, важно научить детей осознанно и ответственно относиться к использованию информации в Интернете, научить их правилам сетевого этикета и возможностям для защиты собственного творчества в сети.

Информационная безопасность в отношении детей обеспечивается комплексом мер и включает в себя государственное регулирование (Федеральный закон от 29.12.2010г. №436-ФЗ “О защите детей от информации, причиняющей вред их здоровью и развитию“), процесс воспитания и

обучения в образовательной организации и дома, а также набор основных правил технического и организационного характера для саморегулирования цифрового поведения пользователей.
На первый взгляд виртуальный мир выглядит более безопасным, чем реальный. Ведь последствия столкновения с киберугрозами не так очевидны, как с физическими. Когда мы были детьми, нас учили азам гигиены – мыть руки и чистить зубы. Мы освоили правила безопасного поведения в реальном мире и передаем их следующим поколениям. Но с развитием технологий наши дети нуждаются в новых знаниях. Наша задача – научить их цифровой гигиене и кибербезопасности, ведь они растут и развиваются в цифровой среде.

1.5. Отличительные особенности.
Дополнительная общеобразовательная общеразвивающая программа «Лето кибербезопасности» составлена на основе проекта «Цифровой ликбез» АНО «Цифровая экономика». Программа составлена в связи с острой необходимостью информирования детей в преддверии летних каникул о грамотных сценариях поведения в сети Интернет, способах реагирования на киберугрозы и других видов мошенничества.

1.6. Цель и задачи программы.
Цель программы – повышение цифровой грамотности и формирование навыков безопасного поведения в цифровой среде

Задачи:
Образовательные:
- формировать основы информационной компетентности;
- обучать правилам «компьютерной гигиены», проводить зарядку для глаз, физкультминутки, контролировать время пребывания за компьютером, информировать о правилах безопасного использования Интернет;
- формировать основы экономической грамотности при использовании Интернета в потребительских целях;
- оценивать основные риски, связанные с приобретением и потреблением товаров и услуг в Интернете (например, распознавать интернет-мошенничество, недобросовестную торговлю и т.д.)

Развивающие:
- развить навыки создания информационных объектов с использованием цифровых ресурсов – сетевых, текстовых, изобразительных, аудио и видео
- развить умение искать и анализировать информацию в Интернете;

Воспитательные:
- воспитать чувство ответственности за себя;
- воспитать нравственные и волевые качества: волю, смелость, активность.

1.7. Категория учащихся.
Данная программа направлена на обучение детей возраста с 10 до 12 лет.
Зачисление осуществляется по заявлению родителей (законных представителей).

1.8. Сроки реализации и объем программы.
Срок реализации программы 14 дней. Общий объём 42 часов.

1.9. Формы организации образовательной деятельности и режим занятий.
Занятия проводятся в разновозрастных группах, численный состав группы - 15 человек
Режим занятий 5 раз в неделю по 3 часа, Продолжительность занятия-45 минут 15 минут перерыв.

1.10. Планируемые результаты и способы их проверки.

Предметные результаты освоения программы обучающиеся
будут знать:
- основы информационной компетентности;
- правила «компьютерной гигиены», проводить зарядку для глаз, физкультминутки, контролировать время пребывания за компьютером, информировать о правилах безопасного использования Интернет;
- основы экономической грамотности при использовании Интернета в потребительских целях
будут уметь:
- оценивать основные риски, связанные с приобретением и потреблением товаров и услуг в Интернете (например, распознавать интернет-мошенничество, недобросовестную торговлю и т.д.)
- искать и анализировать информацию в Интернете

Метапредметные результаты освоения программы:
Обучающиеся будут
- знать основы информационной безопасности. Будут сформированы и развиты комплексы мер (правил, процедур, практических рекомендаций) для управления информационной безопасностью.

Личностные результаты освоения программы:
Результаты развития обучающихся
У учащихся будут сформированы:
- развитие у учащегося коммуникабельности в общение со сверстниками на принципах взаимоуважения и доброжелательности;
- качество проявлять дисциплинированность, трудолюбие и упорство в достижении поставленных целей;

Результаты воспитания:
У учащихся будут сформированы:
- нравственные и волевые качества: волю, смелость, активность.
- чувство ответственности за себя.

Раздел 2. Содержание программы
2.1. Учебный (тематический) план.

