МУНИЦИПАЛЬНОЕ КАЗЕННОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«УШЬИНСКАЯ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА»

«РАССМОТРЕНО»	«СОГЛАСОВАНО»	«УТВЕРЖДАЮ»
На заседании МО классных руководителей протокол № от «30» августа 2024 г. _____Е.И. Вербицкая	Заместитель директора по УР МКОУ «Ушьинская СОШ» _____Т.В. Шандра «30» августа 2024 г.	И. о. директора МКОУ «Ушьинская СОШ» _____ Т. В. Шандра «30» августа 2024 г.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 54FE2DED784B2FA4BE4F8C65C8D05299
Владелец: Шандра Татьяна Викторовна
Действителен: с 18.12.2023 до 12.03.2025

РАБОЧАЯ ПРОГРАММА
внеурочной деятельности общеинтеллектуального направления «Школьная кибердружина»
на 2024-2025 учебный год
5-6 класс

Составила:
педагог-организатор
Елена Петровна Серебрякова

д. Ушья, 2024 г.

Пояснительная записка

Программа внеурочной деятельности «Школьная кибердружина» для обучающихся 5-6 классов имеет общеинтеллектуальную направленность. Программа составлена в соответствии с требованиями ФГОС.

Рабочая программа внеурочной деятельности «Школьная кибердружина» составлена на основе:

1. Федеральный закон от 29.12.2012 № 273-ФЗ (ред. от 25.12.2023) «Об образовании в Российской Федерации» *(с изменениями и дополнениями, вступившими в силу с 01.05.2024)*;
2. Федеральный закон от 19.12.2023 № 618-ФЗ «О внесении изменений в Федеральный закон «Об образовании в Российской Федерации»;
3. Постановление Правительства Российской Федерации от 11.10.2023 № 1678 «Об утверждении Правил применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ» *(начало действия документа - 01.09.2024)*;
4. Приказ Минпросвещения РФ от 31.05.2021 № 287 (ред. от 22.01.2024) «Об утверждении федерального государственного образовательного стандарта основного общего образования» *(начало действия документа - 01.09.2024)*;
5. Приказ Минпросвещения РФ от 19.02.2024 № 110 «О внесении изменений в некоторые приказы Министерства образования и науки Российской Федерации и Министерства просвещения Российской Федерации, касающиеся федеральных государственных образовательных стандартов основного общего образования» *(начало действия документа - 01.09.2024)*;
6. Приказ Минобрнауки РФ от 17.12.2010 № 1897 (ред. от 08.11.2022) «Об утверждении федерального государственного образовательного стандарта основного общего образования»;
7. Приказ Минпросвещения РФ от 27.12.2023 № 1028 «О внесении изменений в некоторые приказы Министерства образования и науки Российской Федерации и Министерства просвещения Российской Федерации, касающиеся федеральных государственных образовательных стандартов основного общего образования и среднего общего образования»;
8. Приказ Минпросвещения РФ от 18.05.2023 № 370 (ред. от 19.03.2024) «Об утверждении федеральной образовательной программы основного общего образования» *(начало действия редакции - 01.09.2024)*;
9. Приказ Минпросвещения РФ от 01.02.2024 № 62 «О внесении изменений в некоторые приказы Министерства просвещения Российской Федерации, касающиеся федеральных образовательных программ основного общего образования и среднего общего образования» *(начало действия документа - 01.09.2024)*;
10. Приказ Минпросвещения РФ от 04.10.2023 № 738 «Об утверждении федерального перечня электронных образовательных ресурсов, допущенных к использованию при реализации имеющих государственную аккредитацию образовательных программ начального общего, основного общего, среднего общего образования»;
11. Приказ Минпросвещения РФ от 31.08.2023 № 650 «Об утверждении Порядка осуществления мероприятий по профессиональной ориентации обучающихся по образовательным программам основного общего и среднего общего образования»;
12. Постановление Главного государственного санитарного врача РФ от 28.09.2020 № 28 «Об утверждении санитарных правил СП 2.4.3648-20 «Санитарно-эпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодежи» (вместе с «СП 2.4.3648-20. Санитарные правила...»);
13. Постановление Главного государственного санитарного врача РФ от 28.01.2021 № 2 (ред. от 30.12.2022) «Об утверждении санитарных правил и норм СанПиН 1.2.3685-21 «Гигиенические нормативы и требования к обеспечению безопасности и (или) безвредности для человека факторов среды обитания» (вместе с «СанПиН 1.2.3685-21. Санитарные правила и нормы...»);

