

Муниципальное бюджетное общеобразовательное учреждение «Школа № 141»
городского округа Самара

Рассмотрено
На заседании МО
Классных руководителей
Протокол № 1
От «28» августа 2025г.
Председатель МО
 Н.В.Пугина



Дополнительная общеобразовательная общеразвивающая
ПРОГРАММА
«Цифровая гигиена»
Направленность: социальная
Возрастная категория: 12 – 17 лет
Срок реализации программы: 1 год

Составитель:
Педагог ДО
МБОУ «Школа № 141» г.о.Самара
Хабибуллин Р.Р.

2025 год

Оглавление

Раздел 1. Пояснительная записка (характеристика программы)	стр. 3
Раздел 2. Содержание программы	стр. 7
Раздел 3. Формы аттестации и оценочные материалы	стр. 9
Раздел 4. Организационно-педагогические условия реализации программы	стр.10
Приложение. Календарно-тематическое планирование	стр. 11

Раздел 1. Пояснительная записка.

Нормативные основания для создания дополнительной общеобразовательной общеразвивающей программы «Цифровая гигиена»:

- Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;
- Указ Президента Российской Федерации от 02.07.2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации»;
- Указ Президента Российской Федерации от 09.11.2022 г. № 809 «Об утверждении основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей»;
- Указ Президента Российской Федерации от 7.05.2024 г. № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года»;
- Концепция развития дополнительного образования до 2030 года (утверждена распоряжением Правительства РФ от 31.03.2022 № 678-р);
- ИЗМЕНЕНИЯ, которые вносятся в распоряжение Правительства РФ от 31.03.2022 №678-р (утверждены распоряжением Правительства РФ от 15.05.2023 №1230-р);
- Стратегия развития воспитания в Российской Федерации на период до 2025 года (утверждена распоряжением Правительства Российской Федерации от 29.05.2015 № 996-р);
- Постановление Правительства РФ от 11.10.2023 № 1678 «Об утверждении Правил применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ»;
- Приказ Министерства просвещения Российской Федерации от 27 июля 2022 г. № 629 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам»;
- Приказ Министерства просвещения РФ от 03.09.2019 № 467 «Об утверждении Целевой модели развития региональных систем дополнительного образования детей»;
- Приказ Министерства просвещения РФ от 21.04.2023 № 302 «О внесении изменений в Целевую модель развития региональных систем дополнительного образования детей, утвержденную приказом Министерства просвещения РФ от 3.09.2019 г. № 467»;
- Постановление Главного государственного санитарного врача РФ от 28.09.2020 № 28 «Об утверждении СП 2.4.3648-20 «Санитарно-эпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодежи»;
- Стратегия социально-экономического развития Самарской области на период до 2030 года (утверждена распоряжением Правительства Самарской области от 12.07.2017 № 441);
- Письмо Министерства образования и науки РФ от 18.11.2015 № 09-3242 «О направлении информации» (с «Методическими рекомендациями по проектированию дополнительных общеразвивающих программ (включая разноуровневые программы)»);
- Письмо министерства образования и науки Самарской области от 30.03.2020 № МО-16-09-01/434-ТУ (с «Методическими рекомендациями по подготовке дополнительных общеобразовательных общеразвивающих программ к прохождению процедуры экспертизы (добровольной сертификации) для последующего включения в реестр образовательных программ, включенных в систему ПФДО»).

Актуальность данной программы обусловлена тем, что курс «Цифровая гигиена» является важной составляющей работы с обучающимися, активно использующими различные сетевые формы общения (социальные сети, игры, пр.). Программа направлена на формирование у учащихся умения безопасного общения в Интернете. С целью мотивации ответственного отношения к обеспечению своей личной безопасности, безопасности своей семьи и своих друзей.

Кроме того, реализация курса создаст условия для сокращения цифрового разрыва между поколениями и позволит родителям выступать в качестве экспертов, передающих опыт.

Отличительные особенности программы. Особенность программы в том, что она позволяет 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 и программа построена по модульной системе (Зраздела-модуля).