№	Название темы	Количество часов			Формы аттестации/ контроля
		Всего часов	Теория	Практика	
1.	Введение в программу, что такое кибербезопасность, «Цифровой ликбез»	3	1	2	Опрос
2.	Виртуальная реальность	3	1	2	Наблюдение
3.	Интернет – травля	3	1	2	Наблюдение
4.	Ты не один	3	1	2	Наблюдение
5.	На игре	3	1	2	Наблюдение
6.	Максимальный репост	3	1	2	Наблюдение
7.	Безопасное общение	3	1	2	Наблюдение
8.	Безопасное использование устройств и соединений	3	1	2	Наблюдение
9.	Безопасность информаций	3	1	2	Наблюдение
10.	Формирование кибербезопасного поведения	3	1	2	Наблюдение
11.	Компьютерные и телефонные вирусы	3	1	2	Наблюдение
12.	Цифровой след	3	1	2	Наблюдение
13.	Безопасность в играх	3	1	2	Наблюдение
14.	Итоговое занятие на платформе https://digital-likbez.datalesson.ru/	3		3	Круглый стол
15.	**Итого:**	**42**	**13**	**29**	

2.2. Содержание учебного плана.

Тема 1. Введение в программу, что такое кибербезопасность, «Цифровой ликбез».
Теория: Что такое кибербезопасность и зачем она нужна.
Практика:
Тема 2. Виртуальная реальность.

Теория: Научить обуающихся на опыте, что профиль в соцсети может сильно отличаться от реального человека.
Практика: Научить как не стать жертвой преступника, создавшего себе привлекательный образ в сети?.

Тема 3. Интернет – травля

Теория: Правила общения в сети. Интернет-травля, как не ввязаться и не стать жертвой. Способы защиты и правовое регулирование
Практика: Просмотр видео-презентаций, обобщить полученный знания в виде круглого стола.

Тема 4. Ты не один.

Теория: Научить обучающихся как не подвергаться кибербуллингу — насмешкам и издевательствам в сети.
Практика: Отработать навыки как ребенок может справиться с ситуацией? Что он может сделать самостоятельно, а в чем ему понадобится помощь взрослых?

Тема 5. На игре.

Теория: Научить обучающихся как не попасть на крючок в сетевой игре
Практика: Просмотр видео-презентаций, обобщить полученный знания в виде круглого стола.

Тема 6. Максимальный репост

Теория: Научить обучающихся навыкам, если на телефон поступает тревожное сообщение... Как с ним поступить? Переслать другу? Или сначала проверить, насколько правдивым является это сообщение? Что может произойти, если все будут пересылать друг другу непроверенную информацию?
Практика: Просмотр видео-презентаций, обобщить полученный знания в виде круглого стола.

Тема 7. Безопасное общение.

Теория: Обучающиеся научатся принципам безопасного общения в сети. Узнают, что такое цифровой след и как его минимизировать.
Практика: Обучающиеся научатся принципам безопасного общения в сети. Узнают, что такое цифровой след и как его минимизировать, а также смогут распознать кибербуллинг и грамотно реагировать в случае столкновения с негативными формами общения в сети. Работа в https://cyber-care.ru/lessonsschool

Тема 8. Безопасное использование устройств и соединений.

Теория: Обучающиеся узнают об основных угрозах, которые встречаются при передаче информации с устройства на устройство и по сети.
Практика: Обучающиеся освоят способы защиты от вредоносных программ. Научатся основным принципам безопасного использования беспроводных соединений, в т.ч. публичного Wi-Fi. Работа в https://cyber-care.ru/lessonsschool

Тема 9. Безопасность информаций.

Теория: Обучающиеся узнают основные принципы безопасного поведения в сети, чтобы избежать негативных последствий интернет-серфинга, обмена почтовыми сообщениями или онлайн-покупок. Научатся распознавать основные схемы социальной инженерии и узнают, что такое фишинг. записи.
Практика: Обучающиеся научатся создавать стойкие пароли и узнают, как защитить свои учетные. Работа в https://cyber-care.ru/lessonsschool

Тема 10. Формирование кибербезопасного поведения.

Теория: Безопасность платежей и данных. Узнаем, как обезопасить себя от кражи, как злоумышленник может похищать данные. Профилактика заражений и гигиена компьютера.
Практика: Просмотр видео-презентаций, обобщить полученный знания в виде круглого стола.

