МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Министерство образования и молодежной политики
Свердловской области
Департамент образования Администрации города Екатеринбурга
Муниципальное автономное общеобразовательное учреждение
лицей № 12 г. Екатеринбург Верх-Исетский район

СОГЛАСОВАНО
Педагогическим советом
МАОУ лицей № 12
(протокол от 30.08.2023 №1)

УТВЕРЖДЕНО
Директор МАОУ лицей №12
Жук В.В.
Приказ №170 от «30» августа 2023г.

РАБОЧАЯ ПРОГРАММА
КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

(основное общее образование)

Екатеринбург, 2023 год

СОДЕРЖАНИЕ

Пояснительная записка

Планируемые результаты освоения курса внеурочной деятельности

- личностные результаты

- метапредметные результаты

- предметные результаты

Содержание курса внеурочной деятельности

Тематическое планирование курса внеурочной деятельности

Пояснительная записка

Общая характеристика

Рабочая программа курса внеурочной деятельности «Информационная безопасность» (далее – программа) для 9 классов составлена на основе положений и требований к результатам освоения основной образовательной программы, представленных в федеральном государственном образовательном стандарте основного общего образования (далее – ФГОС ООО), утвержденного приказом Министерства просвещения Российской Федерации от 31.05.2021 г. № 287 (с изменениями от 18.07.2022 г. № 568), а также с учетом федеральной рабочей программы воспитания.

При разработке программы использовались также следующие нормативные документы:

1. Указ Президента Российской Федерации от 09.11.2022 г. № 809 «Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей»;

2.Стратегия национальной безопасности Российской Федерации. Указ Президента Российской Федерации от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации».

Актуальность курса

Огромные массивы информации обрушиваются на человека ежедневно через газеты и журналы, радио и телевидение, всевозможную рекламу.

Психологи все чаще употребляют термин “сжатие миром”. Плотной стеной мир обступает почти каждого из нас, вынуждая воспринимать информацию вне зависимости от возможностей и желания. Порой информация помогает нам ориентироваться в современном мире, а иногда утомляет и мешает принять правильное решение.

Защита человека от поступающей к нему информации является важнейшей составляющей обеспечения его личной безопасности. Человек должен уметь защищаться от возможных информационных манипуляций.

В условиях информатизации общества высокая информационная культура, обеспечивающая информационную безопасность личности, является необходимостью для успешной деятельности в любой сфере.

Теоретически человек сам может переработать любую информацию, но сделает это гораздо эффективнее, если овладеет знаниями и умениями, которыми располагает информационная культура. Поэтому существует острая потребность общества в организации информационного образования,

призванного обеспечить формирование информационной культуры и информационной безопасности личности и общества в целом.

Формируя информационную безопасность личности необходимо выработать систему противодействия, защиты личности от возможных информационных манипуляций, а также воспитать чувство ответственности за производство и распространение информации, понимание ее последствий, ее негативного влияния на личность и общество.

Актуальность проблемы воспитания информационной культуры, информационной безопасности обусловлена необходимостью получения знаний, навыков и умений, которыми должен владеть каждый человек в современном, изменяющемся информационном мире. Только личность со сформированной информационной культурой может адекватно реагировать на происходящие в мире процессы. В условиях информатизации общества, всех его структур, высокая информационная культура, обеспечивающая информационную безопасность личности, является необходимостью для успешной деятельности в любой сфере.

Цель курса

- 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 интернетзависимости).

Основные задачи курса

- 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.

Место курса

Программа курса рассчитана на 33 часа по 1 часу в неделю, которые могут быть реализованы в течение одного учебного года в составе группы из обучающихся 9 классов.

Взаимосвязь с федеральной рабочей программой воспитания

Программа курса разработана с учетом рекомендаций федеральной рабочей программы воспитания, предполагает объединение учебной и воспитательной деятельности педагогов, нацелена на достижение всех основных групп образовательных результатов – личностных, метапредметных, предметных.

