Муниципальное бюджетное общеобразовательное учреждение
«Заинская средняя общеобразовательная школа № 2»
Заинского муниципального района Республики Татарстан

Принята на заседании
Педагогического совета
Протокол№1
от 29 августа 2024 года

«Утверждаю»
Директор МБОУ «ЗСОШ №2»
_____Данилова В.А.
Приказ №146
«29» августа 2024 г.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП
Сертификат: 7B68A90084B089A04SDC912A9EDE98A1
Владелец: Данилова Валентина Александровна
Действителен с 21.09.2023 до 21.12.2024

ДОПОЛНИТЕЛЬНАЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ

ОБЩЕРАЗВИВАЮЩАЯ ПРОГРАММА

«Цифровая гигиена»

для обучающихся 5-9 классов

на 2024-2025 учебный год

Автор-составитель:

Галимова Р.К., педагог дополнительного образования

ЗАИНСК 2024

Информационная карта образовательной программы

1.	Образовательная организация	МБОУ «ЗСОШ №2» ЗМР РТ
2.	Полное название программы	Цифровая гигиена
3.	Направленность программы	техническая
4.	Сведения о разработчиках	
4.1	ФИО, должность	Галимова Розалия Кирамутдиновна, педагог дополнительного образования
5.	Сведения о программе:	
5.1	Срок реализации	1 год
5.2	Возраст обучающихся	11-15 лет
5.3	Характеристика программы: - тип программы - вид программы - принцип проектирования программы - форма организации содержания и учебного процесса	 модифицированная дополнительная общеобразовательная общеразвивающая программа однопрофильная Принцип последовательного и постепенного расширения теоретических знаний, практических умений и навыков. Групповая
5.4	Цель программы	Обеспечение правильного ввода ребенка в цифровое пространство и корректировка его поведения в виртуальном мире
5.5	Образовательные модули (в соответствии с уровнями сложности содержания и материала программы)	Стартовый уровень – расширение основных тем по предмету информатика
6.	Формы и методы образовательной деятельности	Групповые и индивидуальные практические занятия, самостоятельные работы, творческие отчеты
7.	Формы мониторинга результативности	Беседа с целью проверки полученных знаний. Входная, промежуточная и итоговая аттестация (творческая работа). *Входная:* педагогическое наблюдение, собеседование. *Текущая:* устный опрос, карточки-задания, практическая работа. *Итоговая:* творческая проектная работа
8.	Результат реализации программы	виды аттестации детей, участие в конкурсах
9.	Дата утверждения и последней корректировки программы	29.08.2024г.
10.	Рецензенты	Заместитель директора по воспитательной работе МБОУ «ЗСОШ №2» Красильникова Е.Н.

Пояснительная записка

Программа разработана на основе дополнительной общеразвивающей программы «Заинская средняя общеобразовательная школа№2» ЗМР РТ на 2024-2025 учебный год, принятой на заседании педагогического совета, протокол№1 от 29.08.2024

Основополагающими при проектировании и составлении дополнительной общеразвивающей программы кружка «Цифровая гигиена» являются следующие документы:

1. Федеральный закон об образовании в Российской Федерации от 29.12.2012 №273-ФЗ (с изменениями и дополнениями);

2. Федеральный закон от 31 июля 2020 г. № 304-ФЗ «О внесении изменений в Федеральный закон «Об образовании в Российской Федерации» по вопросам воспитания обучающихся»;

3. Концепция развития дополнительного образования детей до 2030 года, утвержденная Распоряжением Правительства РФ от 31 марта 2022 г. №678-р;

4. Федеральный проект «Успех каждого ребенка» в рамках Национального проекта «Образование», утвержденного Протоколом заседания президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 3.09.2018 №10;

5. Приказ Министерства просвещения Российской Федерации от 3.09.2019 №467 «Об утверждении Целевой модели развития региональных систем дополнительного образования детей»;

6. Федеральный закон от 13 июля 2020 г. №189-ФЗ «О государственном (муниципальном) социальном заказе на оказание государственных (муниципальных) услуг в социальной сфере» (с изменениями и дополнениями, вступившими в силу с 28.12.2022 г.);

7. Приказ Министерства просвещения Российской Федерации от 27 июля 2022 г. №629 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам»;