Тема 11. Компьютерные и телефонные вирусы

Теория: Познакомить учащихся с видами компьютерных вирусов, способами их распространения, профилактикой и методами борьбы с ними, дать понятие “ “вирус”.
Практика: Просмотр видео-презентаций, обобщить полученный знания в виде круглого стола.

Тема: 12. Цифровой след

Практика: Познакомить обучающихся что можно, а что категорически нельзя публиковать в открытом доступе (адрес, геолокация, фото билетов).

Тема 13. Безопасность в играх

Практика: Ознакомить обучающихся с правилами общения в игровых чатах (Roblox, Minecraft), защита аккаунтов от кражи и распознавание токсичного поведения.

Итоговое занятие на платформе https://digital-likbez.datalesson.ru/

Практика: Открытое занятие представляет с собой сессию вопросов-ответов, после просмотра просветительского видеороликов с ресурса, обучающиеся задают вопросы а официальные представители отвечают. В ходе круглого стола провести командную работу.

Раздел 3. Формы аттестации и оценочные материалы.

Виды и формы контроля, фиксации результатов:

- текущий: наблюдение за выполнением приемов и методов в работе, отслеживание активности учащихся в выполнении ими заданий;
- итоговый: обучающие будут проходить игровые ситуации и практические задания.

Аттестация рассчитана на 45 минут и состоит из четырех этапов (станций). За каждое правильно выполненное задание дети получают «ключи» или «токены безопасности».

Критерии оценивания

Предмет оценивания	**Объект оценивания**	**Вид аттестации**
Умения: - вести диалог; Знания: - о киберугрозах и как бороться с ними; - знание сайтов, как безопасно выбирать. - сформированные навыки безопасного поведения в цифровой среде и критическое мышление.	Знания обучающихся	итоговый контроль

Методы отслеживания результатов обучения и воспитания

- открытое педагогическое наблюдение;
- оценка продуктов деятельности детей.

Раздел 4. Комплекс организационно-педагогических условий реализации программы:

4.1. Материально-технические условия реализации программы.

- Компьютер учащегося тип 1;
- Интерактивный программно-апаратный комплекс тип 3. Объекты и средства материально-технического обеспечения курса.

4.2. Кадровое обеспечение программы.

Программа может быть реализована педагогом дополнительного образования с уровнем образования и квалификации, соответствующим Профессиональному стандарту «Педагог дополнительного образования детей и взрослых»

4.3. Учебно-методическое обеспечение.

Название учебной темы	**Форма занятий**	**Название и форма методического материала**	**Методы и приемы организации учебно-воспитательного процесса**
Введение в программу, что такое кибербезопасность, «Цифровой ликбез»	Групповое, теоретическое, практическое	Беседа, рассказ, демонстрация	Наглядные Репродуктивные
Виртуальная реальность	Групповое, теоретическое, практическое	Беседа, рассказ, демонстрация	Наглядные Репродуктивные
Интернет – травля	Групповое, теоретическое, практическое	Беседа, рассказ, демонстрация	Наглядные Репродуктивные
Ты не один	Групповое, теоретическое, практическое	Беседа, рассказ, демонстрация	Наглядные Репродуктивные
На игре	Групповое, теоретическое, практическое	Беседа, рассказ, демонстрация	Наглядные Репродуктивные
Максимальный репост	Групповое, теоретическое, практическое	Беседа, рассказ, демонстрация	Наглядные Репродуктивные
Безопасное общение	Групповое, теоретическое, практическое	Беседа, рассказ, демонстрация	Наглядные Репродуктивные
Безопасное использование устройств и соединений	Групповое, теоретическое, практическое	Беседа, рассказ, демонстрация	Наглядные Репродуктивные

Безопасность информаций	Групповое, теоретическое, практическое	Беседа, рассказ, демонстрация	Наглядные Репродуктивные
Формирование кибербезопасного поведения	Групповое, теоретическое, практическое	Беседа, рассказ, демонстрация	Наглядные Репродуктивные
Компьютерные и телефонные вирусы	Групповое, теоретическое, практическое	Беседа, рассказ, демонстрация	Наглядные Репродуктивные
Цифровой след	Групповое, теоретическое, практическое	Беседа, рассказ, демонстрация	Наглядные Репродуктивные
Безопасность в играх	Групповое, теоретическое, практическое	Беседа, рассказ, демонстрация	Наглядные Репродуктивные
Итоговое занятие на платформе https://digital-likbez.datalesson.ru/	Групповое, практическое	Проведение командной работы	Наглядные Репродуктивные