Программа носит техническую направленность, что позволяет обеспечить достижение следующих целевых ориентиров воспитания на уровне основного общего образования:

- воспитание информационной культуры обучающихся, формированию информационной безопасности личности, созданию условий для повышения готовности подростков к сознательному, профессиональному и культурному самоопределению в целом.

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ

Содержание курса внеурочной деятельности «Информационная безопасность» направлено на достижение обучающимися личностных, метапредметных и предметных результатов при изучении курса.

ЛИЧНОСТНЫЕ РЕЗУЛЬТАТЫ

- освоение обучающимися социального опыта, основных социальных ролей, соответствующих ведущей деятельности возраста, норм и правил общественного поведения, форм социальной жизни в группах и сообществах, включая семью, группы, сформированные по профессиональной деятельности, а также в рамках социального взаимодействия с людьми из другой культурной среды;
- способность обучающихся во взаимодействии в условиях неопределенности, открытость опыту и знаниям других;
- способность действовать в условиях неопределенности, повышать уровень своей компетентности через практическую деятельность, в том числе умение учиться у других людей, осознавать в совместной деятельности новые знания, навыки и компетенции из опыта других;
- навык выявления и связывания образов, способность формирования новых знаний, в том числе способность формулировать идеи, понятия, гипотезы об объектах и явлениях, в том числе ранее не известных, осознавать дефициты собственных знаний и компетентностей, планировать свое развитие;
- умение распознавать конкретные примеры понятия по характерным признакам, выполнять операции в соответствии с определением и простейшими свойствами понятия, конкретизировать понятие примерами, использовать понятие и его свойства при решении задач (далее - оперировать понятиями), а также оперировать терминами и представлениями в области концепции устойчивого развития;
- умение анализировать и выявлять взаимосвязи природы, общества и экономики;
- умение оценивать свои действия с учетом влияния на окружающую среду, достижений целей и преодоления вызовов, возможных глобальных последствий;
- способность обучающихся осознавать стрессовую ситуацию, оценивать происходящие изменения и их последствия;
- воспринимать стрессовую ситуацию как вызов, требующий контрмер; оценивать ситуацию стресса, корректировать принимаемые решения и действия;
- формулировать и оценивать риски и последствия, формировать опыт, уметь находить позитивное в произошедшей ситуации;

- быть готовым действовать в отсутствие гарантий успеха.

гражданское воспитание:

- готовность к выполнению обязанностей гражданина и реализации его прав, уважение прав, свобод и законных интересов других людей;
- представление об основных правах, свободах и обязанностях гражданина, социальных нормах и правилах межличностных отношений в поликультурном и многоконфессиональном обществе;
- представление о способах противодействия коррупции;
- готовность к разнообразной совместной деятельности, стремление к взаимопониманию и взаимопомощи, активное участие в школьном самоуправлении;

патриотическое воспитание:

- технологиям, боевым подвигам и трудовым достижениям народа;

духовно-нравственное воспитание:

- готовность оценивать свое поведение и поступки, поведение и поступки других людей с позиции нравственных и правовых норм с учетом осознания последствий поступков;

физическое воспитание:

- соблюдение правил безопасности, в том числе навыков безопасного поведения в интернет-среде;
- способность адаптироваться к стрессовым ситуациям и меняющимся социальным, информационным и природным условиям, в том числе осмысляя собственный опыт и выстраивая дальнейшие цели;
- умение принимать себя и других, не осуждая;
- умение осознавать эмоциональное состояние себя и других, умение управлять собственным эмоциональным состоянием;
- сформированность навыка рефлексии, признание своего права на ошибку и такого же права другого человека.

трудовое воспитание:

- осознание важности обучения на протяжении всей жизни для успешной профессиональной деятельности и развитие необходимых умений для этого; готовность адаптироваться в профессиональной среде; уважение к труду и результатам трудовой деятельности;
- осознанный выбор и построение индивидуальной траектории образования и жизненных планов с учетом личных и общественных интересов и потребностей.