8. СП 2.4. 3648-20 «Санитарно-эпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодежи», утвержденные Постановлением Главного государственного санитарного врача Российской Федерации от 28.09.2020 г. №28;

9. «Методические рекомендации по проектированию и реализации дополнительных общеобразовательных общеразвивающих программ» в новой редакции, направленные Республиканским центром внешкольной работы Республики Татарстан, г.Казань, 2023 г.;

10. Устав МБОУ «Заинская средняя общеобразовательная школа№2» ЗМР РТ;

Актуальность программы:

Предлагаемая программа предназначена для обучающихся 5 – 9 классов и носит пропедевтический характер поведения обучающихся в виртуальном мире.

Концепция обучения ориентирована на расширение основных тем по учебным предметам «Информатика» и «Основы безопасности жизнедеятельности» за счет привлечения жизненного опыта обучающихся в использовании всевозможных технических устройств (персональных компьютеров, планшетов, смартфонов и пр.), позволяет правильно ввести ребенка в цифровое пространство и корректировать его поведение в виртуальном мире.

Основное содержание программы представлено разделами «Безопасность общения», «Безопасность устройств», «Безопасность информации». Каждый раздел учебного курса завершается выполнением проектной работы по одной из тем, предложенных на выбор учащихся

Цели программы**:**

- формирование активной позиции школьников в получении знаний и умений выявлять информационную угрозу, определять степень ее опасности, предвидеть последствия информационной угрозы и противостоять им;
- обеспечение условий для профилактики негативных тенденций в информационной культуре учащихся, повышения защищенности детей от информационных рисков и угроз.

Задачи программы**:**

- сформировать общекультурные навыки работы с информацией (умения, связанные с поиском, пониманием, организацией, архивированием цифровой информации и ее критическим осмыслением, а также с созданием информационных объектов с использованием цифровых ресурсов (текстовых, изобразительных, аудио и видео);
- создать условия для формирования умений, необходимых для различных форм коммуникации (электронная почта, чаты, блоги, форумы, социальные сети и др.) с различными целями и ответственного отношения к взаимодействию в современной информационно-телекоммуникационной среде;
- сформировать знания, позволяющие эффективно и безопасно использовать технические и программные средства для решения различных задач, в том числе использования компьютерных сетей, облачных сервисов и т.п.;
- сформировать знания, умения, мотивацию и ответственность, позволяющие решать с помощью цифровых устройств и интернета различные повседневные задачи, связанные с конкретными жизненными ситуациями, предполагающими удовлетворение различных потребностей;
- сформировать навыки по профилактике и коррекции зависимого поведения школьников, связанного с компьютерными технологиями и Интернетом.

Основные виды и формы учебных занятий:

Демонстрационная - работу на компьютере выполняет учитель, а учащиеся наблюдают.

Фронтальная - недлительная, но синхронная работа учащихся по освоению или закреплению материала под руководством учителя.

Самостоятельная - выполнение самостоятельной работы с компьютером в пределах одного, двух или части урока. Учитель обеспечивает индивидуальный контроль за работой учащихся.

Творческий проект – выполнение работы в микро группах на протяжении нескольких занятий

Работа консультантов – ученик контролирует работу всей группы кружка.

Занятия кружка несут детям не только приятные минуты совместной творческой игры, но и служат ключом для собственного творчества.

Форма контроля

В качестве домашнего задания предлагаются задания для учащихся по сбору и изучению информации по выбранной теме.

Контроль осуществляется в форме творческих проектов, самостоятельной разработки работ.

Методы обучения

1. **Познавательный** (восприятие, осмысление и запоминание учащимися нового материала с привлечением наблюдения готовых примеров, моделирования, изучения иллюстраций, восприятия, анализа и обобщения демонстрируемых материалов);
2. **Метод проектов** (при усвоении и творческом применении навыков и умений в процессе разработки собственных моделей)
3. **Систематизирующий** (беседа по теме, составление систематизирующих таблиц, схем и т.д.)
4. **Контрольный метод** (при выявлении качества усвоения знаний, навыков и умений и их коррекция в процессе выполнения практических заданий)
5. **Групповая работа** (используется при разработке проектов)

Срок реализации программы: 1 год
Возраст обучающихся**:** возраст обучающихся: 11-15 лет
Наполняемость учебной группы: 15 человек.
Режим занятий: занятия учебной группы проводятся *четыре раза в неделю по 2 часа.*

Планируемые результаты обучения:

Предметные:

Выпускник научится:

- ✓ анализировать доменные имена компьютеров и адреса документов в интернете;
- ✓ безопасно использовать средства коммуникации;
- ✓ безопасно вести и применять способы самозащиты при попытке мошенничества;
- ✓ безопасно использовать ресурсы интернета.