Литература, рекомендуемая для учащихся и родителей

1. Макаров Станислав «Прекрасный, опасный, кибербезопасный мир. Всё, что важно знать детям и взрослым о безопасности в интернете» – М.: 2022. – 568 с.: ил.
2. Тонких И.М., Комаров М.М., Ледовской В.И., Михайлов А.В. Основы Кибербезопасности Москва, 2016 г, 113 стр.

Литература для педагога:

1. Цветкова Марина Серафимовна, Хлобыстова Ирина Юрьевна «Информационная безопасность. Кибербезопасность» Издательство: - Просвещение/Бином, 2020 г.

Интернет ресурсы:

1. https://crushpro.ru/cyber
2. https://abzelil.com/articles/bezopasnost/2022-01-12/kiberbezopasnost-dlya-detey-2651314
3. https://cyber-care.ru/lessonsschool

Приложение 1

Календарный учебный график

№ п/п	Фактическая дата и время проведения занятия	Плановая дата и время проведения занятия	Форма занятия	Кол. часов	Тема занятия	Место проведения	Форма контроля
1.		**08.06.2026** 10:00 – 12:25	Групповое, теоретическое, практическое	3	Тема 1. Введение в программу, что такое кибербезопасность, «Цифровой ликбез»	МБОУ «СОШ №1 г.Ачхой-Мартан»	Опрос
2.		**09.06.2026** 10:00 – 12:25	Групповое, теоретическое, практическое	3	Тема 2. Виртуальная реальность	МБОУ «СОШ №1 г.Ачхой-Мартан»	Наблюдение
3.		**10.06.2026** 10:00 – 12:25	Групповое, теоретическое, практическое	3	Тема 3. Интернет – травля	МБОУ «СОШ №1 г.Ачхой-Мартан»	Наблюдение
4.		**11.06.2026** 10:00 – 12:25	Групповое, теоретическое, практическое	3	Тема 4. Ты не один	МБОУ «СОШ №1 г.Ачхой-Мартан»	Наблюдение
5.		**15.06.2026** 10:00 – 12:25	Групповое, теоретическое, практическое	3	Тема 5. На игре	МБОУ «СОШ №1 г.Ачхой-Мартан»	Наблюдение
6.		**16.06.2026** 10:00 – 12:25	Групповое, теоретическое, практическое	3	Тема 6. Максимальный репост	МБОУ «СОШ №1 г.Ачхой-Мартан»	Наблюдение
7.		**17.06.2026** 10:00 – 12:25	Групповое, теоретическое, практическое	3	Тема 7. Безопасное общение	МБОУ «СОШ №1 г.Ачхой-Мартан»	Наблюдение
8.		**18.06.2026** 10:00 – 12:25	Групповое, теоретическое, практическое	3	Тема 8. Безопасное использование устройств и соединений	МБОУ «СОШ №1 г.Ачхой-Мартан»	Наблюдение
9.		**19.06.2026**	Групповое, теоретическо	3	Тема 9. Безопасность	МБОУ «СОШ №1	Наблюд

		10:00 – 12:25	е, практическое		информаций	г.Ачхой-Мартан»	ение
10.		**22.06.2026** 10:00 – 12:25	Групповое, теоретическое, практическое	3	Тема 10. Формирование кибербезопасного поведения	МБОУ «СОШ №1 г.Ачхой-Мартан»	Наблюдение
11.		**23.06.2026** 10:00 – 12:25	Групповое, теоретическое, практическое	3	Тема 11. Компьютерные и телефонные вирусы	МБОУ «СОШ №1 г.Ачхой-Мартан»	Наблюдение
12.		**24.06.2026** 10:00 – 12:25	Групповое, теоретическое, практическое	3	Тема 12. Цифровой след	МБОУ «СОШ №1 г.Ачхой-Мартан»	Наблюдение
13.		**25.06.2026** 10:00 – 12:25	Групповое, теоретическое, практическое	3	Тема 13. Безопасность в играх	МБОУ «СОШ №1 г.Ачхой-Мартан»	Наблюдение
14.		**26.06.2026** 10:00 – 12:25	Групповое, практическое	3	Итоговое занятие на платформе https://digital-likbez.datalesson.ru/	МБОУ «СОШ №1 г.Ачхой-Мартан»	Итоговая аттестация

Приложение 2

📥 Этап 1: Станция «Генератор паролей» (Индивидуальный зачет)

Проверка навыка создания надежных паролей и понимания конфиденциальности.