Программа рассчитана на 1 год обучения. Занятия проводятся 1 раз в неделю, занятие - 40 мин. Результативность работы можно проследить по итогам тестов, итоговых проектных работ. Диагностика результативности проводится 1 раз в год (май).

Группы формируются без конкурсного отбора на основании заявлений родителей (законных представителей).

Курс рассчитан на 34 часа: в 7-8 классе (один год обучения) – 1 час в неделю. Базовый уровень освоения программы. Процент пассивности (число аудиторных занятий) в среднем составляет 50%.

Цель: обеспечение условий для профилактики негативных тенденций в информационной культуре учащихся, повышения защищенности детей от информационных рисков и угроз; формирование навыков своевременного распознавания онлайн-рисков – (технического, контентного, коммуникационного, потребительского характера и риска интернет-зависимости)

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 ответственными 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 основы профориентационных знаний в области защиты информации;
- сформировать навыки по профилактике и коррекции зависимого поведения школьников, связанного с компьютерными технологиями и Интернетом.

Для занятий по программе «Цифровая гигиена» привлекаются обучающиеся в возрасте 12 – 15 лет. Группы формируются без конкурсного отбора на основании заявлений родителей (законных представителей).

Основными видами деятельности в ходе реализации курса являются:

- игровая;
- познавательная;
- проблемно-ценностное общение;
- досугово-развлекательная;
- социальная.

Формы организации образовательной деятельности: индивидуальная, групповая.

Формы организации учебного занятия – *групповая, индивидуальная, фронтальная, работа в командах (в динамических парах)*, практическое занятие, тренинги. Для преподавания модуля «Информационная безопасность» могут использоваться разнообразные форматы обучения:

- традиционный урок (коллективная и групповая формы работы);

- тренинги (в классической форме или по кейс-методу);

- дистанционное обучение (электронные презентации, видеоролики, почтовые рассылки, микрообучение);

-смешанный формат.

Планируемые результаты освоения курса.

Личностные результаты освоения курса.

У обучающегося будут сформированы:

- понимание и осознание взаимной обусловленности физического, нравственного, психологического, психического и социально-психологического здоровья человека;
- осознание негативных факторов, пагубно влияющих на здоровье;
- умение делать осознанный выбор поступков, поведения, образа жизни, позволяющих сохранить и укрепить здоровье;
- умение сохранить личные персональные данные и обеспечить неприкосновенность личной жизни;
- определять и высказывать под руководством педагога самые простые общие для всех людей правила поведения при сотрудничестве (этические нормы). В предложенных педагогом ситуациях общения и сотрудничества, опираясь на общие для всех простые правила поведения, делать выбор, при поддержке других участников группы и педагога, как поступить.
- умение владеть основами соблюдения норм информационной этики и права;
- умение владеть основами самоконтроля, самооценки, принятия решений и осуществления осознанного выбора в учебной и познавательной деятельности при формировании современной культуры жизни и деятельности;

Метапредметные (познавательные, регулятивные и коммуникативные) результаты.

Обучающийся научится:

- самостоятельно определять цели своего обучения, ставить и формулировать для себя новые задачи в учебе и познавательной деятельности, развивать мотивы и интересы своей познавательной деятельности;
- самостоятельно планировать пути достижения целей, в том числе альтернативные, осознанно выбирать наиболее эффективные способы решения учебных и познавательных задач;
- 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;
- основам самоконтроля, самооценки;
- организовывать учебное сотрудничество и совместную деятельность с учителем и сверстниками; работать индивидуально и в группе: находить общее решение и разрешать конфликты на основе согласования позиций и учета интересов; формулировать, аргументировать и отстаивать свое мнение;
- осознанно использовать речевые средства в соответствии с задачей коммуникации для выражения своих чувств, мыслей и потребностей; планирования и регуляции своей деятельности;
- осознанно использовать средства и методы защиты информации и методы безопасной регуляции своей деятельности в сети Интернет; использовать для решения коммуникативных задач в области безопасности жизнедеятельности различные источники информации, включая Интернет-ресурсы и другие базы данных.
- 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.
- Познакомится с миром профессий в информационном обществе.

Предметные результаты.