Выпускник овладеет:

- ✓ приемами безопасной организации своего личного пространства данных с использованием индивидуальных накопителей данных, интернет-сервисов и т.п.

Выпускник получит возможность овладеть:

- ✓ основами соблюдения норм информационной этики и права;
- ✓ основами самоконтроля, самооценки, принятия решений и осуществления

осознанного выбора в учебной и познавательной деятельности при формировании современной культуры безопасности жизнедеятельности;

- ✓ использовать для решения коммуникативных задач в области безопасности жизнедеятельности различные источники информации, включая Интернет-ресурсы и другие базы данных.

Метапредметные:

Регулятивные универсальные учебные действия.

Обучающийся сможет:

- ✓ идентифицировать собственные проблемы и определять главную проблему;
- ✓ выдвигать версии решения проблемы, формулировать гипотезы, предвосхищать конечный результат;
- ✓ ставить цель деятельности на основе определенной проблемы и существующих возможностей;
- ✓ выбирать из предложенных вариантов и самостоятельно искать средства/ресурсы для решения задачи/достижения цели;
- ✓ составлять план решения проблемы (выполнения проекта, проведения исследования);
- ✓ описывать свой опыт, оформляя его для передачи другим людям в виде технологии решения практических задач определенного класса;
- ✓ оценивать свою деятельность, аргументируя причины достижения или отсутствия планируемого результата;
- ✓ находить достаточные средства для выполнения учебных действий в изменяющейся ситуации и/или при отсутствии планируемого результата;
- ✓ работая по своему плану, вносить коррективы в текущую деятельность на основе анализа изменений ситуации для получения запланированных характеристик продукта/результата;
- ✓ принимать решение в учебной ситуации и нести за него ответственность.

Познавательные универсальные учебные действия.

Обучающийся сможет:

- ✓ выделять явление из общего ряда других явлений;
- ✓ определять обстоятельства, которые предшествовали возникновению связи между явлениями, из этих обстоятельств выделять определяющие, способные быть причиной данного явления, выявлять причины и следствия явлений;
- ✓ строить рассуждение от общих закономерностей к частным явлениям и от частных явлений к общим закономерностям;
- ✓ излагать полученную информацию, интерпретируя ее в контексте решаемой задачи;
- ✓ самостоятельно указывать на информацию, нуждающуюся в проверке, предлагать и применять способ проверки достоверности информации;
- ✓ критически оценивать содержание и форму текста;
- ✓ определять необходимые ключевые поисковые слова и запросы.

Коммуникативные универсальные учебные действия.

Обучающийся сможет:

- ✓ строить позитивные отношения в процессе учебной и познавательной деятельности;
- ✓ критически относиться к собственному мнению, с достоинством признавать ошибочность своего мнения (если оно таково) и корректировать его;
- ✓ договариваться о правилах и вопросах для обсуждения в соответствии с поставленной перед группой задачей;
- ✓ делать оценочный вывод о достижении цели коммуникации непосредственно после завершения коммуникативного контакта и обосновывать его;
- ✓ целенаправленно искать и использовать информационные ресурсы, необходимые для решения учебных и практических задач с помощью средств ИКТ;
- ✓ выбирать, строить и использовать адекватную информационную модель для передачи своих мыслей средствами естественных и формальных языков в соответствии с условиями коммуникации;
- ✓ использовать компьютерные технологии (включая выбор адекватных задаче инструментальных программно-аппаратных средств и сервисов) для решения информационных и коммуникационных учебных задач, в том числе: вычисление, написание писем, сочинений, докладов, рефератов, создание презентаций и др.;
- ✓ использовать информацию с учетом этических и правовых норм;
- ✓ создавать информационные ресурсы разного типа и для разных аудиторий, соблюдать информационную гигиену и правила информационной безопасности.