14. Постановление Главного государственного санитарного врача РФ от 30.12.2022 № 24 «О внесении изменений в санитарные правила и нормы СанПиН 1.2.3685-21 «Гигиенические нормативы и требования к обеспечению безопасности и (или) безвредности для человека факторов среды обитания», утвержденные постановлением Главного государственного санитарного врача Российской Федерации от 28.01.2021 № 2»;

15. Письмо Минпросвещения РФ от 22.05.2023 № 03-870 «О направлении информации» (вместе с «Методическими рекомендациями по введению федеральных основных общеобразовательных программ»);

16. Письмо Минпросвещения РФ от 26.02.2021 № 03-205 «О методических рекомендациях» (вместе с «Методическими рекомендациями по обеспечению возможности освоения основных образовательных программ обучающимися 5-11 классов по индивидуальному учебному плану»);

17. Методические рекомендации «МР 2.4.0331-23. 2.4. Гигиена детей и подростков. Методические рекомендации по обеспечению оптимизации учебной нагрузки в общеобразовательных организациях. Методические рекомендации» (утв. Главным государственным санитарным врачом РФ 10.11.2023);

18. Методические рекомендации «МР 2.4.0330-23. 2.4. Гигиена детей и подростков. Методические рекомендации по обеспечению санитарно-эпидемиологических требований при реализации образовательных программ с применением электронного обучения и дистанционных образовательных технологий. Методические рекомендации» (утв. Главным государственным санитарным врачом РФ 29.08.2023) (вместе с «Рекомендациями для родителей (законных представителей) по сокращению экранного времени у детей»);

19. Приказ Департамента образования и науки Ханты-Мансийского автономного округа – Югры от 18.05.2023 № 10-П-1197 «Об утверждении сроков перехода на обновленные федеральные государственные образовательные стандарты начального общего, основного общего и среднего общего образования в образовательных организациях Ханты-Мансийского автономного округа – Югры»;

20. Устав МКОУ «Ушьинская СОШ»;

21. Основная образовательная программа основного общего образования МКОУ «Ушьинская СОШ» (в том числе: учебный план на 2024-2025 учебный год; календарный учебный график на 2024-2025 учебный год).

Общая характеристика курса

Развитие информационного общества предполагает развитие информационных технологий во всех сферах жизни. Наряду с позитивными результатами информатизация также означает и появление новых угроз. Безопасность в информационном обществе является одним из основных направлений фундаментальных исследований в области информационных технологий.

Педагогическая ценность данной программы заключается в том, что киберугрозы существуют везде, где применяются информационные технологии, следовательно, любой человек может как в профессиональной деятельности, так и в обыденной жизни столкнуться и со спамом, и с вирусами, и со взломом компьютера, и с многими другими проблемами, на которые нужно оперативно реагировать, предотвращая их появление. Программа поможет разобраться в тонкостях завуалированных и нежелательных элементов в киберпространстве, их составляющих, в количественной и качественной защите интеллектуальной собственности и безопасности. Ребенок самостоятельно сможет определять состав киберугроз, принимать решение о их нейтрализации.

Новизна программы заключается в развитии у обучающихся нового взгляда на современные информационные технологии, что способствует пониманию состава различных киберугроз, их происхождения.