МЕТАПРЕДМЕТНЫЕ РЕЗУЛЬТАТЫ

Универсальные учебные познавательные действия:

Базовые логические действия:

- с учетом предложенной задачи выявлять закономерности и противоречия в рассматриваемых фактах, данных и наблюдениях;
- предлагать критерии для выявления закономерностей и противоречий;
- выявлять дефициты информации, данных, необходимых для решения поставленной задачи;
- выявлять причинно-следственные связи при изучении явлений и процессов;
- делать выводы с использованием дедуктивных и индуктивных умозаключений, умозаключений по аналогии, формулировать гипотезы о взаимосвязях;

Базовые исследовательские действия:

- формулировать вопросы, фиксирующие разрыв между реальным и желательным состоянием ситуации, объекта, самостоятельно устанавливать искомое и данное;
- аргументировать свою позицию, мнение;
- проводить по самостоятельно составленному плану опыт, несложный эксперимент, небольшое исследование по установлению особенностей объекта изучения, причинно-следственных связей и зависимостей объектов между собой;
- оценивать на применимость и достоверность информации, полученной в ходе исследования (эксперимента);
- наблюдения, опыта, исследования, владеть инструментами оценки достоверности полученных выводов и обобщений;
- прогнозировать возможное дальнейшее развитие процессов, событий и их последствия в аналогичных или сходных ситуациях, выдвигать предположения об их развитии в новых условиях и контекстах;

Работа с информацией:

- выбирать, анализировать, систематизировать и интерпретировать информацию различных видов и форм представления;
- оценивать надежность информации по критериям, предложенным педагогическим работником или сформулированным самостоятельно;
- эффективно запоминать и систематизировать информацию.

Универсальные учебные коммуникативные действия:

Общение:

- распознавать невербальные средства общения, понимать значение социальных знаков, знать и распознавать предпосылки конфликтных ситуаций и смягчать конфликты, вести переговоры;

- понимать намерения других, проявлять уважительное отношение к собеседнику и в корректной форме формулировать свои возражения;
- в ходе диалога и (или) дискуссии задавать вопросы по существу обсуждаемой темы и высказывать идеи, нацеленные на решение задачи и поддержание благожелательности общения;
- сопоставлять свои суждения с суждениями других участников диалога, обнаруживать различие и сходство позиций;

Совместная деятельность:

- понимать и использовать преимущества командной и индивидуальной работы при решении конкретной проблемы, обосновывать необходимость применения групповых форм
- взаимодействия при решении поставленной задачи;
- принимать цель совместной деятельности, коллективно строить действия по ее достижению: распределять роли, договариваться, обсуждать процесс и результат совместной работы;
- уметь обобщать мнения нескольких людей, проявлять готовность руководить, выполнять поручения, подчиняться;
- планировать организацию совместной работы, определять свою роль (с учетом предпочтений и возможностей всех участников взаимодействия), распределять задачи между членами команды, участвовать в групповых формах работы (обсуждения, обмен мнениями, "мозговые штурмы" и иные);
- выполнять свою часть работы, достигать качественного результата по своему направлению и координировать свои действия с другими членами команды;
- оценивать качество своего вклада в общий продукт по критериям, самостоятельно сформулированным участниками взаимодействия;

Универсальные учебные регулятивные действия:

Самоорганизация:

- выявлять проблемы для решения в жизненных и учебных ситуациях;
- ориентироваться в различных подходах принятия решений (индивидуальное, принятие решения в группе, принятие решений группой);
- самостоятельно составлять алгоритм решения задачи (или его часть), выбирать способ решения учебной задачи с учетом имеющихся ресурсов и собственных возможностей, аргументировать предлагаемые варианты решений;
- составлять план действий (план реализации намеченного алгоритма решения), корректировать предложенный алгоритм с учетом получения новых знаний об изучаемом объекте;