Личностные:

- ✓ осознанное, уважительное и доброжелательное отношение к окружающим людям в реальном и виртуальном мире, их позициям, взглядам, готовность вести диалог с другими людьми, обоснованно осуществлять выбор виртуальных собеседников;
- ✓ готовность и способность к осознанному выбору и построению дальнейшей индивидуальной траектории образования на базе ориентировки в мире профессий и профессиональных предпочтений, с учетом устойчивых познавательных интересов;
- ✓ освоенность социальных норм, правил поведения, ролей и форм социальной жизни в группах и сообществах;
- ✓ сформированность понимания ценности безопасного образа жизни; интериоризация правил индивидуального и коллективного безопасного поведения в информационно-телекоммуникационной среде.

Содержание курса

Введение
Инструктаж по ТБ. Введение в предмет. Знакомство с предметом.

Безопасность общения
Общение в социальных сетях и мессенджерах.
Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент.
С кем безопасно общаться в интернете.
Персональные данные как основной капитал личного пространства в цифровом мире. Правила добавления друзей в социальных сетях. Профиль пользователя. Анонимные социальные сети.
Пароли для аккаунтов социальных сетей.
Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей.
Безопасный вход в аккаунты.
Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.
Настройки конфиденциальности в социальных сетях.
Настройки приватности и конфиденциальности в разных социальных сетях.
Приватностьи конфиденциальность в мессенджерах.
Публикация информации в социальных сетях.
Персональные данные. Публикация личной информации.
Кибербуллинг.
Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга.
Публичные аккаунты.
Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.
Фишинг.
Фишинг как мошеннический прием. Популярные варианты распространения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах.
Выполнение и защита индивидуальных и групповых проектов.

Безопасность устройств
Что такое вредоносный код.
Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.
Распространение вредоносного кода.
Способы доставки вредоносных кодов. Исполняемые файлы и расширения вредоносных кодов. Вредоносная рассылка. Вредоносные скрипты. Способы выявления наличия вредоносных кодов на устройствах. Действия при обнаружении вредоносных кодов на устройствах.
Методы защиты от вредоносных программ.
Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов.
Распространение вредоносного кода для мобильных устройств.
Расширение вредоносных кодов для мобильных устройств. Правила безопасности при

установке приложений на мобильные устройства.
Выполнение и защита индивидуальных и групповых проектов.

Безопасность информации
Социальная инженерия: распознать и избежать.

Приемы социальной инженерии. Правила безопасности при виртуальных контактах.
Ложная информация в Интернете.

Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы.
Безопасность при использовании платежных карт в Интернете.

Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.
Беспроводная технология связи.

Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях.
Резервное копирование данных.

Безопасность личной информации. Создание резервных копий на различных устройствах.
Основы государственной политики в области формирования культуры информационной безопасности.

Доктрина национальной информационной безопасности. Обеспечение свободы и равенства доступа к информации и знаниям. Основные направления государственной политики в области формирования культуры информационной безопасности.
Выполнение и защита индивидуальных и групповых проектов.

Повторение.

Материально-техническое обеспечение

Технические средства обучения:

- компьютер,
- проектор,
- интерактивная доска.

Программное обеспечение:

- ОС MS Windows,
- Microsoft Office,
- антивирусные программы,
- сеть интернет.

Список литературы:

- Бабаш А.В. Информационная безопасность: Лабораторный практикум / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. – М.: КноРус, 2019 – 432 с
- Вехов В. Б. Компьютерные преступления: способы совершения и раскрытия / В.Б. Вехов; Под ред. акад. Б.П. Смагоринского. – М.: Право и закон, 2014 – 182 с.
- Громов Ю.Ю. Информационная безопасность и защита информации:Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. – Ст. Оскол: ТНТ, 2017 – 384 с.
- Дети в информационном обществе http://detionline.com/journal/about
- Ефимова Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. – М.: ЮНИТИ- ДАНА, 2016 – 239 с.