В результате освоения содержания программного материала, обучающиеся по окончании курса должны:

- обосновывать значение занятий в совершенствовании функциональных возможностей человека;
- выполнять технические приёмы и тактические действия, не наносящие вред себе и окружающим при работе с информацией в социальных сетях;
- классифицировать основные правила работы с информацией;
- знать этические нормы работы в сети Интернет;
- Выявлять закономерности и проводить аналогии;
- 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.
- 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.

Воспитательные результаты.

Результаты первого уровня (приобретение школьником социальных знаний):

- приобретение обучающимися знаний о правилах ведения здорового образа жизни, о технике безопасности при занятии спортом, о принятых в обществе нормах отношения к здоровому образу жизни;
- о правилах конструктивной групповой деятельности; о способах организации досуга; о способах самостоятельного поиска, нахождения и обработки информации.
- Формы достижения результатов первого уровня: познавательные беседы, инструктажи, социальные пробы, беседы о здоровом образе жизни. Формы контроля результатов первого уровня: анкетирование.

Результаты второго уровня (формирование ценностного отношения к социальной реальности):

- развитие ценностных отношений школьника к своему здоровью и здоровью окружающих его людей.
- приобретение школьником опыта актуализации спортивно-оздоровительной деятельности в социальном пространстве;
- результаты второго уровня (получение опыта переживания и позитивного отношения к базовым ценностям общества): развитие ценностного отношения подростков к труду, знаниям, своему собственному здоровью и внутреннему миру; получение первоначального опыта самореализации.

- Формы достижения результатов второго уровня: социально-значимые акции в клубе и в школе.
- Формы контроля результатов второго уровня: защита конечного продукта (презентация созданного документа).

Результаты третьего уровня (получение школьником опыта самостоятельного общественного действия):

- опыта самообслуживания, самоорганизации и организации совместной деятельности с другими школьниками; опыта сотрудничества с другими людьми и принятия на себя ответственности за других.
- Формы достижения результатов третьего уровня: исследовательские работы, м.б. социально-значимые акции в социуме (вне ОУ). Формы контроля результатов третьего уровня: исследовательские конференции, конкурсы авторских работ, проекты и т.д.

Формы и способы оценки достижения планируемых результатов:

- Начальный контроль проводится в форме зачетов. Используемый метод – практический контроль.
- Промежуточная аттестация - в форме зачетов и выполнение тестов. Используемые методы – комбинированный (устный и практический) контроль.
- Аттестация по завершении реализации программы проводится в форме зачета, защиты итоговых проектов. Используемые методы – комбинированный (устный и практический) контроль; по итогам 1 и 2 полугодий может выставляться зачет или незачет.

Раздел 2. «Тематическое планирование»

Учебно – тематический план

№п/п	Название раздела	Количество часов			Форма аттестации
		всего	теория	практика	
1.	Техника безопасности при работе в компьютерном классе	1	1	0	зачет
2	Раздел 1. «Безопасность общения»	13	7	6	зачет
3	Выполнение и защита индивидуальных и групповых проектов	3	1	2	зачет
4	Раздел 2. «Безопасность устройств»	10	6	4	зачет
5	Раздел 3. «Безопасность информации»	7	5	2	зачет
	ИТОГО	34	17(50%)	17(50%)	

«Содержание программы с указанием форм организации и видов деятельности»

СОДЕРЖАНИЕ ПРОГРАММЫ

- **Раздел 1. «Безопасность общения»**

- **Техника безопасности.** Теория(1ч): меры предупреждения травматизма на занятиях.
- **Тема 1. Общение в социальных сетях и мессенджерах (Практика 1ч, теория 1ч.)**
- Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент.
- **Тема 2. С кем безопасно общаться в интернете. (Теория 1 час)**
- Персональные данные как основной капитал личного пространства в цифровом мире. Правила добавления друзей в социальных сетях. Профиль пользователя. Анонимные социальные сети.
- **Тема 3. Пароли для аккаунтов социальных сетей.(Практика 1 час)**
- Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей.
- **Тема 4. Безопасный вход в аккаунты. (Практика 1 час)**
- Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.
- **Тема 5. Настройки конфиденциальности в социальных сетях. (Теория 1 час)**
- Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах.
- **Тема 6. Публикация информации в социальных сетях. (Теория 1 час)**
- Персональные данные. Публикация личной информации.
- **Тема 7. Кибербуллинг. (Практика 2 часа, теория -1ч)**
- Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга. Профессии в информационном обществе. Востребованность специалистов по защите информации.
- **Тема 8. Публичные аккаунты. (Практика 1 час)**
- Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.
- **Тема 9. Фишинг. 2 часа.**
- 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. 3 часа.** Социально-активные практики.