Актуальность программы. Всё большее значение приобретает проблема культуры безопасного поведения в киберпространстве. Выполняя социальный заказ общества, современная система образования должна способствовать подготовке подрастающего поколения к жизни, будущей профессиональной деятельности в высокоразвитом информационном обществе. Создание на занятиях ситуаций активного поиска, предоставление возможности сделать собственное «открытие», знакомство с оригинальными путями рассуждений позволят обучающимся реализовать свои возможности, приобрести уверенность в своих силах. В настоящий момент существует острая необходимость подготовки обучающихся, которые смогут эффективно противостоять существующим информационным угрозам.

Отличительной особенностью программы является формирование информационной, научно-технической и эстетической культуры. Программа позволяет изучить различные прикладные программные пакеты и веб-сервисы. Эта программа не даёт ребёнку «уйти в виртуальный мир», учит видеть красоту и привлекательность реального мира, помогает не только защищаться от информационных угроз, но и создавать что-то новое, востребованное обществом.

Категория обучающихся: обучающиеся 5, 6 класса (1 группа – 5 класс, 2 группа – 6 класс).

Срок реализации программы: 34 часа.

Форма и режим занятий: занятия проводятся 1 раз в неделю по 1 академическому часу для каждой группы.

Цели программы: знакомство с принципами обеспечения безопасности в информационном обществе, развитие навыков применения правил кибербезопасности в современном киберпространстве.

Задачи:

Обучающие:

- познакомить обучающихся с основными киберугрозами современного государства и личности, методами противодействия данным угрозам;
- рассмотреть модели функционирования молодежных кибердружин;
- развить познавательные интересы и интеллектуальные способности в процессе ознакомления с основными киберугрозами и их ролью в защите информации.

Развивающие:

- сформировать навыки работы со специализированным программным обеспечением;
- составлять план действий и корректировать его;
- уметь делать выводы и заключения, анализируя проделанную работу;
- формировать информационно-коммуникационную грамотность;
- уметь самостоятельно искать, отбирать, анализировать, представлять, передавать информацию, используя современные информационные технологии.

Воспитательные:

- сформировать у обучающихся представления об основах законодательства в сфере противодействия распространению противоправного информационного контента, ознакомить их с механизмами работы правоохранительных органов в данной сфере;
- выделить ключевые проблемы сохранения национальной безопасности России в условиях информационного противостояния;
- способствовать популяризации профессий, связанных с информационными технологиями;
- обучить проведению уроков безопасного Интернета для обучающихся младших классов.

Программа внеурочной деятельности «Школьная кибердружина» основана на взаимосвязи процессов обучения, воспитания и развития обучающихся. Особенности организации образовательного процесса. Учебный материал рассчитан на последовательное и постепенное освоение теоретических знаний и приобретение практических умений и навыков.

Структура занятий. Занятия строятся в следующей последовательности:

– изучение теоретического материала;

– практические задания (форма организации зависит от сложности материала);

– обсуждение.

Планируемые результаты

Метапредметные результаты:

Овладеть навыками самостоятельного приобретения новых знаний, организации учебной деятельности, поиска средств её осуществления.

Планировать пути достижения целей на основе самостоятельного анализа условий и средств их достижения, выделять альтернативные способы достижения цели и выбирать наиболее эффективный способ, осуществлять познавательную рефлексию в отношении действий по решению учебных и познавательных задач.

Понимать проблему, ставить вопросы, выдвигать гипотезу, давать определение понятиям, классифицировать, структурировать материал, проводить эксперименты, аргументировать собственную позицию, формулировать выводы и заключения.

Соотносить свои действия с планируемыми результатами, осуществлять контроль своей деятельности в процессе достижения результата, определять способы действий в рамках предложенных условий и требований, корректировать свои действия в соответствии с изменяющейся ситуацией.

Создавать, применять и преобразовывать знаки и символы, модели и схемы для решения учебных и познавательных задач.