- Запечников С.В. Информационная безопасность открытых систем. В 2-х т. Т.2 – Средства защиты в сетях / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. – М.: ГЛТ, 2018 – 558 с.
- Защита детей by Kaspersky // https://kids.kaspersky.ru/
- Кузнецова А.В. Искусственный интеллект и информационная безопасность общества / А.В. Кузнецова, С.И. Самыгин, М.В. Радионов. – М.: Русайнс, 2017 – 64 с.
- Наместникова М.С. Информационная безопасность, или На расстоянии одного вируса. 7-9 классы. Внеурочная деятельность. – М.: Просвещение,2019 – 80 с.
- Основы кибербезопасности. // https://www.xn--d1abkefqip0a2f.xnp1ai/index.php/glava-1- osnovy-kiberbezopasnosti-tseli-i-zadachi-kurs
- Цифровая компетентность подростков и родителей. Результаты всероссийского исследования / Г.У. Солдатова, Т.А. Нестик, Е.И. Рассказова,Е.Ю. Зотова. – М.: Фонд Развития Интернет, 2013 – 144 с.

Учебно-тематический план

	Название разделов, тем	**Количество часов**
		Всего
1	Введение	4
2	Безопасность общения	60
3	Безопасность устройств	32
4	Безопасность информации	48
	Итого	144

Календарно-тематическое планирование

№ урока	Тема	Количество часов	Дата			
			план		факт	
			группа 1	*группа 2*	*группа 1*	*группа 2*
Введение (2 занятия – 4 ч.)						
1-2	Правила поведения и ТБ в кабинете информатики и при работе с ПК. Введение.	**2**	04.09.2024	02.09.2024		
3-4	Цифровая гигиена: зачем это нужно? Понятие периметра безопасности.	**2**	06.09	05.09		
Безопасность общения (30 занятий – 60 ч.)						
5-6	Социальная сеть. История возникновения Интернета. История социальных сетей.	**2**	11.09	09.09		
7-8	Понятия Интернетугроз. Изменения границ допустимого в контексте цифрового образа жизни.	**2**	13.09	12.09		
9-10	Мессенджеры. Назначение социальных сетей и мессенджеров.	**2**	18.09	16.09		
11-12	Пользовательский контент. Общение в социальных сетях.	**2**	20.09	19.09		
13-14	Персональные данные как основной капитал личного пространства в цифровом мире.	**2**	25.09	23.09		
15-16	Правила добавления друзей в социальных сетях.	**2**	27.09	26.09		

17-18	Профиль пользователя.	**2**	02.10	30.09		
19-20	Анонимные социальные сети.	**2**	04.10	03.10		
21-22	С кем безопасно общаться в интернете.	**2**	09.10	07.10		
23-24	Пароли для аккаунтов социальных сетей.	**2**	11.10	10.10		
25-26	Сложные пароли. Он-лайн генераторы паролей.	**2**	16.10	14.10		
27-28	Правила хранения паролей. Использование функции браузера по запоминанию паролей.	**2**	18.10	17.10		
29-30	Безопасный вход в аккаунты. Виды аутентификации.	**2**	23.10	21.10		
31-32	Настройки безопасности аккаунта.	**2**	25.10	24.10		
33-34	Работа на чужом компьютере с точки зрения безопасности личного аккаунта.	**2**	30.10	28.10		
35-36	Настройки социальных конфиденциальности в социальных сетях.	**2**	01.11	31.10		
37-38	Настройки приватности и конфиденциальности в разных социальных сетях.	**2**	06.11	04.11		
39-40	Приватность и конфиденциальность в мессенджерах.	**2**	08.11	07.11		
41-42	Публикация информации в социальных сетях.	**2**	13.11	11.11		

43-44	Персональные данные. Публикация личной информации.	**2**	15.11	14.11		
45-46	Кибербуллинг. Определение кибербуллинга. Груминг.	**2**	20.11	18.11		
47-48	Возможные причины кибербуллинга и как его избежать?	**2**	22.11	21.11		
49-50	Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга. Профилактика насилия в Сети	**2**	27.11	25.11		
51-52	Настройки приватности публичных страниц. Правила ведения публичных страниц.	**2**	29.11	28.11		
53-54	Овершеринг. Публичные аккаунты.	**2**	04.12	02.12		
55-56	Фишинг как мошеннический прием. Популярные варианты распространения фишинга.	**2**	06.12	05.12		
57-58	Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах.	**2**	11.12	09.12		
59-60	Выполнение индивидуальных и групповых проектов.	**2**	13.12	12.12		
61-62	Выполнение индивидуальных и групповых проектов.	**2**	18.12	16.12		
63-64	Выполнение и защита индивидуальных и	**2**	20.12	19.12		