- **Раздел 2. «Безопасность устройств» (10ч)(Теория 6- часа, практика-4ч)**
- **Тема 1. Повторение раздела 1. (Теория 1 ч)**
- Повторение раздела 1. «Безопасность общения» Тренинг.(Практика 1ч.)
- **Тема 2. Что такое вредоносный код. (Теория 1 ч)**
- Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.
- **Тема 3. Распространение вредоносного кода. (Теория 1 ч)**
- 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. (Практика 1ч.)
- **Тема 4. Методы защиты от вредоносных программ. (Теория 1 ч)**
- Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов.(Практика 1ч.)
- **Тема 5. Распространение вредоносного кода для мобильных устройств. (Теория 1 ч)**
- Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства.(Практика 1ч.)

- **Раздел 3. «Безопасность информации» (7 часов) (Теория- 5ч, практика-2ч)**
- **Тема 1. Социальная инженерия: распознать и избежать.** (Теория 1 ч)
Приемы социальной инженерии. Правила безопасности при виртуальных контактах.
- **Тема 2. Ложная информация в Интернете.** (Теория 1 ч)
Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы.
- **Тема 3. Безопасность при использовании платежных карт в Интернете.**(Теория 1 ч)
Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.
- **Тема 4. Беспроводная технология связи.** (Теория 1ч., практика 1ч.)
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. (Практика 1 час)
- **Тема 5. Основы государственной политики в области формирования культуры информационной безопасности.** Нормативно-правовые акты.Итоговый тест.(Теория 1ч)

Каждый раздел учебного курса (модуля) завершается выполнением проектной работы по одной из тем, предложенных на выбор учащихся и/или проверочного теста, и/или социально-активными практиками. Эти занятия в качестве волонтерской практики могут быть проведены учащимися, освоившими программу. Для проведения занятий могут быть использованы презентации, проекты, памятки, онлайнзанятия, подготовленные в ходе выполнения учебных заданий по основным темам курса.

Все дидактические игры и задания моделируются в доступном для детей виде, те или иные реальные ситуации, с которыми они сталкиваются в сети Интернет.

Раздел 3. «Формы аттестации и оценочные материалы»

- Аттестация по завершении реализации программы проводится в форме зачета. Используемые методы – комбинированный (устный и практический) контроль. Итоговый контроль проводится в форме результативности тестов и защиты проектов; по итогам 1и 2полугодий может выставляться зачет или незачет.
- Формы контроля на занятиях: текущий; промежуточный; итоговый.
- Формы подведения итогов на учебных занятиях:
 - Вводные занятия: беседа, практические занятия;
 - Учебные занятия: фронтальные и индивидуальные беседы, дидактические карточки, терминологические диктанты, тесты, конкурсы, выполнение практических заданий на занятиях, защита проектов.
 - Итоговое занятие: итоговый тест, итоговый проект и т.д.
- Итоговая диагностика проводится в конце учебного года обучения. По её результатам определяется уровень мастерства, которого достигли обучающиеся за время обучения.
- Промежуточный контроль предусматривает участие в мероприятиях разного уровня: школьных, районных, городских.
- Итоговый контроль проводится по сумме показателей за всё время обучения в данном объединении, а также предусматривает выполнение комплексной работы по единой предложенной схеме.
- **Оценочные материалы Итоговая аттестация Итоговый контроль** проводится по трём блокам и по их результатам определяется уровень мастерства, которого достигли воспитанники за время обучения.
- Блок 1. Определение теоретических знаний и практических умений обучающихся

(Приложение 1)

- Оценочные баллы могут выставляться по шкале: 0б.- minдо5б.-max.