На практике пользоваться основными логическими приемами, методами наблюдения, моделирования, объяснения, решения проблем, прогнозирования и др.

Выполнять познавательные и практические задания, в том числе проектные.

Самостоятельно и аргументированно оценивать свои действия и действия одноклассников, содержательно обосновывая правильность или ошибочность результата и способа действия, адекватно оценивать объективную трудность как меру фактического или предполагаемого расхода ресурсов на решение задачи, а также свои возможности в достижении цели определенной сложности.

Работать в группе – эффективно сотрудничать и взаимодействовать на основе координации различных позиций при выработке общего решения в совместной деятельности;

слушать партнера, формулировать и аргументировать свое мнение, корректно отстаивать свою позицию и координировать ее с позиции партнеров, в том числе в ситуации столкновения интересов; продуктивно разрешать конфликты на основе учета интересов и позиций всех его участников, поиска и оценки альтернативных способов разрешения конфликтов.

Предметные результаты.

Обучающиеся должны знать:

- основные виды угроз в современном информационном пространстве;
- принципы функционирования молодежных кибердружин;
- понятие «киберпростаранство» и основные принципы его защиты;
- наиболее распространённые виды киберпреступлений и правовые аспекты защиты киберпространства;
- основы законодательства в сфере противодействия распространению противоправного информационного контента и механизмы работы правоохранительных органов в данной сфере.

Обучающиеся должны уметь:

- соблюдать нормы информационной этики и права;
- просчитывать угрозы безопасности государства и личности в современном информационном пространстве;
- определять специфику киберугроз в различных сферах деятельности;
- выявлять угрозы и возможности использования «больших данных» в различных сферах деятельности;
- создавать баннеры, видеоролики и виртуальные экспозиции как элементы патриотического и просветительского Интернет-контента;
- проводить уроки безопасного Интернета для обучающихся младших классов как в очном, так и в дистанционном режиме (с применением специализированных информационно-коммуникационных решений).

Обучающиеся должны владеть:

- терминологией в сфере информационной безопасности, растровой и векторной графики, 3D-графики, видеомонтажа, веб-технологий.

Содержание курса

Учебно-тематическое планирование

5-6 класс

Таблица 1

№	Тема	Теория	Практика	Всего	Форма контроля
Модуль 1. Основы безопасного поведения в сети Интернет					
1.	Работа молодежных кибердружин.	7	1	8	Беседа
2.	Новые технологии: возможности и порождаемые ими киберугрозы.	7	1	8	Беседа
Модуль 2. Анализ Интернет-контента					
3.	Автоматизированная информационная система «Поиск».	6	5	11	Практическая работа
4.	Самостоятельный анализ Интернет-контента	4	2	6	Практическая работа
5.	Итоговая аттестация. Практическая работа	0	1	1	Практическая работа
	Итого:	24	10	34	

Содержание курса

Модуль 1. Основы безопасного поведения в сети Интернет.

Тема 1. Работа молодежных кибердружин.

Тема 1.1. Вводное занятие. Инструктаж по ТБ. Обсуждение программ и технологий, изучаемых в ходе работы кружка.

Тема 1.2. Работа молодежных кибердружин.

Тема 1.3. Проведение уроков безопасного Интернета в школах.

Тема 1.4. Большие данные: угрозы и возможности.

Тема 1.5. Защита персональных данных в сети «Интернет».

Тема 1.6. Кейсы о том, какие угрозы для пользователя таит в себе обработка третьими лицами больших пользовательских данных.

Тема 1.7. Какие возможности в различных сферах открывает сбор и обработка больших данных.

Тема 1.8. Как государство защищает киберпространство. Информационные войны. Защита государства и защита киберпространства.

Тема 2. Новые технологии: возможности и порождаемые ими киберугрозы.

Тема 2.1. Ознакомление с программами, используемыми в ходе работы кружка.

Тема 2.2. Понятие «сквозные технологии»: новые возможности и угрозы.