	групповых проектов.					
Безопасность устройств. (16 занятия - 32 ч.)						
65-66	Что такое вредоносный код. Виды вредоносных кодов.	**2**	25.12	23.12		
67-68	Возможности и деструктивные функции вредоносных кодов.	**2**	27.12	26.12		
69-70	Распространение вредоносного кода. Способы доставки вредоносных кодов.	**2**	01.01.2025	30.12		
71-72	Исполняемые файлы и расширения вредоносных кодов. Вредоносная рассылка.	**2**	03.01	02.01.2025		
73-74	Вредоносные скрипты. Способы выявления наличия вредоносных кодов на устройствах.	**2**	08.01	06.01		
75-76	Действия при обнаружении вредоносных кодов на устройствах.	**2**	10.01	09.01		
77-78	Способы защиты устройств от вредоносного кода.	**2**	15.01	13.01		
79-80	Антивирусные программы и их характеристики.	**2**	17.01	16.01		
81-82	Правила и методы защиты от вредоносных кодов и программ.	**2**	22.01	20.01		
83-84	Распространение вредоносного кода для мобильных устройств.	**2**	24.01	23.01		

85-86	Расширение вредоносных кодов для мобильных устройств.	**2**	29.01	27.01		
87-88	Правила безопасности при установке приложений на мобильные устройства.	**2**	31.01	30.01		
89-90	Контентные риски. Настройка и безопасное использование смартфона или планшета. Семейный доступ.	**2**	05.02	03.02		
91-92	Выполнение индивидуальных и групповых проектов.	**2**	07.02	06.02		
93-94	Выполнение индивидуальных и групповых проектов.	**2**	12.02	10.02		
95-96	Выполнение и защита индивидуальных и групповых проектов.	**2**	14.02	13.02		
Безопасность информации. (24 занятий - 48 ч.)						
97-98	Социальная инженерия: распознать и избежать. Приемы социальной инженерии.	**2**	19.02	17.02		
99-100	Правила безопасности при виртуальных контактах.	**2**	21.02	20.02		
101-102	Ложная информация в Интернете.	**2**	26.02	24.02		
103-104	Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей.	**2**	28.02	27.02		
105-106	Фейковые новости. Поддельные страницы.	**2**	05.03	03.03		

107-108	Обращение с деньгами в сети Интернет.	**2**	07.03	06.03		
109-110	Безопасность при использовании платежных карт в Интернете.	**2**	12.03	10.03		
111-112	Транзакции и связанные с ними риски.	**2**	14.03	13.03		
113-114	. Правила совершения он-лайн покупок	**2**	19.03	17.03		
115-116	Безопасность банковских сервисов. Детская пластиковая карта: быть или не быть?	**2**	21.03	20.03		
117-118	Беспроводная технология связи.	**2**	26.03	24.03		
119-120	Уязвимость Wi-Fi-соединений.	**2**	28.03	27.03		
121-122	Публичные и непубличные сети.	**2**	02.04	31.03		
123-124	Правила работы в публичных сетях.	**2**	04.04	03.04		
125-126	Безопасность личной информации	**2**	09.04	07.04		
127-128	Создание резервных копий на различных устройствах.	**2**	11.04	10.04		
129-130	Основы государственной политики в области формирования культуры информационной безопасности.	**2**	16.04	14.04		
131-132	Доктрина национальной информационной безопасности.	**2**	18.04	17.04		
133-134	Обеспечение свободы и равенства доступа к	**2**	23.04	21.04		

	информации и знаниям.					
135-136	Основные направления государственной политики в области формирования культуры информационной безопасности.	**2**	25.04	24.04		
137	Выполнение индивидуальных и групповых проектов.	**1**	30.04	28.04		
138	Выполнение индивидуальных и групповых проектов.	**1**	02.05	01.05		
139	Выполнение и защита индивидуальных и групповых проектов.	**1**	09.05	05.05		
140	Выполнение и защита индивидуальных и групповых проектов.	**1**	14.05	08.05		
141	Повторение.	**1**	16.05	12.05		
142	Повторение.	**1**	21.05	15.05		
143	Повторение.	**1**	17.05	19.05		
144	Повторение.	**1**	21.05	22.05		
ИТОГО		**144**				