№п/п	ФИ ученика	Вид работы									Среднее количество баллов
		1	2	3	4	5	6	7	8	9	
1											

Виды работ для оценки теоретических знаний и практических умений:

1-2- Беседа

3-5-Тесты

6-8- Проекты

9-Конкурсные мероприятия

- Блок 2. Уровень развития личности обучающихся (Приложение 2)

№ п/п	ФИ ученика	Отношение к себе и к людям			Отношение к труду (спорту)		
		Низкий уровень	Средний уровень	Высокий уровень	Низкий уровень	Средний уровень	Высокий уровень
1							

Оценка развития личности обучающихся определяется по отношению: к себе и людям;

- Блок 3. Определение творческого потенциала обучающихся (Приложение 3)

№ п/п	ФИ ученика	Уровень творчества		
		низкий уровень 23 и менее очков	средний уровень от 24 до 44 очков	высокий уровень 45 и более очков
1				

Методика «Определение творческого потенциала». Тест позволяет оценить уровень творческого потенциала, умения принимать нестандартные решения.

Раздел 4. «Организационно-педагогические условия реализации программы»

Учебно-методическое и информационное обеспечение программы

- Дополнительная общеобразовательная общеразвивающая программа «Цифровая гигиена».

Список литературы и информационных источников

(используемая педагогом для разработки программы и организации образовательного процесса)

- 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.
- 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.

5. Защита детей by Kaspersky // <https://kids.kaspersky.ru/>
6. Кузнецова А.В. Искусственный интеллект и информационная безопасность общества / А.В. Кузнецова, С.И. Самыгин, М.В. Радионов. – М.: Русайнс, 2017 – 64 с.
7. Наместникова М.С. Информационная безопасность, или На расстоянии одного вируса. 7-9 классы. – М.: Просвещение, 2019 – 80 с.
8. Основы кибербезопасности. // <https://www.xn--d1abkefqip0a2f.xnp1ai/index.php/glava-1-osnovy-kiberbezopasnosti-tseli-i-zadachi-kurs>
9. 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.

СПИСОК ЛИТЕРАТУРЫ и информационных источников для детей

1. Дети в информационном обществе <http://detionline.com/journal/about>
2. Ефимова Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. – М.: ЮНИТИ- ДАНА, 2016 – 239 с.

Материально-технические условия реализации программы: для занятий используется специальная литература, учебный компьютерный кабинет, ноутбуки, проектор, экран, доска меловая, рабочие столы ученические 2-х местные, стулья.

Календарно – тематическое планирование

№	Содержание занятий	Количество часов		
		всего	теоретические	практические
1	Техника безопасности, меры предупреждения травматизма на занятиях.	1	0	1
Раздел 1. «Безопасность общения»		16		
2-3	Общение в социальных сетях и мессенджерах.	2	1	1
4	С кем безопасно общаться в интернете?	1	1	
5	Пароли для аккаунтов социальных сетей	1		1
6	Безопасный вход в аккаунты	1		1
7	Настройки конфиденциальности в социальных сетях	1		1
8	Публикация информации в социальных сетях	1	1	
9-11	Кибербуллинг	3	1	2
12	Публичные аккаунты	1	1	
13-14	Фишинг. Профессии в информационном обществе.	2	1	1
15-	Выполнение и защита индивидуальных и	3	1	2
17	групповых проектов. Соц. практики.			
Раздел 2. «Безопасность устройств»		9		
18-19	Повторение раздела 1 «Безопасность устройств». Тест.	2	1	1
20	Что такое вредоносный код?	1	1	
21-22	Распространение вредоносного кода	2	1	1
23-24	Методы защиты от вредоносных программ	2	1	1
25-26	Распространение вредоносного кода для мобильных устройств	2	1	1
Раздел 3. «Безопасность информации»		8		
27	Социальная инженерия: распознать и избежать.	1	1	
28	Ложная информация в Интернете.	1	1	
29	Безопасность при использовании платежных карт в Интернете.	1	1	
30-31	Беспроводная технология связи.	2	1	1
32	Резервное копирование данных.	1		1
33-34	Основы государственной политики в области формирования культуры информационной безопасности. Тест.	2	1	1
	Итого	34	17	17