Тема 2.3. Технологии искусственного интеллекта и вопросы кибербезопасности. Сильный и слабый искусственные интеллект.

Тема 2.4. Подходы к созданию искусственного интеллекта: «снизу» и «сверху». Применение элементов искусственного интеллекта в различных отраслях. Применение элементов искусственного интеллекта правоохранительными органами.

Тема 2.5. Технологии «больших данных»: основные сферы применения.

Тема 2.6. Квантовые технологии. Основные представления о квантовой криптографии и квантовых компьютерах.

Тема 2.7. Новые угрозы в сфере взлома каналов данных.

Тема 2.8. Ознакомление с программами, используемыми в ходе работы кружка.

Модуль 2. Анализ Интернет-контента

Тема 3. Автоматизированная информационная система «Поиск».

Тема 3.1. Изучение возможностей и интерфейса Автоматизированной информационной системы «Поиск».

Тема 3.2. Роль кибердружинника и информационном пространстве

Тема 3.3. Основные правила экспертизы информационного пространства

Тема 3.4. Работа с материалами

Тема 3.5. Присвоение меток

Тема 3.6. Работа со списками материалов.

Тема 3.7. Правила фильтрации.

Тема 3.8. Практическая работа. Поиск.

Тема 3.9. Отправка материала в Роскомнадзор.

Тема 3.10. Отправка материалов в правоохранительные органы.

Тема 3.11. Практическая работа.

Тема 4. Самостоятельный анализ Интернет-контента.

Тема 4.1. Ручная проверка

Тема 4.2. Подозрительный контент

Тема 4.3. Проверенный контент.

Тема 4.4. Как происходит проверка контента.

Тема 4.5. Заявка на блокировку.

Тема 4.6. Практическая работа. Образовательный контент.

Тема 5. Итоговая аттестация. Практическая работа

Формы подведения итогов реализации программы внеурочной деятельности

Контроль и оценка знаний предполагает степень достижения обучающихся в решении поставленных задач.

Цель оценки заключается в формировании у ребенка уважительного отношения к себе и поддержания уверенности его в своих силах, возможностях и способностях при освоении учебного материала.

Основными формами контроля реализации программы «Школьная кибердружина» являются:

- индивидуальная;
- фронтальная;
- групповая;
- наблюдения педагога.

Виды контроля реализации дополнительной общеразвивающей программы:

- вводный;
- текущий (проводится на всех этапах изучения);
- тематический (проводится с целью проверки усвоения программного материала по разделам учебно-тематического плана);
- итоговый.

Данные виды контроля дают возможность педагогу оценить уровень знаний, умений и практических навыков каждого обучающегося по данной программе. Контроль носит систематический характер и осуществляется в конце каждой изученной темы при помощи практических работ, носящих групповой и индивидуальный характер.

Для отслеживания динамики освоения данной программы и анализа результатов образовательной деятельности в течение всего учебного процесса осуществляется мониторинг, который включает первичную диагностику, текущий контроль и итоговую аттестацию.

Вводный контроль (первичная диагностика) проводится в начале учебного процесса для определения уровня подготовки обучающихся. Форма проведения – собеседование.

Текущий контроль осуществляется в процессе проведения каждого учебного занятия и направлен на закрепление теоретического материала по изучаемой теме и на формирование практических умений. Форма проведения – педагогическое наблюдение, самооценка обучающихся.

Методическое обеспечение программы

В ходе реализации программы возможно использование различных методов и приёмов организации занятий.

При проектировании занятий необходимо придерживаться следующих принципов системно-деятельностного подхода:

– принцип активной включенности обучающихся в освоение предлагаемой информации;
– принцип деятельности;
– принцип доступности;
– принцип системности;
– принцип рефлексивности;
– принцип мотивации;
– принцип открытости содержания образования.