- делать выбор и брать ответственность за решение;

Самоконтроль:

- владеть способами самоконтроля, самомотивации и рефлексии;
- давать адекватную оценку ситуации и предлагать план ее изменения;
- учитывать контекст и предвидеть трудности, которые могут возникнуть при решении учебной задачи, адаптировать решение к меняющимся обстоятельствам;
- объяснять причины достижения (недостижения) результатов деятельности, давать оценку приобретенному опыту, уметь находить позитивное в произошедшей ситуации;
- вносить коррективы в деятельность на основе новых обстоятельств, изменившихся ситуаций, установленных ошибок, возникших трудностей;
- оценивать соответствие результата цели и условиям;

Принятие себя и других:

- осознанно относиться к другому человеку, его мнению;
- признавать свое право на ошибку и такое же право другого;
- принимать себя и других, не осуждая;
- открытость себе и другим;
- осознавать невозможность контролировать все вокруг.

ПРЕДМЕТНЫЕ РЕЗУЛЬТАТЫ

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.

СОДЕРЖАНИЕ КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ

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 и/или проверочного теста.

Раздел 1. «Безопасность общения»

Тема 1. Общение в социальных сетях и мессенджерах. 1 час.

Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент.

Тема 2. С кем безопасно общаться в интернете. 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. 1 час.

Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей.

Тема 4. Безопасный вход в аккаунты. 1 час.

Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.

Тема 5. Настройки конфиденциальности в социальных сетях. 1 час.

Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах.

Тема 6. Публикация информации в социальных сетях. 1 час.

Персональные данные. Публикация личной информации.

Тема 7. Кибербуллинг. 1 час.

Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой

кибербуллинга. Как помочь жертве кибербуллинга.

Тема 8. Публичные аккаунты. 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 теста и/или защита индивидуальных и групповых проектов 3 часа.

Раздел 2. «Безопасность устройств»

Тема 1. Что такое вредоносный код. 1 час.

Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.

Тема 2. Распространение вредоносного кода. 1 час.

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.

Тема 3. Методы защиты от вредоносных программ. 2 час.

Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов.

Тема 4. Распространение вредоносного кода для мобильных устройств. 1 час.

Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства.

Выполнение теста и/или защита индивидуальных и групповых проектов. 3 часа.

Раздел 3 «Безопасность информации»

Тема 1. Социальная инженерия: распознать и избежать. 1 час.

Приемы социальной инженерии. Правила безопасности при виртуальных контактах.

Тема 2. Ложная информация в Интернете. 1 час.

Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы.

Тема 3. Безопасность при использовании платежных карт в Интернете. 1 час.

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

Тема 4. Беспроводная технология связи. 1 час.

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

Тема 5. Резервное копирование данных. 1 час.

Безопасность личной информации. Создание резервных копий на различных устройствах.

Тема 6. Основы государственной политики в области формирования культуры информационной безопасности. 2 час.

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

Выполнение теста и/или защита индивидуальных и групповых проектов. 3 часа. Повторение. 2 часа.

ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

№ п/п	Тема	Количество часов	Основное содержание	Основные виды деятельности обучающихся
Тема 1. «Безопасность общения»				
1	Общение в социальных сетях и мессенджерах (ВР)	1	Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент.	Выполняет базовые операции при использовании мессенджеров и социальных сетей. Создает свой образ в сети Интернет. Изучает историю и социальную значимость личных аккаунтов в сети Интернет.
2	С кем безопасно общаться в интернете	1	Персональные данные как основной капитал личного пространства в цифровом мире. Правила добавления друзей в социальных сетях. Профиль пользователя. Анонимные социальные сети.	Руководствуется в общении социальными ценностями и установками коллектива и общества в целом. Изучает правила сетевого общения.
3	Пароли для социальных сетей аккаунтов	1	Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей.	Изучает основные понятия регистрационной информации и шифрования. Умеет их применить.
4	Безопасный вход в аккаунты	1	Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.	Объясняет причины использования безопасного входа при работе на чужом устройстве. Демонстрирует устойчивый навык безопасного входа.
5	Настройки конфиденциальности в социальных сетях	1	Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах.	Раскрывает причины установки закрытого профиля. Меняет основные настройки приватности в личном профиле.
6	Публикация информации в социальных сетях	1	Персональные данные. Публикация личной информации.	Осуществляет поиск и использует информацию, необходимую для выполнения поставленных задач.