- **Задание «Секретный код»:** Ребенку выдается карточка с вымышленным персонажем (например, «Любитель котиков, родился в 2017 году, зовут Иван»). Задача — составить для него надежный пароль по правилу ассоциаций, используя буквы, цифры и спецсимволы (Правильный пример: Iv_Kot!2017, плохой пример: vanya2017).
- **Мини-тест «Кому сказать секрет?»:** Ребенок должен распределить карточки с людьми по двум коробкам: «Можно говорить пароль» и «Нельзя говорить пароль».
    - *Варианты на карточках:* мама/папа, лучший друг, администратор игры Roblox, учитель, незнакомец в чате.
    - *Критерий успеха:* В коробке «Можно» должны оказаться только родители.

📧 Этап 2: Станция «Детектив фишинга» (Устная или компьютерная проверка)

Проверка умения распознавать интернет-мошенничество.

- **Задание «Подозрительное письмо»:** На экране или на распечатанном бланке показываются два скриншота сообщений.
    - *Скриншот А:* Письмо от друга: «Привет, посмотри, какую классную собаку я сфотографировал сегодня [ссылка]».
    - *Скриншот Б:* Сообщение от незнакомца: «Внимание! Твой аккаунт заблокируют через 5 минут! Срочно перейди по ссылке и введи пароль: [опасная_ссылка]».
- **Вопросы к ребенку:**

1. Какое письмо опасное и почему? (Ожидаемый ответ: пугают, торопят, просят пароль).
2. Что нужно сделать с этим сообщением? (Ожидаемый ответ: заблокировать, не переходить по ссылке, рассказать родителям).

🌐 Этап 3: Станция «Цифровой след» (Практическая сортировка)

Проверка понимания того, какими данными нельзя делиться в сети.

- **Задание «Собери рюкзак блогера»:** На столе лежат карточки с изображениями различных данных. Ребенок должен «выложить в сеть» (положить в макет экрана телефона) только безопасные карточки.
    - *Опасные карточки (минус баллы):* фото билета на самолет со штрихкодом, домашний адрес, номер телефона мамы, фотография ключей от квартиры, геолокация школы.
    - *Безопасные карточки (плюс баллы):* фото домашнего кота, рисунок робота, отзыв о прочитанной книге, видео с выполненным трюком на самокате (без узнаваемых табличек с улицами).

🎮 Этап 4: Станция «Игровой патруль» (Разбор ситуаций / Кейс-метод)

Проверка правил поведения в онлайн-играх и сетях Wi-Fi.

Ребенку зачитываются три короткие ситуации, он должен выбрать правильное действие:

1. **Ситуация «Подарок в игре»:** «В Roblox незнакомый игрок предлагает бесплатно дать твоему персонажу редкую вещь, но для этого просит твой логин и пароль. Что ты сделаешь?»
2. **Ситуация «Открытый Wi-Fi»:** «Ты пришел в кафе и увидел сеть Wi-Fi без пароля Free_Internet. Тебе нужно зайти в свой аккаунт, где привязана мамина карта. Можно ли подключаться?»
3. **Ситуация «Обидчик в чате»:** «Другой игрок в чате начал писать тебе обидные слова и обзываться. Твои действия?»

🏆 Критерии оценки и подведение итогов

Вместо школьных оценок (двоек и пятерок) используется статусная система:

- **7–8 баллов (максимум):** Супер-агент кибербезопасности. Получает именной сертификат и наклейку на ноутбук/телефон «Мой гаджет под защитой».
- **5–6 баллов:** Младший аналитик безопасности. Получает сертификат и шпаргалку-памятку для повторения правил.
- **Менее 5 баллов:** Стажер. Проводится короткий разбор ошибок в игровой форме, после чего выдается «удостоверение ученика киберакадемии».