Принцип активной включенности обучающихся в освоение предлагаемой

Введение деятельностных технологий в процесс обучения предполагает учет следующих критериев:

- интерактивность;
- игровой, театрализованный контекст;
- совместнаю деятельность ребенка и взрослого;

- учет психологовозрастных особенностей обучающихся;
- использование социокультурных технологий.

Принцип открытости содержания образования предполагает достаточно гибкое использование педагогом предложенной конструкции, не допуская при этом искажения логики, содержательной точности и достоверности информации.

Материально-техническое обеспечение

Реализация программы внеурочной деятельности «Школьная кибердружина» включает следующий перечень необходимого оборудования:

1) компьютеры;
2) мультимедийный проектор;
3) интерактивная доска;
4) доступ к сети-Интернет;
5) программное обеспечение.

Используемая литература

Литература для педагогов

Василенко В.А., Женса А.В. Информационная безопасность и защита информации - М.: РХТУ им. Д.И. Менделеева, 2016 г. - 171 с.

Горюхина Е.Ю., Литвинова Л.И., Ткачева Н.В. Информационная безопасность - Воронеж: Воронежский ГАУ, 2015 г. - 220 с.

Джонс Кейт Дж., Шема Майк, Джонсон Бредли С. Инструментальные средства обеспечения безопасности. - 2-е изд. - М.: НОУ "Интуит", 2016 г. - 914 с.

Кириленко В.П., Алексеев Г.В. Международное право и информационная безопасность государства - СПб.: ГИКиТ, 2016 г. - 396 с.

Леонов А.П. Актуальные проблемы информационной безопасности в контексте глобализации - Минск: Академия МВД, 2015 г. - 5 с.

Нестеров С.А. Основы информационной безопасности. - Учебное пособие - 3-е изд., стер. - СПб.: Лань, 2017 г. - 324 с.

Пулко Т.А. Введение в информационную безопасность. - Учебнометодическое пособие. - Минск: БГУИР, 2016 г. - 156 с.

Сычев Ю.Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов. - М.: РЭУ им. Г.В. Плеханова, 2017 г. - 207 с.

Теплов Э.П. и др. Гуманитарные аспекты информационной безопасности: методология и методика поиска истины, построения доказательств и защиты от манипуляций. - Теплов Э.П., Гатчин Ю.А., Ныркov А.П., Сухостат В.В. – Учебное пособие. – СПб: Университет ИТМО, 2016 г. – 120 с.

Литература для детей и родителей

Бирюков А.А. Информационная безопасность защита и нападение 2-е издание: Издательство: ДМК-Пресс., 2017 г., 434 с.

Бирюков А.А. Информационная безопасность защита и нападение.: Издательство: ДМК-Пресс., 2012 г., 474 с.

Колесниченко Денис. Анонимность и безопасность в интернете. От чайника к пользователю. Самоучитель Издательство: БХВ-Петербург, 2012 г., 240с.

Мазаник Сергей. Безопасность компьютера. Защита от сбоев, вирусов и неисправностей: издательство: ЭКСМО, 2014 г., 256 с.

Мэйволд Э. Безопасность сетей (2-е изд.) Книги» Сетевые Технологии. Название: Безопасность сетей: Издательство: М.: НОУ "Интуит", 2016 г.,571 с.

Савченко Е. Кто, как и зачем следит за вами через Интернет: Москва - Третий Рим, 2012 г., 100 с.

Яковлев В.А. Шпионские и антишпионские штучки: Техническая литература Издательство: Наука и Техника, 2015 г., 320 с.

"Березовый лес" или "лес березовый" /П. Лауфер//Юный эрудит. – 2014 г. - № 3. - С. 24-26.

Сорокина Е.В., Третьяк Т.М. Здоровье и безопасность детей в мире компьютерных технологий и Интернет. [Текст] Учебно-методический комплект. - М.: СОЛОНПРЕСС, 2010 г. - 176 с.: ил.