7	Кибербуллинг	1	Определениет кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга.	Реагирует на опасные ситуации, распознает провокации и попытки манипуляции со стороны виртуальных собеседников.
8	Публичные аккаунты	1	Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.	Решает экспериментальные задачи. Самостоятельно создает источники информации разного типа и для разных аудиторий, соблюдая правила информационной безопасности.
9	Фишинг	2	Фишинг как мошеннический прием. Популярные варианты распространения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах.	Анализ проблемных ситуаций. Разработка кейсов с примерами из личной жизни/жизни знакомых. Разработка и распространение чек-листа (памятки) по противодействию фишингу.
10	Выполнение теста и/или защита индивидуальных и групповых проектов	3		Самостоятельная работа.
Тема 2. «Безопасность устройств»				
1	Что такое вредоносный код	1	Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.	Соблюдает технику безопасности при эксплуатации компьютерных систем. Использует инструментальные программные средства и сервисы адекватно задаче.
2	Распространение вредоносного кода	1	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.	Выявляет и анализирует (при помощи чек-листа) возможные угрозы информационной безопасности объектов.
3	Методы защиты от вредоносных программ	2	Способы защиты устройств от вредоносного кода. Антивирусные	Изучает виды антивирусных программ и правила их установки.

			программы и их характеристики. Правила защиты от вредоносных кодов.	
4	Распространение вредоносного кода для мобильных устройств	1	Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства.	Разрабатывает презентацию, инструкцию по обнаружению, алгоритм установки приложений на мобильные устройства для учащихся более младшего возраста.
5.	Выполнение теста и/или защита индивидуальных и групповых проектов	3		Умеет работать индивидуально и в группе. Принимает позицию собеседника, понимая позицию другого, различает в его речи: мнение (точку зрения), доказательство (аргументы), факты; гипотезы, аксиомы, теории.
Тема 3 «Безопасность информации»				
1	Социальная инженерия: распознать и избежать	1	Приемы социальной инженерии. Правила безопасности при виртуальных контактах.	Находит нужную информацию в базах данных, составляя запросы на поиск. Систематизирует получаемую информацию в процессе поиска.
2	Ложная информация в Интернете	1	Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы.	Определяет возможные источники необходимых сведений, осуществляет поиск информации. Отбирает и сравнивает материал по нескольким источникам. Анализирует и оценивает достоверность информации.
3	Безопасность при использовании платежных карт в Интернете	1	Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.	Приводит примеры рисков, связанных с совершением онлайн покупок (умеет определить источник риска). Разрабатывает возможные варианты решения ситуаций, связанных с рисками использования платежных карт в Интернете.
4	Беспроводная технология связи	1	Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях.	Используя различную информацию, определяет понятия. Изучает особенности и стиль ведения личных и публичных аккаунтов.

5	Резервное копирование данных	1	Безопасность личной информации. Создание резервных копий на различных устройствах.	Создает резервные копии.
6	Основы государственной политики в области формирования культуры информационной безопасности	2	Доктрина национальной информационной безопасности. Обеспечение свободы и равенства доступа к информации и знаниям. Основные направления государственной политики в области формирования культуры информационной безопасности.	Умеет привести выдержки из законодательства РФ: - обеспечивающего конституционное право на поиск, получение и распространение информации; - отражающего правовые аспекты защиты киберпространства.
7	Выполнение теста и/или защита индивидуальных и групповых проектов	3		
8	Повторение	2		
	Итого	33		