Интернет-ресурсы:

http://www.kaspersky.ru - антивирус «Лаборатория Касперского»;

http://www.onlandia.org.ua/rus/ - безопасная web-зона;

http: // www.interneshka.net - международный онлайн-конкурс по безопасному использованию Интернета;

http://www.saferinternet.ru - портал Российского Оргкомитета по безопасному использованию Интернета;

http://www.rgdb.ru - Российская государственная детская библиотека;

http://www.saferinternet.ru/ - Безопасный Интернет. Портал Российского Оргкомитета по проведению Года Безопасного Интернета. Мероприятия, Интернет и законодательство, проблемы и решения, международные ресурсы;

Полезные ссылки для обучающихся:

http://www.symantec.com/ru/ru/norton/clubsymantec/library/articleClubSymantec единый источник сведений о безопасности в Интернете. Статья для родителей «Расскажите детям о безопасности в Интернете». Информация о средствах родительского контроля;

http://www.obzh.info/novosti/novoe/bezopasnost-detei-v-internete.html - Личная безопасность. Основы безопасности жизни. Рекомендации взрослым: как сделать посещение Интернета для детей полностью безопасным;

http://www.ifap.ru/library/book099.pdf - «Безопасность детей в Интернете», компания Microsoft. Информация для родителей: памятки, советы, рекомендации;

http://www.interneshka.net/children/index.phtml - «Интернешка» - детский онлайн-конкурс по безопасному использованию сети Интернет. Советы детям, педагогам и родителям, «полезные ссылки». Регистрация и участие в конкурсе по безопасному использованию сети Интернет;

Календарно-тематическое планирование
5-6 класс

№	Тема	Кол-во часов	Дата план	Дата факт
1.	Вводное занятие. Инструктаж по ТБ. Обсуждение программ и технологий, изучаемых в ходе работы кружка	1		
2.	Работа молодежных кибердружин	1		
3.	Проведение уроков безопасного Интернета в школах	1		
4.	Большие данные: угрозы и возможности	1		
5.	Защита персональных данных в сети «Интернет»	1		
6.	Кейсы о том, какие угрозы для пользователя таит в себе обработка третьими лицами больших пользовательских данных	1		
7.	Какие возможности в различных сферах открывает сбор и обработка больших данных	1		
8.	Как государство защищает киберпространство. Информационные войны. Защита государства и защита киберпространства	1		
9.	Ознакомление с программами, используемыми в ходе работы кружка	1		
10	Понятие «сквозные технологии»: новые возможности и угрозы	1		
11	Технологии искусственного интеллекта и вопросы кибербезопасности. Сильный и слабый искусственные интеллект	1		
12	Подходы к созданию искусственного интеллекта: «снизу» и «сверху». Применение элементов искусственного интеллекта в различных отраслях. Применение элементов искусственного интеллекта правоохранительными органами	1		
13	Технологии «больших данных»: основные сферы применения	1		
14	Квантовые технологии. Основные представления о квантовой криптографии и квантовых компьютерах	1		
15	Новые угрозы в сфере взлома каналов данных	1		
16	Ознакомление с программами, используемыми в ходе работы кружка	1		
17	Изучение возможностей и интерфейса Автоматизированной информационной системы «Поиск»	1		
18	Роль кибердружинника и информационном пространстве	1		
19	Основные правила экспертизы информационного пространства	1		
20	Работа с материалами	1		
21	Присвоение меток	1		
22	Работа со списками материалов	1		
23	Правила фильтрации	1		
24	Практическая работа. Поиск	1		
25	Отправка материала в Роскомнадзор	1		
26	Отправка материалов в правоохранительные органы	1		
27	Практическая работа	1		
28	Ручная проверка	1		
29	Подозрительный контент	1		
30	Проверенный контент	1		

31	Как происходит проверка контента	1		
32	Заявка на блокировку	1		
33	Практическая работа. Образовательный контент	1		
34	**Итоговая аттестация. Практическая работа**	1		
	Итого:	34		